INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 6 Tahun 2024 Page 3144-3160
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

The Role of Institutions Supporting the Investigation of Evidence in Money Laundering Crimes using Cryptocurrency

Asmara Nova Susanto[1✉], Wiwik Afifah[2]
17 Agustus 1945 University Surabaya
Email: asmaranovasusanto@gmail.com[1✉]

Abstrak

Tujuan penulisan jurnal ini adalah untuk menganalisis peran lembaga penegak hukum dalam menelusuri kasus pencucian uang menggunakan Cryptocurrency. Pelaku kejahatan berusaha mencari tempat untuk mencuci uang atau tempat yang tidak dapat melacak harta kekayaan hasil kejahatannya. Cryptocurrency merupakan salah satu bentuk aset yang sulit dilacak karena memiliki sifat anonim dan terdesentralisasi. Metode penulisan jurnal ini menggunakan yuridis normatif. Hasil penelitian, penanganan TPPU menggunakan Cryptocurrency di Indonesia memerlukan peran PPATK, OJK, KPK, BAPPEBTI, Polri, Kejaksaan, Financial Action Task Force (FATF), Interpol, dan Financial Intelligence Unit (FIUs). Peran krusial yang harus dijalankan adalah koordinasi penelusuran aset kripto, mengetahui motif aliran dana, menganalisis pola transaksi, memperoleh bukti, dan mengetahui pihak-pihak yang terlibat. Namun yang dimintai pembuktian harta benda bukan hasil tindak pidana adalah terdakwa, karena dalam TPPU sistem pembuktiannya menggunakan pembuktian terbalik.

Kata Kunci: *Pencucian Uang, Cryptocurrency, Institusi, Reverse Burden of Proof*

Abstract

The purpose of writing the journal is to analyze the role of law enforcement agencies in tracing money laundering cases using Cryptocurrency. The perpetrators of the crime are trying to find a place to launder money or a place that cannot trace the assets resulting from the crime. Cryptocurrency is a form of asset that is difficult to trace because it has anonymous and decentralized properties. The method of writing this journal uses normative juridical. The results of the study are that handling TPPU using Cryptocurrency in Indonesia requires the role of PPATK, OJK, KPK, BAPPEBTI, Polri, Prosecutor's Office, Financial Action Task Force (FATF), Interpol, and Financial Intelligence Units (FIUs). The crucial role that must be carried out is coordination for tracing crypto assets, knowing the motives for the flow of funds, analyzing transaction patterns, obtaining evidence, and knowing the parties involved. However, the defendant is the one who is asked to prove assets that are not the result of a crime, because in TPPU the evidentiary system uses reverse proof.

Keywords: *Money Laundering, Cryptocurrency, Institutions, Reverse Burden of Proof*

INTRODUCTION

Template To address the challenges of globalization and technological advancements, economic crimes, particularly money laundering (TPPU), have undergone increasingly complex transformations . A new form of emerging crime is money laundering through cryptocurrency, which offers anonymity, confidentiality, and decentralization in transactions, making it difficult to trace through conventional financial systems .

Cryptocurrency has become a favored tool for criminals to conceal funds obtained illegally. Transactions conducted on blockchain networks using cryptographic technology allow users to execute transactions without the involvement of traditional financial institutions, making it challenging for authorities to trace them. As a specific type of criminal activity, money laundering through cryptocurrency requires more sophisticated and coordinated legal approaches, particularly in tracking the flow of funds and identifying perpetrators who often employ highly organized and cross-border techniques .

Cryptocurrency enables transactions to be conducted anonymously and without involving traditional financial institutions, making it increasingly used by criminals to hide or obscure the origins of funds obtained through illegal means. This anonymity makes tracking and preventing money laundering more challenging, as cryptocurrency transactions often go undetected by regulated financial systems . As a result, assets obtained from money laundering (TPPU) in the form of untraceable cryptocurrencies have the potential to strengthen criminal networks, fund other crimes, and disrupt economic

stability. This is because such assets cannot be confiscated or returned to the state, thereby harming the economy.

In the context of Indonesia, various institutions play crucial roles in combating money laundering, including PPATK (Indonesian Financial Transaction Reports and Analysis Center), OJK (Financial Services Authority), KPK (Corruption Eradication Commission), BAPPEBTI (Commodity Futures Trading Regulatory Agency), the National Police, and the Attorney General's Office. Each of these institutions has specific authority and responsibilities to support law enforcement against money laundering involving cryptocurrencies. Inter-agency coordination is key to addressing these challenges, particularly to ensure that every stage of tracing and enforcement is carried out effectively. In addition to the roles of investigative agencies, the reverse burden of proof system serves as a critical legal instrument in addressing money laundering involving cryptocurrencies. Under this system, part of the burden of proof is shifted to the defendant, requiring them to demonstrate that the assets they possess are not derived from criminal activities. The reverse burden of proof system, as stipulated in Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, is designed to address the difficulties in proving the link between predicate crimes and the funds that have been laundered by perpetrators.

Based on these considerations, this journal aims to analyze the roles of institutions in tracing money laundering cases and the application of the reverse burden of proof system in court proceedings.

RESEARCH METHOD

This study uses a normative juridical research method, aimed at identifying relevant rules, principles, and legal doctrines to provide answers to the related legal issues. In this study, two approaches are employed: the statutory approach, which involves reviewing the laws and regulations related to Anti-Money Laundering (AML) through Cryptocurrency, and the conceptual approach, which focuses on legal doctrines to understand the regulations and authorities concerning the proof system in handling money laundering involving Cryptocurrency.

RESULT AND DISCUSSION

Regulation of Money Laundering through Cryptocurrency

Pasien Cryptocurrency has become one of the financial instruments that attracts the attention of various parties, including criminals engaged in Money Laundering (TPPU). The anonymous, global, and decentralized nature of cryptocurrency makes it an effective means for concealing the origin of illegal funds. In the legal context, the regulation of TPPU is covered under Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering. The criminal provision for TPPU through cryptocurrency is addressed in Article 3. If someone deposits, transfers, or moves cryptocurrency assets derived from a criminal act through a cryptocurrency trading platform registered in Indonesia, such as Indodax, Pintu, or Tokocrypto, these actions may be subject to Article 3. These platforms are required to comply with Know Your Customer (KYC) procedures, where users must submit their ID cards and complete their personal data when registering an account. Additionally, these platforms are supervised by BAPPEBTI, so if suspicious transaction activity occurs, it can be reported to PPATK. With this regulation, authorities can trace cryptocurrency assets originating from criminal activities through the registered identities of users on the platform. However, the tracking can only confirm the existence or non-existence of the cryptocurrency assets. If the perpetrator places the cryptocurrency assets on a platform located outside of Indonesia's jurisdiction, tracing becomes much more difficult. This is due to the anonymous and decentralized nature of cryptocurrency, which allows perpetrators to conceal their identities and conduct transactions without oversight. The use of Decentralized Exchanges (DEX) or private wallets with smart contracts that do not require user identification further complicates law enforcement efforts, especially when transactions are conducted abroad .

Then, from Article 3 of Law No. 8 of 2010, various elements can be identified, namely:

1. “Actor (Any Person): A person who carries out money laundering actions.
2. Action (Placing, Transferring, Shifting, Spending, Paying, Donating, Depositing, Taking abroad, Changing form, or Exchanging for currency or securities): The actor performs one of the actions mentioned above against assets obtained from criminal acts.
3. Object (Assets): Assets that are known or reasonably suspected to include the proceeds of crime as referred to in Article 2, paragraph (1).
4. Purpose (To Conceal or Disguise the Origin of Assets): The actor intends to conceal or disguise the origin of the assets to prevent them from appearing to be derived from criminal activity.”

In the context of cryptocurrency, although these elements appear clear and theoretically applicable, in practice law enforcement still faces difficulties in proving the elements that incriminate the perpetrators of money laundering (TPPU). The main challenge is the anonymity and decentralization of cryptocurrencies, which complicates the tracking of the identities of the perpetrators and the recipients of assets.

Issues that make the elements of this article difficult to prove:

1. Unknown Recipient: In cryptocurrency transactions, the identity of the recipient cannot be known. The address or hexadecimal code of the smart contract is not directly linked to the user's identity unless they use services that comply with Know Your Customer (KYC) regulations, which is often not the case on Decentralized Exchanges (DEX) platforms or peer-to-peer transactions, such as those on foreign provider platforms. Without a clear recipient identity, it is difficult to prove who received the proceeds of the criminal activity.
2. Lack of Tracking Mechanisms: Blockchain technology does record every transaction that occurs, but it only logs the hexadecimal code of the smart contract, not the user's identity. If the perpetrator distributes the cryptocurrency through several small transactions (smurfing) or uses tools like coin mixers, tracking the origin of the asset becomes very difficult or even impossible. When transactions are fragmented or traced through platforms outside the jurisdiction that comply with regulations, law enforcement faces a deadlock.
3. Anonymity and Decentralization: Anonymity allows perpetrators to perform various actions such as placing, transferring, or paying cryptocurrency assets without being tied to a traceable identity. The decentralized nature of cryptocurrency means that if transactions occur without centralized intermediaries or control, such as in banking, decentralization involves randomized nodes and computer networks. In a decentralized ecosystem, there is no third party that must adhere to Know Your Customer (KYC) procedures, making it impossible for law enforcement to identify the perpetrator or the recipient of the transaction. As a result, cryptocurrency assets can be easily transferred to jurisdictions like Indonesia.

The Role of the Money Laundering Crime Investigation Agency Through Cryptocurrency

The Indonesian government has a strong commitment to assist and prevent money laundering (TPPU) through the creation of Anti-Money Laundering and Counter-Terrorism

Financing (APU-PPT) regulations . Thus, the Anti-Money Laundering Committee (TPPU Committee) was established in accordance with Article 92 Paragraph (2) of Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering, which states: "The establishment of the National Coordination Committee for the Prevention and Eradication of Money Laundering is regulated by a Presidential Regulation." Further implementing regulations regarding the functions and authority of the TPPU committee are stipulated in Presidential Regulation No. 6 of 2012 concerning the National Coordination Committee for the Prevention and Eradication of Money Laundering, as amended by Presidential Regulation No. 117 of 2016 on Amendments to Presidential Regulation No. 6 of 2012 concerning the National Coordination Committee for the Prevention and Eradication of Money Laundering.

Financial Transaction Reports and Analysis Center (PPATK)

In the process of handling money laundering cases, PPATK plays a crucial role, especially in the investigation and inquiry stages. As an institution tasked with supervising and analyzing financial transactions, including suspicious transactions involving cryptocurrency, PPATK provides information and financial intelligence reports to law enforcement agencies such as the prosecutor's office and the police, which then serve as the basis for conducting further investigations. PPATK is not directly involved in the trial or prosecution process. However, the financial analysis reports prepared by PPATK serve as crucial evidence in building a money laundering (TPPU) case. The information provided by PPATK, such as regarding suspicious fund flows or cross-border transactions involving cryptocurrency, helps prosecutors to establish the crime's chronology and link the laundered assets to the predicate crime.

In addition, PPATK collaborates with Financial Intelligence Units (FIUs) in various countries to facilitate international data exchange, which is essential in cross-border TPPU cases. The evidence and analysis of digital transactions generated by PPATK are often presented as evidence in court to strengthen the prosecution’s case. Therefore, PPATK’s role in the TPPU judicial process is at the investigative stage, providing essential data and evidence for prosecution in court.

Article 44, Paragraph (1) grants PPATK broad authority to investigate and analyze money laundering (TPPU) cases, including those involving cryptocurrency transactions, which are anonymous, decentralized, and cross-border in nature. It allows PPATK to request reports and additional information from relevant agencies (subsections a, b, and c)

to track suspicious transaction patterns, and cooperate with international agencies (subsections d and e) to enhance cross-border investigation. Furthermore, it enables PPATK to suspend suspicious transactions (subsection i), recommend electronic communication interception (subsection h), and track the progress of investigations (subsection j). Subsections (k) and (l) empower PPATK to manage digital transaction data and prepare analytical reports, which can be used as strong evidence to trace money flows and establish the connection between criminal activities and the predicate crime.

Financial Services Authority (OJK)

OJK plays a crucial role in preventing and supervising money laundering (TPPU), particularly by ensuring that non-bank financial institutions and cryptocurrency trading platforms comply with relevant regulations. While OJK is not directly involved in trials or prosecutions, its data and reports from supervised institutions can serve as evidence of suspicious cryptocurrency transactions. OJK collaborates with PPATK to monitor transactions and provide investigators with critical information on unusual transaction patterns, which can be used by prosecutors as key evidence in legal proceedings.

According to POJK No. 8 of 2023 regarding the Implementation of Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and the Prevention of the Proliferation of Weapons of Mass Destruction in the Financial Services Sector, OJK plays an important role in the prevention and supervision of AML/CTF, including transactions involving cryptocurrency. This regulation establishes various rules for financial institutions to mitigate the risks of terrorism financing, money laundering, and the funding of other weapons through the implementation of CDD (Customer Due Diligence), KYC (Know Your Customer), and suspicious transaction reporting. Suspicious transaction reports collected by cryptocurrency platforms and submitted to PPATK during investigations become a critical part of the AML/CTF case investigation.

Several key provisions that are relevant include: 1.) Cryptocurrency Transaction Monitoring, Article 47 stipulates that Financial Service Providers (PJK) may delay transactions suspected of being the proceeds of crime, including money laundering, if the transaction involves crypto assets. This provision grants OJK the authority to request the delay of transactions involving suspected digital assets, providing time to investigate and gather further evidence. 2.) Temporary Suspension and Blocking of Transactions: Article 48 supports the temporary suspension of all or part of a transaction when requested by PPATK. This is crucial in the context of cryptocurrency, where assets can be moved quickly

across borders. The ability of OJK to order a temporary suspension of transactions serves as a preventive measure to stop asset movement until the investigation is completed. 3.) Cooperation and Additional Information: Article 83 emphasizes that OJK must cooperate with law enforcement authorities, including providing documents or information related to customers suspected of committing AML/CTF offenses. This is vital for tracking suspicious fund flows in the cryptocurrency sector and linking transactions to the underlying criminal activity, thus forming the evidence base in legal proceedings. With these provisions in place, OJK plays a key role in strengthening oversight of cryptocurrency-based transactions and supporting law enforcement efforts to prevent money laundering practices. Inter-agency cooperation enables OJK to ensure the compliance of financial institutions, including cryptocurrency asset trading providers, so that suspicious transactions can be identified, analyzed, and processed further to maintain the integrity of the financial system.

Corruption Eradication Commission (KPK)

The KPK plays a vital role in handling Money Laundering Crimes (TPPU) stemming from corruption, overseeing the investigation and prosecution stages, especially when cryptocurrency is used to launder illicit proceeds. The KPK works closely with PPATK to track suspicious fund flows and with OJK to ensure cryptocurrency trading platforms comply with KYC regulations. During investigations, the KPK traces money laundering patterns using blockchain analysis to link cryptocurrency transactions to perpetrators' digital wallets. If cryptocurrency is used to conceal corruption proceeds, the KPK can seize or freeze the assets, provided the trading platform is located in Indonesia, and use them as evidence in court.

The KPK has a specific mandate to handle corruption crimes, including the handling of money laundering related to corruption cases. Based on Article 74 of Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes, investigations into money laundering crimes are carried out by investigators, including the KPK, if the predicate crime is corruption. This means the KPK has the authority to investigate assets suspected of originating from corruption, allowing the investigation of money laundering and corruption crimes to be merged according to Article 75 of the Money Laundering Law. This merger aims to speed up the process and ensure clarity in tracking assets that need to be seized to recover state losses. The procedure for investigating and prosecuting money laundering alongside the predicate crime carried out by the KPK also involves

several additional steps in accordance with the Criminal Procedure Code (KUHAP). This process includes providing guidance from public prosecutors, case file submissions, and coordination between investigators and prosecutors, which may extend the handling time. However, under the doctrine of lex specialis, the regulations in the Money Laundering Law function as special rules that make this process more effective compared to general criminal procedure law .

The prosecution of money laundering cases with corruption as the predicate crime, carried out by prosecutors at the KPK (Corruption Eradication Commission), is part of the authority of prosecutors under the control of the Indonesian Attorney General's Office, with a special mandate to prosecute cases at the KPK. This reinforces that the KPK can carry out prosecutions for money laundering cases where the predicate crime is corruption, allowing the entire investigation and prosecution process to be conducted in a synergistic and effective manner. At the prosecution stage, the KPK presents evidence gathered from investigations, including digital transactions conducted through cryptocurrency. This evidence is used to support the charges against money laundering perpetrators in court. Therefore, the KPK's position in the legal process of money laundering cases spans all key stages, from investigation and inquiry to prosecution, with a crucial role in gathering and presenting evidence related to money laundering originating from corruption.

Commodity Futures Trading Regulatory Agency (Bappebti)

Bappebti is responsible for overseeing cryptocurrency trading in Indonesia, particularly on futures platforms, ensuring compliance with anti-money laundering (AML) regulations, including Know Your Customer (KYC) policies. It monitors and reports suspicious transactions to PPATK and maintains transparent reporting systems to provide transaction data to law enforcement like PPATK, KPK, and the police. Bappebti is also part of the National Coordination Committee for the Prevention and Eradication of Money Laundering (TPPU), tasked with regulating commodity futures trading under Law No. 8 of 2010. The committee, chaired by the Coordinating Minister for Political, Legal, and Security Affairs, includes 13 government agencies, with Bappebti serving as a supervisory and regulatory body for TPPU prevention.

To address money laundering risks, Bappebti implements Risk-Based Supervision through Sectoral and Individual Risk Assessments (SRA and IRA). These assessments help identify and mitigate risks at both the sectoral and individual levels. Under Presidential

Regulation No. 117 of 2016, Bappebti is required to report suspicious transactions to PPATK, where they are analyzed further. If the transactions are linked to money laundering, PPATK forwards the findings to law enforcement for further action.

Indonesian National Police (Polri)

The National Police of Indonesia (Polri) plays a key role in investigating money laundering involving cryptocurrency, collaborating with PPATK, OJK, and KPK. Polri uses digital forensics technology to trace anonymous cryptocurrency transactions on the blockchain, gathering evidence and conducting asset seizures during investigations. Upon receiving analysis results from PPATK, Polri begins investigations, verifying information and gathering evidence, with authority to arrest, detain, and search as per the Criminal Procedure Code (KUHAP) and Article 16 of Law Number 2 of 2002 on the Indonesian National Police. After completing the investigation, Polri submits the case to the public prosecutor, ensuring the connection between illicit assets and the predicate crime is clearly explained, facilitating prosecution as outlined in Article 69 of Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering (TPPU). This coordinated effort ensures that money laundering cases involving cryptocurrency are brought to court with sufficient evidence.

In comparison with Singapore, the regulations for handling money laundering cases in Singapore are found in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA 1992). The CDSA regulates measures for combating and preventing money laundering related to criminal cases, including corruption and drug trafficking . This law requires every individual and institution in Singapore, including financial institutions, to report suspicious transactions and enables the Commercial Affairs Department (CAD) to investigate and seize assets suspected of originating from illegal activities. The CAD is part of the police department in Singapore. Sections 36, 37, and 39 of the CDSA 1992 assist authorities in gathering crucial evidence related to suspicious fund flows and allow investigators to access financial records to trace the origin of assets suspected to be proceeds of crime. Furthermore, Sections 40 and 41 of the CDSA 1992 grant search powers, allowing investigators to find physical evidence, including documents and relevant items, and provide a solid legal basis for the detention of such items during the investigation process. Sections 45, 46, and 47 of the CDSA 1992 also regulate reporting obligations to strengthen the investigation process by ensuring that all parties with information about money laundering contribute to the disclosure of

important information, without fear of legal repercussions. Additionally, Section 76 of the CDSA 1992 grants authorities the power to arrest individuals suspected of being involved in money laundering and conduct a full investigation into the alleged offense. With this authority, the authorities can take decisive action against suspects, including temporary detention to prevent the suspect from fleeing or destroying evidence. This power is crucial in accelerating the money laundering investigation process, granting investigators the authority to handle suspects with necessary preventive measures to secure existing evidence. In addition to the CDSA, Singapore also refers to the Monetary Authority of Singapore (MAS), which issues guidelines and regulations for financial institutions. MAS mandates financial institutions to implement KYC and CDD procedures and report suspicious transactions to the CAD.

Indonesian Attorney General's Office

The role of the Attorney General's Office in coordinating the prosecution of Money Laundering Crimes (TPPU) involving Cryptocurrency is very important. In addition to cooperating and coordinating with the National Police (Polri) during the investigation process, the Attorney General's Office is responsible for the prosecution stage, where they collaborate with investigative agencies such as the Financial Transaction Reports and Analysis Center (PPATK), the Corruption Eradication Commission (KPK), and the National Police (Polri) to gather the necessary evidence for the court process . In the context of Money Laundering (TPPU) using Cryptocurrency, the Prosecutor’s Office must understand the patterns of digital financial crimes and how these digital assets are used to disguise the proceeds of criminal acts. The Prosecutor’s Office also plays a role in coordinating prosecution strategies, ensuring that digital evidence collected through cryptocurrency digital forensics is properly presented in court. This evidence may include digital transaction trails and blockchain network patterns. The Prosecutor’s Office is responsible for drafting strong charges based on the evidence provided by investigative agencies and conducting effective prosecution of money laundering perpetrators using cryptocurrency.

In Singapore, after an investigation by the Commercial Affairs Department (CAD), the prosecution, represented by the Attorney-General's Chambers (AGC), plays a central role in prosecuting money laundering cases. AGC is responsible for evaluating the evidence submitted by CAD to assess the viability of prosecution, as well as applying for confiscation orders to seize assets related to money laundering, as outlined in Sections 6, 7, and 8 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of

Benefits) Act 1992 (CDSA 1992). This ensures that the proceeds of crime cannot be used or transferred by the suspect during the legal process. Additionally, AGC drafts the charges and presents evidence in court to prove the suspect's involvement in money laundering under Section 76 of the CDSA 1992. In cross-border money laundering cases, AGC also collaborates with foreign authorities to share information and extradite perpetrators, as provided in Section 48 of the CDSA 1992. The role of AGC ensures that the legal process is effective in confiscating illegal assets and punishing offenders in accordance with Singaporean law.

Financial Action Task Force (FATF), Interpol, and Financial Intelligence Units (FIUs)

Due to the cross-border nature of cryptocurrency, international cooperation is crucial in tracing evidence of money laundering and terrorism financing (TPPU). Institutions in Indonesia, such as PPATK, the Indonesian National Police (Polri), and the Attorney General's Office, collaborate with FATF, Interpol, and Financial Intelligence Units (FIUs) in various countries.

FATF is an international organization that sets global standards for preventing money laundering and terrorism financing, including in cryptocurrency use. It issues guidelines for monitoring crypto transactions and requires virtual asset service providers to implement KYC and CDD measures. FATF monitors compliance, placing non-compliant countries on a "high-risk" list, potentially leading to sanctions. It also promotes international collaboration to track and freeze crypto assets involved in cross-border financial crimes.

Interpol plays a crucial role in investigating cross-border money laundering (ML) cases involving cryptocurrency, which is often anonymous. It collaborates with registered crypto trading platforms to identify suspicious transaction patterns and uses the Interpol Global Complex for Innovation (IGCI) to facilitate information exchange, provide technical support, and develop tools to trace transactions. With the help of platforms complying with KYC regulations, Interpol can track the identities of potential perpetrators in cryptocurrency-based money laundering networks.

FIUs (Financial Intelligence Units) analyze Suspicious Transaction Reports (STR) related to money laundering (TPPU), including those involving cryptocurrency, to identify patterns linked to illegal activities. In cross-border cases, FIUs collaborate with counterparts through the Egmont Group network, facilitating the exchange of STR data to

track asset movements across countries. If suspicious patterns are identified, the information is forwarded to domestic law enforcement for further investigation, potentially leading to asset seizures. This collaboration aids in tracing and investigating cryptocurrency-based money laundering activities across borders.

Reverse Burden of Proof System in Cryptocurrency-Related Money Laundering

The reverse burden of proof system in Indonesia, inspired by countries like Malaysia and Singapore, is used in a limited manner, particularly in cases of gratification and bribery. The idea gained attention during President Abdurrahman Wahid's era in response to the House of Representatives' memorandum, as the complexity of proving corruption cases highlighted the need for an extraordinary proof system to combat the crime more effectively. Historically, policy changes related to the burden of proof began with Government Regulation in Lieu of Law (Perpu) No. 24 of 1960 concerning the Investigation, Prosecution, and Examination of Corruption Crimes, which introduced the concept of semi-reverse burden of proof. Article 5, paragraph (1) of the law required suspects to provide explanations regarding the origin of their assets, including the assets of their family members and legal entities under their management. Before this law was enacted, there were no specific regulations governing the reversal of the burden of proof, as corruption at the time was still considered an ordinary offense that could be addressed using conventional proof systems . Furthermore, the reverse burden of proof system was further clarified through Law Number 3 of 1971 on the Eradication of Corruption, which was later repealed and replaced by Law Number 31 of 1999 on the Eradication of Corruption. However, under this law, the primary burden of proof remained with the public prosecutor. This weakness was eventually addressed through Law Number 20 of 2001 on Amendments to Law Number 31 of 1999 on the Eradication of Corruption, based on Article 37A Paragraph (1), which introduced a reverse burden of proof with limited and balanced characteristics. This provides a strong legal foundation for the implementation of the reverse burden of proof system in Indonesia, particularly in handling corruption cases.

Here are the stages undertaken in the reverse proof process, which include:

1. Investigation Stage

   During the investigation stage, investigators begin collecting preliminary information related to suspected corruption and the assets owned by the suspect. The primary focus of this stage is to identify indications that the suspect’s assets do not align with their official or legitimate income. If there is an inconsistency in the amount or

source of wealth, the reverse proof system can be applied to compel the suspect to provide an adequate explanation regarding the origin of their assets.

2. Inquiry Stage

   If the investigation results lead to sufficient evidence, the process moves to the inquiry stage. At this stage, investigators summon the suspect to provide clarification and prove the source of their wealth. The suspect is required to submit documents supporting claims that their wealth was obtained legally. If the suspect cannot provide sufficient explanations or evidence, this can be used by investigators as an indication of corrupt practices.

3. Prosecution Stage

   The public prosecutor then compiles the case file based on findings from the investigation and inquiry stages. At this stage, the prosecutor evaluates the collected evidence and assesses whether the suspect has adequately explained the origins of their assets. Under the reverse proof system, the defendant is obligated to demonstrate that their wealth was acquired through legal and legitimate means. If the defendant fails to provide convincing evidence, the prosecutor will use this failure as a basis to strengthen the charges against them.

4. Trial Stage

   In court, the defendant is given the opportunity to present evidence proving the legality of their wealth's origins. The judge evaluates all evidence from both the defendant and the prosecutor. If the defendant fails to provide sufficient evidence, the judge may conclude that the wealth originates from corrupt practices, strengthening the prosecutor’s case. The defendant must disclose all assets, including those of their spouse, children, and associates linked to the alleged crime. The trial serves as the primary forum to determine whether the wealth was legally obtained or connected to corruption, with reverse proof playing a key role in this determination.

The reverse burden of proof system is highly relevant in money laundering (TPPU) cases, where complex techniques are used to conceal the source of illicit wealth. This system reduces the burden on prosecutors, as proving the origin of assets can be difficult due to complex transaction networks. Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering adopts this system, requiring defendants to prove that

their assets are not derived from criminal activities. Articles 77 and 78 of the law mandate that defendants demonstrate the lawful origin of their wealth, with judges having the authority to request evidence such as financial documents or witnesses. This system helps expedite cases and supports asset confiscation when linked to criminal acts, particularly in corruption and money laundering.

CONCLUSION

The handling of Money Laundering (TPPU) through Cryptocurrency in Indonesia is carried out through the formation of the National Coordination to Prevent and Combat Money Laundering as outlined in Article 92 Paragraph (2) of Law Number 8 of 2010, along with Presidential Regulation Number 117 of 2016 as its implementing regulation. This committee involves several law enforcement and financial supervisory agencies such as PPATK, OJK, KPK, Bappebti, the Indonesian National Police, and the Prosecutor's Office. This crime demands strict supervision and coordinated law enforcement due to the anonymous and hard-to-trace nature of Cryptocurrency. Collaboration between agencies is crucial to address these challenges, particularly in analyzing suspicious transactions and ensuring compliance with existing regulations. On the other hand, collaboration with international institutions such as the Financial Action Task Force (FATF), Interpol, and Financial Intelligence Units (FIUs) can make cryptocurrency asset tracing easier, as crypto transactions are cross-border.

With a reversed burden of proof system, the defendant is required to prove that their wealth is not derived from criminal activities, especially in cases involving assets disguised through complex financial transactions, such as Cryptocurrency. This process involves proving at various stages, from investigation to trial, where the defendant must present sufficient evidence to explain the origin of their wealth. This facilitates law enforcement, providing a stronger foundation for prosecutors and judges in handling Money Laundering cases, and accelerating the confiscation of assets derived from crimes.

REFERENCES

Agus, A. (2022). Pembuktian tindak pidana suap dalam undang-undang Tindak Pidana Korupsi. Jurnal Hukum Tri Pantang, 7(2), 100-110.

Al Fath. (2023). Peranan dan peningkatan PPATK dalam mendukung upaya pencegahan pencucian uang oleh pejabat di Indonesia (Studi kasus Rafael Alun). Jurnal Hukum

Statuta, 3(1), 53–62.

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210-216.

Basit, B. (2023). Urgensi perlindungan hukum perusahaan exchanger cryptocurrency terhadap aliran transaksi dari pengguna anonim wallet decentralized exchange. COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat, 2(11), 1–15.

Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the system of money laundering. Baltic Journal of Economic Studies, 4(5), 75–81.

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.

Flora, H. S., Syah, K., Erwin, E., Laila, S. A. N., & Lawra, R. D. (2024). Comparative analysis of criminal laws on money laundering in ASEAN countries: Between justice and protection. Review UNES, 6(3), 8930.

Haris, B. S. (2024). Added value and challenges of the follow-the-money approach in environmental crimes. AML/CFT Journal: The Journal of Anti Money Laundering and Countering The Financing of Terrorism, 2(2), 111–125.

Ida Ayu Setyawati. (2014). Beban pembuktian terbalik dalam perkara money laundering dengan predicate crime tindak pidana korupsi. Brawijaya Law Student Journal, 1(2).

Karaseran, I. O. (2015). Peran kejaksaan dalam penyidikan dan penuntutan tindak pidana pencucian uang. Lex Crimen, 4(4).

Lasmadi, S., & Sudarti, E. (2021). Pembuktian terbalik pada tindak pidana pencucian uang. Refleksi Hukum: Jurnal Ilmu Hukum, 5(2), 199-218.

Nelson, F. M., Prosperiani, M. D., Ramadhan, C. R., & Andini, P. P. (2024). Cracking the code: Investigating the hunt for crypto assets in money laundering cases in Indonesia. Journal of Indonesian Legal Studies, 9(1), 89-130.

Putri, T., Amiludin, A., Ahmad, D. N., & Hidayatulloh, H. (2023). Inadequate cryptocurrency and money laundering regulations in Indonesia (Comparative law of US and Germany). Yustisia Jurnal Hukum, 12(1), 1–15.

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.

Sembiring, P. E. (2024). Menilai pemberlakuan pembuktian terbalik pada tindak pidana

pencucian uang sebagai kejahatan proxy di dalam aset kripto. Integritas: Jurnal Antikorupsi, 10(1), 53-64.

Sikumbang, F. S., & Damayanti, S. (2022). Optimalisasi peran Bappebti dalam pengawasan transaksi aset cryptocurrency di Indonesia. Jurnal Ilmu Sosial dan Ilmu Politik Malikussaleh (JSPM), 3(2), 325-336.

Simoes, J. E., Ferreira, E., Menasche, D. S., & Campos, C. A. V. (2021). Blockchain privacy through merge avoidance and mixing services: A hardness and an impossibility result. Peer-to-Peer Networking and Applications, 14(5), 2831–2842.

Wattie, A. F. (2015). Peran PPATK dalam penyidikan tindak pidana pencucian uang. Lex Crimen, 4(3).

Wiryadi, U., Gifari, F., & Chariansyah, H. (2024). Kedudukan dan kewenangan Komisi Pemberantasan Korupsi (KPK) dalam ketatanegaraan Indonesia pasca undang-undang baru. Begawan Abioso, 14(2), 109–116.

Yanuar, M. A. (2022). Kewenangan penyidik Otoritas Jasa Keuangan dalam menyidik tindak pidana pencucian uang. AML/CFT Journal: The Journal of Anti Money Laundering and Countering The Financing of Terrorism, 1(1), 67–86.