journal of anti-money laundering / countering the financing of terrorism

Original paper

Digital Grants as a Mode of Money Laundering from Tax Crimes

Rama Nova Hariyanto*, Mohammad Syafi'i, Median Dwi Restana
Directorate General of Taxes, Ministry of Finance of the Republic of Indonesia, Indonesia

Corresponding author: ramanova50@gmail.com

Keywords:
Digital Forensic Investigation, Grant, Money Laundering, Red Flag Theory, Tax Crime

Submitted: 4 April 2026
Accepted: 22 June 2026
Published: 28 June 2026

Abstract

The development of cryptocurrency, blockchain, and digital finance has given rise to digital asset grants as a new form of wealth transfer that can potentially be exploited for money laundering (ML) originating from tax crimes. Their pseudonymous, cross-jurisdictional and decentralized nature creates obstacles in identification, oversight and legal proof. This study aims to identify the characteristics of suspicious digital asset grants, analyze the application of Red Flag Theory in risk detection and examine the role of Digital Forensic Investigation in proving their connection to tax crimes as a predicate offense. The study employs a normative juridical method using statutory, conceptual and literature review approaches. Analysis is conducted through the integration of Red Flag Theory, blockchain forensics, wallet attribution analysis, beneficial ownership investigation, digital-tax evidence correlation and fund flow reconstruction. Results indicate that high-risk indicators include anonymous donors, unidentifiable beneficial owners, blockchain layering, cross-chain transactions, use of privacy technologies and discrepancies between grant values and the recipient's economic profile. This study produces a Digital Asset Grant Red Flag Model, a Risk Matrix, an Early Warning System, and an integrated model of Red Flag Theory with Digital Forensic Investigation as a systematic framework for detecting, investigating, and verifying digital asset grants used as instruments of money laundering originating from tax crimes

***To cite this article*:** Hariyanto, R. N., Syafi'i, M., & Restana, M. D. 2026. *Digital Grants as a Mode of Money Laundering from Tax Crimes. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 4(2):196-213, https://doi.org/10.59593/amlcft.2025.v4i2.294

Introduction

A grant is a legal institution known since Roman law through the concept of *donation*, namely the voluntary transfer of property without compensation to enrich another party. This concept subsequently evolved in modern civil law systems, including in Indonesia, as a

mechanism for the gratuitous transfer of property rights.[1] Traditionally, grants have been used for family, social and religious purposes, with objects in the form of land, buildings, money, or other tangible assets, supported by formal documentation and clearly identifiable parties. The development of digital technology has given rise to digital grants, namely the transfer of value through electronic money, digital wallets, crypto assets, digital tokens and crowdfunding platforms. Since the emergence of blockchain technology and crypto assets, grants can be executed quickly, across national borders and without conventional financial intermediaries.[2]

From a taxation perspective, under Minister of Finance Regulation Number 114 of 2025, grants have special characteristics because they may be excluded from the tax base if certain conditions are met. This regulation provides legal provisions on the income tax treatment of assistance, donations and grants, limited to property transfers that are social, religious, educational or familial in nature.[3] Additionally, within the implementation of Coretax DJP since January 2025, grants meeting the requirements as income excluded from income tax objects must still be reported in the Annual Tax Return (SPT). Reporting is carried out through Attachment L-2 Part B as "Income Not Constituting a Tax Object," and if the assets derived from the grant are still held or controlled at the end of the tax year, they must also be listed in Attachment L-1 Part A regarding the list of assets at the end of the tax year. Accordingly, the Coretax DJP system applies a dual reporting approach (*dual reporting*) reporting based on the source of asset acquisition and reporting based on the asset position held at the end of the tax period.[4]

The grant reporting system in Coretax DJP remains declaratory (*self-assessment based reporting*) as it relies heavily on information submitted by taxpayers. Furthermore, it does not yet explicitly require disclosure of the beneficial owner, verification of the source of funds, or the application of anti-money laundering red flag indicators to grants being reported. Consequently, it potentially creates oversight gaps, particularly for large-value grants, cross-jurisdictional grants, or digital asset-based grants that possess higher degrees of anonymity and transactional complexity.[5]

Unlike conventional grants, digital grants are characterized by speed, cross-jurisdictional, and pseudonymity, making it difficult to identify beneficial owners and trace sources of funds. This increases the risk of digital grants being misused for tax avoidance, income concealment, and money laundering. For this reason, the study of digital grants is important in supporting the effectiveness of tax oversight.[6] However, to date, Coretax DJP development has not yet incorporated automatic mechanisms specifically designed to detect indications of misuse or to classify digital grants, virtual assets, or blockchain-based transactions as a separate risk category. Mechanisms within Coretax DJP remain limited with respect to data integration, *data matching*, *risk profiling*, and *compliance risk management* so the effectiveness of digital grant identification is highly dependent on the availability of third-party data, the quality of taxpayer

[1]Reza Fahlepy et al., "*Status Peralihan Sertifikat Hak Atas Tanah Berdasarkan Surat Hibah di Bawah Tangan*" [Certificate of Land Title Transfer Based on a Private Grant Deed], *Jurnal de Jure 13*, no. 1 (2024): 101–102.

[2]Organisation for Economic Co-operation and Development (OECD), *Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues* (Paris: OECD Publishing, 2020): 17–22.

[3]Indonesia, *Minister of Finance Regulation Number 114/PMK.03/2025 on Assistance or Donations and Granted Assets Excluded as Income Tax Objects* (Jakarta: Ministry of Finance of the Republic of Indonesia, 2020), Article 2 paragraph (3). (Directorate General of Taxes)

[4]Nora Galuh Candra Asmarani, "How to Report Non-Taxable Income in the Annual Tax Return via Coretax," *DDTC News*, February 26, 2026.

[5]Directorate General of Taxes, *Coretax Manual — Annual Personal Income Tax Return Reporting* (Jakarta: DJP, 2024).

[6]Directorate General of Taxes, "Coretax DJP as an Integrated Digital Tax System," *Pajak.go.id*, 2025.

reporting and the system's capacity to detect discrepancies between economic profiles, asset accretion, and reported income sources.[7]

These oversight gaps do not preclude taxpayers from using them to disguise the nature of assets (*disguising the illicit origin of assets*).[8] The practice of disguising the nature of assets derived from tax crimes through grant documents can be analyzed within Indonesia's positive law framework, particularly based on the provisions of the Law on Money Laundering and Tax Law. Law Number 8 of 2010 on Prevention and Eradication of Money Laundering, in Article 2 paragraph (1), places tax crimes as one of the predicate offenses that can generate proceeds which subsequently become the object of money laundering.[9]

The limitations in identifying digital grants allow transactions to be conducted through virtual assets, crypto wallets or digital platforms not yet integrated with tax data sources.[10] Consequently, approaches are needed to anticipate potential tax crimes and money laundering that exploit digital assets, including crypto assets and blockchain-based transactions.[11] A number of studies have highlighted the relationship between tax crimes and money laundering. Riccardi and Reuter (2024)[12] explain that money laundering strategies are influenced by offenders' choices and the degree of oversight in the sector used. Nurferyanto and Takahashi (2024)[13] affirm that tax crimes are increasingly complex and require data integration, technology and inter-agency coordination. Mintoff and Vella (2024)[14] show that money laundering is closely linked to predicate offenses, including tax evasion, through the use of various financial instruments. Fhatnur and Sugama Ali (2024)[15] emphasize the importance of the follow-the-money approach and the use of financial data in uncovering money laundering, while Anjani, Aulia and Widiastuti (2024)[16] highlight the need to strengthen oversight and control systems within the anti-money laundering regime. Slemrod (2019)[17] and Levi (2018)[18] explain the linkage between tax evasion, taxpayer behavior, and the use of money laundering techniques to conceal proceeds of crime. Garnasih (2016)[19] affirms that tax crimes constitute

[7]Directorate General of Taxes, "DJP Launches Compliance Risk Management (CRM) Application for Law Enforcement and Assessment CRM," April 8, 2022.
[8]World Bank, *Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Reference Guide and Information on the Use of the Financial Intelligence Unit and Financial Information by Development Agencies*, accessed April 16, 2026.
[9]Law Number 8 of 2010 on Prevention and Eradication of Money Laundering, Article 2 paragraph (1).
[10]Directorate General of Taxes, "Coretax DJP: 1 Application, 7 Benefits," February 7, 2025.
[11]OECD, *Bringing Tax Transparency to Crypto-Assets: An Update* (Paris: OECD Publishing, 2024).
[12]Michele Riccardi and Peter Reuter, "The Varieties of Money Laundering and the Determinants of Offender Choices," *European Journal on Criminal Policy and Research 30* (2024): 333–358.
[13]Dwi Nurferyanto and Yoshi Takahashi, "Combating Tax Crimes in Indonesia: Tackling the Issue Head-On," *Humanities and Social Sciences Communications 11* (2024): 1556.
[14]Yana Mintoff and Mary Grace Vella, "Money Laundering and the Crime Nexus: A Case Study in Malta," *Journal of Financial Crime 6*, no. 2 (2024): 1–15.
[15]Yoga Fhatnur and Sugama Ali, "Dynamics and Strategies of Law Enforcement of Money Laundering Offences in Indonesia," *Indonesian Journal of Law and Economics Review 19*, no. 2 (2024).
[16]Aulia Anjani and Heni Widiastuti, "The Puzzle of Money Laundering: A Literature Review of Regulations and Implications," *Journal of Accounting and Investment 25*, no. 3 (2024): 1088–1108.
[17]Joel Slemrod, "Tax Compliance and Enforcement," *Journal of Economic Literature 57*, no. 4 (2019).
[18]Michael Levi and Peter Reuter, "Money Laundering, Risks and Regulation," *Crime and Justice 34*, no. 1 (2006): 289–375.
[19]Yenti Garnasih, *Law Enforcement of Money Laundering in Indonesia* [Penegakan Hukum Tindak Pidana Pencucian Uang di Indonesia] (Jakarta: Kencana, 2016).

one of the predicate offenses of money laundering. Meanwhile, Maharani et al. (2025)[20] examine grants in the context of tax avoidance through grant deeds.

Prior research has not specifically analyzed digital grants as a mode of money laundering arising from the concealment of proceeds from tax crimes. The absence of specific regulations and the lack of adequate risk indicators further impede oversight of technologies such as *non-custodial wallets*, *privacy coins*, *mixing services* and DeFi, through which the concealment of fund flows related to tax crimes and money laundering can be conducted in complex ways. Therefore, this study fills that gap through the Red Flag Theory and Digital Forensic Investigation approaches[21] by examining the characteristics of the fund flow mode of digital grants used, and how the application of ***Red Flag Theory*** identifies suspicious digital grants through risk indicators such as transactions lacking clear economic purpose, use of high-risk crypto wallet addresses, anonymous donors, abnormal transaction frequency and cross-jurisdictional transfer patterns.[22] Subsequently, Digital Forensic Investigation is used to trace transaction trails, identify inter-wallet relationships and uncover the flow of digital grant funds allegedly originating from tax crimes and subsequently concealed through crypto assets and blockchain technology.[23] This is done to identify the characteristics of digital grants, analyze the application of Red Flag Theory and examine the role of Digital Forensic Investigation in verifying the connection between digital grant fund flows and tax crimes as a predicate offense. This study is expected to contribute to the examination of the application of Red Flag Theory and Digital Forensic Investigation, as well as to the development of tax law, money laundering, evidentiary law and digital forensics. It is also intended as a guide for government and legislators in formulating oversight systems and regulations that are more adaptive to the development of blockchain technology, crypto assets and digital financial transactions.

The pseudonymous, cross-jurisdictional and decentralized characteristics of digital grants render the oversight and evidentiary process more complex than conventional financial transactions.[24] The identity of parties in blockchain transactions is often represented through cryptographic addresses, while the transfer of digital assets can be made directly between countries without passing through traditional financial institutions, thereby increasing the challenges for tax authorities and law enforcement in identifying relevant parties, tracing fund flows and proving tax crimes and money laundering.[25]

This research constitutes normative juridical legal research. Analysis is conducted through a statutory approach (*statute approach*), a conceptual approach (*conceptual approach*), and a doctrinal approach by examining legislation, legal principles, doctrines, legal theories, and literature related to tax crimes, money laundering, digital grants, crypto assets and electronic evidence.[26] Additionally, the study examines the application of Red Flag Theory and Digital Forensic Investigation in the identification and proof of digital grant transactions allegedly

[20]Mentari Rizkika Maharani, Vira Wijaya, Carolina Isabela Sinawan, Aurynanda Salsabila, and Zenzai Ayu Alvina, "The Validity of Grant Deeds Used by Taxpayers for Tax Avoidance," *Jurnal USM Law Review 8*, no. 1 (2025): 128–142.

[21]M. J. B. Siringoringo and S. M. Simanjuntak, "Auditor Capability on the Effectiveness of Red Flags in Fraud Detection," *Jurnal Ilmiah Manajemen Kesatuan 13*, no. 1 (2025): 124–126.

[22]FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020): 5–16.

[23]H. F. Atlam et al., "Blockchain Forensics: A Systematic Literature Review of Techniques, Tools, and Challenges," *Electronics 13*, no. 17 (2024): 1–3.

[24]OECD*, Delivering Tax Transparency to Crypto-Assets: A Step-by-Step Guide to Understanding and Implementing the Crypto-Asset Reporting Framework (CARF)* (Paris: OECD Publishing, 2024): 4–7.

[25]Arindam Misra, *Tax Policy Handbook for Crypto Assets* (2024): 3–5.

[26]Tunggul Ansari Setia Negara, "Normative Legal Research in Indonesia: Its Origin and Approaches," Audi Et AP*: Journal of Legal Studies 4,* no. 1 (2023): 4–6.

originating from tax crimes. Analysis is conducted qualitatively using the statutory approach and conceptual approach to examine the characteristics of digital grants, the effectiveness of Red Flag Theory in detecting suspicious transactions and the role of Digital Forensic Investigation in proving tax crimes and money laundering under Indonesia's positive law. The research is descriptive-analytical in nature, describing the relevant legal provisions while analyzing the relationship between tax crimes, digital grants, money laundering, and digital evidence. Research data are obtained from primary, secondary and tertiary legal materials collected through library research.[27]

Discussion

Characteristics of Digital Grants as a Mode of Money Laundering Originating from Tax Crimes

Under Article 1666 of the Indonesian Civil Code, a grant is an agreement made by the grantor during his or her lifetime to transfer an object or right gratuitously to the recipient and, in principle, cannot be revoked. The validity of a grant is not only determined by the intent of the parties, but must also satisfy the requirements for a valid agreement as provided in Article 1320 of the Civil Code, the object of the grant must be owned by the grantor and there must be acceptance by the recipient.[28] With the development of digital technology, the object of grants is no longer limited to conventional assets but also encompasses digital assets such as *cryptocurrency* and digital tokens that have economic value and can be transferred.

A digital grant is the donation of assets or economic value conducted through electronic means, including crypto assets, digital tokens and other digital assets that can be owned, transferred, and transacted digitally through blockchain technology or similar distributed systems. [29] Its development is supported by blockchain technology, cryptocurrency, crowdfunding, and decentralized finance (DeFi). Blockchain as a distributed ledger technology provides transaction records that are transparent, permanent and difficult to manipulate, while cryptocurrency enables thedirect transfer of value without traditional financial intermediaries. Digital assets are managed through *digital wallets* that use cryptographic mechanisms involving *public keys* and *private keys* to receive, store and transfer digital assets.[30]

This combination of technologies creates a new ecosystem that enables the transfer of wealth in the form of digital grants. On the other hand, the characteristics of digital assets increase the risk of tax crimes and money laundering. Funds derived from tax evasion, false tax reporting, income concealment, or other tax crimes can be converted into crypto assets, moved through various wallets and blockchain networks then transferred back in the form of transactions that appear legitimate in order to conceal the origin of the funds.[31] In this scheme, digital grants can be used as instruments of *layering* and *integration* to disguise the origin of criminal proceeds.

Indications of digital grant misuse can be identified through various red flags, including anonymous donors, use of multiple wallets, cross-jurisdictional transactions without clear economic purpose, use of *privacy coins*, *mixers* or *tumblers*, decentralized finance (DeFi) platforms and grant values disproportionate to the economic profiles of the parties involved.

[27]Kharisma Benuf and Muhamad Azhar, "Legal Research Methodology as an Instrument for Unraveling Contemporary Legal Problems," *Jurnal Gema Keadilan 7*, no. 1 (2020): 24–28.
[28]M. Fadillah, "Legal Certainty Regarding Granted Land Without a Land Deed Official Deed," *Jurnal Nalar 2,* no. 1 (2023): 51–53.
[29]OECD, *Delivering Tax Transparency to Crypto-Assets* (Paris: OECD Publishing, 2024): 20.
[30]FATF*, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020): 7–9.
[31]H. F. Atlam et al., "Blockchain Forensics," *Electronics 13*, no. 17 (2024): 10–15.

These characteristics may indicate attempts to conceal identity, disguise the origin of funds and launder proceeds from tax crimes.[32]

Risk is also heightened when there is no verifiable legal, family, social, or business relationship between the grantor and recipient.[33] To identify and prove such misuse, Red Flag Theory and Digital Forensic Investigation are employed. Red Flag Theory is used to detect suspicious transaction patterns, while Digital Forensic Investigation is used to conduct *blockchain tracing*, *wallet attribution*, *transaction mapping* and *beneficial ownership analysis.* [34] Through this approach, the flow of digital funds can be traced such that its connection to tax crimes and money laundering can be proven under Indonesia's positive law.

Identification of Digital Grants Through the Red Flag Theory Approach

According to Joseph T. Wells, Red Flag Theory holds that a fraudulent act or criminal offense generally leaves behind warning indicators (*warning signs*) that can be used to identify the risk of irregularities.[35] The theory assumes that illegal activities tend to produce anomalies in the source of funds, transaction patterns, actor profiles and inter-party relationships. A red flag is not a piece of evidence but a risk indicator that serves as the basis for further analysis and investigation. The more indicators found, the higher the risk level of a transaction.

In the field of taxation, this theory helps identify discrepancies between economic profiles and transaction values,[36] use of third parties, transactions lacking economic substance and unreported asset ownership.[37] In the anti-money laundering regime, commonly used indicators include unclear sources of funds, layering, cross-jurisdictional transfers, use of anonymous accounts or wallets and unexplainable increases in wealth.[38]

The development of blockchain, cryptocurrency, and digital finance has given rise to digital grants as a new form of wealth transfer with the risk of being misused for money laundering originating from tax crimes. Their pseudonymous, fast and cross-jurisdictional characteristics[39] demand the application of Red Flag Theory as an early detection mechanism to differentiate between legitimate and high-risk transactions.

In this study, digital grant risk indicators are grouped into four categories. First, *source risk*, including anonymous donors, unclear sources of funds, high-risk wallets, and funds originating from high-risk jurisdictions. Second, *transaction risk*, such as cross-jurisdictional transfers, use of multiple wallets, *private wallets*, mixers, cross-chain transactions and layering patterns. Third, *beneficiary risk*, namely grant values disproportionate to the recipient's economic profile. Fourth, *relationship risk*, constituting the absence of any relationship or supporting documentation that can explain the relationship between the donor and recipient.[40]

[32]FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2024): 18–25.
[33]FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, updated 2021): 54–58.
[34]OECD, *Fighting Tax Crime — The Ten Global Principles, 2nd ed.* (Paris: OECD Publishing, 2021): 83–87.
[35]Joseph T. Wells, Principles of Fraud Examination, 5th ed. (Hoboken, NJ: John Wiley & Sons, 2017): 24–26.
[36]Yating Lin et al., "TaxThemis: Interactive Mining and Exploration of Suspicious Tax Evasion Group" (2020).
[37]Emre A. Akartuna, Michael Levi, and Georgios A. Antonopoulos, "Money Laundering Typologies and Trends: A Typological Scoping Review of Money Laundering Methods," *Security Journal 38* (2025): 1–31.
[38]Willem Prasetyo, "The Nominee Scheme Through the Lens of Anti-Money Laundering Law" (2025).
[39]Hugo Almeida, Pedro Pinto, and Ana Fernández Vilas, "A Review on Cryptocurrency Transaction Methods for Money Laundering" (2023).
[40]FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020): 9–24.

The results of this red flag identification serve as the basis for conducting Digital Forensic Investigation to trace fund flows, uncover the beneficial owner and prove the connection to tax crimes and money laundering. Based on the categories above, this study develops a risk assessment model using a cumulative approach.[41] Each red flag indicator is assigned a specific score based on the level of risk it entails. The more indicators found in a digital grant transaction, the higher the risk level of that transaction.

Table 1. Risk Assessment Model

Number of Red Flags	Risk Level
1–2 indicators	Low Risk
3–4 indicators	Moderate Risk
5–6 indicators	High Risk
> 6 indicators	Very High Risk

Source: Constructed by the Author based on the Risk-Based Approach of FATF (2020, 2021, 2024).

This model is not used to declare that a transaction constitutes a criminal act, but to determine investigative priorities. The matrix below depicts the main indicators used in this study:

Table 2. Red Flag Indicator Matrix

Category	Red Flag Indicator
Source Risk	Anonymous donor
Source Risk	Unclear source of funds
Source Risk	Funds originating from a high-risk jurisdiction
Transaction Risk	Cross-jurisdictional transfer
Transaction Risk	Use of private wallets
Transaction Risk	Use of mixer or tumbler
Transaction Risk	Complex layering
Transaction Risk	Cross-chain transaction
Beneficiary Risk	Unreasonable grant value
Beneficiary Risk	Recipient's economic profile does not match
Relationship Risk	No legal relationship
Relationship Risk	No basis for the grant

Source: Compiled by the Author based on FATF (2020; 2021; 2024), OECD (2021), and Atlam et al. (2024).

The matrix serves as an initial instrument for identifying digital grant transactions that require further investigation. In the context of tax crimes, the digital grant red flag model is used to identify the possibility that funds received as a grant actually originate from tax law violations.

As an example:

> *An individual receives a digital grant valued at IDR 20 billion in the form of cryptocurrency from a donor of unknown identity. The funds originate from a private wallet, previously passed through a mixer, and were transferred through several countries. Furthermore, the recipient has no legal relationship with the donor and cannot explain the reason for receiving the grant.*

In this example, several red flags are present simultaneously, namely:

[41] Financial Services Authority of Saint Vincent and the Grenadines, Conducting AML/CFT/CPF Institutional Risk Assessments Guidelines (2022).

1. Anonymous donor;
2. Cross-jurisdictional transfer;
3. Use of a *private wallet;*
4. Use of a *mixer;*
5. Unreasonable grant value;
6. Absence of a legal relationship; and
7. Unclear source of funds.

Based on the model developed, digital grant transactions meeting a number of risk indicators can be categorized as very high risk and made investigative priorities. Assessment is conducted through three main risk groups: *Source Risk*, *Transaction Risk* and *Beneficiary Risk*, analyzed using the Red Flag Theory approach.[42]

Source Risk assesses the transparency of the donor's identity, beneficial owner and source of funds. Risk increases when the donor is anonymous, the identity cannot be verified, multiple wallets are used, or platforms without a Know Your Customer (KYC) mechanism are utilized. Risk also arises when the true beneficial owner is unknown, when nominees or intermediaries are involved, or when the beneficial owner is concealed. Know Your Customer (KYC) Theory emphasizes the importance of the process of identifying, verifying, and continuously monitoring parties conducting transactions in order to understand their identity, transaction purpose, source of funds, and actual beneficial owner.[43] Risk further arises in the case of shell companies and when the source of funds cannot be explained, is inconsistent with the donor's economic profile, or originates from a high-risk jurisdiction. The lower the transparency of the source of funds, the higher the potential connection to tax crimes and money laundering.

Transaction Risk focuses on transaction patterns and mechanisms that indicate attempts to conceal the origin of funds. Main indicators include *blockchain layering*, *cross-chain transactions*, *high-frequency transfers* and *structuring transactions*. Complex, multi-layered transaction patterns that lack clear economic purpose indicate the possibility of money laundering through digital grants.

Meanwhile, *Beneficiary Risk* assesses the reasonableness of the recipient's economic profile, the relationship with the donor and the purpose of the grant. Risk increases when the grant value is disproportionate to the recipient's economic condition, there is no verifiable relationship between the parties, or the grant purpose is not supported by adequate documentation.[44] Such conditions may indicate the use of nominees or concealment of asset ownership.

To measure the overall risk level, this study uses the Digital Grant Risk Matrix as an *Early Warning System* instrument. An Early Warning System is an early detection mechanism that uses risk indicators to identify potential irregularities before they develop into more complex criminal acts.[45] This matrix helps determine examination priorities and serves as the basis for conducting Digital Forensic Investigation to trace fund flows and prove their connection to tax crimes and money laundering.

Risk assessment is based on three main indicator groups. First, Source Risk covering donor identity, beneficial owner and source of funds. Second, Transaction Risk comprising

[42]FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020): 7–24.

[43]FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations)* (Paris: FATF, 2023): 59–66.

[44]FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations)* (Paris: FATF, 2023): 61–66.

[45] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management Integrating with Strategy and Performance* (Durham, NC: COSO, 2017): 89–103.

blockchain layering, cross-chain transactions, high-frequency transfers, and structuring transactions. Third, Beneficiary Risk covering the recipient's economic profile, the donor–recipient relationship and the consistency of the grant's purpose. The more indicators identified, the higher the risk that the digital grant is being used as an instrument of money laundering, as shown in the table below:

Table 3. Digital Grant Risk Indicator Matrix

Risk Category	Red Flag Indicator	Risk Level	Notes
Source Risk	Donor identity unclear	High	Risk level determinations represent the author's assessments based on the FATF Risk-Based Approach and a synthesis of indicators drawn from FATF (2020; 2021; 2024), OECD (2021), and Atlam et al. (2024).
Source Risk	*Beneficial owner unknown*	High	
Source Risk	*Source of funds cannot be explained*	High	
Transaction Risk	*Blockchain layering*	High	
Transaction Risk	*Cross-chain transaction*	Moderate–High	
Transaction Risk	*High-frequency transfer*	Moderate	
Transaction Risk	*Structuring transaction*	High	
Beneficiary Risk	*Economic profile does not match*	High	
Beneficiary Risk	*Donor–recipient relationship unclear*	High	
Beneficiary Risk	*Grant purpose cannot be verified*	Moderate–High	

Source: Compiled by the Author based on FATF (2020; 2021; 2024), OECD (2021), and Atlam et al. (2024).

Based on the matrix, each indicator can be used to measure the risk level of a digital grant transaction. Furthermore, to provide a more objective assessment, each indicator is assigned a risk weight as follows:

Table 4. Risk Scoring System

Risk Level	Score	Application of scores to research indicators:	Indicator Score
Low	1	Donor identity unclear	3
Moderate	2	Beneficial owner unknown	3
High	3	Source of funds unclear	3
		Blockchain layering	3
		Cross-chain transaction	2
		High-frequency transfer	2
		Structuring transaction	3
		Economic profile does not match	3
		Donor–recipient relationship unclear	3

Grant purpose cannot be verified	2

Source: Constructed by the Author based on the Risk-Based Approach of FATF (2020; 2021; 2024).
Note: The scoring system is a product of the author's development based on the FATF Risk-Based Approach. Weights are assigned by considering the degree of relevance of each indicator to the risk of money laundering originating from tax crimes through digital grants.
The maximum total score is: **10 indicators × 3 = 30 points**

Based on the total score obtained, digital grant transactions can be classified into four risk categories.

Table 5. Risk Level Classification

Total Score	Risk Level
0 – 7	Low Risk
8 – 15	Moderate Risk
16 – 23	High Risk
24 – 30	Very High Risk

Source: Compiled by the Author based on the FATF Risk-Based Approach and the Digital Grant Risk Matrix developed in this study.
Note: Risk level classification is a product of the author's development based on the cumulative total score of Source Risk, Transaction Risk, Beneficiary Risk and Relationship Risk indicators. Score ranges are set to differentiate levels of oversight and investigative priority based on the Risk-Based Approach.

Table 6. Classification Interpretation

No.	Classification	Description
1	Low Risk	The transaction shows few red flag indicators and generally still exhibits characteristics consistent with legitimate activity.
2	Moderate Risk	Several indicators requiring additional verification have been identified, but they do not yet demonstrate a strong indication of money laundering.
3	High Risk	A significant combination of indicators has been found, rendering the transaction worthy of investigative priority.
4	Very High Risk	Nearly all red flag indicators have been identified, strongly suggesting that the digital grant is being used as an instrument for concealing proceeds of tax crimes.

Source: Compiled by the Author based on FATF (2020; 2021; 2024) and OECD (2021).

Risk level interpretation is a product of the author's development based on the number and significance of red flag indicators identified. The more risk indicators found in a transaction, the higher the priority for verification, investigation and Digital Forensic Investigation required. As an example, the application of the Risk Matrix is simulated as follows:

Table 7. Risk Matrix Application Simulation

As an illustration, consider a digital grant transaction with the following characteristics:	Scores obtained: Indicator Score	Indicator Score
• Anonymous donor	Donor identity unclear	3
• *Beneficial owner* unknown.	Beneficial owner unknown	3
• Funds originate from a wallet whose source cannot be explained.	Source of funds unclear	3

• Funds passed through multiple wallets (*layering*).	*Blockchain layering*	3
• Funds moved across blockchains.	*Cross-chain transaction*	2
• Grant value is very large relative to the recipient's economic profile.	Economic profile does not match	3
• No legal relationship between donor and recipient.	Donor–recipient relationship unclear	3
Total Score		20

Source: Author's simulation based on the Digital Grant Risk Matrix developed from FATF (2020; 2021; 2024), OECD (2021), and Atlam et al. (2024).

Note: The case in this table is a hypothetical simulation used to test the application of the Digital Grant Risk Matrix. The total score is derived by summing the weights of each indicator according to the scoring system developed in this study.

Based on the risk matrix, a score of 20 falls within the **High Risk** category, making the transaction eligible for Digital Forensic Investigation. The results of the study indicate that the risk of digital grants cannot be assessed based on a single indicator, but rather through a combination of interrelated red flags. The more indicators identified, the higher the likelihood that the transaction is connected to money laundering originating from tax crimes. To support early detection, this study develops the Digital Grant Risk Matrix as a systematic assessment instrument for identifying, classifying, and prioritizing high-risk transactions. This model is integrated into an Early Warning System (EWS) that combines Red Flag Theory, Risk-Based Approach, and Digital Financial Crime Detection.

EWS implementation is carried out in two stages: collection of digital grant transaction data and red flag screening. Analysis focuses on Source Risk, Transaction Risk, and Beneficiary Risk, assessed using the risk scoring system. The results of this assessment serve as the basis for determining examination priorities and conducting Digital Forensic Investigation to trace fund flows and uncover indications of digital grant-based money laundering.

The third stage is Risk Scoring and Classification, in which, following the screening process, the system calculates the total risk score obtained. The final stage of the EWS is to generate alerts based on the risk level of the digital grant transaction. Alerts are classified as Green, Yellow, Orange, and Red Alerts. The higher the risk level, the greater the need for verification, further analysis and Digital Forensic Investigation as the basis for risk-based handling. The operational model can be described as follows:

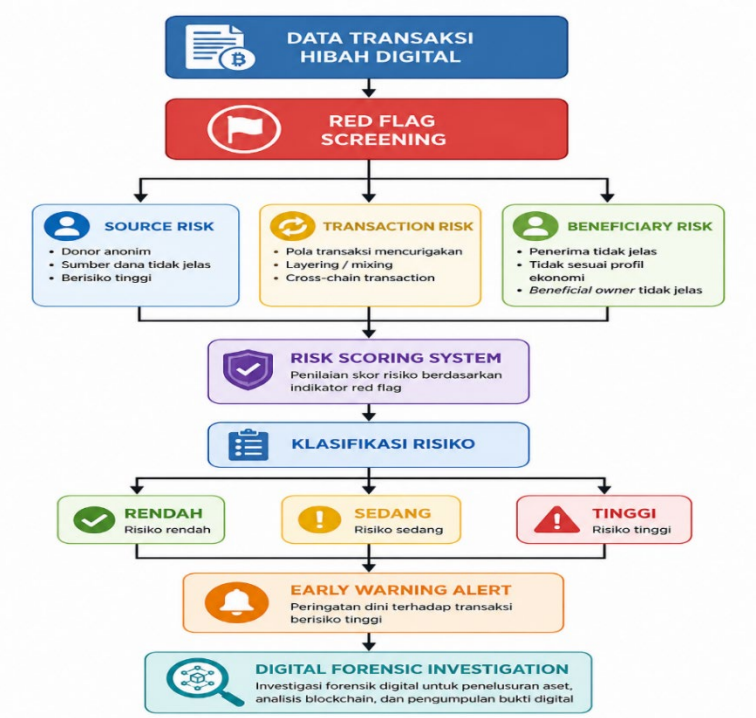

Figure 1. Conceptual Model: Digital Transaction Risk Flow Diagram — Developed by the Author

Source: Compiled by the Author based on FATF (2020; 2021; 2024), OECD (2021), and Atlam et al. (2024)

This study demonstrates that Digital Forensic Investigation is conducted after a digital grant transaction reaches a certain risk level based on red flag identification results. To support this process, an Early Warning System (EWS) model is developed that integrates Red Flag Theory and the risk-based approach through three main parameters: Source Risk, Transaction Risk and Beneficiary Risk.

The results of the study indicate that the more risk indicators appearing simultaneously, the higher the potential connection of the transaction to money laundering originating from tax crimes. Through the Digital Grant Risk Matrix and EWS, transactions can be classified based on their risk level, thereby supporting early detection, tax oversight and the determination of investigative priorities in a more systematic and effective manner.

Digital Forensic Investigation in Proving Digital Grants

Digital Forensic Investigation is a scientific method for identifying, collecting, preserving, analyzing, and presenting digital evidence to support the investigation, inquiry, and legal proof process. According to Eoghan Casey, Digital Forensic Investigation is a scientific process conducted to identify, secure, collect, examine, analyze and present digital evidence in order to reconstruct an event that is legally relevant. Through this approach, electronic transaction trails, crypto assets, digital wallets, transaction metadata and inter-party relationships can be traced, enabling the disclosure of money laundering schemes conducted through digital grants.[46] In financial crimes, this approach does not merely function to find electronic evidence, but also to trace fund flows, identify perpetrators and beneficial owners and link digital transactions to the underlying criminal offense.

[46]Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 4th ed. (Amsterdam: Academic Press, 2020): 3–5.

Its execution encompasses the stages of identification, collection, preservation, examination, analysis, and reporting, with regard to the principles of legality, integrity, accountability and chain of custody. Blockchain forensics is a specialized method that exploits the transparent, permanent, and traceable nature of blockchain to support digital asset investigations. In this study, blockchain forensics is used to verify red flag indicators, trace sources of funds, identify donors and beneficial owners, and uncover the connection between digital grants and tax crimes and money laundering. Techniques employed include blockchain transaction tracing, wallet attribution analysis, cluster analysis, transaction mapping and flow of funds analysis.

Blockchain transaction tracing functions to reconstruct the flow of digital assets from their source to their final destination through analysis of transaction history, inter-wallet relationships and fund movement patterns. *Wallet attribution analysis* is used to link wallet addresses to specific individuals or entities through blockchain data, KYC, OSINT (Open Source Intelligence), [47] and electronic device information. Both methods help uncover anonymous donors, unclear sources of funds, layering patterns and hidden inter-party relationships. Analysis is further reinforced through *cluster analysis* and *transaction mapping*, which can identify transaction networks, fan-in, fan-out and circular transaction patterns, as well as money laundering structures involving multiple wallets. Furthermore, *cryptocurrency exchange analysis* is used to link blockchain activity with user data on crypto asset platforms to identify account owners and origins of funds.

To uncover the party who truly controls the assets, *beneficial ownership investigation* is employed. Cassara, through the Follow the Money approach, explains that financial crime investigations must trace who actually enjoys the true economic benefit (*ultimate beneficiary*) of a transaction or corporate structure;[48] and Madinger emphasizes that AML investigations must be able to identify the individual behind the nominee, shell company, trust, or complex ownership structure used to conceal criminal proceeds.[49] All findings are then correlated with tax data to prove the relationship between digital assets, digital grants, and tax crimes as the predicate offense.

The results of the study indicate that effective proof does not rely solely on blockchain evidence, but also on the ability to link digital evidence with tax and financial data. Reconstruction of digital grant fund flows serves as the primary instrument for uncovering the source of funds, concealment patterns, and their connection to tax crimes and money laundering. In this study, digital grant fund flows can be reconstructed through the following stages:

[47]Mark M. Lowenthal*, Intelligence: From Secrets to Policy, 8th ed*. (Washington, DC: CQ Press, 2019): 108–110.

[48]John A. Cassara, *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails* (Hoboken, NJ: Wiley, 2020): 95–110.

[49]John Madinger, *Money Laundering: A Guide for Criminal Investigators, 4th ed*. (Boca Raton: CRC Press, 2022): 113–128.

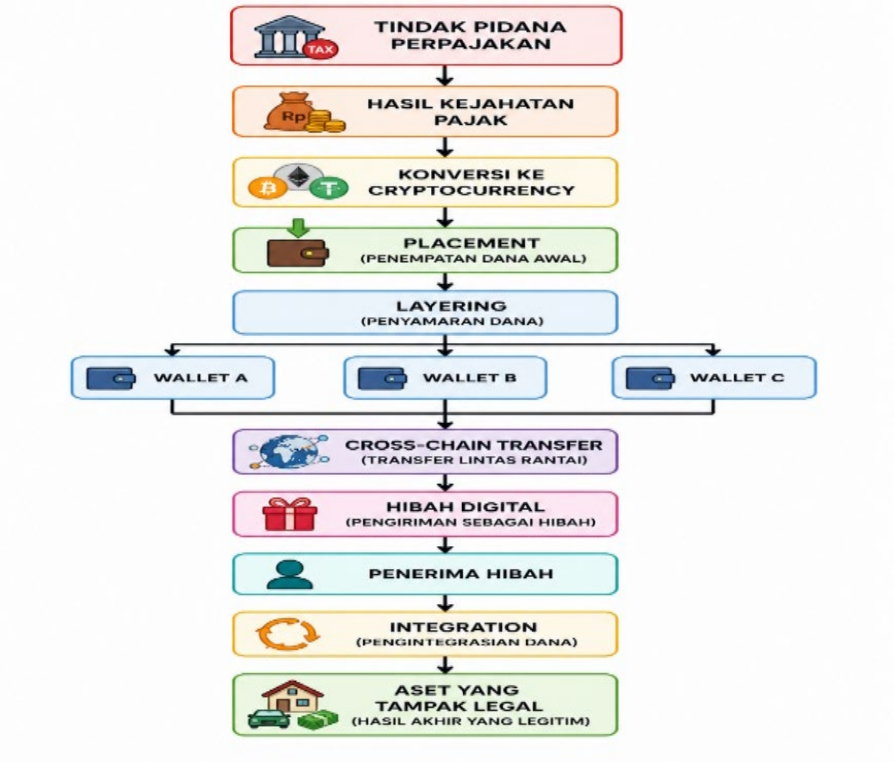

Figure 2. Conceptual Model: Digital Money Laundering Process Flow — Developed by the Author

Source: Compiled by the Author based on FATF (2020; 2021; 2024), OECD (2021), and Atlam et al. (2024)

The model demonstrates how digital grants can be used as an instrument for integrating tax crime proceeds into the economic system under a legitimate appearance. This study reconstructs fund flows through the integration of various Digital Forensic Investigation methods, including Blockchain Transaction Tracing, Wallet Attribution Analysis, Cluster Analysis, Transaction Mapping, Cryptocurrency Exchange Analysis and Beneficial Ownership Investigation.

This approach is used to trace digital assets, identify related parties and uncover beneficial owners. In the context of tax crimes and money laundering, this method helps prove unreported income, concealed assets and the stages of placement, layering and integration.[50] The results serve as the basis for proving the connection between digital grants and money laundering schemes originating from tax crimes. The evidentiary model developed in this study can be described as follows:

[50]FATF, *Guidance on Beneficial Ownership of Legal Persons (Paris: FATF, 2023): 7–14; FATF, Mutual Evaluation Report of Indonesia* (Paris: FATF, 2023).

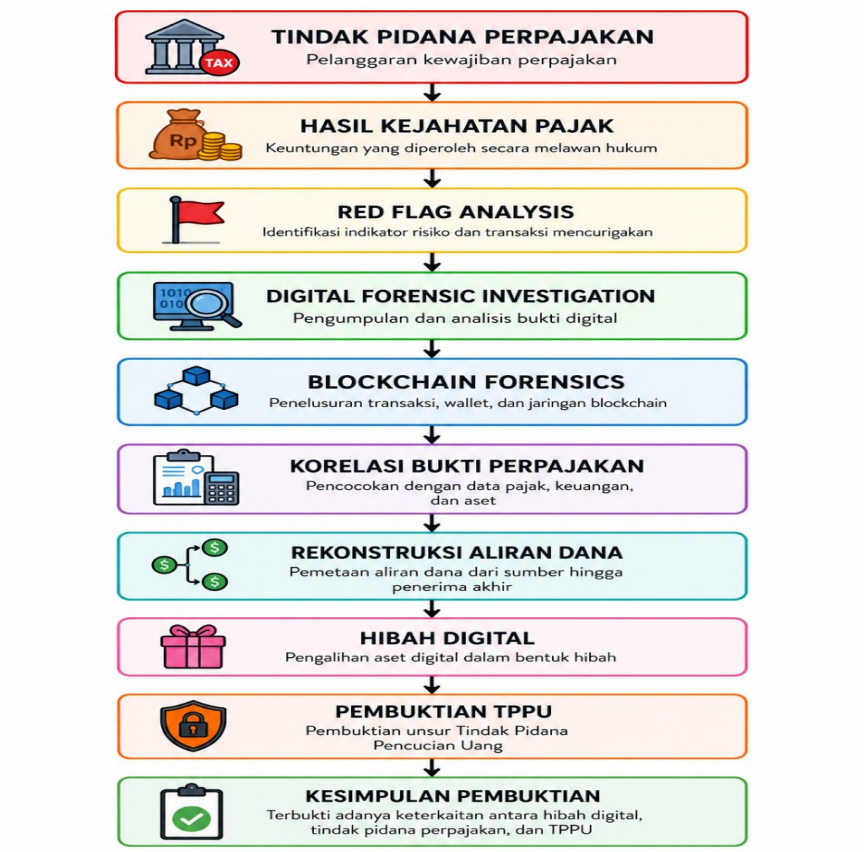

Figure 3. Conceptual Model: Tax Crime Process Flow — Developed by the Author
Source: Conceptual model developed by the Author based on Red Flag Theory, Digital Forensic Investigation, Blockchain Forensics, and the ML Evidentiary Framework.

The Digital Grant Evidentiary Model is the result of the author's synthesis integrating Red Flag Theory as a risk identification mechanism, Digital Forensic Investigation and Blockchain Forensics as methods for collecting and analyzing digital evidence and correlation with tax data to prove tax crimes as the predicate offense in money laundering.

This study demonstrates that proof of digital grants is carried out through an interconnected chain of processes, beginning from red flag identification, through digital forensic analysis, to fund flow reconstruction. This approach integrates digital evidence and tax data with an emphasis on the economic substance of transactions. Blockchain provides a permanent and traceable transaction trail, while Blockchain Transaction Tracing, Wallet Attribution Analysis, Cluster Analysis, and Transaction Mapping effectively uncover fund flows, beneficial owners and layering patterns. KYC data from cryptocurrency exchanges also helps connect digital identities with legal identities.

Furthermore, the correlation between digital evidence and tax data is key to proving tax crimes as a predicate offense in digital asset-based money laundering schemes. Article 69 of Law Number 8 of 2010 affirms that the investigation, prosecution, and examination of money laundering does not require prior proof of the predicate offense.[51] The strengthening of digital

[51]F. Yurendo, Santrawan T. Paparang, and A. Fitrian, "The Urgency of Amending the Phrase 'No Prior Proof of Predicate Offense Required' in Article 69 of the Money Laundering Law," *Journal Evidence of Law 4*, no. 1 (2025): 360–369.

grant transaction oversight becomes increasingly relevant in the era of Coretax DJP, which prioritizes data integration, digitalization of tax administration and risk-based oversight.

Conclusion

This study concludes that digital grants constitute a high-risk mechanism that can potentially be misused as an instrument of money laundering originating from tax crimes. This risk is influenced by the characteristics of blockchain technology, which is pseudonymous and cross-jurisdictional, as well as by the still limited oversight and regulation governing it. The results of the study indicate that Red Flag Theory can be used as an effective framework for detecting indications of digital grant misuse through the identification of Source Risk, Transaction Risk, and Beneficiary Risk indicators. These indicators can then be integrated into a Digital Grant Red Flag Model, Risk Matrix and Early Warning System (EWS) to strengthen risk-based detection and oversight mechanisms. Furthermore, Digital Forensic Investigation plays an important role in converting risk indicators into evidentiary instruments through the application of blockchain forensics, transaction tracing, beneficial owner identification and fund flow reconstruction. The integration of both approaches produces a Digital Grant Evidentiary Model that provides a comprehensive framework for proving the connection between digital grants, tax crimes and money laundering.

From a policy standpoint, the government needs to establish specific regulations on digital grants that govern reporting obligations, source of funds transparency and beneficial ownership disclosure.

References

Akartuna, Emre A., Michael Levi, and Georgios A. Antonopoulos. “Money Laundering Typologies and Trends: A Typological Scoping Review of Money Laundering Methods.” *Security Journal 38* (2025): 1–31.

Almeida, Hugo, Pedro Pinto, and Ana Fernández Vilas. “A Review on Cryptocurrency Transaction Methods for Money Laundering.” 2023.

Anjani, Aulia, and Heni Widiastuti. “The Puzzle of Money Laundering: A Literature Review of Regulations and Implications.” *Journal of Accounting and Investment 25*, no. 3 (2024): 1088–1108.

Asmarani, Nora Galuh Candra. “Cara Laporkan Penghasilan yang Bukan Objek Pajak di SPT via Coretax.” DDTC News, February 26, 2026.

Atlam, H. F., et al. “Blockchain Forensics: A Systematic Literature Review of Techniques, Tools, and Challenges.” Electronics 13, no. 17 (2024): 1–15.

Benuf, Kharisma, and Muhamad Azhar. “Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer.” *Jurnal Gema Keadilan 7*, no. 1 (2020): 20–33.

Cassara, John A. Money Laundering and Illicit Financial Flows: Following the Money and Value Trails. Hoboken, NJ: Wiley, 2020.

Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th ed. Amsterdam: Academic Press, 2020.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management Integrating with Strategy and Performance. Durham, NC: COSO, 2017.

Direktorat Jenderal Pajak. Buku Manual Coretax – Pelaporan SPT Tahunan PPh Orang Pribadi. Jakarta: Direktorat Jenderal Pajak, 2024.

———. “Coretax DJP Hadir sebagai Sistem Pajak Digital Terpadu.” Pajak.go.id, 2025.

———. “Coretax DJP: 1 Aplikasi 7 Manfaat.” Pajak.go.id, February 7, 2025.

———. “DJP Luncurkan Aplikasi Compliance Risk Management (CRM) Penegakan Hukum dan CRM Penilaian.” April 8, 2022.

Fahlepy, Reza, et al. “Status Peralihan Sertifikat Hak Atas Tanah Berdasarkan Surat Hibah di Bawah Tangan.” *Jurnal de Jure 13*, no. 1 (2024): 101–115.

Financial Action Task Force (FATF). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021.

———. Guidance on Beneficial Ownership of Legal Persons. Paris: FATF, 2023.

———. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations). Paris: FATF, 2023.

———. Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2024.

———. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. Paris: FATF, 2020.

Fhatnur, Yoga Sugama Ali. “Dynamics and Strategies of Law Enforcement of Money Laundering Offences in Indonesia (Dinamika dan Strategi Penegakan Hukum Tindak Pidana Pencucian Uang di Indonesia).” *Indonesian Journal of Law and Economics Review 19*, no. 2 (2024).

Garnasih, Yenti. Penegakan Hukum Tindak Pidana Pencucian Uang di Indonesia. Jakarta: Kencana, 2016.

Lin, Yating, et al. “TaxThemis: Interactive Mining and Exploration of Suspicious Tax Evasion Group.” 2020.

Lowenthal, Mark M. Intelligence: From Secrets to Policy. 8th ed. Washington, DC: CQ Press, 2019.

Madinger, John. Money Laundering: A Guide for Criminal Investigators. 4th ed. Boca Raton: CRC Press, 2022.

Maharani, Mentari Rizkika, Vira Wijaya, Carolina Isabela Sinawan, Aurynanda Salsabila, and Zenzai Ayu Alvina. “Keabsahan Akta Hibah yang Digunakan Wajib Pajak untuk Penghindaran Pajak.” Jurnal USM Law Review 8, no. 1 (2025): 128–142.

Mintoff, Yana, and Mary Grace Vella. “Money Laundering and the Crime Nexus: A Case Study in Malta.” Journal of Financial Crime 6, no. 2 (2024): 1–15.

Nurferyanto, Dwi, and Yoshi Takahashi. “Combating Tax Crimes in Indonesia: Tackling the Issue Head-On.” Humanities and Social Sciences Communications 11 (2024): 1556.

Organisation for Economic Co-operation and Development (OECD). Bringing Tax Transparency to Crypto-Assets: An Update. Paris: OECD Publishing, 2024.

———. Delivering Tax Transparency to Crypto-Assets: A Step-by-Step Guide to Understanding and Implementing the Crypto-Asset Reporting Framework (CARF). Paris: OECD Publishing, 2024.

———. Fighting Tax Crime: The Ten Global Principles. 2nd ed. Paris: OECD Publishing, 2021.

———. Inheritance Taxation in OECD Countries. Paris: OECD Publishing, 2021.

———. Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues. Paris: OECD Publishing, 2020.

Riccardi, Michele, and Peter Reuter. “The Varieties of Money Laundering and the Determinants of Offender Choices.” *European Journal on Criminal Policy and Research 30* (2024): 333–358.

Setia Negara, Tunggul Ansari. “Normative Legal Research in Indonesia: Its Origin and Approaches.” *Audi Et AP: Journal of Legal Studies 4, no. 1* (2023): 1–12.

Siringoringo, M. J. B., and S. M. Simanjuntak. "Auditor Capability on the Effectiveness of Red Flags in Fraud Detection." *Jurnal Ilmiah Manajemen Kesatuan 13*, no. 1 (2025): 124–126.

Slemrod, Joel. "Tax Compliance and Enforcement." *Journal of Economic Literature 57*, no. 4 (2019): 904–954.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Wells, Joseph T. Principles of Fraud Examination. 5th ed. Hoboken, NJ: John Wiley & Sons, 2017.

World Bank. Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Reference Guide and Information on the Use of the Financial Intelligence Unit and Financial Information by Development Agencies. Washington, DC: World Bank.

Yurendo, F., Santrawan T. Paparang, and A. Fitrian. "Urgensi Perubahan Frasa 'Tidak Wajib Dibuktikan Terlebih Dahulu Tindak Pidana Asal' dalam Pasal 69 Undang-Undang Tindak Pidana Pencucian Uang." *Journal Evidence of Law* 4, no. 1 (2025): 360–369.