

## Hibah Digital sebagai Modus Pencucian Uang dari Kejahatan Perpajakan

Rama Nova Hariyanto\*, Mohammad Syafi'i, Median Dwi Restana

Direktorat Jenderal Pajak, Kementerian Keuangan Republik Indonesia, Indonesia

Korespondensi penulis: ramanova50@gmail.com

*Kata Kunci:*  
Digital Forensic  
Investigation, Hibah, Red  
Flag Theory, Tindak Pidana  
Pencucian Uang, Tindak  
Pidana Perpajakan

### Abstrak

Perkembangan *cryptocurrency*, *blockchain* dan keuangan digital telah melahirkan hibah aset digital sebagai bentuk baru transfer kekayaan yang berpotensi dimanfaatkan untuk Tindak Pidana Pencucian Uang (TPPU) yang bersumber dari tindak pidana perpajakan. Sifatnya yang *pseudonim*, lintas yurisdiksi, dan terdesentralisasi menimbulkan kendala dalam identifikasi, pengawasan, serta pembuktian hukum. Penelitian ini bertujuan mengidentifikasi karakteristik hibah aset digital yang mencurigakan, menganalisis penerapan *Red Flag Theory* dalam deteksi risiko, dan mengkaji peran *Digital Forensic Investigation* dalam pembuktian keterkaitannya dengan tindak pidana perpajakan sebagai *predicate crime*. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan studi kepustakaan. Analisis dilakukan melalui integrasi *Red Flag Theory*, *blockchain forensics*, *wallet attribution analysis*, *investigasi beneficial ownership*, korelasi bukti digital dan perpajakan, serta rekonstruksi aliran dana. Hasil penelitian menunjukkan bahwa risiko tinggi ditandai oleh donor anonim, *beneficial owner* yang tidak jelas, *blockchain layering*, transaksi lintas rantai (*cross-chain*), penggunaan teknologi privasi, serta ketidaksesuaian nilai hibah dengan profil ekonomi penerima. Penelitian ini menghasilkan Model *Red Flag* Hibah Aset Digital, Matriks Risiko, *Early Warning System* dan model integrasi *Red Flag Theory* dengan *Digital Forensic Investigation* sebagai kerangka sistematis untuk mendeteksi, menginvestigasi, dan memverifikasi hibah aset digital yang digunakan sebagai sarana TPPU yang berasal dari tindak pidana perpajakan.

Dikirimkan: 4 April 2026

Diterima: 22 Juni 2026

Diterbitkan: 28 Juni 2026

Copyright (c) Author



**Untuk mensitasi artikel ini:** Hariyanto, R. N., Syafi'i, M., & Restana, M. D. 2026. Hibah Digital sebagai Modus Pencucian Uang dari Kejahatan Perpajakan. *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>

### Pendahuluan

Hibah merupakan institusi hukum yang telah dikenal sejak masa hukum Romawi melalui konsep *donatio*, yaitu pemberian harta secara sukarela tanpa imbalan untuk memperkaya pihak lain. Konsep ini kemudian berkembang dalam sistem hukum perdata modern, termasuk di

Indonesia, sebagai mekanisme pengalihan hak atas harta secara cuma-cuma.<sup>1</sup> Secara tradisional, hibah digunakan untuk kepentingan keluarga, sosial, keagamaan, dan pemberian dengan objek berupa tanah, bangunan, uang, atau aset berwujud lainnya yang didukung oleh dokumen formal dan identitas para pihak yang jelas. Perkembangan teknologi digital telah melahirkan hibah digital, yaitu pengalihan nilai melalui uang elektronik, dompet digital, aset kripto, token digital, dan platform *crowdfunding*. Sejak munculnya teknologi *blockchain* dan aset kripto, hibah dapat dilakukan secara cepat, lintas negara, dan tanpa perantara keuangan konvensional.<sup>2</sup>

Dalam perspektif perpajakan sesuai Peraturan Menteri Keuangan Nomor 114 Tahun 2025, hibah memiliki karakteristik khusus karena dapat dikecualikan dari objek pajak apabila memenuhi persyaratan tertentu. Kebijakan ini memberikan ketentuan hukum mengenai perlakuan Pajak Penghasilan atas bantuan, sumbangan dan hibah hanya sebatas untuk pengalihan kekayaan yang bersifat sosial, keagamaan, pendidikan atau kekeluargaan.<sup>3</sup> Sebagai tambahan dalam implementasi Coretax Direktorat Jenderal Pajak (DJP) sejak bulan Januari 2025, mengatur tentang penerimaan hibah yang memenuhi persyaratan sebagai penghasilan yang dikecualikan dari objek Pajak Penghasilan tetap wajib dilaporkan dalam Surat Pemberitahuan (SPT) Tahunan. Mekanisme pelaporan dilakukan melalui lampiran L-2 bagian B sebagai "Penghasilan yang Tidak Termasuk Objek Pajak", dan apabila harta yang berasal dari hibah masih dimiliki atau dikuasai pada akhir tahun pajak, harta tersebut juga wajib dicantumkan dalam lampiran L-1 bagian A mengenai daftar harta pada akhir tahun pajak. Dengan demikian, sistem Coretax menerapkan pendekatan pelaporan ganda (*dual reporting*), yaitu pelaporan berdasarkan sumber perolehan harta dan pelaporan berdasarkan posisi harta yang dimiliki pada akhir periode pajak.<sup>4</sup>

Sistem pelaporan hibah dalam Coretax DJP masih bersifat deklaratif (*self-assessment based reporting*) karena sangat bergantung pada informasi yang disampaikan oleh wajib pajak. Lebih lanjut belum secara eksplisit mensyaratkan pengungkapan *beneficial owner*, verifikasi asal-usul dana (*source of funds*), maupun penerapan indikator risiko pencucian uang (*anti-money laundering red flags*) terhadap hibah yang dilaporkan. Akibatnya berpotensi menimbulkan celah pengawasan, terutama pada hibah bernilai besar, hibah lintas yurisdiksi atau hibah berbasis aset digital yang memiliki karakteristik anonimitas dan kompleksitas transaksi yang lebih tinggi.<sup>5</sup>

Berbeda dengan hibah konvensional, hibah digital memiliki karakteristik cepat, lintas yurisdiksi, dan bersifat *pseudonym*, sehingga menyulitkan identifikasi *beneficial owner* serta penelusuran sumber dana. Kondisi ini meningkatkan risiko penyalahgunaan hibah digital untuk penghindaran pajak, penyamaran penghasilan, dan pencucian uang. Oleh karena itu, kajian hibah digital menjadi penting untuk mendukung efektivitas pengawasan perpajakan.<sup>6</sup> Namun, sampai dengan saat ini, pengembangan Coretax DJP belum mencakup mekanisme otomatis yang secara spesifik ditujukan untuk mendeteksi indikasi penyalahgunaan atau mengklasifikasikan hibah digital, aset virtual maupun transaksi berbasis *blockchain* sebagai

<sup>1</sup> Reza Fahlepy et al., "Status Peralihan Sertifikat Hak Atas Tanah Berdasarkan Surat Hibah di Bawah Tangan," *Jurnal de Jure* 13, no. 1 (2024): 101–102

<sup>2</sup> 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.

<sup>3</sup> Indonesia, *Peraturan Menteri Keuangan Nomor 114/PMK.03/2025 tentang Bantuan atau Sumbangan, serta Harta Hibahan yang Dikecualikan sebagai Objek Pajak Penghasilan* (Jakarta: Kementerian Keuangan Republik Indonesia, 2020), Pasal 2 ayat (3). ([Direktorat Jenderal Pajak](#))

<sup>4</sup> Nora Galuh Candra Asmarani, "Cara Laporkan Penghasilan yang Bukan Objek Pajak di SPT via Coretax," *DDTC News*, 26 Februari 2026.

<sup>5</sup> Direktorat Jenderal Pajak, *Buku Manual Coretax – Pelaporan SPT Tahunan PPh Orang Pribadi* (Jakarta: DJP, 2024)

<sup>6</sup> Direktorat Jenderal Pajak, "Coretax DJP Hadir sebagai Sistem Pajak Digital Terpadu," [Pajak.go.id](#), 2025.

kategori risiko tersendiri. Mekanisme dalam Coretax DJP terbatas dalam integrasi data, *data matching*, *risk profiling* dan *compliance risk management* sehingga efektivitas identifikasi hibah digital sangat bergantung pada ketersediaan data pihak ketiga, kualitas pelaporan wajib pajak, serta kemampuan sistem dalam mendeteksi ketidaksesuaian antara profil ekonomi, pertambahan kekayaan dan sumber penghasilan yang dilaporkan.<sup>7</sup>

Celah pengawasan tersebut tidak menutup kemungkinan digunakan oleh Wajib Pajak untuk menyamarkan sifat harta (*disguising the illicit origin of assets*).<sup>8</sup> Praktik penyamaran sifat harta yang berasal dari tindak pidana perpajakan melalui dokumen hibah dapat dianalisis dalam kerangka hukum positif Indonesia, khususnya berdasarkan ketentuan dalam Undang-Undang Tindak Pidana Pencucian Uang (UU TPPU) dan Undang-Undang Perpajakan. Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang mengatur dalam Pasal 2 ayat (1) yang menempatkan tindak pidana perpajakan sebagai salah satu tindak pidana asal (*predicate offence*) yang dapat menghasilkan harta kekayaan yang selanjutnya menjadi objek pencucian uang.<sup>9</sup>

Keterbatasan dalam mengidentifikasi hibah digital memungkinkan transaksi dilakukan melalui aset virtual, dompet kripto atau *platform digital* yang belum terintegrasi dengan sumber data perpajakan.<sup>10</sup> Sebagai hasilnya, diperlukan pendekatan untuk mengantisipasi potensi tindak pidana perpajakan dan pencucian uang yang memanfaatkan aset digital, termasuk aset *kripto* dan transaksi berbasis *blockchain*.<sup>11</sup> Sejumlah penelitian telah menyoroti hubungan antara tindak pidana perpajakan dan tindak pidana pencucian uang (TPPU). Riccardi dan Reuter (2024)<sup>12</sup> menjelaskan bahwa strategi pencucian uang dipengaruhi oleh pilihan pelaku dan tingkat pengawasan sektor yang digunakan. Nurferyanto dan Takahashi (2024)<sup>13</sup> menegaskan bahwa kejahatan perpajakan semakin kompleks dan memerlukan integrasi data, teknologi serta koordinasi antarlembaga. Mintoff dan Vella (2024)<sup>14</sup> menunjukkan bahwa pencucian uang berkaitan erat dengan tindak pidana asal, termasuk penggelapan pajak, melalui pemanfaatan berbagai instrumen keuangan. Fhatnur dan Sugama Ali (2024)<sup>15</sup> menekankan pentingnya pendekatan *follow the money* dan pemanfaatan data keuangan dalam mengungkap TPPU, sedangkan Anjani, Aulia dan Widiastuti (2024)<sup>16</sup> menyoroti perlunya penguatan pengawasan dan sistem pengendalian dalam rezim anti pencucian uang. Slemrod (2019)<sup>17</sup> dan Levi (2018)<sup>18</sup>

<sup>7</sup> Direktorat Jenderal Pajak, "DJP Luncurkan Aplikasi Compliance Risk Management (CRM) Penegakan Hukum dan CRM Penilaian," 8 April 2022

<sup>8</sup> 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

<sup>9</sup> Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Pasal 2 ayat (1);

<sup>10</sup> Direktorat Jenderal Pajak, "Coretax DJP: 1 Aplikasi 7 Manfaat"; 7 Februari 2025.

<sup>11</sup> Organisation for Economic Co-operation and Development (OECD), *Bringing Tax Transparency to Crypto-Assets: An Update* (Paris: OECD Publishing, 2024)

<sup>12</sup> Riccardi, Michele, dan Peter Reuter. "The Varieties of Money Laundering and the Determinants of Offender Choices." *European Journal on Criminal Policy and Research* 30 (2024): 333–358

<sup>13</sup> Nurferyanto, Dwi, dan Yoshi Takahashi. "Combating Tax Crimes in Indonesia: Tackling the issue Head-On." *Humanities and Social Sciences Communications* 11 (2024): 1556

<sup>14</sup> Mintoff, Yana, dan Mary Grace Vella. "Money Laundering and the Crime Nexus: A Case Study in Malta." *Journal of Financial Crime* 6, no. 2 (2024): 1–15

<sup>15</sup> Fhatnur, Yoga Sugama Ali. 2024. "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 (2).

<sup>16</sup> Anjani, Aulia, dan 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

<sup>17</sup> Slemrod, Joel. "Tax Compliance and Enforcement." *Journal of Economic Literature* 57, no. 4 (2019).

<sup>18</sup> Levi, Michael dan Peter Reuter. "Money Laundering, *Risks and Regulation*" *Crime and Justice* 34, no. 1 (2006): 289–375.

menjelaskan keterkaitan antara penggelapan pajak, perilaku wajib pajak dan penggunaan teknik pencucian uang untuk menyembunyikan hasil kejahatan. Garnasih (2016)<sup>19</sup> menegaskan bahwa tindak pidana perpajakan merupakan salah satu tindak pidana asal TPPU. Sementara itu, Maharani dkk. (2025)<sup>20</sup> mengkaji hibah dalam konteks penghindaran pajak melalui akta hibah.

Penelitian terdahulu belum secara khusus menganalisis hibah digital sebagai modus pencucian uang yang berasal dari menyamarkan dana hasil tindak pidana perpajakan. Ketiadaan pengaturan khusus dan belum adanya indikator risiko yang memadai semakin menghambat pengawasan teknologi seperti *non-custodial wallet*, *privacy coin*, *mixing service* dan *DeFi* di mana dimungkinkan penyamaran aliran dana terkait dengan tindak pidana perpajakan dan pencucian uang yang dilakukan secara kompleks. Oleh karena itu, penelitian ini mengisi kesenjangan tersebut melalui pendekatan *Red Flag Theory* dan *Digital Forensic Investigation*<sup>21</sup> dengan cara membahas bagaimana karakteristik modus aliran dana hibah digital yang digunakan dan bagaimana penerapan *Red Flag Theory* dalam mengidentifikasi hibah digital yang mencurigakan melalui indikator-indikator risiko seperti transaksi yang tidak memiliki tujuan ekonomi yang jelas, penggunaan alamat dompet kripto berisiko tinggi, donor anonim, frekuensi transaksi yang tidak wajar dan pola transfer lintas yurisdiksi.<sup>22</sup> Selanjutnya, *Digital Forensic Investigation* digunakan untuk menelusuri jejak transaksi, mengidentifikasi hubungan antar *wallet* serta mengungkap aliran dana hibah digital yang diduga berasal dari tindak pidana perpajakan dan kemudian disamakan melalui aset kripto maupun teknologi *blockchain*<sup>23</sup> dengan tujuan untuk mengidentifikasi karakteristik hibah digital, menganalisis penerapan *Red Flag Theory*, serta mengkaji peran *Digital Forensic Investigation* dalam menguji keterkaitan aliran dana hibah digital dengan tindak pidana perpajakan sebagai *predicate crime*. Penelitian ini diharapkan memberikan kontribusi kajian penerapan *Red Flag Theory* dan *Digital Forensic Investigation* serta dalam pengembangan hukum perpajakan, tindak pidana pencucian uang, pembuktian, dan forensik digital. Selain itu menjadi panduan bagi pemerintah dan pembentuk peraturan perundang-undangan dalam merumuskan sistem pengawasan dan regulasi yang lebih adaptif terhadap perkembangan teknologi *blockchain*, aset kripto dan transaksi keuangan digital.

Karakteristik hibah digital yang bersifat *pseudonim*, lintas yurisdiksi dan terdesentralisasi menyebabkan proses pengawasan dan pembuktian menjadi lebih kompleks dibandingkan transaksi keuangan konvensional.<sup>24</sup> Identitas para pihak dalam transaksi *blockchain* sering kali direpresentasikan melalui alamat kriptografis, sementara perpindahan aset digital dapat dilakukan secara langsung antar negara tanpa melalui lembaga keuangan tradisional, sehingga meningkatkan tantangan bagi otoritas perpajakan dan penegak hukum dalam melakukan identifikasi pihak terkait, penelusuran aliran dana serta pembuktian tindak pidana perpajakan dan pencucian uang.<sup>25</sup>

Penelitian ini merupakan penelitian hukum yuridis normatif. Analisis dilakukan melalui pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual*

<sup>19</sup> Yenti Garnasih. *Penegakan Hukum Tindak Pidana Pencucian Uang di Indonesia*. Jakarta: Kencana, 2016.

<sup>20</sup> Mentari Rizkika Maharani, Vira Wijaya, Carolina Isabela Sinawan, Aurnyanda Salsabila, dan Zenzai Ayu Alvina, "Keabsahan Akta Hibah yang Digunakan Wajib Pajak untuk Penghindaran Pajak," *Jurnal USM Law Review* 8, no. 1 (2025): 128–142

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

<sup>22</sup> Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020), 5–16

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

<sup>24</sup> Organisation for Economic Co-operation and Development (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

<sup>25</sup> Arindam Misra, *Tax Policy Handbook for Crypto Assets* (2024), 3–5

*approach*) dan pendekatan doktrinal dengan mengkaji peraturan perundang-undangan, asas hukum, doktrin, teori hukum serta literatur yang berkaitan dengan tindak pidana perpajakan, tindak pidana pencucian uang, hibah digital, aset kripto dan pembuktian elektronik.<sup>26</sup> Selain itu, penelitian mengkaji penerapan *Red Flag Theory* dan *Digital Forensic Investigation* dalam identifikasi serta pembuktian transaksi hibah digital yang diduga berasal dari tindak pidana perpajakan. Analisis dilakukan secara kualitatif menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*) untuk mengkaji karakteristik hibah digital, efektivitas penerapan *Red Flag Theory* dalam mendeteksi transaksi mencurigakan serta peran *Digital Forensic Investigation* dalam pembuktian tindak pidana perpajakan dan tindak pidana pencucian uang berdasarkan hukum positif Indonesia. Bersifat deskriptif-analitis, yaitu menguraikan ketentuan hukum yang relevan sekaligus menganalisis keterkaitan antara tindak pidana perpajakan, hibah digital, pencucian uang dan pembuktian digital. Data penelitian diperoleh dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang dikumpulkan melalui studi kepustakaan.<sup>27</sup>

## Pembahasan

### Karakteristik Hibah Digital Sebagai Modus Tindak Pidana Pencucian Uang Yang Berasal Dari Tindak Pidana Perpajakan.

Hibah menurut Pasal 1666 KUH Perdata merupakan perjanjian yang dilakukan oleh penghibah pada saat masih hidup untuk menyerahkan suatu benda atau hak secara cuma-cuma kepada penerima hibah dan pada prinsipnya tidak dapat ditarik kembali. Keabsahan hibah tidak hanya ditentukan oleh adanya kehendak para pihak, tetapi juga harus memenuhi syarat sah perjanjian sebagaimana diatur dalam Pasal 1320 KUH Perdata, objek hibah harus merupakan milik penghibah, serta adanya penerimaan oleh penerima hibah.<sup>28</sup> Seiring perkembangan teknologi digital, objek hibah tidak lagi terbatas pada aset konvensional, tetapi juga mencakup aset digital seperti *cryptocurrency* dan token digital yang memiliki nilai ekonomi yang dapat dialihkan.

Hibah digital merupakan pemberian aset atau nilai ekonomi yang dilakukan melalui sarana elektronik, termasuk aset kripto, token digital, dan aset digital lainnya yang dapat dimiliki, dialihkan, serta ditransaksikan secara digital melalui teknologi *blockchain* atau sistem terdistribusi sejenis.<sup>29</sup> Perkembangannya didukung oleh teknologi *blockchain*, *cryptocurrency*, *crowdfunding*, dan *decentralized finance (DeFi)*. *Blockchain* sebagai teknologi pencatatan terdistribusi menyediakan catatan transaksi yang transparan, permanen dan sulit dimanipulasi sedangkan *cryptocurrency* memungkinkan perpindahan nilai secara langsung tanpa perantara keuangan tradisional. Pengelolaan aset digital dilakukan melalui *digital wallet* yang menggunakan mekanisme kriptografi berupa *public key* dan *private key* untuk menerima, menyimpan dan mentransfer aset digital.<sup>30</sup>

Kombinasi teknologi tersebut menciptakan ekosistem baru yang memungkinkan pengalihan kekayaan dalam bentuk hibah digital. Di sisi lain, Karakteristik aset digital meningkatkan risiko tindak pidana perpajakan dan tindak pidana pencucian uang (TPPU). Dana

---

<sup>26</sup> Tunggal 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

<sup>27</sup> Kharisma Benuf dan Muhamad Azhar, "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Jurnal Gema Keadilan* 7, no. 1 (2020): 24–28

<sup>28</sup> M. Fadillah, "Kepastian Hukum Terhadap Tanah Hibah Tanpa Akta PPAT," *Jurnal Nalar* 2, no. 1 (2023): 51–53

<sup>29</sup> Organisation for Economic Co-operation and Development (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), 20

<sup>30</sup> Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020), 7–9.

yang berasal dari penggelapan pajak, pelaporan pajak yang tidak benar, menyembunyian penghasilan atau tindak pidana perpajakan lainnya dapat dikonversi menjadi aset kripto, dipindahkan melalui berbagai *wallet* dan jaringan *blockchain*, kemudian dialihkan kembali dalam bentuk transaksi yang tampak sah untuk menyamarkan asal-usul dana.<sup>31</sup> Dalam skema ini, hibah digital berpotensi digunakan sebagai sarana *layering* dan *integration* untuk menyamarkan asal-usul dana hasil kejahatan.

Indikasi penyalahgunaan hibah digital dapat diidentifikasi melalui berbagai *Red flag*, antara lain donor anonim, penggunaan banyak *wallet*, transaksi lintas yurisdiksi tanpa tujuan ekonomi yang jelas, pemanfaatan *privacy coin*, *mixer* atau *tumbler*, *platform decentralized finance (DeFi)*, serta nilai hibah yang tidak sebanding dengan profil ekonomi pihak yang terlibat. Karakteristik tersebut dapat mengindikasikan upaya menyembunyian identitas, penyamaran asal-usul dana dan pencucian uang yang berasal dari tindak pidana perpajakan.<sup>32</sup>

Risiko juga meningkat apabila tidak terdapat hubungan hukum, keluarga, sosial, atau bisnis yang dapat diverifikasi antara pemberi dan penerima hibah.<sup>33</sup> Untuk mengidentifikasi dan membuktikan penyalahgunaan tersebut, dipergunakan *Red Flag Theory* dan *Digital Forensic Investigation*. *Red Flag Theory* digunakan untuk mendeteksi pola transaksi yang mencurigakan, sedangkan *Digital Forensic Investigation* digunakan untuk melakukan *blockchain tracing*, *wallet attribution*, *transaction mapping* dan *beneficial ownership analysis*.<sup>34</sup> Melalui pendekatan tersebut, aliran dana digital dapat ditelusuri sehingga keterkaitannya dengan tindak pidana perpajakan dan TPPU dapat dibuktikan berdasarkan hukum positif Indonesia.

### Identifikasi Hibah Digital Melalui Pendekatan *Red Flag Theory*

Menurut Joseph T. Wells, teori *Red flag* menjelaskan bahwa suatu tindakan *fraud* atau tindak pidana umumnya meninggalkan indikator-indikator peringatan (*warning signs*) yang dapat digunakan untuk mengidentifikasi adanya risiko penyimpangan.<sup>35</sup> Teori ini berasumsi bahwa aktivitas ilegal cenderung menimbulkan anomali pada sumber dana, pola transaksi, profil pelaku serta hubungan antar pihak. *Red flag* bukan merupakan alat bukti, melainkan indikator risiko yang menjadi dasar untuk analisis dan investigasi lebih lanjut. Semakin banyak indikator yang ditemukan, semakin tinggi tingkat risiko suatu transaksi.

Dalam bidang perpajakan, teori ini membantu mengidentifikasi ketidaksesuaian antara profil ekonomi dan nilai transaksi,<sup>36</sup> penggunaan pihak ketiga, transaksi tanpa substansi ekonomi serta kepemilikan aset yang tidak dilaporkan.<sup>37</sup> Dalam rezim anti pencucian uang, indikator yang umum digunakan meliputi sumber dana yang tidak jelas, transaksi berlapis (*layering*), transfer lintas yurisdiksi, penggunaan rekening atau *wallet* anonim, serta peningkatan kekayaan yang tidak dapat dijelaskan secara wajar.<sup>38</sup>

---

<sup>31</sup> H. F. Atlam et al., "Blockchain Forensics: A Systematic Literature Review of Techniques, Tools, and Challenges," *Electronics* 13, no. 17 (2024): 10–15

<sup>32</sup> FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2024), 18–25

<sup>33</sup> Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, updated 2021), 54–58

<sup>34</sup> Organisation for Economic Co-operation and Development (OECD), *Fighting Tax Crime – The Ten Global Principles*, 2nd ed. (Paris: OECD Publishing, 2021), 83–87

<sup>35</sup> Joseph T. Wells, *Principles of Fraud Examination*, 5th ed. (Hoboken, NJ: John Wiley & Sons, 2017), 24–26.

<sup>36</sup> Yating Lin et al., "TaxThemis: Interactive Mining and Exploration of Suspicious Tax Evasion Group" (2020)

<sup>37</sup> Emre A. Akartuna, Michael Levi, dan Georgios A. Antonopoulos, "Money Laundering Typologies and Trends: A Typological Scoping Review of Money Laundering Methods," *Security Journal* 38 (2025): 1–31

<sup>38</sup> Willem Prasetyo, "The Nominee Scheme Through the Lens of Anti-Money Laundering Law" (2025)

Perkembangan *blockchain*, *cryptocurrency* dan keuangan digital melahirkan hibah digital sebagai bentuk baru transfer kekayaan yang memiliki risiko penyalahgunaan untuk pencucian uang yang berasal dari tindak pidana perpajakan. Karakteristiknya yang *pseudonim*, cepat dan lintas yurisdiksi<sup>39</sup> menuntut penerapan *Red Flag Theory* sebagai mekanisme deteksi dini untuk membedakan transaksi yang wajar dan berisiko tinggi.

Dalam penelitian ini, indikator risiko hibah digital dikelompokkan ke dalam empat kategori. Pertama, *source risk*, meliputi donor anonim, sumber dana tidak jelas, *wallet* berisiko tinggi dan dana yang berasal dari yurisdiksi berisiko. Kedua, *transaction risk*, seperti transfer lintas yurisdiksi, penggunaan banyak *wallet*, *private wallet*, *mixer*, *cross-chain transaction* dan pola *layering*. Ketiga, *beneficiary risk*, yaitu nilai hibah yang tidak sebanding dengan profil ekonomi penerima. Keempat, *relationship risk*, berupa tidak adanya hubungan atau dokumen pendukung yang dapat menjelaskan hubungan antara pemberi dan penerima hibah.<sup>40</sup>

Hasil identifikasi *Red flag* tersebut menjadi dasar pelaksanaan *Digital Forensic Investigation* untuk menelusuri aliran dana, mengungkap *beneficial owner* dan membuktikan keterkaitannya dengan tindak pidana perpajakan maupun tindak pidana pencucian uang. Berdasarkan kategori di atas, penelitian ini mengembangkan model penilaian risiko yang menggunakan pendekatan kumulatif.<sup>41</sup> Setiap indikator *Red flag* diberikan nilai tertentu berdasarkan tingkat risiko yang ditimbulkan. Semakin banyak indikator yang ditemukan dalam suatu transaksi hibah digital, semakin tinggi tingkat risiko transaksi tersebut.

**Tabel 1. Model Penilaian Risiko**

Jumlah <i>Red flag</i>	Tingkat Risiko
1–2 indikator	Risiko Rendah
3–4 indikator	Risiko Sedang
5–6 indikator	Risiko Tinggi
> 6 indikator	Risiko Sangat Tinggi

Sumber : Konstruksi Penulis berdasarkan pendekatan *Risk-Based Approach* FATF (2020, 2021, 2024).

Model ini tidak digunakan untuk menyatakan bahwa suatu transaksi merupakan tindak pidana, tetapi digunakan untuk menentukan prioritas investigasi. Matriks berikut menggambarkan indikator utama yang digunakan dalam penelitian ini:

**Tabel 2. Matriks Indikator *Red flag***

Kategori	Indikator <i>Red flag</i>
Source Risk	Donor anonim
Source Risk	Sumber dana tidak jelas
Source Risk	Dana berasal dari yurisdiksi berisiko
Transaction Risk	Transfer lintas yurisdiksi
Transaction Risk	Penggunaan <i>private wallet</i>
Transaction Risk	Penggunaan mixer atau tumbler
Transaction Risk	Layering yang kompleks
Transaction Risk	<i>Cross-chain transaction</i>
Beneficiary Risk	Nilai hibah tidak wajar
Beneficiary Risk	Profil ekonomi penerima tidak sesuai
Relationship Risk	Tidak ada hubungan hukum

<sup>39</sup> Hugo Almeida, Pedro Pinto, dan Ana Fernández Vilas, “A Review on Cryptocurrency Transaction Methods for Money Laundering” (2023)

<sup>40</sup> Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020), 9–24

<sup>41</sup> Financial Services Authority of Saint Vincent and the Grenadines, *Conducting AML/CFT/CPF Institutional Risk Assessments Guidelines* (2022)

Relationship Risk

Tidak ada dasar pemberian hibah

Sumber: Diolah oleh Penulis berdasarkan FATF (2020; 2021; 2024), OECD (2021), dan Atlam et al. (2024)

Matriks tersebut menjadi instrumen awal untuk mengidentifikasi transaksi hibah digital yang memerlukan investigasi lebih lanjut. Dalam konteks tindak pidana perpajakan, model *Red flag* hibah digital digunakan untuk mengidentifikasi kemungkinan bahwa dana yang diterima sebagai hibah sebenarnya berasal dari hasil pelanggaran perpajakan.

Sebagai contoh :

Seorang individu menerima hibah digital senilai Rp. 20 miliar dalam bentuk *cryptocurrency* dari donor yang tidak diketahui identitasnya. Dana tersebut berasal dari *private wallet*, sebelumnya melewati *mixer* dan ditransfer melalui beberapa negara. Selain itu, penerima tidak memiliki hubungan hukum dengan donor serta tidak dapat menjelaskan alasan penerimaan hibah.

Dalam contoh tersebut ditemukan beberapa *Red flag* sekaligus, yaitu:

1. Donor anonim;
2. Transfer lintas yurisdiksi;
3. Penggunaan *private wallet*;
4. Penggunaan *mixer*;
5. Nilai hibah tidak wajar;
6. Tidak adanya hubungan hukum; dan
7. Sumber dana tidak jelas.

Berdasarkan model yang dikembangkan, transaksi hibah digital yang memenuhi sejumlah indikator risiko dapat dikategorikan sebagai berisiko sangat tinggi dan menjadi prioritas investigasi. Penilaian dilakukan melalui tiga kelompok risiko utama, yaitu *Source Risk*, *Transaction Risk* dan *Beneficiary Risk*, yang dianalisis menggunakan pendekatan *Red Flag Theory*.<sup>42</sup>

*Source Risk* menilai transparansi identitas donor, *beneficial owner* dan asal-usul dana. Risiko meningkat apabila donor bersifat anonim, identitas tidak dapat diverifikasi, menggunakan banyak *wallet* atau memanfaatkan *platform* tanpa mekanisme *Know Your Customer* (KYC). Risiko juga muncul ketika pemilik manfaat sebenarnya tidak diketahui, melibatkan *nominee* atau perantara atau *beneficial owner* tersembunyi. Teori *Know Your Customer* (KYC) menekankan pentingnya proses identifikasi, verifikasi dan pemantauan berkelanjutan terhadap pihak yang melakukan transaksi guna memahami identitas, tujuan transaksi, sumber dana serta pihak penerima manfaat sebenarnya (*beneficial owner*).<sup>43</sup> perusahaan cangkang, serta ketika sumber dana tidak dapat dijelaskan, tidak sesuai dengan profil ekonomi donor atau berasal dari yurisdiksi berisiko tinggi. Semakin rendah transparansi sumber dana, semakin tinggi potensi keterkaitannya dengan tindak pidana perpajakan dan pencucian uang.

*Transaction Risk* berfokus pada pola dan mekanisme transaksi yang menunjukkan upaya penyamaran asal-usul dana. Indikator utamanya meliputi *blockchain layering*, *cross-chain transaction*, *high-frequency transfer* dan *structuring transaction*. Pola transaksi yang kompleks, berlapis dan tidak memiliki tujuan ekonomi yang jelas mengindikasikan kemungkinan adanya upaya pencucian uang melalui hibah digital.

Sementara itu, *Beneficiary Risk* menilai kewajaran profil ekonomi penerima, hubungan dengan donor dan tujuan hibah. Risiko meningkat apabila nilai hibah tidak sebanding dengan

<sup>42</sup> Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020), 7–24

<sup>43</sup> Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations)* (Paris: FATF, 2023), 59–66.

kondisi ekonomi penerima, tidak terdapat hubungan yang dapat diverifikasi antara para pihak atau tujuan hibah tidak didukung dokumen yang memadai.<sup>44</sup> Kondisi tersebut dapat mengindikasikan penggunaan *nominee* atau penyamaran kepemilikan aset.

Untuk mengukur tingkat risiko secara keseluruhan, penelitian ini menggunakan Matriks Risiko Hibah Digital sebagai instrumen *early warning system*. *Early Warning System* merupakan mekanisme deteksi dini yang menggunakan indikator-indikator risiko untuk mengidentifikasi potensi penyimpangan sebelum berkembang menjadi tindak pidana yang lebih kompleks<sup>45</sup>. Matriks ini membantu menentukan prioritas pemeriksaan dan menjadi dasar pelaksanaan *Digital Forensic Investigation* guna menelusuri aliran dana serta membuktikan keterkaitannya dengan tindak pidana perpajakan dan pencucian uang.

Penilaian risiko didasarkan pada tiga kelompok indikator utama. Pertama, *Source Risk* yang mencakup identitas donor, *beneficial owner* dan asal-usul dana. Kedua, *Transaction Risk* yang meliputi *blockchain layering*, *cross-chain transaction*, *high-frequency transfer*, dan *structuring transaction*. Ketiga, **Beneficiary Risk** yang mencakup profil ekonomi penerima, hubungan donor-penerima dan kesesuaian tujuan hibah. Semakin banyak indikator yang teridentifikasi, semakin tinggi risiko bahwa hibah digital digunakan sebagai sarana pencucian uang. Ditunjukkan sebagaimana tabel di bawah ini :

**Tabel 3. Matriks Indikator Risiko Hibah Digital**

Kategori Risiko	Indikator Red flag	Tingkat Risiko	Keterangan
Source Risk	Identitas donor tidak jelas	Tinggi	Penetapan tingkat risiko merupakan hasil penilaian penulis berdasarkan pendekatan Risk-Based Approach FATF dan sintesis indikator yang ditemukan dalam FATF (2020; 2021; 2024), OECD (2021), dan Atlam et al. (2024).
Source Risk	<i>Beneficial owner</i> tidak diketahui	Tinggi	
Source Risk	Asal-usul dana tidak dapat dijelaskan	Tinggi	
Transaction Risk	Layering <i>blockchain</i>	Tinggi	
Transaction Risk	<i>Cross-chain transaction</i>	Sedang-Tinggi	
Transaction Risk	High frequency transfer	Sedang	
Transaction Risk	Structuring transaction	Tinggi	
Beneficiary Risk	Profil ekonomi tidak sesuai	Tinggi	
Beneficiary Risk	Hubungan donor dan penerima tidak jelas	Tinggi	
Beneficiary Risk	Tujuan hibah tidak dapat diverifikasi	Sedang-Tinggi	

Sumber: Diolah oleh Penulis berdasarkan Financial Action Task Force (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (2020); FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021); FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (2024); OECD, *Fighting Tax Crime – The Ten Global Principles* (2021); dan Atlam et al. (2024).

<sup>44</sup> Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Recommendations)* (Paris: FATF, 2023), 61–66.

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

Berdasarkan matriks tersebut, setiap indikator dapat digunakan untuk mengukur tingkat risiko suatu transaksi hibah digital. Selain itu, untuk memberikan penilaian yang lebih objektif, setiap indikator diberikan bobot risiko sebagai berikut:

**Tabel 4. Sistem Skoring Risiko**

Tingkat Risiko	Skor	Penerapan skor terhadap indikator penelitian:	
		Indikator	Skor
Rendah	1	Identitas donor tidak jelas	3
Sedang	2	<i>Beneficial owner</i> tidak diketahui	3
Tinggi	3	Asal-usul dana tidak jelas	3
		<i>Layering blockchain</i>	3
		<i>Cross-chain transaction</i>	2
		<i>High frequency transfer</i>	2
		<i>Structuring transaction</i>	3
		Profil ekonomi tidak sesuai	3
		Hubungan donor dan penerima tidak jelas	3
		Tujuan hibah tidak dapat diverifikasi	2

Sumber: Konstruksi Penulis berdasarkan pendekatan *Risk-Based Approach* FATF (2020; 2021; 2024).

**Catatan:** Sistem skoring merupakan hasil pengembangan penulis berdasarkan pendekatan *Risk-Based Approach* FATF. Pembobotan diberikan dengan mempertimbangkan tingkat relevansi masing-masing indikator terhadap risiko tindak pidana pencucian uang yang berasal dari tindak pidana perpajakan melalui hibah digital.

Total skor maksimum adalah: **10 indikator × 3 = 30 poin**

Berdasarkan total skor yang diperoleh, transaksi hibah digital dapat diklasifikasikan ke dalam empat kategori risiko.

**Tabel 5. Klasifikasi Tingkat Risiko**

Total Skor	Tingkat Risiko
0 – 7	Risiko Rendah
8 – 15	Risiko Sedang
16 – 23	Risiko Tinggi
24 – 30	Risiko Sangat Tinggi

Sumber: Diolah oleh Penulis berdasarkan *Risk-Based Approach* Financial Action Task Force (FATF) dan Matriks Risiko Hibah Digital yang dikembangkan dalam penelitian ini.

**Catatan:** Klasifikasi tingkat risiko merupakan hasil pengembangan penulis berdasarkan total skor kumulatif dari indikator *Source Risk*, *Transaction Risk*, *Beneficiary Risk* dan *Relationship Risk*. Rentang skor ditetapkan untuk membedakan tingkat prioritas pengawasan dan investigasi berdasarkan pendekatan *Risk-Based Approach*.

**Tabel 6. Interpretasi klasifikasi**

No	Klasifikasi	Uraian
1	Risiko Rendah	Transaksi hanya menunjukkan sedikit indikator <i>Red flag</i> dan secara umum masih memiliki karakteristik yang wajar.
2	Risiko Sedang	Ditemukan beberapa indikator yang memerlukan verifikasi tambahan, namun belum cukup menunjukkan adanya indikasi kuat pencucian uang.
3	Risiko Tinggi	Ditemukan kombinasi indikator yang signifikan sehingga transaksi layak menjadi prioritas investigasi.
4	Risiko Sangat Tinggi	Ditemukan hampir seluruh indikator <i>Red flag</i> yang menunjukkan kemungkinan kuat bahwa hibah digital digunakan sebagai sarana penyamaran hasil tindak pidana perpajakan.

Sumber: Diolah oleh Penulis berdasarkan FATF (2020; 2021; 2024) dan OECD (2021)

Interpretasi klasifikasi risiko merupakan hasil pengembangan penulis berdasarkan jumlah dan tingkat signifikansi indikator *Red flag* yang teridentifikasi. Semakin banyak indikator risiko yang ditemukan dalam suatu transaksi, semakin tinggi prioritas verifikasi, investigasi dan *Digital Forensic Investigation* yang diperlukan. Sebagai contoh akan disimulasikan dalam penerapan Matriks Risiko sebagaimana di bawah ini :

**Tabel 7. Simulasi Penerapan Matriks Risiko.**

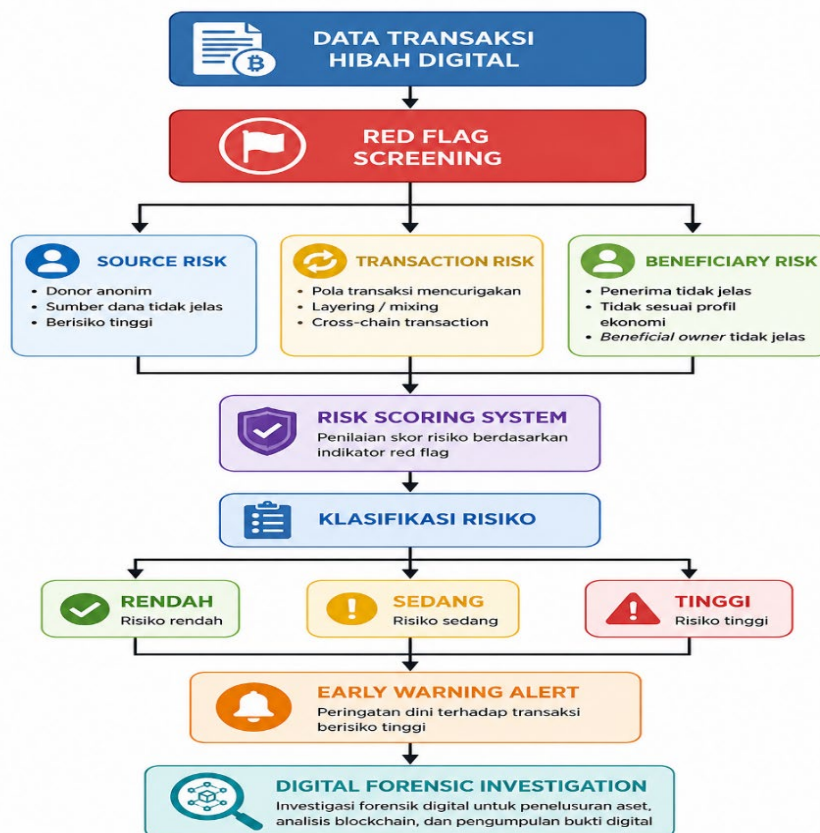
Sebagai ilustrasi, misalkan terdapat transaksi hibah digital dengan karakteristik sebagai berikut:	Skor yang diperoleh:	Indicator Score
1. Donor anonim	Identitas donor tidak jelas	3
2. <i>Beneficial owner</i> tidak diketahui.	<i>Beneficial owner</i> tidak diketahui	3
3. Dana berasal dari wallet yang tidak dapat dijelaskan sumbernya.	Asal-usul dana tidak jelas	3
4. Dana melewati beberapa wallet ( <i>layering</i> ).	<i>Layering blockchain</i>	3
5. Dana berpindah antar <i>blockchain</i>	<i>Cross-chain transaction</i>	2
6. Dana berpindah antar <i>blockchain</i> .	Profil ekonomi tidak sesuai	3
7. Tidak terdapat hubungan hukum antara donor dan penerima	Hubungan donor dan penerima tidak jelas	3
<b>Total Score</b>		<b>20</b>

Sumber: Simulasi Penulis berdasarkan Matriks Risiko Hibah Digital yang dikembangkan dari FATF (2020; 2021; 2024), OECD (2021), dan Atlam et al. (2024).

Catatan: Kasus pada tabel ini merupakan simulasi hipotetis yang digunakan untuk menguji penerapan Matriks Risiko Hibah Digital. Total skor diperoleh dari penjumlahan bobot masing-masing indikator berdasarkan sistem skoring yang dikembangkan dalam penelitian ini.

Berdasarkan matriks risiko, skor 20 termasuk dalam kategori **Risiko Tinggi**, sehingga transaksi tersebut layak menjadi objek *Digital Forensic Investigation*. Hasil penelitian menunjukkan bahwa risiko hibah digital tidak dapat dinilai berdasarkan satu indikator, melainkan melalui kombinasi berbagai *Red flag* yang saling berkaitan. Semakin banyak indikator yang teridentifikasi, semakin tinggi kemungkinan transaksi tersebut terkait dengan tindak pidana pencucian uang yang berasal dari tindak pidana perpajakan. Untuk mendukung deteksi dini, penelitian ini mengembangkan Matriks Risiko Hibah Digital sebagai instrumen penilaian yang sistematis dalam mengidentifikasi, mengklasifikasikan dan memprioritaskan transaksi berisiko tinggi. Model ini diintegrasikan ke dalam *Early Warning System* (EWS) yang menggabungkan *Red Flag Theory*, *Risk-Based Approach* dan *Digital Financial Crime Detection*.

Penerapan EWS dilakukan melalui dua tahap, yaitu pengumpulan data transaksi hibah digital dan *Red flag screening*. Analisis difokuskan pada *Source Risk*, *Transaction Risk*, dan *Beneficiary Risk* yang dinilai menggunakan sistem skor risiko. Hasil penilaian tersebut menjadi dasar penentuan prioritas pemeriksaan serta pelaksanaan *Digital Forensic Investigation* untuk menelusuri aliran dana dan mengungkap indikasi pencucian uang berbasis hibah digital. Tahap ketiga adalah *Risk Scoring and Classification* di mana Setelah proses screening dilakukan, sistem menghitung total skor risiko yang diperoleh. Tahap akhir EWS adalah menghasilkan peringatan berdasarkan tingkat risiko transaksi hibah digital. Peringatan diklasifikasikan menjadi *Green*, *Yellow*, *Orange* dan *Red Alert*. Semakin tinggi tingkat risiko, semakin besar kebutuhan verifikasi, analisis lanjutan, hingga *Digital Forensic Investigation* sebagai dasar penanganan berbasis risiko. Model operasional dapat digambarkan sebagai berikut:



**Gambar 1. Model Konseptual Diagram alur risiko transaksi digital yang Dikembangkan Penulis**

Sumber: Diolah oleh Penulis berdasarkan FATF (2020; 2021; 2024), OECD (2021), dan Atlam et al. (2024)

Penelitian ini menunjukkan bahwa *Digital Forensic Investigation* dilakukan setelah transaksi hibah digital mencapai tingkat risiko tertentu berdasarkan hasil identifikasi *Red flag*. Untuk mendukung proses tersebut, dikembangkan model *Early Warning System* (EWS) yang mengintegrasikan *Red Flag Theory* dan *risk-based approach* melalui tiga parameter utama: *Source Risk*, *Transaction Risk*, dan *Beneficiary Risk*.

Hasil penelitian menunjukkan bahwa semakin banyak indikator risiko yang muncul secara bersamaan, semakin tinggi potensi keterkaitan transaksi dengan pencucian uang yang berasal dari tindak pidana perpajakan. Melalui Matriks Risiko Hibah Digital dan EWS, transaksi dapat diklasifikasikan berdasarkan tingkat risikonya sehingga mendukung deteksi dini, pengawasan perpajakan, serta penentuan prioritas investigasi secara lebih sistematis dan efektif.

### **Digital Forensic Investigation Dalam Pembuktian Hibah Digital**

*Digital Forensic Investigation* merupakan metode ilmiah untuk mengidentifikasi, mengumpulkan, memelihara, menganalisis, dan menyajikan bukti digital guna mendukung proses penyelidikan, penyidikan dan pembuktian hukum. Menurut Eoghan Casey, *Digital Forensic Investigation* merupakan proses ilmiah yang dilakukan untuk mengidentifikasi, mengamankan, mengumpulkan, memeriksa, menganalisis dan menyajikan bukti digital guna merekonstruksi suatu peristiwa yang relevan secara hukum. Melalui pendekatan ini, jejak transaksi elektronik, aset kripto, dompet digital, metadata transaksi dan hubungan antar pihak dapat ditelusuri sehingga memungkinkan pengungkapan skema pencucian uang yang dilakukan melalui hibah digital.<sup>46</sup> Dalam kejahatan keuangan, pendekatan ini tidak hanya berfungsi menemukan bukti elektronik, tetapi juga menelusuri aliran dana, mengidentifikasi pelaku dan *beneficial owner*, serta menghubungkan transaksi digital dengan tindak pidana yang mendasarinya.

Pelaksanaannya mencakup tahapan identifikasi, pengumpulan, preservasi, pemeriksaan, analisis dan pelaporan dengan memperhatikan prinsip legalitas, integritas, akuntabilitas dan *chain of custody*. *Blockchain Forensics*, yaitu metode khusus yang memanfaatkan sifat *blockchain* yang transparan, permanen, dan dapat ditelusuri untuk mendukung investigasi aset digital. Dalam penelitian ini, *Blockchain Forensics* digunakan untuk memverifikasi indikator *Red flag*, menelusuri sumber dana, mengidentifikasi donor dan *beneficial owner*, serta mengungkap keterkaitan hibah digital dengan tindak pidana perpajakan dan pencucian uang. Teknik yang digunakan meliputi *blockchain transaction tracing*, *wallet attribution analysis*, *cluster analysis*, *transaction mapping*, dan *flow of funds analysis*.

*Blockchain transaction tracing* berfungsi merekonstruksi aliran aset digital dari sumber hingga tujuan akhir melalui analisis riwayat transaksi, hubungan antar *wallet* dan pola perpindahan dana. Sementara itu, *wallet attribution analysis* digunakan untuk menghubungkan alamat *wallet* dengan individu atau entitas tertentu melalui data *blockchain*, KYC, OSINT (Open Source Intelligence),<sup>47</sup> maupun informasi perangkat elektronik. Kedua metode tersebut membantu mengungkap donor anonim, sumber dana yang tidak jelas, pola *layering*, serta hubungan tersembunyi antar pihak. Analisis juga diperkuat melalui *cluster analysis* dan *transaction mapping* yang mampu mengidentifikasi jaringan transaksi, pola *fan-in*, *fan-out*, *circular transaction*, serta struktur pencucian uang yang melibatkan banyak *wallet*. Selain itu, *cryptocurrency exchange analysis* digunakan untuk menghubungkan aktivitas *blockchain* dengan data pengguna pada platform aset kripto guna mengidentifikasi pemilik akun dan asal-usul dana.

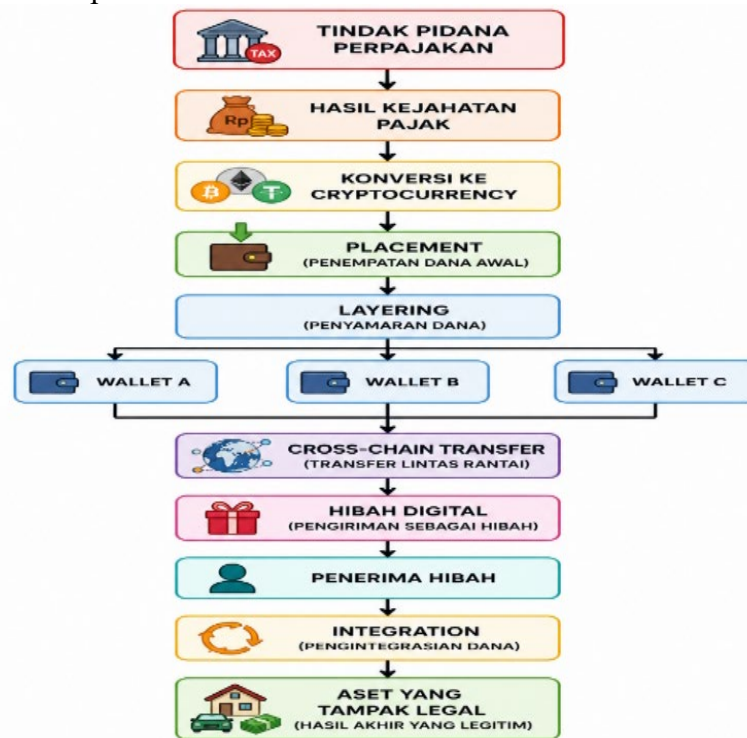
---

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

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

Untuk mengungkap pihak yang sebenarnya mengendalikan aset, digunakan *beneficial ownership investigation*. Cassara melalui pendekatan **Follow the Money** menjelaskan bahwa investigasi kejahatan keuangan harus menelusuri siapa pihak yang menikmati manfaat ekonomi sebenarnya (*ultimate beneficiary*) dari suatu transaksi atau struktur korporasi<sup>48</sup> serta menurut Madinger menekankan bahwa investigasi AML harus mampu mengidentifikasi individu yang berada di balik nominee, perusahaan cangkang, trust atau struktur kepemilikan kompleks yang digunakan untuk menyamarkan hasil kejahatan.<sup>49</sup> Seluruh temuan kemudian dikorelasikan dengan data perpajakan guna membuktikan hubungan antara aset digital, hibah digital dan tindak pidana perpajakan sebagai *predicate crime*.

Hasil penelitian menunjukkan bahwa pembuktian yang efektif tidak hanya bergantung pada bukti *blockchain* tetapi juga pada kemampuan mengaitkan bukti digital dengan data perpajakan dan keuangan. Rekonstruksi aliran dana hibah digital menjadi instrumen utama untuk mengungkap sumber dana, pola penyamaran, serta keterkaitannya dengan tindak pidana perpajakan dan pencucian uang. Dalam penelitian ini, aliran dana hibah digital dapat direkonstruksi melalui tahapan berikut:



**Gambar 2. Model Konseptual Alur proses pencucian uang digital yang Dikembangkan Penulis**

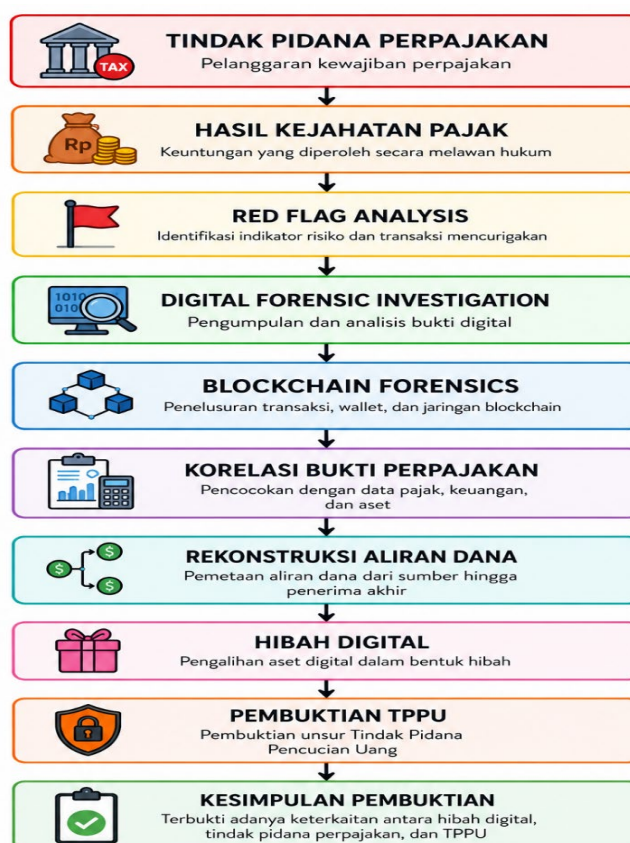
Sumber: Diolah oleh Penulis berdasarkan FATF (2020; 2021; 2024), OECD (2021), dan Atlam et al. (2024)

Model tersebut menunjukkan bagaimana hibah digital dapat digunakan sebagai sarana integrasi hasil tindak pidana perpajakan ke dalam sistem ekonomi yang tampak sah. Penelitian ini merekonstruksi aliran dana melalui integrasi berbagai metode *Digital Forensic Investigation*, seperti *Blockchain Transaction Tracing*, *Wallet Attribution Analysis*, *Cluster Analysis*, *Transaction Mapping*, *Cryptocurrency Exchange Analysis* dan *Beneficial ownership Investigation*.

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

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

Pendekatan tersebut digunakan untuk menelusuri aset digital, mengidentifikasi pihak terkait serta mengungkap *beneficial owner*. Dalam konteks tindak pidana perpajakan dan TPPU, metode ini membantu membuktikan penghasilan yang tidak dilaporkan, aset yang disembunyikan, serta tahapan *placement*, *layering* dan *integration*.<sup>50</sup> Hasilnya menjadi dasar pembuktian keterkaitan hibah digital dengan skema pencucian uang yang berasal dari tindak pidana perpajakan. Model pembuktian yang dikembangkan dalam penelitian ini dapat digambarkan sebagai berikut:



L  
**Gambar 3. Model Konseptual Alur proses tindak pidana perpajakan yang Dikembangkan Penulis**

Sumber: Model Konseptual yang Dikembangkan Penulis berdasarkan *Red Flag Theory*, *Digital Forensic Investigation*, *Blockchain Forensics*, dan Kerangka Pembuktian TPPU

Model Pembuktian Hibah Digital merupakan hasil sintesis penulis yang mengintegrasikan *Red Flag Theory* sebagai mekanisme identifikasi risiko, *Digital Forensic Investigation* dan *Blockchain Forensics* sebagai metode pengumpulan dan analisis bukti digital, serta korelasi dengan data perpajakan untuk membuktikan tindak pidana perpajakan sebagai *predicate crime* dalam tindak pidana pencucian uang

Penelitian ini menunjukkan bahwa pembuktian hibah digital dilakukan melalui rangkaian proses yang saling terhubung, mulai dari identifikasi *Red flag*, analisis forensik digital, hingga rekonstruksi aliran dana. Pendekatan ini mengintegrasikan bukti digital dan data perpajakan dengan menitikberatkan pada substansi ekonomi transaksi. *Blockchain* menyediakan jejak transaksi yang permanen dan dapat ditelusuri, sementara *Blockchain Transaction Tracing*, *Wallet Attribution Analysis*, *Cluster Analysis* dan *Transaction Mapping* efektif mengungkap

<sup>50</sup> Financial Action Task Force, *Guidance on Beneficial Ownership of Legal Persons* (Paris: FATF, 2023), 7–14; Financial Action Task Force, *Mutual Evaluation Report of Indonesia* (Paris: FATF, 2023)

aliran dana, *beneficial owner* serta pola *layering*. Data KYC dari *cryptocurrency exchange* turut membantu menghubungkan identitas digital dengan identitas hukum.

Selain itu korelasi antara bukti digital dan data perpajakan merupakan kunci pembuktian tindak pidana perpajakan sebagai *predicate crime* dalam skema TPPU berbasis aset digital. Pasal 69 Undang-Undang Nomor 8 Tahun 2010 menegaskan bahwa penyidikan, penuntutan dan pemeriksaan tindak pidana pencucian uang tidak mensyaratkan pembuktian terlebih dahulu terhadap tindak pidana asal.<sup>51</sup> Penguatan pengawasan transaksi hibah digital menjadi semakin relevan dalam era Coretax DJP yang mengedepankan integrasi data, digitalisasi administrasi perpajakan, dan pengawasan berbasis risiko.

## Kesimpulan

Penelitian ini menyimpulkan bahwa hibah digital merupakan mekanisme berisiko tinggi yang berpotensi disalahgunakan sebagai sarana tindak pidana pencucian uang yang berasal dari tindak pidana perpajakan. Risiko tersebut dipengaruhi oleh karakteristik teknologi *blockchain* yang bersifat *pseudonym*, lintas yurisdiksi serta masih terbatasnya pengawasan dan regulasi yang mengaturnya. Hasil penelitian menunjukkan bahwa *Red Flag Theory* dapat digunakan sebagai kerangka yang efektif untuk mendeteksi indikasi penyalahgunaan hibah digital melalui identifikasi indikator *Source Risk*, *Transaction Risk* dan *Beneficiary Risk*. Indikator tersebut selanjutnya dapat diintegrasikan ke dalam *Model Red Flag Hibah Digital*, Matriks Risiko, dan *Early Warning System* (EWS) guna memperkuat mekanisme deteksi dan pengawasan berbasis risiko. Selain itu, *Digital Forensic Investigation* memiliki peran penting dalam mengubah indikator risiko menjadi alat bukti melalui penerapan *Blockchain Forensics*, penelusuran transaksi, identifikasi *beneficial owner* dan rekonstruksi aliran dana. Integrasi kedua pendekatan tersebut menghasilkan Model Pembuktian Hibah Digital yang memberikan kerangka komprehensif untuk membuktikan keterkaitan antara hibah digital, tindak pidana perpajakan dan tindak pidana pencucian uang.

Dari sisi kebijakan, pemerintah perlu membentuk regulasi khusus mengenai hibah digital yang mengatur kewajiban pelaporan, transparansi sumber dana serta pengungkapan *beneficial ownership*.

## Daftar Pustaka

- 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.

---

<sup>51</sup> F. Yurendo, Santrawan T. Paparang, dan A. Fitriani, "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

- 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. Fitriani. “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.