ISSN Print 2615-5648
ISSN Online 2615-174X

Volksgeist

Editorial Office: Faculty of Sharia, Universitas Islam Negeri Profesor Kiai Haji Saifuddin Zuhri Purwokerto, Indonesia, Jalan Jend. A. Yani No. 40 A Purwokerto Jawa Tengah 531226 Indonesia
Phone: +62281-635624 Fax: +62281- 636653
E-mail: volksgeist@uinsaizu.ac.id
Website: http://ejournal.uinsaizu.ac.id/index.php/volksgeist

Discourse Using Blockchain Technology for the Enforcement of Money Laundering Crimes in Indonesia

Article

Author
Chairul Huda[1*], Puan Dinaphia Yunan[1], Zulhilmi Bin Paidi[2].

[1] Faculty of Law, Universitas Muhammadiyah Jakarta, Indonesia
[2] Universiti Utara Malaysia, Malaysia

Corresponding Author:
[*] Chairul Huda, *Email: chairulhuda448@gmail.com*

Data:
Received: Mar 29, 2025;
Accepted: Des 04, 2025
Published: Des 10, 2025

DOI:
10.24090/volksgeist.v8i2.13376

Abstract

Money laundering is a crime aimed at concealing the origin of funds derived from illegal activities, which has become increasingly difficult to detect with the growth of digital transactions and cryptocurrency use. Blockchain, as a distributed ledger technology, can record transactions permanently, transparently, and securely, making it a promising tool to support Anti-Money Laundering (AML) systems. This study examines the role of blockchain in strengthening Indonesia's AML framework amid rapid growth in digital financial transactions and increasing complexity of money laundering methods. The significant rise in suspicious transaction reports, particularly through digital wallets, e-money, and cryptocurrencies, indicates a shift of money laundering practices to digital channels that challenge existing oversight and law enforcement mechanisms. The study employs a qualitative approach through literature review and secondary data analysis to assess how blockchain features such as immutability, transparency, transaction pattern analysis, and cross-border tracking can enhance detection and verification of suspicious fund flows. The results suggest that blockchain has the potential to strengthen KYC procedures, enhance forensic capabilities, and provide verifiable electronic evidence. Nevertheless, regulatory and institutional limitations remain. OJK Regulation No. 27 of 2024 does not yet incorporate blockchain analytics, regulate privacy coins, mixers, or cross-chain laundering, nor provide a technology-based supervisory framework. Challenges also exist in evidentiary standards, digital chain-of-custody mechanisms, and technical capacity of law enforcement. Effective implementation of blockchain in Indonesia's AML system requires regulatory refinement, institutional strengthening, and alignment with FATF standards.

Keywords: *Blockchain; money laundering; law enforcement; digital financial system.*

INTRODUCTION

Money laundering is a criminal act aimed at concealing or obscuring the origin of money obtained through illegal activities.[1] The primary goal of money laundering is to transform funds derived from illicit activities into money that appears legitimate and lawful. This practice is often conducted in a highly covert manner, making it extremely difficult for law enforcement agencies in many countries to detect and identify suspicious transactions.[2] Furthermore, laundered money is frequently used in various legitimate economic activities, further complicating efforts to detect and combat crime. The phenomenon of money laundering not only harms individuals or specific groups but also poses a threat to the global economy as a whole. Successful money laundering can obstruct law enforcement efforts and provide criminals with access to financial resources they would otherwise be unable to enjoy.[3] Money laundering is undoubtedly a threat to global security.[4] Financial institutions face significant difficulties in combating money laundering practices.[5]

As technology advances, the identification of money laundering practices must also be continuously updated to keep pace with the new methods employed by criminals. One technology that shows significant potential in addressing this issue is blockchain technology.[6] Initially known as the underlying technology for cryptocurrency, blockchain has evolved over time and is now being utilized across various sectors, including the analysis and tracking of financial transactions. One of the reasons blockchain is used to identify money laundering is that financial transactions, including money laundering activities, are often carried out through banking systems.[7] Blockchain can help enhance the ability to analyze and identify financial transactions, including the flow of funds that may be linked to money laundering practices.

Blockchain is a technology designed to record every transaction transparently and securely.[8] Each transaction recorded in the blockchain is permanent and cannot be altered, and it is timestamped with a clear record of time. This feature makes blockchain an extremely effective tool for enhancing transparency in financial transaction systems. When a transaction is recorded in the blockchain, the

---

1 Benjámin Villányi, "Money Laundering: History, Regulations, and Techniques," *Oxford Research Encyclopedia of Criminology*, April 26, 2021, https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-708.

2 Ehi Eric Esoimeme, "Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules," *Journal of Money Laundering Control* 24, no. 1 (2021): 201–12, https://doi.org/10.1108/JMLC-05-2020-0053.

3 Ammar Oad et al., "Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection," *Electronics* 10, no. 15 (2021): 1766, https://doi.org/10.3390/electronics10151766.

4 Milind Tiwari, Jamie Ferrill, Adrian Gepp, and Kuldeep Kumar, "Factors Influencing the Choice of Technique to Launder Funds: The APPT Framework," *Journal of Economic Criminology* 1 (September 2023): 1, https://doi.org/10.1016/j.jeconc.2023.100006.

5 Berkan Oztas, Deniz Cetinkaya, Festus Adedoyin, Marcin Budka, Gokhan Aksu, and Huseyin Dogan, "Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry," *Future Generation Computer Systems* 159 (October 2024): 161, https://doi.org/10.1016/j.future.2024.05.027.

6 Yan Zhang and Peter Trubey, "Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection," *Computational Economics* 54, no. 3 (2019): 1043–63, https://doi.org/10.1007/s10614-018-9864-z.

7 Christoph Wronka, "'Cyber-Laundering': The Change of Money Laundering in the Digital Age," *Journal of Money Laundering Control* 25, no. 2 (2022): 330–44, https://doi.org/10.1108/JMLC-04-2021-0035; Danda B. Rawat et al., "Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems," *Journal of Cybersecurity and Privacy* 1, no. 1 (2020): 4–18, https://doi.org/10.3390/jcp1010002.

8 Sandeep Kumar Panda and Suresh Chandra Satapathy, "Drug Traceability and Transparency in Medical Supply Chain Using Blockchain for Easing the Process and Creating Trust between Stakeholders and Consumers," *Personal and Ubiquitous Computing* 28, no. 1 (2024): 75–91, https://doi.org/10.1007/s00779-021-01588-3.

information can be accessed by various parties with no opportunity to manipulate or alter the data. With the ability to permanently record transactions that can be verified by all parties, blockchain can help create a more trustworthy transaction ecosystem that is harder to manipulate.

Several previous studies have also highlighted the great potential of blockchain in the identification and verification of financial transactions. For example, Thommandru & Chakka (2023) suggested that the use of blockchain in financial institutions is an ideal platform to provide user identification and verification solutions.[9] They emphasized that with blockchain, transaction data can be easily accessed and verified, providing greater transparency in the money transfer process. Another study by Bjelajac & Momcilo (2022) demonstrated that the use of blockchain technology, particularly through Bitcoin, has assisted law enforcement in apprehending criminals, such as drug dealers and child pornography traffickers, even though the transactions are anonymous.[10] This indicates that blockchain has immense potential in supporting efforts to detect and combat crime, including money laundering.

Blockchain is relevant in Indonesia due to its transparent, distributed, and tamper-resistant nature, which supports improved data governance and transaction monitoring effectiveness. Bank Indonesia emphasizes that distributed ledger technology has the potential to strengthen the reliability of the national payment system and expand the reach of financial services.[11] OJK also places blockchain as the foundation for the development of the digital asset ecosystem, especially in consumer protection and strengthening supervision.[12]

Globally, money laundering patterns using cryptocurrency show an upward trend, especially through mixers, P2P services, and decentralized platforms that make it difficult to track assets. The Chainalysis Crypto Crime Report 2024 notes that cross-chain layering techniques and the use of anonymization protocols have increased significantly. This makes crypto assets a strategic tool for international criminal).[13]

A number of countries have integrated blockchain technology into strengthening their Anti-Money Laundering (AML) regimes. South Korea requires VASPs to verify identities and report transactions based on the Virtual Asset User Protection Act.[14] Singapore enforces strict oversight of Travel Rule implementation through the MAS regulatory framework.[15] The United States, through FinCEN, requires the collection and transmission of sender and recipient information in accordance

---

[9] Abhishek Thommandru and Dr Benarji Chakka, "Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks," *Sustainable Futures* 5 (December 2023): 100107, https://doi.org/10.1016/j.sftr.2023.100107.

[10] Željko Bjelajac and Momčilo Bajac, "Blockchain Technology and Money Laundering," *Law Theory & Prac.* 39, no. 2 (2022): 21–38, https://doi.org/10.5937/ptp2202021B.\\uc0\\u8220{}Blockchain Technology and Money Laundering,\\uc0\\u8221{} {\\i{}Law Theory & Prac.} 39, no. 2 (2022

[11] Bank Indonesia, *Blueprint Sistem Pembayaran Indonesia 2025* (Jakarta: Bank Indonesia, 2020), 17.

[12] Otoritas Jasa Keuangan, *Peta Jalan Pengembangan Inovasi Teknologi Sektor Jasa Keuangan 2023–2028* (Jakarta: OJK, 2023), 9.

[13] Chainalysis, *Crypto Crime Report 2024* (New York: Chainalysis Inc., 2024): 22-25, https://www.chainalysis.com/reports/crypto-crime-2024.

[14] Financial Services Commission Korea, *Virtual Asset User Protection Act: Enforcement Decree* (Seoul: FSC Korea, 2023), 4.

[15] Monetary Authority of Singapore, *Guidelines on Provision of Digital Payment Token Services to the Public* (Singapore: MAS, 2021), 12.

with BSA/Travel Rule regulations.[16] The European Union has reinforced similar provisions through Regulation (EU) 2023/1113 and EBA technical guidelines.[17]

The Financial Action Task Force (FATF) is the leading authority setting standards in the field of anti-money laundering and countering the financing of terrorism. However, it is important to note the potential for unintended negative impacts resulting from the expansion of FATF standards.[18] FATF expanded Recommendation 16 on virtual assets through the Travel Rule, which requires the provision of sender and recipient information in every cross-border transfer. However, many developing countries are not yet ready due to limitations in digital identity systems, interoperability costs, and weak supervisory capacity. The FATF emphasized that these challenges hinder compliance and increase the risk of cross-border criminal abuse of virtual assets.[19]

In Indonesia, a permanent member of the Financial Action Task Force (FATF), the development and innovation of the Anti-Money Laundering (AML) system is crucial. Indonesia is expected to continuously enhance its capabilities and trust in efforts to combat money laundering and terrorist financing. A report from the Financial Transaction Reports and Analysis Center (PPATK) in 2024 revealed that the rapid growth of online-based transactions poses a serious threat to the existing AML system. Official data from PPATK compiled through the One Data Indonesia Portal shows that the number of Suspicious Financial Transaction Reports (LTKM) has increased significantly in the last five years. In 2020, there were 68,057 reports, increasing to 82,184 reports in 2021, then increasing to 94,801 reports in 2022.[20] This number rose sharply in 2023 with a total of 183,801 reports, although it declined again to 141,312 reports in 2024 based on monthly data compilation.[21]

According to PPATK, the higher the proportion of Money Laundering Crimes (TPPU) that use digital channels, especially e-wallets and electronic money. PPATK data quoted by the media shows that as of May 2024, there were 6,581 LKTM reports related to e-wallets / e-money, with a total of 1,571,485 suspicious transactions.[22] This suspicious transaction figure has increased dramatically compared to the January–May 2023 period, which only saw 325,563 transactions, an increase of around 380%.[23] In addition, compared to the January–May 2022 period, which only recorded 106,652 suspicious transactions, the growth in suspicious digital transactions has increased by

---

16 Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (Washington, DC: U.S. Department of the Treasury, 2019), 7.

17 European Banking Authority, *Guidelines on the Travel Rule under Regulation (EU) 2023/1113* (Paris: EBA, 2024), 10–11.

18 Georgios Pavlidis, "The Dark Side of Anti-Money Laundering: Mitigating the Unintended Consequences of FATF Standards," *Journal of Economic Criminology* 2 (December 2023): 1, https://doi.org/10.1016/j.jeconc.2023.100040.

19 Financial Action Task Force (FATF), *Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 28 October 2021), Annex A (interpretive note on Recommendation 15), 5-6, https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

20 Portal Data Indonesia, "Jumlah Laporan Transaksi Keuangan Mencurigakan (LTKM) Tahun 2019–2022," diakses dari Portal Data Indonesia, https://data.go.id/dataset/dataset/jumlah-laporan-transaksi-keuangan-mencurigakan-ltkm-tahun-2019-2022.

21 Portal Data Indonesia, "Jumlah Laporan Transaksi Keuangan Mencurigakan (LTKM) per Bulan Tahun 2024," diakses dari Portal Data Indonesia, https://data.go.id/dataset/dataset/jumlah-laporan-transaksi-keuangan-mencurigakan-ltkm-per-bulan-tahun-2024.

22 Edi Suwiknyo, "Bank Swasta hingga Dompet Digital Rawan Pencucian Uang, Judi & Penipuan Dominan," Bisnis.com, 24 Juni 2024, https://kabar24.bisnis.com/read/20240624/16/1776360/bank-swasta-hingga-dompet-digital-rawan-pencucian-uang-judi-penipuan-dominan.

23 *Ibid*.

more than 1,373%.[24] This surge reinforces PPATK's claim that financial digitization opens up new opportunities for money laundering, as digital channels have now become one of the dominant routes used by financial criminals.[25]

Based on this data, a better information system supported by robust technology is needed.[26] In this context, blockchain could serve as a solution to improve the efficiency and effectiveness of monitoring and analyzing financial transactions that may be linked to money laundering. However, despite blockchain technology proving effective in various applications, the limitations of its implementation in Indonesia need to be considered. One of the primary limitations is the low level of understanding and adoption of blockchain technology among the public, including within the banking and financial sectors.[27] Furthermore, while blockchain offers better transparency, challenges related to regulation and oversight remain obstacles that need to be addressed. Research discussing the application of blockchain technology in the legal context in Indonesia, particularly in strengthening the anti-money laundering system, is still limited. Therefore, this study aims to fill the gap in literature and make an important contribution to the development of blockchain technology within Indonesia's legal system.

The importance of problem identification and the objectives of this research cannot be overlooked. The problem identification in this study serves as a crucial first step in exploring the underlying issues within the existing system for combating money laundering, and how blockchain technology can be utilized to address these issues. This study aims to analyze the potential application of blockchain technology in strengthening the anti-money laundering system in Indonesia, particularly in terms of transaction transparency and enhanced detection capabilities for suspicious fund flows. By identifying and understanding these issues, it is hoped that this research will contribute significantly to reinforcing Indonesia's legal infrastructure, enhancing global trust in the Indonesian legal system, and ultimately impacting economic growth and social welfare.

Although several studies in Indonesia have examined the use of cryptocurrency in money laundering crimes, most are normative in nature and focus on general regulatory aspects without specifically analyzing how blockchain data can be used as evidence in criminal proceedings.[28] Research by Gayung Utama and Pudji Astuti (2022) analyzes the criminalization of Bitcoin as a means of money laundering from a legal perspective and identifies normative requirements that are not yet sufficient to prosecute perpetrators.[29] Subsequently, research by Musfiratul Ilmi and

[24] Harian Jogja, "Transaksi E-Money dan E-Wallet Kini Jadi Modus Baru Pencucian Uang," 24 Juni 2024, https://ekbis.harianjogja.com/read/2024/06/24/502/1179029/transaksi-e-money-dan-e-wallet-kini-jadi-modus-baru-pencucian-uang.

[25] Dany Saputra, "PPATK Endus Modus Baru Pencucian Uang, Ada e-Wallet hingga Bitcoin Cs," Bisnis.com, 26 Juni 2024, https://kabar24.bisnis.com/read/20240626/16/1777366/ppatk-endus-modus-baru-pencucian-uang-ada-e-wallet-hingga-bitcoin-cs.

[26] Pusat Pelaporan dan Analisis Transaksi Keuangan, "Laporan Tahunan PPATK Tahun 2024," Pusat Pelaporan dan Analisis Transaksi Keuangan, 2024, https://www.ppatk.go.id/publikasi/read/255/laporan-tahunan-ppatk-tahun-2024.html.

[27] Nripendra P. Rana et al., "Analysis of Challenges for Blockchain Adoption within the Indian Public Sector: An Interpretive Structural Modelling Approach," *Information Technology & People* 35, no. 2 (2022): 548–76, https://doi.org/10.1108/ITP-07-2020-0460.

[28] Nadia Wulandari Rotty, Anggita Cahyani, Daffa Khalisha Nabila, Rachmah Fidiastuti, and Regentio Candrika Komala Dewa, "Pemanfaatan Cryptocurrency dalam Tindak Pidana Pencucian Uang," *Jurnal Hukum Statuta* 1, no. 2 (2022): 142, https://doi.org/10.35586/jhs.v1i2.8588.

[29] Gayung Utami and Pudji Astuti, "Analisis Yuridis Penggunaan Cryptocurrency (Bitcoin) sebagai Sarana Tindak Pidana Pencucian Uang," *Novum: Jurnal Hukum* 10, no. 01 (2023): 150, https://doi.org/10.2674/novum.v0i0.50069.

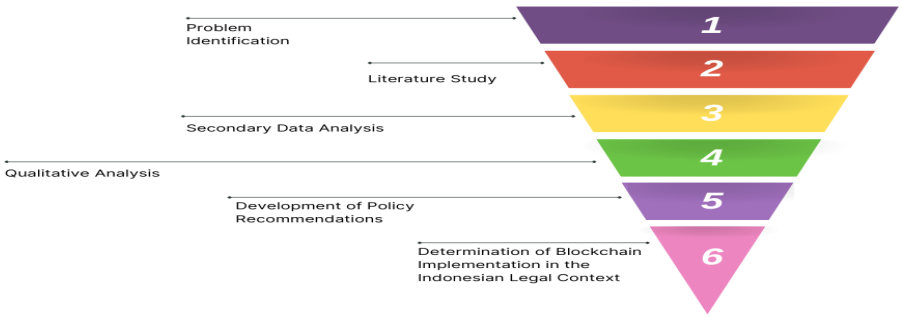
Putri Mei Lestari Lubis (2023) highlighted the challenges of proving cryptocurrency-based money laundering in the Indonesian judicial system, such as transaction anonymity and digital forensic limitations.[30] However, there has been no comprehensive study evaluating the readiness of national regulations, including the role of the OJK, BI, and PPATK in using a blockchain-based supervisory framework. In addition, academic literature in the field of blockchain AML in Indonesia tends to focus on technical or regulatory (normative) approaches, while in-depth legal analysis of the criminal and procedural implications of law enforcement on digital assets is still relatively limited. Law enforcement against money laundering still faces obstacles in both substantive and procedural aspects, as stipulated in the Anti-Money Laundering Law.[31]

The objective of this research is to explore and examine in depth how blockchain technology can be implemented within Indonesia's legal system to detect and prevent money laundering. This study also aims to identify the challenges that may arise in implementing blockchain technology in Indonesia, as well as provide policy recommendations that could strengthen the AML system in the country. Thus, this research is expected to offer innovative and practical solutions to address the increasingly complex issue of money laundering in the digital age.

RESEARCH METHODS

This study uses a qualitative approach with literature study as the main method. The study aims to explore and analyze the potential application of blockchain technology in strengthening the Anti-Money Laundering (AML) system in Indonesia. The research steps to be carried out are as follows:

Figure 1: *Stages of Study*



Source: *Results of personal data processing*

This research began with the process of identifying issues related to the effectiveness of anti-money laundering (AML) systems in Indonesia, particularly obstacles in detecting suspicious

[30] Musfiratul Ilmi and Putri Mei Lestari Lubis, "Tantangan Pembuktian Tindak Pidana Pencucian Uang melalui Cryptocurrency dalam Sistem Hukum Pidana Indonesia," *El-Iqthisady: Jurnal Hukum Ekonomi Syariah* 7, no. 1 (2025): 452, https://doi.org/10.24252/el-iqthisady.v7i1.57409.

[31] Eddy Rifai and H.S. Tisnanta, "Role of Law Enforcement to Prevent Cyber Laundering and Asset Recovery from Overseas," *International Journal of Cyber Criminology* 16, no. 1 (2022): 110, https://doi.org/10.5281/zenodo.4766559.

transactions in digital-based financial activities. This stage explored the core issues arising from the increasing use of financial technology, while assessing the potential use of blockchain as an approach capable of strengthening the ability to detect irregular cash flows. After the problems were formulated, this study continued with an in-depth literature review of various relevant scientific sources. The literature reviewed covered blockchain technology, its application in AML systems in various jurisdictions, and its implementation mechanisms in Indonesia. Various scientific articles, journals, reports from international institutions such as the FATF, and case studies related to blockchain serve as references for understanding how this technology can increase transparency, accelerate verification, and assist in identifying suspicious transaction patterns.

The next stage is the analysis of secondary data obtained from government reports, financial supervisory agency documents such as OJK and PPATK, and other scientific sources discussingthe use of blockchain in the financial sector. This analysis is used to map the legal and regulatory context applicable in Indonesia, so that the readiness of the national legal system in adopting blockchain technology to support AML mechanisms can be evaluated. Furthermore, this study uses qualitative analysis techniques with a descriptive approach to assess the potential and challenges of integrating blockchain into Indonesia's AML system. This analysis highlights the technical and regulatory obstacles that arise in the adoption process, including infrastructure limitations, standardization needs, and institutional readiness in the financial sector.

The results of this analysis then form the basis for formulating policy recommendations addressed to the government, regulatory authorities, and the banking sector. These recommendations focus on strategic steps that can be taken to optimize the application of blockchain within the Indonesian legal framework, particularly covering relevant regulatory analysis, such as the Electronic Information and Transaction Law (UU ITEE), as well as the possibility of applying blockchain as valid electronic evidence in accordance with developments in criminal procedure law in Indonesia.

ANALYSIS AND DISCUSSION

Blockchain Potential in Combat Money Laundering

Blockchain is a technology that stores data in a decentralized and distributed manner, where each data is stored in blocks that are sequentially linked. Each block contains information about transactions and other data, with a unique code from the previous block, making it secure and difficult to manipulate.[32] Blockchain represents a major breakthrough in business and technology worldwide. In the future, blockchain technology will revolutionize financial systems due to its ability to store data in a single master ledger that cannot be altered, as it includes an accurate timestamp of when the transaction occurred. This is due to the characteristics of blockchain, as outlined by Monrat et al. (2019), including decentralization, persistency, anonymity, and auditability.[33] While blockchain allows for a high level of anonymity, this technology also has an equal capacity to identify and trace suspicious transactions, including those originating from anonymous entities.[34] Blockchain tracks and identifies suspicious transactions as follows:

[32] Nazanin Zahed Benisi et al., "Blockchain-Based Decentralized Storage Networks: A Survey," *Journal of Network and Computer Applications* 162 (2020), https://doi.org/10.1016/j.jnca.2020.102656.

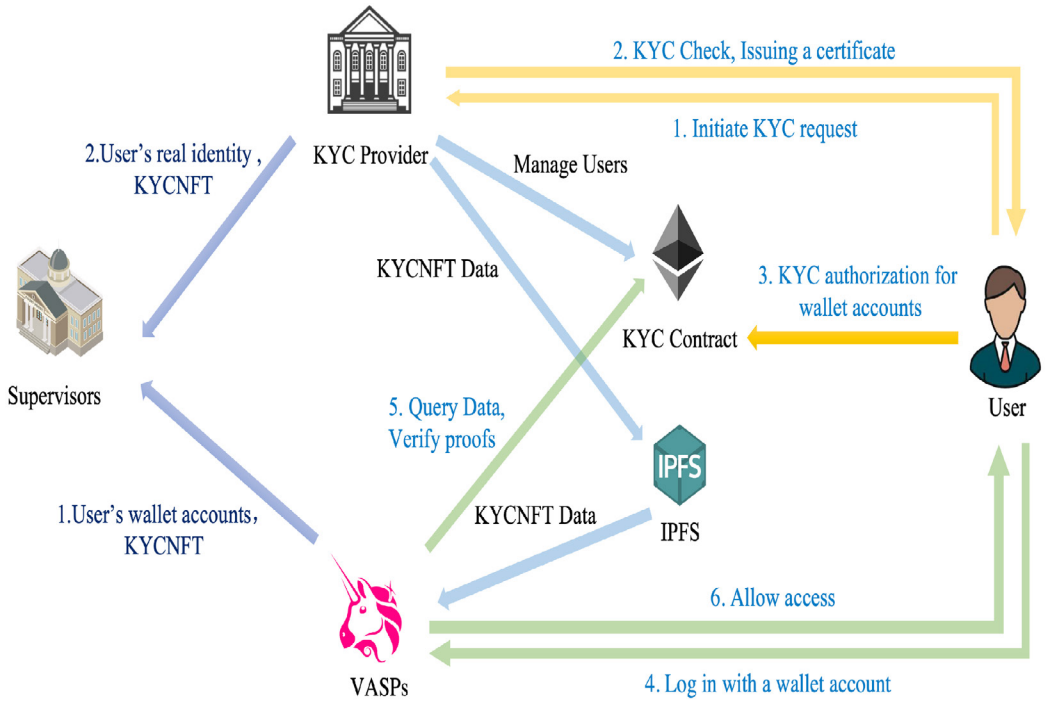
[33] Ahmed Afif Monrat et al., "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," *IEEE Access* 7 (2019): 117134–51, https://doi.org/10.1109/ACCESS.2019.2936094.

[34] Bjelajac and Bajac, "Blockchain Technology and Money Laundering."

1. Irreversible Transactions and Traces Connected to the Real World

Blockchain's pseudonymous usage, which does not directly reveal the identity, will be tracked through the user's address, which then refers to the initial record of the ledger.[35] When a user intends to convert assets, such as cryptocurrency, into currency or performs large transactions, identity verification through the Know Your Customer (KYC) method is required.[36] From here, law enforcement can trace and identify individuals involved in suspicious or illegal transactions. The architecture of the blockchain transaction scheme and its relationship with KYC providers is shown in Figure 2.

Figure 2: *The Architecture of the Blockchain Transaction Scheme and its Relationship with KYC Providers*



Source: *Sun et al., Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains, 2022, 6.*

2. Transaction Pattern Analysis

Transaction pattern analysis is conducted using the blockchain forensic method. This method is employed to observe transactions and identify suspicious patterns within the blockchain. The identification process begins with analyzing transaction anomaly algorithms or algorithms with unusual transaction patterns.[37] For example, transactions involving large amounts that occur

[35] Zhang and Trubey, "Machine Learning and Sampling Scheme."

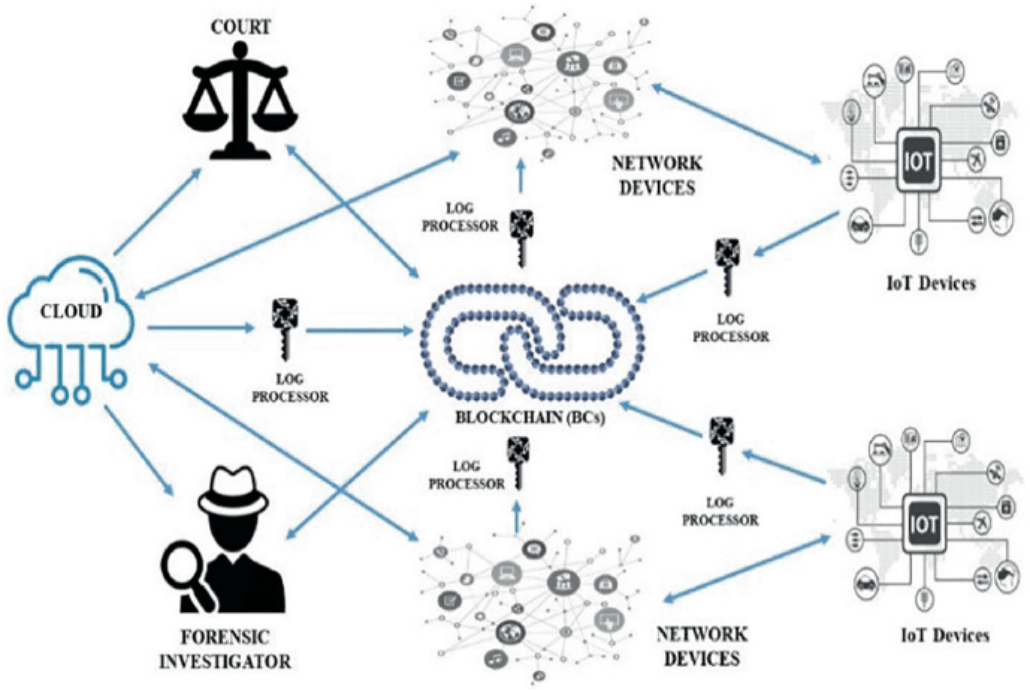
[36] Iwa Salami, "Challenges and Approaches to Regulating Decentralized Finance," *AJIL Unbound* 115 (2021): 425–29, https://doi.org/10.1017/aju.2021.66; Nigang Sun et al., "A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains," *Sustainability* 14, no. 21 (2022): 14584, https://doi.org/10.3390/su142114584.

[37] Nadia Pocher et al., "Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics," *Electronic Markets* 33, no. 1 (2023): 37, https://doi.org/10.1007/s12525-023-00654-3.

suddenly and repeatedly from the same address or from addresses that have never interacted before would be considered transaction anomalies. Additionally, blockchain has an address detection feature that can analyze and identify addresses that might be owned by the same entity, even though different addresses are used.[38]

To examine and analyze the appropriate blockchain data, specialized tools and methods are required. These two elements form the foundation for identifying illegal activities and ensuring that regulations are adhered to. A forensic illustration of blockchain can be seen in the following Figure 3.

Figure 3: *Tools and Techniques for Blockchain Forensics*



Source: *Salvation Data., Blockchain and Digital Investigation: Insights and Impacts, 2024.*[39]

Various forensic tools have been developed to assist in investigating activities on the blockchain network, particularly in detecting crimes involving cryptocurrency assets. Chainalysis has become one of the most popular tools due to its ability to analyze transactions comprehensively, identify fund movement patterns, and map the relationships between addresses on the blockchain.[40] Its functionality is crucial in uncovering illegal activities such as money laundering or digital fraud.[41] Additionally, Elliptic is used by many law enforcement agencies to track the origin and destination

[38] Seyed Mohammad Hosseini et al., "Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations," *Electronics* 12, no. 6 (2023): 1283, https://doi.org/10.3390/electronics12061283.

[39] Salvation Data, "Blockchain and Digital Investigation: Insights and Impacts," 2024, https://www.salvationdata.com/knowledge/digital-investigation/.

[40] Wanshui Song et al., "Blockchain Data Analysis from the Perspective of Complex Networks: Overview," *Tsinghua Science and Technology* 28, no. 1 (2023): 176–206, https://doi.org/10.26599/TST.2021.9010080.

[41] Yuliia Volkova et al., "Crypto Market Experience: Navigating Regulatory Challenges in Modern Conditions," *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan* 24, no. 2 (2024): 178–94, https://doi.org/10.30631/alrisalah.v24i2.1625.

of cryptocurrency transactions, thus making it easier to identify suspicious fund flows. CipherTrace is also a top choice because it supports various types of cryptocurrencies and excels in blockchain security intelligence, assisting investigators in uncovering digital crime cases.[42]

In the transaction tracking process, investigators utilize several analysis techniques. Graph analysis is used to understand complex relationships between blockchain addresses and detect suspicious patterns. Meanwhile, heuristic analysis allows for the grouping of addresses owned by a single entity, thereby reducing the anonymity of transactions. Additionally, timestamp analysis helps sort transactions chronologically, providing a clear picture of the sequence of actions taken by the perpetrators.

Although blockchain provides a permanent transaction trail, this technology has weaknesses that reduce its effectiveness in AML practices. First, privacy coins (e.g., Zcash, Monero) and mixing services (mixers/tumblers) significantly reduce on-chain traceability, making value trail analysis difficult.[43] Second, the DeFi ecosystem and cross-chain mechanisms enable the separation and migration of funds between chains, breaking up previously traceable flows, while off-ramps (OTC, peer-to-peer) allow conversion to fiat without adequate KYC mechanisms.[44] Since most addresses are pseudonymous, on-chain evidence must be combined with off-chain data (KYC, platform logs, transaction evidence) to establish a legal link between the address and the real subject.[45]

3. Cross-Border Fund Flows

International organizations such as the Financial Action Task Force (FATF) have collaborated with member countries to share data in order to detect suspicious activities.[46] FATF provides guidelines for Virtual Asset Service Providers (VASPs), which include cryptocurrency exchanges, digital wallets, and other digital asset-related services, to exchange information regarding cryptocurrency, digital wallets, and related digital assets. These guidelines require compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations for service providers operating in the cryptocurrency and digital asset sectors.[47] They also mandate the reporting of suspicious transactions (Suspicious Transaction Reporting), which includes transactions on the blockchain, as well as maintaining transaction histories to ensure that fund flows can be traced and monitored, even when using decentralized blockchain systems.

---

42 Nitish Kumar and Abhishek Vaish, "Use of Blockchain Technology in Digital Forensics: Where and How?," *In Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures, Pp. 1-16. CRC Press*, 2025.

43 George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn, "An Empirical Analysis of Anonymity in Zcash," *Proceedings of the 27th USENIX Security Symposium* (USENIX Association, 2018), 468, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf.

44 Alireza Hedayati and Hourieh Hosseini, "A Survey on Blockchain: Challenges, Attacks, Security, and Privacy," *International Journal of Smart Electrical Engineering* 10, no. 4 (2021): 141, https://oiccpress.com/ijsee/article/view/16433.

45 Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Proceedings of the 2013 Internet Measurement Conference (IMC)* (ACM, 2013), 1, https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

46 Nankpan Moses Nanyun and Alireza Nasiri, "Role of FATF on Financial Systems of Countries: Successes and Challenges," *Journal of Money Laundering Control* 24, no. 2 (2021): 234–45, https://doi.org/10.1108/JMLC-06-2020-0070.

47 Georgios Pavlidis, "International Regulation of Virtual Assets under FATF's New Standards," *Journal of Investment Compliance* 21, no. 1 (2020): 1–8, https://doi.org/10.1108/JOIC-08-2019-0051.

In addition, VASPs are obliged to maintain transaction histories and ensure traceability of fund flows, even when operating within decentralized blockchain systems. Although blockchain technology offers pseudonymity, analytical techniques such as blockchain forensics and transaction clustering can de-anonymize users and allow for the tracking of illicit activities.[48] This is reinforced by FATF's "Travel Rule", which requires VASPs to exchange specific information (originator and beneficiary data) for transactions above a certain threshold, typically USD/EUR 1,000. This rule is designed to prevent criminals from exploiting regulatory loopholes between jurisdictions.

Furthermore, the implementation of AML/CFT (Countering the Financing of Terrorism) frameworks among VASPs is critical to addressing the risks identified by FATF's Risk-Based Approach (RBA). Member countries are encouraged to assess the risks associated with digital assets and develop proportionate measures, including the enhanced due diligence (EDD) for higher-risk customers or transactions.[49]

Scholarly studies highlight that while regulatory measures by international organizations like FATF have significantly improved the oversight of VASPs, challenges remain. These include differences in regulatory adoption across jurisdictions, technological limitations in blockchain analysis, and privacy concerns raised by the collection and sharing of personal data.[50] Cross-border cooperation and harmonization of regulatory frameworks are essential to closing these regulatory gaps and ensuring the effectiveness of global AML/CFT efforts.[51]

In terms of objectives, on-chain records support the FATF's goal of improving the traceability of fund flows. However, compliance with Recommendation 15 (the "Travel Rule" obligation to provide sender/recipient information) is not achieved solely by the existence of a public ledger. The FATF emphasizes that R.15 requires VASPs to collect, store, and transmit customer metadata and work across jurisdictions; therefore, effective implementation requires technical interoperability (Travel Rule schema), VASP operational compliance, and secure data exchange mechanisms, not just on-chain analytics.[52]

Countries that are more advanced in virtual asset supervision demonstrate a combination of strict regulators and the adoption of on-chain forensic tools. Singapore (MAS) implements operational guidelines and supervisory requirements for digital payment token service providers. The United States (FinCEN) emphasizes the application of BSA/Travel Rule regulations on crypto asset business models. The European Union codifies transaction information requirements through Regulation (EU) 2023/1113 and EBA guidelines. South Korea tightens VASP registration and oversight. Successful implementation in these jurisdictions generally combines KYC/KYB

---

48 Chamunorwa Chitsungo, "Harnessing Digital Strategies to Combat Cryptocurrency-Enabled Crimes: Addressing Money Laundering, Illicit Trade, and Cyber Threats," *American Journal of International Relations* 9, no. 7 (2024): 77–106, https://doi.org/10.47672/ajir.2523.

49 Emmanuel Mathias, "Leveraging Anti-Money Laundering Measures to Improve Tax Compliance and Help Mobilize Domestic Revenues," *IMF Working Papers* 2023, no. 083 (2023): 1, https://doi.org/10.5089/9798400240409.001.

50 Vinden Wylde et al., "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Computer Science* 3, no. 2 (2022): 127, https://doi.org/10.1007/s42979-022-01020-4.

51 Nizan Geslevich Packin and Uri Volovelsky, "DIGITAL ASSETS, ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM: AN ANALYSIS OF EVOLVING REGULATIONS AND ENFORCEMENT IN THE ERA OF NFTS," *The Cambridge Handbook on Law and Policy for NFTs (Nizan Geslevich Packin, Ed.)*, 2023.

52 Financial Action Task Force (FATF), *Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 28 October 2021), Annex A (interpretive note on Recommendation 15), 27–28, https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

obligations, metadata exchange mechanisms, and cooperation between regulators and forensic service providers (analytics vendors).

Blockchain forensics has become an important tool in uncovering large-scale criminal networks. The PlusToken case shows how on-chain analysis helps trace stolen funds to large wallets, identify liquidation paths through OTC and exchanges, and provide evidence for cross-jurisdictional enforcement actions.[53] Other forensic reports (e.g., exchange hack investigations) show that successful investigations typically combine on-chain traces with off-chain data (KYC, exchange logs) and international cooperation.[54]

Technically, blockchain immutability supports the criteria of evidence integrity (authenticity and non-alteration), but the aspect of decentralization poses procedural challenges. The Criminal Procedure Code (KUHAP) and developments in the Electronic Information and Transactions Law (ITE Law) recognize electronic evidence, but in order for on-chain data to be accepted as evidence, the following are required: proof of chain-of-custody and convincing forensic procedures, linking on-chain addresses to legal subjects through KYC or contextual evidence, and expert testimony that can explain the technical aspects to the judge. Without adequate forensic mechanisms and certification, the technical power of blockchain does not automatically fulfill all the requirements of evidence according to the Criminal Procedure Code. Procedural adjustments and improvements in the capabilities of law enforcement agencies and courts are needed. International cooperation is very important to effectively combat crimes related to cryptocurrency.[55]

Know Your Customer (KYC) and Blockchain as Evidence of Money Laundering

In the implementation of Anti-Money Laundering (AML), banks play a crucial role in analyzing the source of funds. Banks assess the flow of money through the Know Your Customer (KYC) procedure. This procedure has long been recognized in Indonesia, as regulated by Bank Indonesia in Regulation Number 3/10/PBI/2001.[56] The implementation of conventional KYC procedures still presents challenges to AML because the identity of the individual involved is based on the customer's form, where they are asked to complete the required information. Customer data, such as identity, company profile, income sources, and other documents, can be fabricated or updated, creating loopholes in AML.[57] Electronic transactions in Indonesia also utilize the E-KYC procedure to perform digital identity verification. The e-KYC process uses biometric technologies such as facial recognition or fingerprint scanners, along with digital document matching.

Several banks and companies have begun implementing blockchain as a means to establish stronger controls.[58] For example, HSBC, Deutsche Bank, and Mitsubishi UFJ Financial Group have

[53] Chainalysis, "PlusToken Scammers Didn't Just Steal $2+ Billion Worth of Cryptocurrency. They May Also Be Driving Down the Price of Bitcoin," *Chainalysis Blog*, 16 December 2019, https://www.chainalysis.com/blog/plustoken-scam-bitcoin-price.

[54] Chainalysis, *Crypto Crime Report 2024*.

[55] I. Nyoman Sucitrawan et al., "Money Laundering Criminal Liability Through Crypto Asset Exchange in Indonesia," *International Journal of Law, Crime and Justice* 1, no. 3 (2024): 314–21, https://doi.org/10.62951/ijlcj.v1i3.190.

[56] Bank Indonesia Regulation Number 3/10/PBI/2001 of 2001 Concerning the Implementation of Know Your Customer Principles.

[57] Wafula Anna Mercy Nafula, *Challenges Of Implementing Effective Anti-Money Laundering Strategies In Kenyan Commercial Banks*, n.d.

[58] Mohamad Osmani et al., "Blockchain for next Generation Services in Banking and Finance: Cost, Benefit, Risk and Opportunity Analysis," *Journal of Enterprise Information Management* 34, no. 3 (2021): 884–99, https://doi.org/10.1108/JEIM-02-2020-0044.

used blockchain technology to test KYC information exchange services. The results indicate that this model can provide certainty in terms of digital security and consumer data protection. Additionally, the process becomes more efficient, as data exchange makes it easier to reject consumer data that has been previously rejected by other banks. This demonstrates that money laundering and high-risk identities can be mitigated using technology, which in turn helps maintain market integrity.[59] For a more detailed comparison, Table 1 below presents a comparison of conventional KYC with blockchain-based KYC:

Table 1: *Comparison of Conventional KYC compared to KYC Using Blockchain*

Aspects	Conventional KYC	KYC Using Blockchain
Verification[60]	Direct manual document checks and third-party data checks	Automated process possible without the need for a third party
Data Management and Security[61]	Data is stored on centralized servers, vulnerable to hacking or data leaks	Data is encrypted and stored on a decentralized network, not dependent on a single storage point
Processing Time[62]	Relatively time consuming	The process is faster because it uses decentralized technology and automation
Costs[63]	High costs for manual verification processes and data maintenance	Lower costs due to the use of blockchain that does not use third parties
Privacy Risks[64]	Customer data can be vulnerable to leaks if the system that stores the data is hacked	Data is encrypted and managed with higher privacy controls, minimizing the risk of privacy breaches

Source: *Analyzed from a study of several literatures (sources are listed in the footnotes)*

This table demonstrates that blockchain-based KYC can be a more effective and efficient tool in analyzing financial flows. While it is recognized that technological barriers in implementation will pose challenges, it must be emphasized that the Financial Action Task Force (FATF), as the international body overseeing AML efforts, should play a greater role in assisting member countries in adopting blockchain technology. Thommandru (2023) concluded that the KYC mechanism, when applied through blockchain technology in financial institutions, is an ideal platform for providing user identification and verification solutions, ensuring that data transfer is readily accessible.[65]

---

[59] Thommandru and Chakka, "Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks."

[60] Prarthana P. Rajapurohit et al., "Enhancing KYC Verification: A Secure and Efficient Approach Utilizing Blockchain Technology," Springer 966 (n.d.): 149–64, https://doi.org/10.1007/978-981-97-2004-0_10.

[61] Diksha Malhotra et al., "How Blockchain Can Automate KYC: Systematic Review," Springer 122 (2022): 1987–2021, https://doi.org/1987–2021.

[62] Bulut Karadag et al., "Blockchain-Based KYC Model for Credit Allocation in Banking," IEEE Access 12 (2024): 80176–82, https://doi.org/10.1109/ACCESS.20*24*.3410874.

[63] Sahil Bhatia et al., "Cost-Efficient Blockchain-Based e-KYC Platform Using Biometric Verification," IEEE, 2024, 403–8, https://doi.org/10.1109/ICOIN59985.2024.10572111.

[64] Md. Abdul Hannan et al., "A Systematic Literature Review of Blockchain-Based e-KYC Systems," Computing 105, no. 10 (2023): 2089–118, https://doi.org/10.1007/s00607-023-01176-8.

[65] Thommandru and Chakka, "Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks."

Indonesia's infrastructure for blockchain-based KYC implementation is still in a transitional phase because technical standards, data interoperability, and cybersecurity readiness are not yet fully mature at the regulatory and financial institution levels. The OJK and Bank Indonesia both emphasize the need for a robust digital identity architecture before decentralized verification can be widely adopted, while PPATK highlights the increasing need for analytics and cross-institutional data integration to support digital transaction monitoring. These limitations are even more apparent when compared to the weaknesses of conventional KYC, which is still predominantly used, such as repetitive manual processes, reliance on physical documents that are prone to forgery, the risk of data leaks due to centralized storage, and the absence of audit trails that can be verified in real time. The combination of unprepared digital infrastructure and fundamental weaknesses in traditional KYC demonstrates the urgency of implementing a distributed identity system, but also shows that its adoption requires strengthening data governance, technical standards, and institutional capacity before it can be implemented effectively.

When blockchain is used as a tool to determine money laundering, a fundamental question arises: how is it regarded as an accepted piece of evidence? In the application of evidence law in Indonesian courts, electronic documents are not formally regulated under procedural law but have been expanded in various statutes, such as the Corruption Eradication Commission Law, the Electronic Information and Transactions Law (ITE Law), and the Constitutional Court Law. For electronic-based evidence, Article 5, paragraph (1) of the ITE Law states that Electronic Information and/or Electronic Documents and/or their printouts are legally valid evidence.[66]

Blockchain, as evidence, can be categorized as electronic evidence. Article 5, paragraph (1) of the ITE Law clarifies that electronic information and/or electronic documents, as well as printouts of electronic information or electronic documents, constitute Electronic Evidence (Digital Evidence). Meanwhile, printouts of electronic information and documents would be considered physical evidence.

In legal proceedings, it can be said that Indonesia's judicial system still faces challenges when applying algorithm-based data evidence. Traditional legal proceedings require physical authenticity, while blockchain relies on the credibility of algorithms, meaning that accuracy of input data and technology integrity are critical.[67] For instance, if a bank teller makes a mistake in recording the identity number of a customer opening a new account, it could cause unforeseen complications during future Anti-Money Laundering (AML) investigations. This is because blockchain analysis is automatically conducted based on the initial data stored in the blockchain. Conversely, in traditional AML processes, investigators or courts can manually review data thoroughly, including identifying any errors in the data or information.

In the context of procedural law, the use of blockchain as evidence faces additional challenges in the form of the absence of digital chain-of-custody standards in the Criminal Procedure Code, the lack of forensic guidelines that establish methods for verifying hashes, timestamps, or on-chain metadata, and the limited capacity of experts to comprehensively explain ledger mechanisms to judges. The decentralized nature of blockchain also raises questions about which authority is

[66] Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions (2024), 1.

[67] Xukang Wang et al., "Blockchain in the Courtroom: Exploring Its Evidentiary Significance and Procedural Implications in U.S. Judicial Processes," *Frontiers in Blockchain* 7 (April 2024): 1306058, https://doi.org/10.3389/fbloc.2024.1306058.

authorized to authenticate and guarantee data integrity. Without a clear procedural framework, the technical power of blockchain does not automatically meet the formal and material requirements of evidence under Indonesian criminal procedural law.

In the United States, the use of blockchain as evidence is supported by experts to strengthen its evidentiary value. Experts evaluate the procedures involved in ensuring the validity of blockchain data inputs to confirm the accuracy and authenticity of the information. This is done to ensure that justice is achieved and, more importantly, to maintain a balanced process between the reliability of technology and the validation of manual records to obtain the full truth. For example, in the case of United States vs. Costanzo, which involved money laundering through the conversion of peer-to-peer digital tokens from drug trade proceeds, expert witnesses played a role in explaining the function of Bitcoin and the operations of blockchain, as well as the mechanisms used to disguise drug sale proceeds as digital tokens. Bitcoin is a decentralized cryptocurrency that has gained popularity over the past few years.[68] In the context of evidence law in Indonesia, an original document is considered valid if it has a wet stamp attached to it. The existence of electronic evidence, as regulated by Indonesian legal provisions, demonstrates that the use of blockchain technology for AML is strongly supported.

Regulation and Urgency of Utilizing Blockchain Technology in Money Laundering Crimes in Indonesia

The Financial Services Authority (OJK) and Bank Indonesia (BI) are working to build a robust financial system through the integration of digital technology to mitigate the risk of money laundering. The shift in cryptocurrency supervisory authority from the Commodity Futures Trading Regulatory Agency (Bappebti) to the OJK reflects the government's orientation to consolidate the regulation of the digital financial sector under a more comprehensive supervisory regime. This shift reflects the need to adapt regulations to the dynamics of financial technology and increasingly complex digital asset transaction models.

The OJK issued Regulation No. 27 of 2024 concerning the Implementation of Digital Financial Asset Trading, Including Cryptocurrency. This regulation provides a legal framework for digital financial asset trading based on the principles of order, transparency, efficiency, and security.[69] The regulation emphasizes the obligations of governance, risk management, market integrity, information security, and money laundering prevention mechanisms.[70] The establishment of this legal framework provides certainty for digital asset businesses and builds a supervisory structure that is expected to increase investor confidence in the fintech and crypto asset sectors.

The relevance of Regulation 27/2024 to the anti-money laundering (AML) regime requires in-depth evaluation. The regulation governs digital asset trading activities, but does not yet provide technical guidelines on the use of blockchain analytics technology as a basis for detecting suspicious transactions. Rules on monitoring cash flows, mapping risks based on on-chain transactions, and

[68] Emad Badawi and Guy-Vincent Jourdan, "Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review," *IEEE Access* 8 (2020): 200021, https://doi.org/10.1109/ACCESS.2020.3034816.

[69] Regulation of the Financial Services Authority of the Republic of Indonesia Number 27 of 2024 Concerning the Implementation of Digital Financial Assets Trading Including Crypto Assets (2024), 27.

[70] Istianah Zainal Asyiqin et al., "Cryptocurrency as a Medium of Rupiah Exchange: Perspective Sharia Islamic Law and Jurisprudential Analysis," *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, November 22, 2024, 227–92, https://doi.org/10.24090/volksgeist.v7i2.10975.

methods for identifying crypto money laundering patterns have not yet been regulated operationally.[71] This situation creates a gap that affects the effectiveness of digital financial supervision.

The OJK's technical capacity in blockchain supervision is an important factor. Supervising digital asset transactions requires blockchain analysts, cyber-forensic experts, on-chain analytics tools, and budgetary support for the development of supervisory technology (SupTech). These resource constraints have the potential to create an imbalance between the complexity of blockchain-based crimes and the ability of supervisory institutions to conduct early detection. Regulations in Singapore and the United Kingdom show a higher level of progress. The Monetary Authority of Singapore (MAS) requires Virtual Asset Service Providers (VASPs) to use blockchain analysis tools as part of their risk assessment. The UK's Financial Conduct Authority (FCA) imposes similar obligations on crypto service providers, so that transaction monitoring does not rely solely on manual reports, but also on automated analytics technology. This model places blockchain technology as an integral element in the AML regime.

Several gaps in OJK Regulation 27/2024 need to be addressed strategically. The regulation does not require the use of blockchain forensic tools for VASPs, meaning that the tracking of high-risk transactions may not be optimal. This regulation also does not cover privacy coins, mixers, and cross-chain laundering, even though these instruments are the most commonly used tools in crypto money laundering practices. There is also a regulatory gap in the absence of provisions on blockchain-based surveillance technology (SupTech), which should be utilized by authorities to improve the effectiveness of monitoring.

The implications of the absence of specific regulations regarding the use of blockchain for AML purposes have a direct impact on law enforcement. The lack of clarity in technical guidelines makes it difficult for authorities to obtain standardized on-chain transaction data. There is an increased risk of digital assets being used as a means of money laundering that is more difficult to track. This situation is not in line with Financial Action Task Force (FATF) standards, particularly those related to virtual asset transparency, travel rules, and risk-based monitoring. This regulatory gap hinders Indonesia's fulfillment of its international obligations and may affect the FATF's assessment of the effectiveness of the national AML/CFT regime.

The urgency of strengthening blockchain regulations in the context of AML is growing as digital financial activities involving illegal fintech, online gambling, investment fraud, and high-risk e-commerce transactions increase. The incomplete normative space regarding the use of blockchain technology as a transaction analysis tool has resulted in a monitoring system that is unable to keep up with the development of digital asset-based criminal methods. This condition emphasizes the need for regulatory updates with a more comprehensive forensic technology approach.

CONCLUSION

Blockchain technology has strategic potential to strengthen law enforcement against money laundering in Indonesia through its ability to track transactions, analyze fund flow patterns, and integrate with digital identification mechanisms. This technology provides opportunities to improve the effectiveness of detection and tracing of high-risk transactions. An evaluation of the applicable

[71] Nur Fadhilah Mappaselleng et al., "Beyond the Surface: Exploring the Next Level of Terrorism on the Dark Web," *Jambura Law Review* 7, no. 1 (2025): 309–35, https://doi.org/10.33756/jlr.v7i1.26150.

regulatory framework shows that current regulations do not yet provide an adequate operational basis for the use of blockchain analytics. OJK Regulation No. 27 of 2024 does not yet require the use of forensic tools, does not regulate privacy coins and cross-chain laundering practices, and does not provide technical guidelines for law enforcement officials. This also indicates a need to strengthen the technical capacity of supervisory agencies and digital evidence standards in the judicial process. The research findings confirm the need for policy updates that explicitly include the use of blockchain technology in the enforcement of TPPU laws. Strengthening regulations, improving institutional capabilities, developing surveillance technology, and establishing digital evidence standards are important steps to ensure blockchain's contribution to the effectiveness of the AML/CFT system in Indonesia. Future research should thoroughly examine the mechanism of blockchain implementation in Indonesia's AML system, including the application of digital transaction analytics to detect suspicious fund flows. Researchers can explore the effectiveness of blockchain in supporting KYC procedures, digital forensics, and electronic evidence in court. Further studies can focus on the integration of blockchain with crypto assets, digital wallets, privacy coins, mixers, and cross-chain laundering to identify regulatory and technical loopholes. Researchers can also assess the readiness of supervisory agencies, the capacity of law enforcement agencies, and the development of digital chain-of-custody standards to support legally valid evidence. The results of this research are expected to provide practical recommendations for policymakers and the financial sector in strengthening the blockchain-based AML system in Indonesia.

REFERENCES

Asyiqin, Istianah Zainal, M. Fabian Akbar, and Manuel Beltrán Genovés. "Cryptocurrency as a Medium of Rupiah Exchange: Perspective Sharia Islamic Law and Jurisprudential Analysis." *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, November 22, 2024, 227–92. https://doi.org/10.24090/volksgeist.v7i2.10975.

B. Rawat, Danda, Vijay Chaudhary, and Ronald Doku. "Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems." *Journal of Cybersecurity and Privacy* 1, no. 1 (2020): 4–18. https://doi.org/10.3390/jcp1010002.

Bank Indonesia Regulation Number 3/10/PBI/2001 of 2001 Concerning the Implementation of Know Your Customer Principles.

Benisi, Nazanin Zahed, Mehdi Aminian, and Bahman Javadi. "Blockchain-Based Decentralized Storage Networks: A Survey." *Journal of Network and Computer Applications* 162 (2020). https://doi.org/10.1016/j.jnca.2020.102656.

Bhatia, Sahil, Lokendra Vishwakarma, and Debasis Das. "Cost-Efficient Blockchain-Based e-KYC Platform Using Biometric Verification." IEEE, 2024, 403–8. https://doi.org/10.1109/ICOIN59985.2024.10572111.

Bjelajac, Željko, and Momčilo Bajac. "Blockchain Technology and Money Laundering." *Law Theory & Prac.* 39, no. 2 (2022): 21–38. https://doi.org/10.5937/ptp2202021B.

Chitsungo, Chamunorwa. "Harnessing Digital Strategies to Combat Cryptocurrency-Enabled Crimes: Addressing Money Laundering, Illicit Trade, and Cyber Threats." *American Journal of International Relations* 9, no. 7 (2024): 77–106. https://doi.org/10.47672/ajir.2523.

Esoimeme, Ehi Eric. "Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules." *Journal of Money Laundering Control* 24, no. 1 (2021): 201–12. https://doi.org/10.1108/JMLC-05-2020-0053.

Hannan, Md. Abdul, Md. Atik Shahriar, Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad Shahriar Rahman. "A Systematic Literature Review of Blockchain-Based e-KYC Systems." *Computing* 105, no. 10 (2023): 2089–118. https://doi.org/10.1007/s00607-023-01176-8.

Hosseini, Seyed Mohammad, Joaquim Ferreira, and Paulo C. Bartolomeu. "Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations." *Electronics* 12, no. 6 (2023): 1283. https://doi.org/10.3390/electronics12061283.

Karadag, Bulut, A. Halim Zaim, and Akhan Akbulut. "Blockchain-Based KYC Model for Credit Allocation in Banking." *IEEE Access* 12 (2024): 80176–82. https://doi.org/10.1109/ACCESS.2024.3410874.

Kumar, Nitish, and Abhishek Vaish. "Use of Blockchain Technology in Digital Forensics: Where and How?" *In Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures, Pp. 1-16. CRC Press*, 2025.

Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions (2024).

Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. "How Blockchain Can Automate KYC: Systematic Review." *Springer* 122 (2022): 1987–2021. https://doi.org/1987–2021.

Mappaselleng, Nur Fadhilah, Nadiah Khaeriah Kadir, Abd Kadir Ahmad, Zul Khaidir Kadir, and Normiati Normiati. "Beyond the Surface: Exploring the Next Level of Terrorism on the Dark Web." *Jambura Law Review* 7, no. 1 (2025): 309–35. https://doi.org/10.33756/jlr.v7i1.26150.

Mathias, Emmanuel. "Leveraging Anti-Money Laundering Measures to Improve Tax Compliance and Help Mobilize Domestic Revenues." *IMF Working Papers* 2023, no. 083 (2023): 1. https://doi.org/10.5089/9798400240409.001.

Monrat, Ahmed Afif, Olov Schelen, and Karl Andersson. "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities." *IEEE Access* 7 (2019): 117134–51. https://doi.org/10.1109/ACCESS.2019.2936094.

Nafula, Wafula Anna Mercy. *Challenges Of Implementing Effective Anti-Money Laundering Strategies In Kenyan Commercial Banks*. n.d.

Nanyun, Nankpan Moses, and Alireza Nasiri. "Role of FATF on Financial Systems of Countries: Successes and Challenges." *Journal of Money Laundering Control* 24, no. 2 (2021): 234–45. https://doi.org/10.1108/JMLC-06-2020-0070.

Oad, Ammar, Abdul Razaque, Askar Tolemyssov, Munif Alotaibi, Bandar Alotaibi, and Chenglin Zhao. "Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection." *Electronics* 10, no. 15 (2021): 1766. https://doi.org/10.3390/electronics10151766.

Osmani, Mohamad, Ramzi El-Haddadeh, Nitham Hindi, Marijn Janssen, and Vishanth Weerakkody. "Blockchain for next Generation Services in Banking and Finance: Cost, Benefit, Risk and

Opportunity Analysis." *Journal of Enterprise Information Management* 34, no. 3 (2021): 884–99. https://doi.org/10.1108/JEIM-02-2020-0044.

Packin, Nizan Geslevich, and Uri Volovelsky. "DIGITAL ASSETS, ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM: AN ANALYSIS OF EVOLVING REGULATIONS AND ENFORCEMENT IN THE ERA OF NFTS." *The Cambridge Handbook on Law and Policy for NFTs (Nizan Geslevich Packin, Ed.)*, 2023.

Panda, Sandeep Kumar, and Suresh Chandra Satapathy. "Drug Traceability and Transparency in Medical Supply Chain Using Blockchain for Easing the Process and Creating Trust between Stakeholders and Consumers." *Personal and Ubiquitous Computing* 28, no. 1 (2024): 75–91. https://doi.org/10.1007/s00779-021-01588-3.

Pavlidis, Georgios. "International Regulation of Virtual Assets under FATF's New Standards." *Journal of Investment Compliance* 21, no. 1 (2020): 1–8. https://doi.org/10.1108/JOIC-08-2019-0051.

Pocher, Nadia, Mirko Zichichi, Fabio Merizzi, Muhammad Zohaib Shafiq, and Stefano Ferretti. "Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics." *Electronic Markets* 33, no. 1 (2023): 37. https://doi.org/10.1007/s12525-023-00654-3.

Pusat Pelaporan dan Analisis Transaksi Keuangan. "Laporan Tahunan PPATK Tahun 2024." Pusat Pelaporan dan Analisis Transaksi Keuangan, 2024. https://www.ppatk.go.id/publikasi/read/255/laporan-tahunan-ppatk-tahun-2024.html.

Rajapurohit, Prarthana P., Nisarga Bhaskar, Pranav Kumaar, and Shruti Jadon. "Enhancing KYC Verification: A Secure and Efficient Approach Utilizing Blockchain Technology." *Springer* 966 (n.d.): 149–64. https://doi.org/10.1007/978-981-97-2004-0_10.

Rana, Nripendra P., Yogesh K. Dwivedi, and D. Laurie Hughes. "Analysis of Challenges for Blockchain Adoption within the Indian Public Sector: An Interpretive Structural Modelling Approach." *Information Technology & People* 35, no. 2 (2022): 548–76. https://doi.org/10.1108/ITP-07-2020-0460.

Regulation of the Financial Services Authority of the Republic of Indonesia Number 27 of 2024 Concerning the Implementation of Digital Financial Assets Trading Including Crypto Assets (2024).

Salami, Iwa. "Challenges and Approaches to Regulating Decentralized Finance." *AJIL Unbound* 115 (2021): 425–29. https://doi.org/10.1017/aju.2021.66.

Salvation Data. "Blockchain and Digital Investigation: Insights and Impacts." 2024. https://www.salvationdata.com/knowledge/digital-investigation/.

Song, Wanshui, Wenyin Zhang, Jiuru Wang, et al. "Blockchain Data Analysis from the Perspective of Complex Networks: Overview." *Tsinghua Science and Technology* 28, no. 1 (2023): 176–206. https://doi.org/10.26599/TST.2021.9010080.

Sucitrawan, I. Nyoman, M. Arief Amrullah, and Fanny Tanuwijaya Tanuwijaya. "Money Laundering Criminal Liability Through Crypto Asset Exchange in Indonesia." *International Journal of Law, Crime and Justice* 1, no. 3 (2024): 314–21. https://doi.org/10.62951/ijlcj.v1i3.190.

Sun, Nigang, Yuanyi Zhang, and Yining Liu. "A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains." *Sustainability* 14, no. 21 (2022): 14584. https://doi.org/10.3390/su142114584.

Thommandru, Abhishek, and Dr Benarji Chakka. "Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks." *Sustainable Futures* 5 (December 2023): 100107. https://doi.org/10.1016/j.sftr.2023.100107.

Villányi, Benjámin. "Money Laundering: History, Regulations, and Techniques." *Oxford Research Encyclopedia of Criminology*, April 26, 2021. https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-708.

Volkova, Yuliia, Bohdan Bon, Anton Borysenko, Yuliia Leheza, and Yevhen Leheza. "Crypto Market Experience: Navigating Regulatory Challenges in Modern Conditions." *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan* 24, no. 2 (2024): 178–94. https://doi.org/10.30631/alrisalah.v24i2.1625.

Wang, Xukang, Ying Cheng Wu, and Zhe Ma. "Blockchain in the Courtroom: Exploring Its Evidentiary Significance and Procedural Implications in U.S. Judicial Processes." *Frontiers in Blockchain* 7 (April 2024): 1306058. https://doi.org/10.3389/fbloc.2024.1306058.

Wronka, Christoph. "'Cyber-Laundering': The Change of Money Laundering in the Digital Age." *Journal of Money Laundering Control* 25, no. 2 (2022): 330–44. https://doi.org/10.1108/JMLC-04-2021-0035.

Wylde, Vinden, Nisha Rawindaran, John Lawrence, et al. "Cybersecurity, Data Privacy and Blockchain: A Review." *SN Computer Science* 3, no. 2 (2022): 127. https://doi.org/10.1007/s42979-022-01020-4.

Zhang, Yan, and Peter Trubey. "Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection." *Computational Economics* 54, no. 3 (2019): 1043–63. https://doi.org/10.1007/s10614-018-9864-z.