Indonesian Journal of Criminal Law Studies
ISSN 2548-1568 (Print) 2548-1576 (Online)
Vol. 10 Issue 2 (2025) 615-658
The title has been indexed by **SCOPUS**, **SINTA**
DOI: https://doi.org/10.15294/ijcls.v10i2.28795
Online since: November 5, 2025

Indonesian Journal of
CRIMINAL LAW STUDIES
A peer-reviewed journal published by **Faculty of Law Universitas Negeri Semarang, Indonesia**.
Online at https://journal.unnes.ac.id/journals/ijcls/index

Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries

Dadang Herli Saputra[a] ✉, Fardana Kusumah[b]

[a] Faculty of Law, Universitas Sultan Ageng Tirtayasa, Indonesia
[b] Faculty of Law, Central China Normal University, China

✉ Corresponding Email: dadang.herli@untirta.ac.id

Abstract

This study explores the role of blockchain forensics in addressing evidentiary challenges arising from crypto-based corruption in developing countries. As cryptocurrencies become increasingly used to obscure illicit financial flows, traditional evidentiary mechanisms often fall short in tracing, authenticating, and prosecuting corruption involving digital assets. The normative legal research method is employed, using statutory, conceptual, comparative, and futuristic approaches to examine both the current limitations and future possibilities of legal frameworks. The research is descriptive-prescriptive in nature, aiming not only to describe the existing problems but also to propose legal reform strategies to enhance the capacity of law enforcement and judicial systems in handling crypto-related corruption. Through content analysis, the study compares how countries such as the United States and Estonia have integrated blockchain forensic tools into anti-corruption efforts, contrasting these with the institutional and regulatory challenges faced by developing nations such as Indonesia.

Findings reveal that without clear legal standards for blockchain evidence, and without adequate cross-border cooperation, digital corruption will continue to exploit the evidentiary gaps in emerging legal systems. The study concludes by recommending the adoption of integrated legal-technical frameworks that recognize blockchain evidence, support forensic technology capacity building, and promote global alignment in anti-corruption strategies.

Keywords

Blockchain Forensics; Crypto-Based Corruption; Evidentiary Challenges; Digital Evidence; Developing Countries.

HOW TO CITE:

Chicago Manual of Style Footnote:

[1] Dadang Herli Saputra, and Fardana Kusumah. "Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries." *Indonesian Journal of Criminal Law Studies 10*, no 2 (2025): 615-658. https://doi.org/10.15294/ijcls.v10i2.28795.

Chicago Manual of Style for Reference:

Saputra, Dadang Herli, and Fardana Kusumah. "Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries." *Indonesian Journal of Criminal Law Studies 10*, no 2 (2025): 615-658. https://doi.org/10.15294/ijcls.v10i2.28795.

Introduction

Corruption remains a serious threat to sustainable development, clean governance, and social justice around the world.[1] However, the forms, methods, and mediums of corruption have undergone significant transformation in the past two decades, particularly in response to the rapid evolution of digital technologies and the globalization of financial systems. One emerging phenomenon is the use of blockchain technology and digital assets especially cryptocurrency as instruments of corruption.[2] This phenomenon, often referred to as crypto-based corruption, involves the movement, concealment, or laundering of illicit funds obtained through corruption via blockchain-based transactions. This development poses serious challenges for evidentiary systems in criminal justice, especially in developing countries that lack the legal and technological infrastructure to address it effectively.[3]

The global growth of cryptocurrency adoption has been exponential, transforming the financial landscape and reshaping how value is transferred and stored across borders.[4] According to the Crypto.com Market Sizing Report (2023), the number of global cryptocurrency users surpassed 580 million by the end of 2023 an unprecedented surge from 420 million in 2022. This rapid expansion is driven by factors such as increasing

[1] Herawan Sauni et al., "Beyond Borders: Shedding Light on Foreign Bribery through an Islamic Legal Lens," *Al-Istinbath: Jurnal Hukum Islam* 9, no. 2 (September 2024): 649–78, https://doi.org/10.29240/JHI.V9I2.9752.

[2] Adrianit Ibrahimi and Besa Arifi, "Corruption and Cryptocurrency - Blockchains as Corruption Tools," *Academicus International Scientific Journal* 26 (July 2022): 93–103, https://doi.org/10.7336/ACADEMICUS.2022.26.06.

[3] Petr Wawrosz and Jan Lánský, "Cryptocurrencies and Corruption," *Ekonomicky Casopis* 69, no. 7 (2021): 687–705, https://doi.org/10.31577/EKONCAS.2021.07.02.

[4] Ahmet Kaplan, "Cryptocurrency and Corruption: Auditing with Blockchain BT - Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities," in *Auditing Ecosystem and Strategic Accounting in the Digital Era*, ed. Tamer Aksoy and Umit Hacioglu (Cham: Springer International Publishing, 2021), 325–38, https://doi.org/10.1007/978-3-030-72628-7_15.

institutional interest, decentralized finance (DeFi) innovations, and growing accessibility through mobile platforms and digital wallets. However, this massive uptake has also introduced heightened vulnerabilities within financial systems. In parallel, the Chainalysis Crypto Crime Report 2024 revealed a troubling trend: illicit crypto transactions reached over USD 24.2 billion, with approximately USD 3.1 billion linked specifically to corruption-related crimes. These include embezzlement of public funds, laundering of bribe payments, and the concealment of politically exposed persons' (PEPs) assets using anonymized blockchain mechanisms. This development highlights an emerging pattern in which blockchain networks despite their promises of transparency, immutability, and traceability are increasingly manipulated by actors skilled in exploiting pseudonymous features, mixing services, and cross-chain obfuscation. These methods create layers of complexity that challenge conventional legal and forensic tools, especially in jurisdictions where regulatory oversight and digital investigative capabilities are still evolving.[5]

Blockchain's inherent features decentralization, pseudonymity, and irreversibility make it an ideal mechanism for actors seeking to obscure corrupt financial transactions. Unlike traditional bank accounts that can be monitored, frozen, or subpoenaed through formal legal processes, cryptocurrency wallets are often anonymous and immune to centralized intervention.[6] Funds can be transferred globally within seconds, using decentralized exchanges (DEXs), crypto mixers, and privacy-enhancing coins such as Monero or Zcash. Additionally, multi-signature wallets allow for shared control of funds among conspirators, further complicating asset

[5] Lamprini Zarpala and Fran Casino, "A Blockchain-Based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario," *Digital Finance* 3, no. 3 (2021): 301–32, https://doi.org/10.1007/s42521-021-00035-5.

[6] Varun Jain et al., "Blockchain Empowerment in Sanctions and AML Compliance: A Transparent Approach," *International Journal of Computer Trends and Technology* 72, no. 5 (May 2024): 11–26, https://doi.org/10.14445/22312803/IJCTT-V72I5P102.

tracing and confiscation efforts. Consequently, traditional evidentiary tools such as witness testimony, financial records, or audit reports are often insufficient to trace and prove digital corruption cases effectively.

Several real-world cases from various jurisdictions vividly illustrate how cryptocurrency has been integrated into corrupt schemes, often with cross-border ramifications. In West Africa, for instance, an energy infrastructure initiative involving multiple international contractors was overshadowed by allegations of public sector corruption. Authorities suspected that senior officials used Bitcoin to launder bribes received from foreign entities, exploiting the relative anonymity of blockchain wallets to move funds across borders without triggering conventional financial oversight. These digital transactions were often layered through multiple wallets and routed through mixers or privacy coins to obscure their origin and destination, making traditional financial tracking tools ineffective.[7] In another instance, Brazilian anti-corruption investigators uncovered that during a high-profile political financing probe, illicit campaign donations were systematically converted into cryptocurrency to avoid detection. These digital assets were then funneled through shell corporations that operated exclusively online, often registered in offshore jurisdictions with lax compliance regulations. The digital nature of these transactions complicated the evidentiary process, as tracing the flow of funds required advanced blockchain analysis and cooperation with international crypto-exchanges and forensic firms.[8] Meanwhile, the Malaysian 1MDB case although originating before the mainstreaming of blockchain forensics provides an example of how digital assets began to enter the landscape of financial crime. Later investigations, as new forensic tools became available,

[7] Harsh Verma, "The Impact of Cryptocurrency on Money Laundering Practices," *African Journal of Commercial Studies* 5, no. 2 (August 2024): 51–60, https://doi.org/10.59413/AJOCS/V5.I.2.1.

[8] G Tziakouris, "Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective," *IEEE Security & Privacy* 16, no. 4 (2018): 92–94, https://doi.org/10.1109/MSP.2018.3111243.

raised the possibility that cryptocurrency may have played a role in further dispersing the embezzled public funds. Allegations emerged that parts of the diverted money had been routed through digital wallets, exploiting regulatory blind spots and the slow institutional adaptation to crypto-assets at the time. These cases reflect a broader trend in which actors involved in corruption are increasingly leveraging blockchain-based financial infrastructures to hide, convert, and transmit illicit assets beyond the reach of traditional legal and financial controls.[9]

Developing countries including Indonesia, Nigeria, and the Philippines struggle to confront this new wave of corruption. Their legal systems remain heavily reliant on conventional evidentiary structures, often codified in criminal procedural codes that do not account for digital or decentralized technologies. For instance, Indonesia's Code of Criminal Procedure (KUHAP) recognizes only five main types of evidence: witness testimony, expert opinion, documents, indications, and defendant statements. While Indonesia's Electronic Information and Transactions Law acknowledges the legal standing of electronic evidence, it does not clearly define or standardize blockchain data such as wallet addresses, transaction hashes, or smart contract logs as admissible forms of proof.

This regulatory vacuum is compounded by technical and institutional limitations. The World Bank Digital Economy Report 2022 indicates that only 27% of developing countries have the forensic digital infrastructure required to conduct blockchain-based investigations. In Indonesia, for example, there is no integrated system between the Financial Transaction Reports and Analysis Center (PPATK), the Cyber Crime Unit of the National Police, and the Corruption Eradication Commission (KPK) for

[9] Saminu Salisu, Velitchko Filipov, and Barry Pene, "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation," *International Conference on Cyber Warfare and Security* 18, no. 1 (February 2023): 338–47, https://doi.org/10.34190/ICCWS.18.1.947.

tracing or managing digital assets obtained through corruption. In most cases, seized crypto assets are either unrecognized in legal proceedings or fail to meet evidentiary thresholds due to a lack of regulatory clarity and forensic validation.

In contrast, developed countries have made significant advances in integrating blockchain forensics into criminal investigations and evidentiary practices. In the United States, the Federal Rules of Evidence (FRE) accommodate digital evidence, including blockchain records, as primary admissible evidence.[10] Agencies such as the Department of Justice (DOJ) and the Internal Revenue Service (IRS) maintain dedicated cybercrime units that collaborate with blockchain analytics firms like Chainalysis, Elliptic, and CipherTrace to identify wallet ownership, trace crypto flows, and conduct on-chain audits. In the FBI v. Colonial Pipeline ransomware case (2021), blockchain evidence was used successfully in federal court to identify and recover ransom payments made in Bitcoin.[11]

Estonia offers another compelling example of a technologically advanced and legally adaptive system. Not only has Estonia integrated blockchain into its national administrative infrastructure, but it has also developed legal provisions that formally recognize blockchain-based evidence in criminal and administrative proceedings. Its X-Road digital backbone allows for real-time interagency data verification, including anti-corruption monitoring. Estonian courts accept transaction hashes, digital

[10] Xukang Wang, 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): 1–7, https://doi.org/10.3389/FBLOC.2024.1306058/BIBTEX.

[11] Md Hasibul Alam Ratul, Sepideh Mollajafari, and Martin Wynn, "Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution," *Sustainability 2024, Vol. 16, Page 10885* 16, no. 24 (December 2024): 1–20, https://doi.org/10.3390/SU162410885.

time-stamping, and wallet forensics as valid forms of primary evidence provided they meet criteria for authenticity, integrity, and traceability.[12]

Despite these advances, most developing nations face four major challenges in incorporating blockchain forensics into anti-corruption enforcement. First is the regulatory challenge: most legal systems lack specific frameworks to classify blockchain data as a distinct and legitimate evidentiary form. Second is the technical challenge: investigative bodies often lack the tools and trained personnel to interpret blockchain data or perform forensic tracing. Third is the financial and geopolitical challenge: since most blockchain evidence spans jurisdictions, international cooperation under Mutual Legal Assistance Treaties (MLATs) and digital evidence protocols is essential but often underdeveloped. Fourth is the epistemological challenge: the legal culture in many countries still views non-traditional evidence with skepticism, leading judges and prosecutors to resist reliance on complex or unfamiliar technologies.

Given this context, comprehensive reform of evidentiary laws in developing countries is urgently needed. Such reform must move beyond incremental digital adaptation and embrace a paradigm shift that aligns legal standards with emerging technologies. This includes amending criminal procedure laws to explicitly define blockchain data as a form of admissible evidence; developing national digital forensic laboratories capable of investigating blockchain transactions; training judges, prosecutors, investigators, and defense lawyers in crypto-forensics; and establishing regulatory interoperability with international frameworks such as the UN Convention Against Corruption (UNCAC) and the Budapest Convention on Cybercrime.

[12] Rois Saputro et al., "Prerequisites for the Adoption of the X - Road Interoperability and Data Exchange Framework: A Comparative Study," *International Conference on EDemocracy & EGovernment*, April 2020, 216–22, https://doi.org/10.1109/ICEDEG48599.2020.9096704.

This study aims to respond to these challenges by examining blockchain forensics and its integration into the evidentiary systems of developing countries, particularly within corruption cases. Employing a normative legal research method, the study utilizes statutory, conceptual, comparative, and futuristic approaches. The statutory approach analyzes the existing gaps in evidentiary law; the conceptual approach explores the legal status of blockchain evidence; the comparative approach highlights the best practices from countries such as the United States and Estonia; and the futuristic approach projects potential reforms needed for legal systems to remain adaptive in a digitalized, transnational era. The research is both descriptive and prescriptive describing existing weaknesses and prescribing a forward-looking framework for evidentiary reform.

Several studies have explored blockchain forensics from a technical and security-driven perspective, yet they fall short in addressing its evidentiary relevance within legal systems, particularly in corruption cases. Atlam et al. (2024) conducted a systematic review of blockchain forensics methodologies, such as address clustering and chain analytics, and emphasized the absence of standard forensic protocols, but did not analyze how these tools function within criminal procedure law especially in developing nations.[13] Similarly, Agarwal et al. (2023) proposed an AI-based detection system for cryptocurrency fraud, combining machine learning and blockchain forensics to achieve 97.5% accuracy, yet their focus remained on fraud detection, not on the admissibility of such evidence in court or its role in prosecuting crypto-based corruption.[14] Meanwhile, Elmougy and Liu (2023) introduced Elliptic++, a graph-based forensic

[13] G Kogias et al., "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions," *Electronics 2024, Vol. 13, Page 3568* 13, no. 17 (September 2024): 1–37, https://doi.org/10.3390/ELECTRONICS13173568.

[14] Udit Agarwal et al., "Blockchain and Crypto Forensics: Investigating Crypto Frauds," *International Journal of Network Management* 34, no. 2 (March 2024): e2255, https://doi.org/10.1002/NEM.2255;WGROUP:STRING:PUBLICATION.

dataset and analysis framework for identifying illicit transactions in the Bitcoin network, but their research did not extend into how this data could be integrated into evidentiary frameworks or applied in the context of anti-corruption litigation, particularly in jurisdictions with weak digital legal infrastructure.[15] In contrast, this study adopts a normative and comparative legal approach to examine how blockchain forensic evidence can be formally recognized and operationalized in corruption proceedings in developing countries, offering prescriptive reforms to address legal, institutional, and procedural gaps.

Method

This This study employs a normative legal research method[16], also referred to as doctrinal legal research. This approach is used to examine and analyze positive legal norms such as statutes, legal principles, and jurisprudence that are relevant to the use of blockchain-based forensic evidence in corruption cases. Within this context, blockchain forensics is positioned as an emerging evidentiary method that challenges the limitations of conventional legal frameworks in criminal procedure, particularly in the prosecution of crypto-based corruption in developing countries. The research adopts four complementary approaches: the statutory approach, conceptual approach, comparative approach, and futuristic approach.[17] The statutory approach is used to review and interpret relevant legislation in Indonesia and other

[15] Youssef Elmougy and Ling Liu, "Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* 1 (May 2023): 3979–90, https://doi.org/10.1145/3580305.3599803.

[16] Akhmad Akhmad, Zico Junius Fernando, and Papontee Teeraphan, "Unmasking Illicit Enrichment: A Comparative Analysis of Wealth Acquisition Under Indonesian, Thailand and Islamic Law," *Journal of Indonesian Legal Studies* 8, no. 2 (2023): 899–934, https://doi.org/10.15294/jils.v8i2.69332.

[17] Zico Junius Fernando et al, "Preventing Bribery in the Private Sector Through Legal Reform Based on Pancasila," *Cogent Social Sciences* 8, no. 1 (2022): 1–14, https://doi.org/10.1080/23311886.2022.2138906.

jurisdictions, including criminal procedure codes, anti-corruption laws, digital evidence regulations, and cryptocurrency governance. This includes a detailed examination of the Indonesian Criminal Procedure Code (KUHAP), the Corruption Eradication Law, the Law on Electronic Information and Transactions (ITE), and their implementing regulations. The conceptual approach is applied to clarify and analyze the core legal concepts involved in the study such as "electronic evidence," "digital assets," "blockchain transactions," and "digital forensics." This approach helps determine the theoretical compatibility (or incompatibility) of these emerging evidentiary forms with existing evidentiary doctrines. It further seeks to define a conceptual framework that can support the recognition of blockchain-based evidence within modern legal systems. The comparative approach is used to analyze how advanced jurisdictions specifically the United States and Estonia have integrated blockchain forensics into their evidentiary and criminal justice systems. The U.S. is selected due to its extensive use of blockchain evidence in federal courts, backed by legal precedents and cooperation with forensic firms such as Chainalysis and CipherTrace. Estonia, on the other hand, represents a digital pioneer that has embedded blockchain into its public administration and legal processes, including its acceptance of transaction hashes and blockchain logs as admissible primary evidence. These comparative insights are intended to provide normative and practical guidance for reform in developing countries, particularly Indonesia. The futuristic approach is used to project legal developments and recommend forward-looking reforms in criminal evidentiary law. Given the rapidly evolving nature of blockchain technology and crypto-based crimes, this approach is essential for anticipating future legal needs and aligning regulatory systems with global technological advancements. It focuses on designing a proactive evidentiary framework that can address transnational corruption, digital assets, and decentralized financial ecosystems. This study is descriptive-prescriptive in nature.[18] It is descriptive in that it maps and explains current institutional, legal, and regulatory challenges that hinder the effective use of blockchain evidence in corruption trials in developing countries. At the same time, it is prescriptive, offering normative proposals to reform existing evidentiary laws, institutional capacities, and cross-border legal cooperation, to improve legal readiness for prosecuting digital corruption. To examine and interpret legal data, this study uses content analysis as the core analytical technique. Content analysis allows for a qualitative examination of legislation, judicial decisions, international conventions, and scholarly literature related to blockchain forensics and evidentiary law.[19] This includes analyzing the internal coherence, interpretive consistency, and normative gaps in current legal instruments, as well as identifying areas where legal reform is needed to respond effectively to blockchain-based evidence and modern digital forensics. Through this methodological framework, the research aims to contribute both theoretically and practically to the reform of evidentiary law in developing countries. It seeks to build an integrated model that bridges the gap between technological advancements in blockchain and the legal systems that must increasingly rely on such tools in the fight against corruption.

Result and Discussion

A. The Rise of Crypto-Based Corruption and Its Impact on Evidentiary Structures

The exponential advancement of blockchain technology and the mainstream adoption of cryptocurrencies have revolutionized not only the

[18] Hendra Karianga and Zico Junius Fernando, “The Damage of the Shadow Economy: The Urgency of Addressing Foreign Bribery in Indonesia,” *Pakistan Journal of Criminology* 16, no. 2 (April 2024): 783–96, https://doi.org/10.62271/PJC.16.2.783.796.

[19] Muchamad Satria Endriana et al., “Green Financial Crime: Expose About Financial Crime In The Environment And Renewable Energy World,” *IOP Conference Series: Earth and Environmental Science* 1270, no. 1 (December 2023): 012012, https://doi.org/10.1088/1755-1315/1270/1/012012.

global financial system but also the methods by which economic crimes particularly corruption are committed and concealed.[20] Traditionally, corruption involved traceable patterns: bribes were paid in cash, misappropriated public funds moved through banks, and financial trails were often documented in audit reports or accounting systems. However, with the rise of crypto-based corruption, these patterns are no longer predictable. The shift from physical and fiat-based corruption to decentralized digital assets has dramatically undermined conventional evidentiary mechanisms, posing acute challenges for law enforcement, prosecutors, and the judiciary.

Crypto-based corruption refers to the utilization of digital currencies such as Bitcoin, Ethereum, and privacy coins like Monero as vehicles for committing, laundering, or hiding the proceeds of corrupt activities.[21] This phenomenon is not purely hypothetical. In 2023 alone, according to Chainalysis, over USD 3.1 billion worth of cryptocurrency was linked to corruption-related offenses, including illegal public procurement, political finance manipulation, and cross-border embezzlement. What makes this form of corruption particularly insidious is its integration with decentralized financial (DeFi) ecosystems, enabling real-time, anonymous transfers across jurisdictions without the need for conventional banking intermediaries.

The technological features of blockchain systems further complicate evidentiary processes. Most public blockchains are pseudonymous, meaning that while every transaction is publicly recorded and immutable, the identities of wallet holders are not directly linked to legal entities or

[20] Aziz N. Berdiev, Rajeev K. Goel, and James W. Saunoris, "Global Cryptocurrency Use, Corruption, and the Shadow Economy: New Insights into the Underlying Linkages," *American Journal of Economics and Sociology* 83, no. 3 (May 2024): 609–29, https://doi.org/10.1111/AJES.12566.

[21] Chad Albrecht et al., "The Use of Cryptocurrencies in the Money Laundering Process," *Journal of Money Laundering Control* 22, no. 2 (May 2019): 210–16, https://doi.org/10.1108/JMLC-12-2017-0074/FULL/XML.

individuals unless additional off-chain data is available.[22] This feature alone severely restricts traditional evidentiary approaches, which rely heavily on direct links between suspects and physical or digital assets. In a typical corruption case, proving the nexus between a defendant and illicit funds often requires establishing ownership, custody, and control. In the crypto context, however, proving ownership of a wallet address especially one created through decentralized applications or accessed via privacy tools demands a different kind of forensic methodology.

Further exacerbating the issue is the emergence of *crypto-mixers* and *tumblers*, which fragment and shuffle transactions across multiple wallets to obscure their origin. Mixers like Tornado Cash or ChipMixer allow corrupt actors to launder assets by breaking the traceability chain, thus rendering blockchain records practically useless unless additional forensic tools are employed. The use of *privacy coins* cryptocurrencies with built-in anonymization protocols poses even greater barriers. Coins like Monero and Zcash use stealth addresses and ring signatures, which make it nearly impossible for conventional forensic analysis to detect or reconstruct transaction histories. In legal proceedings, these technical realities create a form of "evidentiary opacity," whereby acts of corruption can no longer be illuminated by traditional documentary or testimonial evidence.[23]

Another critical impact of crypto-based corruption is on asset tracing and seizure. In many jurisdictions, asset recovery laws are designed for tangible or banked assets, requiring court orders to freeze accounts or seize properties. However, crypto-assets can be transferred across borders instantly and without government oversight. Even when suspects are

[22] Shaurya Negi et al., "The Preservation of Digital Evidences Through Blockchain Technology," *Proceedings - 2023 IEEE World Conference on Applied Intelligence and Computing, AIC 2023*, 2023, 954–58, https://doi.org/10.1109/AIC57670.2023.10263968.

[23] Wiebe Koerhuis, Tahar Kechadi, and Nhien An Le-Khac, "Forensic Analysis of Privacy-Oriented Cryptocurrencies," *Forensic Science International: Digital Investigation* 33 (June 2020): 1–7, https://doi.org/10.1016/J.FSIDI.2019.200891.

identified, recovering illicit funds stored in cold wallets (offline digital storage) or decentralized vaults is beyond the reach of most legal systems.[24] According to a 2022 Interpol report, over $1 billion in crypto-assets connected to corruption and fraud cases remain unrecoverable due to lack of legal mechanisms and forensic capacity in the countries involved.

The challenges are particularly acute in developing countries, where legal systems and institutional infrastructure remain underprepared to address crimes involving blockchain technology. Most anti-corruption laws and evidentiary rules were drafted before the emergence of digital assets, and therefore fail to capture the unique characteristics of blockchain-based data. In Indonesia, for example, the Criminal Procedure Code (Kitab Undang-Undang Hukum Acara Pidana or KUHAP) adheres to a traditional classification of evidence as set forth in Pasal 184 ayat (1) KUHAP, which recognizes only five categories of valid evidence: (a) witness testimony (keterangan saksi), (b) expert testimony (keterangan ahli), (c) documents (surat), (d) indications (petunjuk), and (e) defendant's statement (keterangan terdakwa). This taxonomy leaves little room for the direct recognition of blockchain-derived proof, such as transaction hashes, smart contract records, or digital wallet identifiers, which do not easily fit within these rigid categories. To some extent, the Indonesian Law on Electronic Information and Transactions (ITE Law) provides a broader evidentiary foundation. Pasal 5 ayat (1) UU ITE affirms that "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah" ("Electronic Information and/or Electronic Documents and/or their printouts constitute valid legal evidence"). Furthermore, Pasal 5 ayat (2) UU ITE explicitly states that such electronic evidence shall be treated the same as other legal evidence recognized under KUHAP. However, the law's formulation does not explicitly extend to

[24] Tziakouris, "Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective."

decentralized and anonymized data, which are typical of blockchain systems. Unlike conventional electronic records (emails, databases, or digitized documents) that can be clearly attributed to a party, blockchain data often involve pseudonymous addresses and decentralized validation processes, creating interpretive and practical challenges in evidentiary acceptance. This normative gap creates uncertainty in cases of crypto-based corruption or money laundering. For instance, if an investigator uncovers a series of suspicious Ethereum transactions linked to bribe payments, the technical data (hashes, wallet addresses, and smart contract logs) may be probative but face obstacles in being classified as surat (documents) under Pasal 187 KUHAP or as valid petunjuk (indications) under Pasal 188 KUHAP, given the lack of clear statutory recognition. While courts could attempt to analogize blockchain records to electronic documents under the ITE Law, the absence of explicit acknowledgment of blockchain's decentralized nature could weaken the evidentiary weight assigned to such proof.

Moreover, judicial actors judges, prosecutors, and defense attorneys often lack the digital literacy required to interpret or evaluate blockchain-based evidence effectively. In many cases, prosecutors are unable to present crypto-forensic evidence in a manner that meets the evidentiary threshold due to the absence of statutory guidelines, procedural safeguards, or judicial precedents. Even when digital transaction records are available, defense lawyers may challenge their admissibility based on chain-of-custody concerns or the difficulty in authenticating decentralized data under existing procedural norms. The lack of institutional training and standardized forensic protocols further compounds the uncertainty, leading to judicial reluctance to rely on such evidence.

This shift in criminal modus operandi also reshapes the architecture of evidentiary systems themselves. Legal traditions rooted in paper-based documentation and direct testimony are now confronted with machine-generated, automated, and algorithmically validated records. Blockchain evidence is not "written" in the traditional sense, but rather encoded in cryptographic formats and logged into distributed databases.[25] For this reason, conventional forensic methods such as signature analysis, handwriting verification, or banking correspondence audits become irrelevant. Instead, new expertise in data analysis, digital cryptography, and chain-of-custody verification must be developed and embedded within criminal justice institutions.

The global nature of cryptocurrency transactions introduces further evidentiary complexity due to jurisdictional fragmentation. Crypto-based corruption often involves actors, platforms, and wallets located in multiple legal territories.[26] A bribe paid in Bitcoin in Jakarta may be laundered through a mixing service hosted in Russia and then stored in a cold wallet in Switzerland. To build a prosecutable case, investigators must collect evidence across borders, which typically requires mutual legal assistance treaties (MLATs), international cooperation, and data-sharing agreements.[27] However, most developing countries lack the bilateral or multilateral instruments needed to access blockchain data held abroad or by foreign exchanges. Even when cooperation is possible, the latency of cross-border legal communication undermines the real-time nature of blockchain transactions, allowing illicit assets to dissipate long before evidence is gathered.

[25] David Billard, "Blockchain-Based Digital Evidence Inventory," *Journal of Advances in Information Technology* 10, no. 2 (May 2019): 41–47, https://doi.org/10.12720/JAIT.10.2.41-47.

[26] Casey Watters, "When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment," *Laws* 12, no. 2 (April 2023): 1–16, https://doi.org/10.3390/LAWS12020033.

[27] Alexander A. Berengaut and Lars Lensdorf, "The CLOUD Act at Home and Abroad," *Computer Law Review International* 20, no. 4 (August 2019): 111–17, https://doi.org/10.9785/CRI-2019-200404.

The rise of decentralized finance (DeFi) and non-custodial platforms further erodes the effectiveness of existing evidentiary practices. Unlike centralized exchanges that require Know-Your-Customer (KYC) protocols, DeFi platforms allow users to swap assets, earn interest, and move funds without providing legal identity.[28] These platforms are governed by smart contracts rather than corporate entities, making legal enforcement or compliance virtually impossible. As a result, even when authorities identify illegal activity, they often cannot compel a response or cooperation from the platforms involved. In evidentiary terms, this creates a vacuum: transactions exist and can be publicly verified, but the means to attribute them to a specific legal actor are absent.

Complicating matters further is the evolving landscape of tokenization and digital asset innovation. Increasingly, illicit proceeds are not merely stored as cryptocurrency but are converted into *non-fungible tokens (NFTs)*, *stablecoins*, or even *wrapped tokens* that are harder to trace due to their movement across multiple blockchains.[29] The fragmentation of digital assets across layer-1 and layer-2 protocols complicates forensic reconstruction and requires multi-chain investigative capacity. For example, a corrupt official may transfer Ethereum-based tokens to Binance Smart Chain, convert them to privacy tokens, and then move them to a gaming platform or virtual real estate environment. Each step further distances the transaction from traceable evidence, complicating admissibility and relevance under evidentiary rules.

Another important dimension is the lack of international standards regarding blockchain-based evidence. While organizations such as the Financial Action Task Force (FATF) have issued recommendations on

[28] Dirk Andreas Zetzsche, Douglas W. Arner, and Ross P. Buckley, "Decentralized Finance (DeFi)," *SSRN Electronic Journal*, September 2020, 1–32, https://doi.org/10.2139/SSRN.3539194.

[29] Dimitris Kafteranis, Huseyin Unozkan, and Umut Turksen, "Know Your NFTS," *International Journal of Law in Changing World* 2, no. 3 (November 2023): 18–51, https://doi.org/10.54934/IJLCW.V2I3.57.

virtual asset service providers (VASPs) and suspicious transaction reporting, there is no global framework for evaluating blockchain evidence in court.[30] This leaves judges and legal practitioners in developing countries without benchmarks for authenticity, reliability, or probative value. Unlike fingerprint analysis or DNA evidence which have internationally accepted forensic protocols blockchain forensics remains fragmented, proprietary, and inconsistently applied. Some tools like Chainalysis Reactor or Elliptic Forensics are widely used in the West but are inaccessible or cost-prohibitive for institutions in the Global South. In sum, the rise of crypto-based corruption is not merely a shift in criminal behavior it is a structural disruption to evidentiary systems rooted in 20th-century legal models. The opacity, speed, and jurisdictional ambiguity introduced by blockchain transactions challenge the foundations of legal attribution, asset recovery, and admissibility of proof. While the technological landscape continues to evolve, the law struggles to keep pace, especially in resource-constrained settings. Developing countries thus face an urgent need to adapt their evidentiary rules, institutional capacities, and forensic methodologies to address a form of corruption that is increasingly decentralized, digitized, and difficult to prosecute using conventional means.

B. Blockchain Forensics as a Technological Tool in Modern Criminal Investigations

Investigation into crypto-enabled crimes ranging from money laundering to illicit finance and modern corruption now heavily relies on a specialized discipline known as blockchain forensics. This discipline leverages the inherent transparency and immutability of public and private blockchain ledgers to unravel complex transactions and trace the movement of digital assets across a global, decentralized infrastructure. Unlike traditional

[30] Lukas König et al., “Comparing Blockchain Standards and Recommendations,” *Future Internet* 12, no. 12 (December 2020): 1–17, https://doi.org/10.3390/FI12120222.

financial or document-based investigations, blockchain forensics is uniquely designed to crack pseudonymous transaction systems by linking wallet activity to real-world identities through a combination of on-chain analysis, heuristic assessments, and cross-referencing with off-chain data sources.

At its core, blockchain forensics begins with address clustering, a method that groups individual wallet addresses controlled by the same entity. By analyzing patterns such as shared inputs or concurrent transactions, investigators can build clusters of addresses that correlate likely to the same actor. These clusters form the basis for mapping funds flow across the blockchain. This mapping relies heavily on transaction graph analysis, which employs graph theory to detect the pathways chains of transactions that move illicit funds from one wallet to another. In corruption prosecutions, this enables investigators to follow the money from a disputed public contract or electoral financing, through multiple wallets, mixers, or exchanges, until it eventually reaches a point where attribution can be made.

A key technical element in this forensic work is transaction hashing. Every blockchain transaction is identified by a cryptographic hash a unique digital fingerprint that permanently ties a transaction to a specific block in the chain. Hashes are essential for verifying the integrity and chronological sequence of transactions, as they remain immutable once embedded in a confirmed block.[31] These hashes also aid in constructing immutable audit trails, which investigators can present in a court of law as proof of the occurrence and authenticity of specific transactions. When combined with

[31] Gregory S. Wales et al., "Multimedia Stream Hashing: A Forensic Method for Content Verification," *Journal of Forensic Sciences* 68, no. 1 (January 2023): 289–300, https://doi.org/10.1111/1556-4029.15148;WGROUP:STRING:PUBLICATION.

timestamp data, transactions can be placed in precise chronological context, reinforcing their relevance to investigative narratives.

Wallet attribution marks another pivotal innovation. With most blockchains preserving user anonymity, identification relies on linking wallets to known individuals or institutions. Blockchain forensic tools employ a range of strategies from following flows into regulated centralized crypto exchanges, which often require *Know-Your-Customer* (KYC) data, to leveraging open source intelligence (OSINT). Publicly available information such as social media profiles, leaked data, or metadata from phishing campaigns can all contribute clues. In corruption cases, this means tracing illicit funds to accounts held by public officials or shell companies, providing critical links between digital activity and judicially relevant actors.

To execute these complex tasks at scale, specialized platforms have emerged. Chainalysis offers products like Reactor for visual analytics and KYT for AML screening, enabling investigators to spot patterns of suspicious activity in real time. Elliptic adds capabilities to identify high-risk wallets especially on less common chains and to perform forensic analysis across emerging tokens and DeFi protocols. Meanwhile, CipherTrace brings a unique focus on anti-money laundering compliance, offering rule-based risk scoring and end-to-endensics. These tools differ in scope and technique, but they share common features: transaction clustering, risk scoring, multi-chain tracing, and wallet entity profiling, all anchored in secure data collection, chain-of-custody preservation, and forensic reporting.

The emergence of cross-chain forensic capabilities has marked a critical evolution in investigative power. Criminals frequently engage in chain hopping transferring crypto assets between multiple blockchains (e.g., from Ethereum to Binance Smart Chain, then to Monero) to dissipate traceability and exploit network fragmentation. Advanced forensic tools can reconcile transactions across varying ledgers, reconstruct fund chains, and identify the different "hops" in illicit fund trajectories. Techniques such as peel chains where small test amounts are sent before the major sum and dusting attacks sending minuscule amounts to expose wallet connections can now be detected through analytical heuristics built into forensic platforms. However, not all cryptographic techniques are accessible to forensic analysis. Services such as crypto mixers (e.g. Tornado Cash) deliberately muddle trail clarity by aggregating multiple users' funds, mixing them, and distributing them across diverse addresses to break transparent flow. Similarly, privacy coins like Monero, Zcash, and others employ stealth addresses and ring signatures to conceal sender, receiver, and amounts effectively anonymizing transactions.[32] These mechanisms pose significant challenges, even to sophisticated forensic platforms, and often necessitate legal recourse such as targeted subpoenas, cooperation from node operators, or multilayered source triangulation with OSINT.

Another dimension is the technical challenge of verifying forensic findings for court use. Transcripts from blockchain forensics must meet evidentiary standards: they require documented chain-of-custody, methodical preservation procedures, and the ability to withstand defense scrutiny. This entails secure collection often pulling raw data from nodes or archive services certifying it against tampering through cryptographic signing, and building robust reports detailing the analytical methods used. In cross-jurisdictional scenarios, investigators must also navigate data access restrictions and legal standards that may vary between countries. Weak chain-of-custody can invalidate even the most compelling forensic findings in a courtroom.

[32] Edward Henry Young et al., "Evaluating Tooling and Methodology When Analysing Bitcoin Mixing Services after Forensic Seizure," *2021 International Conference on Data Analytics for Business and Industry, ICDABI 2021*, 2021, 650–54, https://doi.org/10.1109/ICDABI53623.2021.9655843.

Despite these limitations, blockchain forensics remains a powerful investigatory tool. Law enforcement agencies must pair technical capacity with legal readiness: investigators must be trained in deriving and interpreting on-chain intelligence; prosecutors must understand how to integrate blockchain data into case narratives; and forensic experts must articulate complex technical processes in a legally coherent and accessible manner. Collaboration across sectors public prosecutors, tech companies, crypto exchanges, cybersecurity firms, and international law enforcement is essential to obtain subpoenaed data, contextualized insights, and timely intervention across network borders.

In corruption investigations, blockchain forensic methods are now instrumental in several key stages: uncovering suspect transfers (tracing and clustering), verifying illicit funds (hash and timestamp confirmation), linking transfers to specific actors (wallet attribution), and constructing a narrative backed by transaction evidence. While not a panacea, these tools address a critical gap in investigative arsenals. As corruption evolves leveraging DeFi, NFTs, stablecoins, and even smart contract-based token logic for concealment blockchain forensics will need to adapt, integrating AI for anomaly detection, enhancing OSINT integration, and embedding multi-chain analysis into mainstream digital forensic practice.

C. Comparative Legal Frameworks for Admitting Blockchain Evidence in Criminal Courts

The increasing reliance on digital assets in illicit activities including corruption, fraud, and money laundering has compelled legal systems worldwide to reconsider how evidence derived from decentralized technologies, such as blockchain, can be admitted in criminal proceedings.[33]

[33] Liza Ahmad et al., "Blockchain-Based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management," in *ACM International Conference Proceeding Series* (Association for

However, the degree to which blockchain evidence is legally recognized and procedurally integrated varies significantly across jurisdictions. This section offers a comparative analysis of how blockchain-derived evidence is treated within the evidentiary frameworks of both developed countries specifically the United States and Estonia and a developing country, Indonesia. The aim is to explore the regulatory, procedural, and institutional factors that either facilitate or hinder the admissibility of blockchain evidence in criminal courts, with particular attention to cases involving crypto-based corruption.

In the United States, the legal system has demonstrated a relatively adaptive and pragmatic approach to digital evidence, including that derived from blockchain transactions. As a common law jurisdiction, the U.S. permits considerable discretion by judges in determining the admissibility of novel forms of evidence, provided they meet criteria such as relevance, authenticity, reliability, and compliance with procedural safeguards. Under the Federal Rules of Evidence (FRE) especially Rule 901 a party seeking to introduce evidence must present sufficient evidence to support a finding that the item is what the proponent claims it to be. In practice, blockchain transaction records, wallet addresses, and metadata such as timestamps and hash values can be admitted as evidence if supported by expert testimony and forensic validation.

Federal agencies such as the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and the Internal Revenue Service (IRS) regularly work with blockchain forensic firms such as Chainalysis, Elliptic, and CipherTrace to trace illicit crypto flows in corruption, sanctions evasion, and money laundering cases.[34] These firms provide visual analysis

Computing Machinery, 2020), 1–6, https://doi.org/10.1145/3407023.3409199;CSUBTYPE:STRING:CONFERENCE.

[34] Jain et al., “Blockchain Empowerment in Sanctions and AML Compliance: A Transparent Approach.”

tools, risk scores, and wallet attribution services that can link pseudonymous wallet activity to real-world individuals or entities. Once corroborated by off-chain data, including Know Your Customer (KYC) documentation from centralized exchanges, blockchain evidence is frequently used in indictments and has been accepted in federal courts. Importantly, the U.S. also enforces robust AML (Anti-Money Laundering) and KYC obligations through agencies such as FinCEN, which enhances the traceability and forensic usability of blockchain transactions within its jurisdiction. Another advantage the United States holds is its ability to issue enforceable subpoenas to domestic cryptocurrency exchanges and data custodians. Many high-profile corruption cases involving digital assets have succeeded in the U.S. legal system due to its strong institutional cooperation, prosecutorial expertise, and judicial willingness to engage with technologically complex evidence. Courts routinely rely on expert witnesses, including digital forensic specialists, to explain the nature and probative value of blockchain records in lay terms, ensuring their alignment with traditional evidentiary standards.

The Estonian approach illustrates how deep institutional integration of blockchain technology can enhance a legal system's responsiveness to digital evidence. Unlike jurisdictions that treat blockchain as a novelty or isolate it within financial regulation, Estonia has embedded blockchain as a core component of its e-governance model.[35] By deploying blockchain in critical sectors such as healthcare, land administration, judicial records, and government audits, Estonia has cultivated both technical capacity and institutional trust in the technology. This systemic use of blockchain has normalized its application and reduced resistance within legal and procedural contexts. As a result, Estonia's judiciary is equipped not only

[35] Silvia Semenzin, David Rozas, and Samer Hassan, "Blockchain-Based Application at a Governmental Level: Disruption or Illusion? The Case of Estonia," *Policy and Society* 41, no. 3 (July 2022): 386–401, https://doi.org/10.1093/POLSOC/PUAC014.

with the technical literacy to interpret blockchain data but also with procedural mechanisms that formally admit such data as valid legal evidence. Hashed transaction records and timestamped metadata, for example, are not treated as peripheral or supplementary, but are central to evidentiary evaluation so long as they adhere to established standards of authenticity, integrity, and chain of custody.[36] Furthermore, the admissibility of smart contract records and blockchain logs within criminal trials reflects a forward-thinking procedural framework that bridges technological sophistication with legal reliability. Estonia's model demonstrates how aligning national digital infrastructure with legal procedural reform creates an ecosystem where blockchain forensics is not merely possible, but practically operational and judicially legitimate. Estonia's legal system represents a pioneering model in integrating blockchain forensics within the broader framework of criminal procedure. Unlike many jurisdictions where digital evidence is often relegated toa supplementary role, Estonia's procedural laws recognize blockchain-based records such as transaction hashes, smart contract logs, and timestamped metadata as primary evidence admissible in court. This elevated evidentiary status is reinforced by the country's robust *e-justice* infrastructure, which enables the digital submission, secure storage, and real-time cross-verification of blockchain records. By incorporating Public Key Infrastructure (PKI), Estonia ensures that the authenticity and integrity of submitted digital evidence are cryptographically verifiable, mitigating the risk of tampering or forgery. Institutionally, Estonia has built the necessary technical foundation to operationalize blockchain forensics. Under the oversight of the Ministry of Justice, digital forensic laboratories are staffed with dedicated blockchain analysts who possess the capability to trace on-chain transactions, attribute wallet ownership using Open-Source

[36] Pablo López-Aguilar and Agusti Solanas, "An Effective Approach to the Cross-Border Exchange of Digital Evidence Using Blockchain," *Lecture Notes in Electrical Engineering* 866 (2022): 132–38, https://doi.org/10.1007/978-3-030-95498-7_19.

Intelligence (OSINT) techniques, and evaluate the structural integrity of decentralized data. These experts play a critical role in transforming raw blockchain data into legally actionable forms suitable for prosecution.

In parallel, Estonia invests continuously in judicial capacity-building, ensuring that judges and legal professionals are not only aware of emerging technologies but also trained in their procedural implications. Judicial education programs regularly cover topics such as crypto-assets, distributed ledger technologies, and the legal treatment of digital financial crimes. This ongoing training ensures that courtroom decisions remain aligned with technological realities, closing the gap between legal reasoning and digital complexity.[37] Estonia's approach offers a cohesive model in which technological integration, legal reform, and institutional readiness converge to enable a responsive and future-proof criminal justice system. What distinguishes Estonia is its ability to harmonize legal, technological, and institutional frameworks. Judges, prosecutors, and investigators operate within a unified digital ecosystem that enables fast, secure, and procedurally consistent management of blockchain evidence. International cooperation mechanisms, such as participation in Eurojust and Europol, further enhance its capacity to handle cross-border digital crimes including crypto-related corruption. Estonia's proactive legislation, such as the Digital Evidence Act, explicitly accommodates new forms of digital records and sets the standard for evidentiary admissibility based on data integrity, auditability, and forensic traceability.

In stark contrast, Indonesia represents the typical challenges faced by developing countries in adapting legal systems to blockchain evidence. The Indonesian Code of Criminal Procedure (KUHAP) still adheres to a traditional classification of five forms of admissible evidence: witness

[37] Katrin Nyman Metcalf, "How to Build E-Governance in a Digital Society: The Case of Estonia," *Revista Catalana de Dret Públic*, 2019, 1–7.

testimony, expert opinion, documentary evidence, indication, and defendant confession. Although the Law on Electronic Information and Transactions (ITE Law) recognizes electronic and digital documents as valid evidence, the law remains vague on the specifics of blockchain data such as how to verify transaction hashes, authenticate wallet addresses, or handle metadata from smart contracts. This lack of specificity results in substantial legal ambiguity regarding the admissibility of blockchain-based evidence.

Another important legal framework in the Indonesian context is Law Number 31 of 1999 in conjunction with Law Number 20 of 2001 on the Eradication of Corruption. Although the modus operandi of perpetrators may involve the use of crypto assets to conceal or transfer the proceeds of crime, the core offense remains corrupt practices as regulated under provisions concerning bribery, gratuities, embezzlement, and abuse of authority. This means that crypto-based corruption is still subject to the lex specialis of anti-corruption law. The main issue does not lie in the absence of criminal norms, but rather in evidentiary challenges, particularly regarding the recognition of blockchain data as admissible evidence. Therefore, legal reform should not be confined merely to the Criminal Procedure Code (KUHAP) or the Information and Electronic Transactions Law (UU ITE), but must also extend to the harmonization and broader interpretation of evidentiary rules within the Anti-Corruption Law to make them more adaptive to digital transactions.

Institutionally, Indonesia has yet to establish specialized digital forensic labs capable of analyzing blockchain transactions for criminal investigations. Coordination among key law enforcement and regulatory agencies such as the Financial Transaction Reports and Analysis Center (PPATK), the Anti-Corruption Commission (KPK), and the Cyber Crime Unit of the National Police (Bareskrim Siber) is fragmented, and there is no unified framework for managing or authenticating blockchain evidence. This institutional gap severely limits Indonesia's capacity to prosecute crypto-based corruption cases, even when digital transaction data is available.

Moreover, Indonesian courts rarely encounter blockchain evidence, and when they do, judicial unfamiliarity and procedural conservatism often result in its exclusion or dismissal. The absence of national forensic standards for blockchain data such as methods of collection, verification, documentation, and chain of custody prevents law enforcement from presenting blockchain evidence with the level of reliability expected in criminal proceedings. Cross-border cooperation for accessing crypto exchange records or foreign-based data is further hindered by the lack of Mutual Legal Assistance Treaties (MLATs) tailored to blockchain-related crimes.[38]

The comparative analysis makes clear that legal recognition and courtroom admissibility of blockchain evidence are shaped by a confluence of regulatory clarity, institutional readiness, technological infrastructure, and judicial literacy. The United States and Estonia illustrate that successful integration of blockchain evidence is not only a matter of statutory reform but also of cross-sectoral coordination, capacity building, and legal-cultural openness to innovation. Conversely, Indonesia's experience reveals the legal and operational inertia that hampers effective criminal prosecution in the age of digital finance.

To overcome these barriers, developing countries must invest in multi-layered reforms. These include updating criminal procedure codes to explicitly define and regulate blockchain-based evidence, establishing

[38] Anna Maria Osula, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data," *Masaryk University Journal of Law and Technology* 9, no. 1 (June 2015): 43–64, https://doi.org/10.5817/MUJLT2015-1-4.

technical protocols for forensic verification, training judges and prosecutors in crypto-related crimes, and promoting regional legal harmonization to facilitate cross-border cooperation. Only through such holistic measures can jurisdictions ensure that digital evidence derived from blockchain technologies becomes a reliable and admissible component of modern criminal justice systems particularly in the fight against high-level corruption.

D. Designing a Normative and Institutional Model for Blockchain Evidence in Developing Countries

The rapid growth of blockchain-based technologies has significantly transformed the nature of criminal investigations, particularly in corruption-related cases involving digital assets. Unlike traditional financial crimes that rely on bank transfers or physical evidence, illicit activities in the digital economy often utilize cryptocurrencies and decentralized networks, which pose unique challenges for law enforcement.[39] These challenges are especially severe in developing countries, where legal systems are still catching up with the technological complexities of blockchain forensics. In this context, designing a robust legal and institutional model for the effective use of blockchain evidence becomes an urgent necessity, not only to ensure justice in individual cases but also to safeguard the integrity of public institutions from technologically advanced corrupt practices.

At the normative level, most developing countries still rely on outdated criminal procedure codes that fail to accommodate the admissibility of blockchain-based evidence. Legal provisions often do not recognize transaction hashes, smart contract logs, or digital wallet data as

[39] Hiroki Kuzuno and Christian Karam, "Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin," *ECrime Researchers Summit, ECrime*, June 2017, 9–16, https://doi.org/10.1109/ECRIME.2017.7945049.

legitimate forms of proof in criminal trials.[40] This normative gap renders digital evidence procedurally vulnerable and susceptible to exclusion in court. Reforming the law to explicitly classify blockchain artifacts as admissible evidence is therefore the foundational step. Such reforms should include precise definitions of blockchain-based records, authentication requirements, and rules for preserving the integrity and chain of custody of digital data throughout an investigation and trial. Without these legal anchors, courts remain reluctant or ill-equipped to process technologically complex but highly probative evidence.

However, legal recognition alone is insufficient without strong institutional capacity to support the collection, analysis, and use of blockchain evidence. Many developing countries lack specialized digital forensic units capable of tracking crypto transactions or de-anonymizing blockchain activity. Establishing national laboratories with technical teams trained in blockchain analytics is crucial. These institutions must be equipped with forensic tools such as Chainalysis, Elliptic, or CipherTrace to trace the movement of digital assets across decentralized networks. In parallel, there must be protocols in place to ensure that the data extracted from these tools is translated into legally acceptable formats, supported by detailed reports, verifiable logs, and expert certifications.[41]

Human capacity is equally essential. Investigators, prosecutors, judges, and defense lawyers need comprehensive training to understand how blockchain technologies work and how to interpret evidence derived from them. Without this foundational literacy, legal actors cannot effectively assess the authenticity, reliability, or contextual meaning of blockchain evidence. Judicial training institutions must therefore introduce

[40] Gorizky and Supardi, "Blockchain as Electronic Evidence Against Crypto Crimes in Indonesia," *Media Iuris* 7, no. 3 (October 2024): 545–62, https://doi.org/10.20473/MI.V7I3.56116.

[41] Lilita Infante et al., "Recovery CAT: A Digital Forensics Tool for Cryptocurrency Investigations," in *12th International Symposium on Digital Forensics and Security, ISDFS 2024* (Institute of Electrical and Electronics Engineers Inc., 2024), 1–5, https://doi.org/10.1109/ISDFS60797.2024.10527279.

new curricula that integrate technical modules on digital forensics, crypto-assets, and the evidentiary use of decentralized data structures. This will help ensure that due process is upheld while accommodating the realities of modern crime.

Beyond training, there is a critical need to institutionalize standard operating procedures (SOPs) for handling blockchain evidence. These SOPs must govern every stage of the evidentiary process from collection and storage to courtroom presentation while maintaining forensic soundness and legal validity. Drawing inspiration from standards issued by organizations like the U.S. NIST or the European Union Agency for Cybersecurity (ENISA), such procedures should provide detailed guidance on how to seize blockchain data, maintain its digital chain of custody, and prepare it for judicial review. In the absence of such standardized methods, the credibility and admissibility of blockchain evidence will remain contested in courts.[42]

The inherently cross-border nature of blockchain transactions also necessitates international legal cooperation. Many perpetrators of corruption use blockchain precisely because of its pseudonymity and its ability to move assets across borders with little oversight. Thus, countries must include blockchain evidence within the scope of Mutual Legal Assistance Treaties (MLATs) and actively participate in international frameworks such as the United Nations Convention against Corruption (UNCAC). These mechanisms enable countries to request exchange records, forensic data, or expert assistance from jurisdictions where crypto exchanges and data custodians are based. Without such transnational cooperation, local investigations into crypto-facilitated corruption may be

[42] G Pestana, W Antunes, and J Carvalho, "Digital Chain of Custody Operational Framework," in *2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense)*, 2023, 417–22, https://doi.org/10.1109/TechDefense59795.2023.10380890.

rendered ineffective.

To operationalize these treaties, governments should establish digital evidence coordination units within their ministries or prosecutorial offices. These units would serve as points of contact for cross-border requests and ensure that data sharing adheres to legal, technical, and privacy standards. They would also liaise with international forensic service providers and facilitate cooperation with blockchain analytics firms operating across multiple jurisdictions. In addition, the role of the private sector is indispensable. Many exchanges, custodial wallet providers, and blockchain platforms hold data that can aid criminal investigations, but they often operate under minimal regulatory obligations in developing countries. Governments must impose stronger legal duties on these actors such as Know Your Customer (KYC) and data retention policies and create mechanisms for compliance monitoring. Establishing cooperative public–private partnerships (PPPs) can also bridge the knowledge and infrastructure gap, enabling law enforcement to benefit from cutting-edge private-sector expertise and threat intelligence.

Moreover, regional collaboration offers a powerful strategy for capacity building. Regional organizations like ASEAN, the African Union, or the Organization of American States can initiate shared frameworks for crypto evidence management, harmonize laws, and develop joint training programs. Such regional solidarity is essential to counteract jurisdictional arbitrage by bad actors who exploit legal inconsistencies across borders. Ultimately, constructing a normative and institutional model for blockchain evidence in developing countries is not merely a question of technology it is a multidimensional reform agenda that touches upon legal modernization, institutional development, international diplomacy, and inter-sectoral cooperation. If properly executed, this model can enable developing nations to confront high-tech corruption with resilience, legal credibility, and international legitimacy. Conversely, failure to adapt will only widen the impunity gap, allowing perpetrators of crypto-based corruption to evade justice by operating in the blind spots of outdated criminal systems.

In addition to long-term structural reforms, developing countries such as Indonesia also need short-term, pragmatic strategies to respond to the rapid adoption of crypto assets. These swift measures may include utilizing the Financial Transaction Reports and Analysis Center (PPATK) to conduct crypto-based suspicious transaction profiling, strengthening ad hoc coordination between the Corruption Eradication Commission (KPK), the National Police, and Bappebti for data sharing, as well as establishing temporary technical cooperation with global blockchain forensics firms such as Chainalysis or Elliptic through memorandums of understanding. At the same time, the Financial Services Authority (OJK) and Bappebti can tighten KYC/AML requirements for local exchanges, which serve as the main entry point for crypto transactions. Additionally, short and small-scale training programs for investigators, prosecutors, and judges on basic wallet tracing techniques may serve as an emergency solution to prevent law enforcement from falling behind. Through this approach, Indonesia can construct a practical bridge toward an ideal legal model while maintaining the effectiveness of anti-corruption efforts in the digital era.

Conclusion

The rise of blockchain technology has introduced a new frontier in the digitalization of criminal conduct, particularly in corruption cases that involve crypto-assets and decentralized transactions. This phenomenon presents significant evidentiary challenges, especially for developing countries whose legal and institutional frameworks are not yet fully equipped to confront technologically sophisticated crimes. This research underscores that while blockchain forensics holds considerable promise as a modern investigative tool through techniques such as transaction tracing, hashing, and wallet attribution the most critical challenge lies in how such evidence can be admitted, interpreted, and procedurally managed within criminal justice systems. Normative unpreparedness remains a fundamental issue, as many criminal procedural laws in developing countries fail to explicitly recognize or regulate the authentication and admissibility of blockchain-based evidence. This legal vacuum is exacerbated by the lack of institutional infrastructure, such as digital forensic laboratories and investigative bodies capable of processing blockchain data in a forensically sound and legally valid manner. Compounding this is the limited technological literacy among law enforcement, prosecutors, judges, and legal practitioners, as well as the absence of standardized operating procedures for the handling and presentation of blockchain evidence in court. Moreover, the transnational nature of blockchain transactions poses additional legal and logistical obstacles, particularly in jurisdictions where international legal cooperation remains weak or outdated. Offenders can exploit jurisdictional gaps to obscure illicit flows of funds, making it difficult to trace or seize assets without cross-border collaboration. This highlights the urgent need for developing countries to modernize their Mutual Legal Assistance frameworks and participate actively in international instruments such as the United Nations Convention against Corruption (UNCAC), with specific adaptations to accommodate blockchain-based digital evidence. This research proposes the formulation of a normative and institutional model tailored for developing countries that integrates legal reform, institutional strengthening, capacity-building initiatives, public–private partnerships, and regional and global cooperation. Such a model must be forward-looking, adaptable, and grounded in the principles of due process and evidentiary integrity. Legal reforms should not only recognize blockchain artifacts as valid evidence but also outline clear rules for their verification, handling, and use in judicial proceedings. Ultimately, blockchain forensics is not merely a technological issue but a multidimensional legal reform agenda. For developing countries, it presents both a challenge and an opportunity to enhance the transparency, efficiency, and resilience of their legal systems in combating corruption in the digital age. Countries that fail to respond to these shifts risk being left behind, while those that act decisively may emerge as leaders in the global fight against technologically enabled corruption. Bridging the evidentiary gap is not only essential for ensuring accountability but also for reaffirming the rule of law in the face of rapidly evolving digital threats.

References

Agarwal, Udit, Vinay Rishiwal, Sudeep Tanwar, and Mano Yadav. "Blockchain and Crypto Forensics: Investigating Crypto Frauds." *International Journal of Network Management* 34, no. 2 (March 2024): e2255. https://doi.org/10.1002/NEM.2255;WGROUP:STRING:PUBLICATION.

Ahmad, Liza, Salam Khanji, Farkhund Iqbal, and Faouzi Kamoun. "Blockchain-Based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management." In *ACM International Conference Proceeding Series*, 1–6. Association for Computing Machinery, 2020. https://doi.org/10.1145/3407023.3409199;CSUBTYPE:STRING:CONFERENCE.

Akhmad, Akhmad, Zico Junius Fernando, and Papontee Teeraphan. "Unmasking Illicit Enrichment: A Comparative Analysis of Wealth Acquisition Under Indonesian, Thailand and Islamic Law." *Journal of Indonesian Legal Studies* 8, no. 2 (2023): 899–934. https://doi.org/10.15294/jils.v8i2.69332.

Albrecht, Chad, Kristopher Mc Kay Duffin, Steven Hawkins, and Victor Manuel Morales Rocha. "The Use of Cryptocurrencies in the Money Laundering Process." *Journal of Money Laundering Control* 22, no. 2 (May 2019): 210–16. https://doi.org/10.1108/JMLC-12-2017-0074/FULL/XML.

Berdiev, Aziz N., Rajeev K. Goel, and James W. Saunoris. "Global Cryptocurrency Use, Corruption, and the Shadow Economy: New Insights into the Underlying Linkages." *American Journal of*

Economics and Sociology 83, no. 3 (May 2024): 609–29. https://doi.org/10.1111/AJES.12566.

Berengaut, Alexander A., and Lars Lensdorf. "The CLOUD Act at Home and Abroad." *Computer Law Review International* 20, no. 4 (August 2019): 111–17. https://doi.org/10.9785/CRI-2019-200404.

Billard, David. "Blockchain-Based Digital Evidence Inventory." *Journal of Advances in Information Technology* 10, no. 2 (May 2019): 41–47. https://doi.org/10.12720/JAIT.10.2.41-47.

Elmougy, Youssef, and Ling Liu. "Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics." *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* 1 (May 2023): 3979–90. https://doi.org/10.1145/3580305.3599803.

Endriana, Muchamad Satria, Yusriadi, Ana Silviana, and Zico Junius Fernando. "Green Financial Crime: Expose About Financial Crime In The Environment And Renewable Energy World." *IOP Conference Series: Earth and Environmental Science* 1270, no. 1 (December 2023): 012012. https://doi.org/10.1088/1755-1315/1270/1/012012.

Gorizky, and Supardi. "Blockchain as Electronic Evidence Against Crypto Crimes in Indonesia." *Media Iuris* 7, no. 3 (October 2024): 545–62. https://doi.org/10.20473/MI.V7I3.56116.

Ibrahimi, Adrianit, and Besa Arifi. "Corruption and Cryptocurrency - Blockchains as Corruption Tools." *Academicus International Scientific Journal* 26 (July 2022): 93–103. https://doi.org/10.7336/ACADEMICUS.2022.26.06.

Infante, Lilita, Roger A. Hallman, John Hays, Evelyn Cronnon, and Uri Stav. "Recovery CAT: A Digital Forensics Tool for Cryptocurrency Investigations." In *12th International Symposium on Digital Forensics and Security, ISDFS 2024*, 1–5. Institute of Electrical and Electronics Engineers Inc., 2024. https://doi.org/10.1109/ISDFS60797.2024.10527279.

Jain, Varun, Anandaganesh Balakrishnan, Pradeep Chintale, Sivanagaraju Gadiparthi, and Madhavi Najana. "Blockchain Empowerment in Sanctions and AML Compliance: A Transparent Approach." *International Journal of Computer Trends and Technology* 72, no. 5

(May 2024): 11–26. https://doi.org/10.14445/22312803/IJCTT-V72I5P102.

Kafteranis, Dimitris, Huseyin Unozkan, and Umut Turksen. "Know Your NFTS." *International Journal of Law in Changing World* 2, no. 3 (November 2023): 18–51. https://doi.org/10.54934/IJLCW.V2I3.57.

Kaplan, Ahmet. "Cryptocurrency and Corruption: Auditing with Blockchain BT - Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities." In *Auditing Ecosystem and Strategic Accounting in the Digital Era*, edited by Tamer Aksoy and Umit Hacioglu, 325–38. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-72628-7_15.

Karianga, Hendra, and Zico Junius Fernando. "The Damage of the Shadow Economy: The Urgency of Addressing Foreign Bribery in Indonesia." *Pakistan Journal of Criminology* 16, no. 2 (April 2024): 783–96. https://doi.org/10.62271/PJC.16.2.783.796.

Koerhuis, Wiebe, Tahar Kechadi, and Nhien An Le-Khac. "Forensic Analysis of Privacy-Oriented Cryptocurrencies." *Forensic Science International: Digital Investigation* 33 (June 2020): 1–7. https://doi.org/10.1016/J.FSIDI.2019.200891.

Kogias, G, Panagiotis A Karkazis, Michael G Xevgenis, Hany F Atlam, Ndifon Ekuri, Muhammad Ajmal Azad, and Harjinder Singh Lallie. "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions." *Electronics 2024, Vol. 13, Page 3568* 13, no. 17 (September 2024): 1–37. https://doi.org/10.3390/ELECTRONICS13173568.

König, Lukas, Yuliia Korobeinikova, Simon Tjoa, and Peter Kieseberg. "Comparing Blockchain Standards and Recommendations." *Future Internet* 12, no. 12 (December 2020): 1–17. https://doi.org/10.3390/FI12120222.

Kuzuno, Hiroki, and Christian Karam. "Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin." *ECrime Researchers Summit, ECrime*, June 2017, 9–16. https://doi.org/10.1109/ECRIME.2017.7945049.

López-Aguilar, Pablo, and Agusti Solanas. "An Effective Approach to the

Cross-Border Exchange of Digital Evidence Using Blockchain." *Lecture Notes in Electrical Engineering* 866 (2022): 132–38. https://doi.org/10.1007/978-3-030-95498-7_19.

Metcalf, Katrin Nyman. "How to Build E-Governance in a Digital Society: The Case of Estonia." *Revista Catalana de Dret Públic*, 2019, 1–7.

Negi, Shaurya, Akshay Kumar, Shweta Pandey, Nagendar Yamsani, Rajesh Singh, and Rajat Balyan. "The Preservation of Digital Evidences Through Blockchain Technology." *Proceedings - 2023 IEEE World Conference on Applied Intelligence and Computing, AIC 2023*, 2023, 954–58. https://doi.org/10.1109/AIC57670.2023.10263968.

Osula, Anna Maria. "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data." *Masaryk University Journal of Law and Technology* 9, no. 1 (June 2015): 43–64. https://doi.org/10.5817/MUJLT2015-1-4.

Pestana, G, W Antunes, and J Carvalho. "Digital Chain of Custody Operational Framework." In *2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense)*, 417–22, 2023. https://doi.org/10.1109/TechDefense59795.2023.10380890.

Ratul, Md Hasibul Alam, Sepideh Mollajafari, and Martin Wynn. "Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution." *Sustainability 2024, Vol. 16, Page 10885* 16, no. 24 (December 2024): 1–20. https://doi.org/10.3390/SU162410885.

Salisu, Saminu, Velitchko Filipov, and Barry Pene. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation." *International Conference on Cyber Warfare and Security* 18, no. 1 (February 2023): 338–47. https://doi.org/10.34190/ICCWS.18.1.947.

Saputro, Rois, Ingrid Pappel, Heiko Vainsalu, Silvia Lips, and Dirk Draheim. "Prerequisites for the Adoption of the X - Road Interoperability and Data Exchange Framework: A Comparative Study." *International Conference on EDemocracy & EGovernment*, April 2020, 216–22. https://doi.org/10.1109/ICEDEG48599.2020.9096704.

Sauni, Herawan, Zico Junius Fernando, David Aprizon Putra, Saivol

Virdaus, and Aris Hardinanto. “Beyond Borders: Shedding Light on Foreign Bribery through an Islamic Legal Lens.” *Al-Istinbath: Jurnal Hukum Islam* 9, no. 2 (September 2024): 649–78. https://doi.org/10.29240/JHI.V9I2.9752.

Semenzin, Silvia, David Rozas, and Samer Hassan. “Blockchain-Based Application at a Governmental Level: Disruption or Illusion? The Case of Estonia.” *Policy and Society* 41, no. 3 (July 2022): 386–401. https://doi.org/10.1093/POLSOC/PUAC014.

Tziakouris, G. “Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective.” *IEEE Security & Privacy* 16, no. 4 (2018): 92–94. https://doi.org/10.1109/MSP.2018.3111243.

Verma, Harsh. “The Impact of Cryptocurrency on Money Laundering Practices.” *African Journal of Commercial Studies* 5, no. 2 (August 2024): 51–60. https://doi.org/10.59413/AJOCS/V5.I.2.1.

Wales, Gregory S., Jeff M. Smith, Douglas S. Lacey, and Catalin Grigoras. “Multimedia Stream Hashing: A Forensic Method for Content Verification.” *Journal of Forensic Sciences* 68, no. 1 (January 2023): 289–300. https://doi.org/10.1111/1556-4029.15148;WGROUP:STRING:PUBLICATION.

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): 1–7. https://doi.org/10.3389/FBLOC.2024.1306058/BIBTEX.

Watters, Casey. “When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment.” *Laws* 12, no. 2 (April 2023): 1–16. https://doi.org/10.3390/LAWS12020033.

Wawrosz, Petr, and Jan Lánský. “Cryptocurrencies and Corruption.” *Ekonomicky Casopis* 69, no. 7 (2021): 687–705. https://doi.org/10.31577/EKONCAS.2021.07.02.

Young, Edward Henry, Christos Chrysoulas, Nikolaos Pitropakis, Pavlos Papadopoulos, and William J. Buchanan. “Evaluating Tooling and Methodology When Analysing Bitcoin Mixing Services after Forensic Seizure.” *2021 International Conference on Data Analytics for Business* *and Industry, ICDABI 2021*, 2021, 650–54. https://doi.org/10.1109/ICDABI53623.2021.9655843.

Zarpala, Lamprini, and Fran Casino. "A Blockchain-Based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario." *Digital Finance* 3, no. 3 (2021): 301–32. https://doi.org/10.1007/s42521-021-00035-5.

Zetzsche, Dirk Andreas, Douglas W. Arner, and Ross P. Buckley. "Decentralized Finance (DeFi)." *SSRN Electronic Journal*, September 2020, 1–32. https://doi.org/10.2139/SSRN.3539194.

Zico Junius Fernando et al. "Preventing Bribery in the Private Sector Through Legal Reform Based on Pancasila." *Cogent Social Sciences* 8, no. 1 (2022): 1–14. https://doi.org/10.1080/23311886.2022.2138906.

***

DECLARATION OF CONFLICTING INTERESTS

The authors states that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

This research received no external funding.

ACKNOWLEDGMENT

We would like to express our deepest gratitude to all individuals and institutions who contributed to the development of this article. In particular, we extend our thanks to the Faculty of Law, Universitas Sultan Ageng Tirtayasa (FH Untirta), for its ongoing support of legal research and academic inquiry. We are especially indebted to the scholars, authors, and researchers whose works spanning books, journal articles, and empirical studies have provided the critical foundation upon which this analysis rests. Their intellectual contributions have played a significant role in shaping the theoretical and comparative perspectives reflected in this study. We also value the insights offered during internal discussions with colleagues and peers, whose thoughtful questions and constructive feedback helped refine the focus and enhance the relevance of our findings. While this article did not involve research with human subjects and therefore did not require ethical approval or Institutional Review Board (IRB) clearance, we maintained our commitment to academic integrity, transparency, and the responsible use of all cited sources. We recognize that every scholarly effort is part of an ongoing conversation, and we sincerely welcome feedback, suggestions, or critiques from readers. It is our hope that this article contributes meaningfully to the discourse on financial crime, governance reform, and legal innovation, and that it encourages further dialogue among academics, practitioners, policymakers, and civil society.

HISTORY OF ARTICLE

Submitted	: June 25, 2025
Revised	: July 21, 2025
Accepted	: October 31, 2025
Published	: November 5, 2025

About Author(s)

Dadang Herli Saputra is a senior lecturer in criminal law at the Faculty of Law, Sultan Ageng Tirtayasa University (Untirta), with a distinguished background as a retired Police Commissioner and extensive expertise in criminal law, policing, and legal forensics. He holds multiple academic degrees, including a Ph.D. in Criminal Law from Universitas Padjadjaran, and several master's degrees in law, public administration, and notarial studies. Over the course of his career, he has served in numerous high-level law enforcement positions and has been actively involved as an expert witness in various criminal proceedings across Indonesia. His academic contributions include a wide range of peer-reviewed publications on criminal justice, cybercrime, financial crimes, and victim protection, and he frequently speaks at national seminars and legal training forums. He has also participated in international comparative legal and policing studies in countries such as the Netherlands, France, Switzerland, and China. Currently, he serves as the Chairman of the Banten Chapter of the Indonesian Society of Criminal Law and Criminology (MAHUPIKI) and is a member of several expert councils in the field of criminal law.

Fardana Kusumah is a prosecutor at the Attorney General's Office of the Republic of Indonesia and is currently pursuing his doctoral studies at Central China Normal University in Wuhan, China. He has more than ten years of experience in law enforcement, particularly in the areas of corruption and intelligence, and has a strong interest in cybercrime and transnational crime. Fardana also holds a CHFI (Computer Hacking Forensic Investigator) certification from EC-Council to support his expertise in handling cybercrime cases. Email: frdnksmh@gmail.com.

This page intentionally left blank