Journal of Law and Legal Reform
Vol. 6 Issue 3 (2025) 1411–1450
DOI: https://doi.org/10.15294/jllr.v6i3.22472
Online since: July 31, 2025

https://journal.unnes.ac.id/journals/jllr

Blockchain and Corporate Criminal Liability: Law Reform and the Technological Revolution in Corporate Accountability

Herlina Manullang [a] ✉, Zico Junius Fernando [b], Asrul Ibrahim Nur [c]

[a] Faculty of Law, Universitas HKBP Nommensen, Indonesia
[b] Faculty of Law, Universitas Bengkulu, Indonesia
[c] Géza-Marton Doctoral School of Legal Studies, University of Debrecen

✉ corresponding email: herlinamanullang@uhn.ac.id

Abstract

The rapid development of blockchain technology is reshaping various dimensions of governance, particularly in strengthening corporate accountability and addressing corporate criminal liability. This paper examines how blockchain, through its inherent features of decentralization, transparency, immutability, and smart contracts, can offer innovative tools to reform legal frameworks governing corporate behavior. These features enable more robust compliance monitoring, secure and tamper-proof evidence handling, and efficient fraud detection mechanisms. By integrating blockchain into corporate governance systems, companies can enhance regulatory compliance and reduce the risks of misconduct. Smart contracts, in particular, allow the automation of enforcement procedures, minimizing human error and corruption while increasing legal predictability. This paper further explores how blockchain facilitates proactive legal oversight and redefines how liability is tracked and enforced within corporate structures. Despite its potential, the adoption of blockchain within legal systems faces several challenges, including regulatory ambiguity, privacy issues, and the necessity for international legal harmonization. To illustrate the real-world application of blockchain in legal reforms, this study presents comparative case analyses from jurisdictions that

are at the forefront of blockchain regulation and implementation in corporate governance. Ultimately, this paper argues that blockchain serves not merely as a technological tool but as a catalyst for transforming the philosophy and practice of corporate criminal liability. To realize its full potential, collaborative efforts among legislators, regulators, and private sector actors are essential. The paper concludes with strategic recommendations for incorporating blockchain into corporate criminal law, aiming to enhance transparency, ensure compliance, and strengthen governance frameworks in line with technological progress.

Keywords
Blockchain, Corporate Criminal Liability, Law Reform, Corporate Accountability, Smart Contracts.

Introduction

Over the past few decades, advancements in digital technology have transformed many aspects of life, including how companies operate and interact with stakeholders. Digitalization has accelerated global economic growth by enabling more efficient transactions, greater transparency, and broader access to international markets.[1] However, these developments have also introduced new challenges, particularly in terms of corporate accountability and criminal liability. As digital technology becomes more sophisticated, corporations can manage vast amounts of data. Still, at the same time, it creates opportunities for illegal practices that are difficult for regulators and law enforcement agencies to detect. Corporate crimes have become increasingly complex with the growing use of digital technology in business operations. Various types of violations, such as financial statement manipulation, money laundering, tax evasion, and digital fraud, are becoming more challenging to identify and prove in court.[2] Corporations can exploit technology to obscure financial flows, evade tax obligations, or deceive investors and

[1] Andreia de Bem Machado et al., "Knowledge Management and Digital Transformation for Industry 4.0: A Structured Literature Review," *Knowledge Management Research & Practice* 20, no. 2 (March 4, 2022): 320–38, https://doi.org/10.1080/14778238.2021.2015261.

[2] Rashmi Mandayam, "The Role of Digital Forensics in Corporate Fraud Investigations," *IJIRMPS - International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences* 12, no. 6 (December 13, 2024): 1–4, https://doi.org/10.37082/IJIRMPS.V12.I6.231752.

consumers. The use of complex algorithms and business structures spanning multiple jurisdictions presents significant challenges for law enforcement in establishing the elements of crimes committed by corporate entities.

Several major scandals in modern economic history have demonstrated how weaknesses in regulation and oversight can have widespread economic and societal impacts. The Enron scandal in 2001, for example, revealed how financial statement manipulation and non-transparent accounting practices led to the company's bankruptcy, causing significant losses for investors and employees.[3] The Lehman Brothers case in 2008 was one of the key factors in the global financial crisis, where high-risk financial practices and a lack of oversight of derivative financial instruments contributed to the collapse of the banking system.[4] The Volkswagen Dieselgate scandal in 2015 exposed how large corporations can systematically commit fraud by manipulating vehicle emissions data, affecting both the environment and public trust in the automotive industry.[5] The Wirecard fraud case in 2020 further highlighted how corporations can exploit regulatory weaknesses in the financial sector to create fictitious financial reports and mislead investors.[6] The FTX scandal in 2022 illustrated the significant risks arising from the lack of regulation in the digital asset and cryptocurrency sector, where investor funds were misused due to the absence of adequate

---

[3] Robert Feldman, "Enron," in *Professionalism and Values in Law Practice* (Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2020), 54–63, https://doi.org/10.4324/9780429244704-12.

[4] Rosalind Z. Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy H: The Global Contagion," *SSRN Electronic Journal*, April 8, 2015, 1–26, https://doi.org/10.2139/SSRN.2593081.

[5] Luann J. Lynch, Cameron Cutro, and Elizabeth Bird, "The Volkswagen Emissions Scandal," *SSRN Electronic Journal*, November 10, 2021, 1–17, https://doi.org/10.2139/SSRN.2975251.

[6] Fabian Maximilian Johannes Teichmann, Sonia Ruxandra Boticiu, and Bruno S. Sergi, "Wirecard Scandal. A Commentary on the Biggest Accounting Fraud in Germany's Post-War History," *Journal of Financial Crime* 31, no. 5 (October 16, 2023): 1166–73, https://doi.org/10.1108/JFC-12-2022-0301/FULL/XML.

oversight mechanisms.[7] The development of various corporate crime cases shows that existing regulations and oversight mechanisms are often unable to anticipate the complexity of crimes committed by modern business entities. The imbalance between technological innovation and regulatory preparedness creates legal loopholes that corporations can exploit to evade legal responsibility.

According to PwC's Global Economic Crime and Fraud Survey 2022, around 46% of companies worldwide have undergone at least one form of economic crime in the past two years. Additionally, the World Economic Forum (WEF) stated that losses due to financial crimes committed by corporations reached USD 42 billion per year, with a trend that continues to increase along with the development of cybercrime and digital transactions. Transparency International, in its Corruption Perceptions Index (CPI) 2023 report, also showed that around 50% of large-scale corruption cases in the world involve corporations, either in the form of bribery, conflicts of interest, or abuse of power.

In Indonesia, data from the Corruption Eradication Commission (KPK) in 2023 revealed that more than 70% of corruption cases handled involved private companies and state-owned enterprises (BUMN).[8] Meanwhile, the Financial Services Authority (OJK) reported in 2022 that losses due to fraud in the banking and digital investment sectors reached more than IDR 20 trillion in the past year. This indicates that the mechanisms for corporate oversight and regulation still have many loopholes, necessitating more effective legal reforms to ensure corporate accountability and criminal liability.

Amid these challenges, blockchain technology has emerged as a promising solution for enhancing transparency, accountability, and law enforcement against corporations. Blockchain is a decentralized, secure, and immutable transaction recording system, making it highly suitable

---

[7] Esther Lea Ledoux and Nadia Smaili, "Cryptocurrency Fauds: The FTX Story," *Journal of Financial Crime*, 2024, 1–7, https://doi.org/10.1108/JFC-01-2024-0022/FULL/XML.

[8] Nathan Junino Jahja, Nor Farizal Mohammed, and Norziana Lokman, "Corruption Cases in Relation to State-Owned Enterprise in Indonesia," *Proceedings of the International Conference in Technology, Humanities and Management (ICTHM 2023), 12-13 June, 2023, Istanbul, Turkey* 131 (November 15, 2023): 533–43, https://doi.org/10.15405/EPSBS.2023.11.46.

for corporate financial oversight and regulation. Forbes (2023) reported that blockchain has been increasingly adopted across various industries, particularly in fraud prevention, financial auditing, and suspicious transaction detection.

The Deloitte 2023 report stated that over 55% of multinational companies worldwide have begun integrating blockchain into their compliance and internal audit systems. This technology enables all transactions to be recorded in a transparent system that authorities can audit without the risk of data manipulation. The European Union, through the European Blockchain Partnership (EBP), has developed blockchain-based systems to monitor financial transactions and prevent money laundering. In the United States, the Securities and Exchange Commission (SEC) has started utilizing blockchain to track insider trading transactions and regulatory violations in capital markets.

In the banking sector, several countries have implemented Blockchain-Based Financial Regulation (BBFR), allowing financial authorities and regulators to directly monitor corporate financial activities within the blockchain ecosystem without intermediaries. China, for instance, has developed a "Blockchain Judicial Platform" for financial supervision and corporate crime investigations. Meanwhile, in Singapore, blockchain has been incorporated into the Know Your Customer (KYC) system to enhance banking transaction transparency and reduce money laundering risks.

Indonesia is still in the early stages of adopting blockchain for regulatory purposes. However, Bank Indonesia (BI) and the Financial Services Authority (OJK) have begun developing Central Bank Digital Currency (CBDC) and blockchain-based transaction monitoring systems to improve oversight of digital transactions and banking activities.[9] This marks an initial step toward blockchain implementation to strengthen corporate criminal law reforms in Indonesia.

Although blockchain offers numerous benefits for corporate accountability and law enforcement, its implementation still faces

---

[9] Archa Erica, Silva Wulandari, and Riya Widayanti, "Data Security Transformation: The Significant Role of Blockchain Technology," *Blockchain Frontier Technology* 3, no. 2 (January 31, 2024): 107–12, https://doi.org/10.34306/BFRONT.V3I2.466.

various challenges, particularly in regulation, privacy, and cross-border legal interoperability. One of the primary challenges is the absence of a global regulatory standard on how blockchain can be utilized in corporate criminal law. Currently, different countries have varying approaches to regulating blockchain technology.

According to the Global Blockchain Regulation 2023 report, only about 30% of countries worldwide have specific regulations regarding blockchain adoption in legal systems, while the rest are still in the policy formulation stage. The European Union, through the Markets in Crypto-Assets Regulation (MiCA), has begun regulating blockchain and crypto assets in financial markets. Still, these regulations have yet to address corporate criminal liability aspects fully.[10] Meanwhile, in the United States, the SEC is still working on adapting financial sector regulations to blockchain technology without hindering industrial innovation.

In Indonesia, blockchain regulations remain limited to the crypto asset and financial transaction sectors, as outlined in the Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No. 5 of 2019 on crypto asset trading. However, there is still no specific legal framework governing the use of blockchain in corporate compliance systems and corporate criminal law enforcement. This presents a significant challenge for legal reform in Indonesia, which is to keep pace with technological advancements and adopt more modern regulations.

Other challenges apart from regulation are data privacy and security risks. While blockchain is inherently transparent, concerns remain about protecting personal data and confidential business information stored in the system. Some companies remain hesitant to adopt this technology due to fears of data breaches and potential exploitation by irresponsible parties. Therefore, legal regulations must strike a balance between transparency and privacy protection in implementing blockchain for corporate criminal liability.

As blockchain technology continues to evolve and corporate crime becomes increasingly complex, legal reforms are essential to ensure the

---

[10] James Ross and Giles Swan, "The Markets in Crypto Assets Regulation: What Should Firms Be Doing Now?," *Journal of Financial Compliance* 7, no. 4 (May 1, 2024): 302–8, https://doi.org/10.69554/ISTO4753.

legal system can adapt to the digital era. These reforms should not only involve updating regulations related to blockchain but also modernizing the judicial system, enhancing regulatory capacity, and fostering international cooperation in harmonizing corporate criminal law.

Countries such as America, England, Estonia, and Singapore have made significant strides in adapting their legal frameworks to technological advancements. Indonesia should learn from more advanced regulatory models to develop a legal system that is more responsive to emerging challenges in corporate criminal law enforcement. With technology-driven legal reforms, corporate crimes can be more effectively prevented and prosecuted, fostering a business ecosystem that is more transparent, accountable, and just in the future.

Previous studies have emphasized the crucial role of blockchain technology in strengthening corporate accountability and reforming corporate criminal law. Aro et al. (2024) demonstrated that blockchain enhances corporate governance and transparency through immutable recording systems, significantly reducing opportunities for corporations to manipulate financial data.[11] In the context of criminal law, Kesarkar (2024) highlighted the importance of blockchain in supporting law enforcement, particularly in the financial sector, which is vulnerable to money laundering and cybercrime.[12] Elst and Lafarre (2019) also underscored how smart contracts can reinforce shareholder accountability and facilitate automated reporting within corporate legal systems.[13] Meanwhile, Teichmann et al. (2023), through their analysis of the Wirecard scandal, revealed substantial weaknesses in conventional accounting systems that could be addressed by integrating blockchain

---

[11] Opeyemi E. Aro et al., "Blockchain Technology as a Tool for Corporate Governance and Transparency," *International Journal of Science and Research Archive* 13, no. 1 (October 30, 2024): 2479–93, https://doi.org/10.30574/IJSRA.2024.13.1.1971.

[12] Tejal Kesarkar, "Blockchain Technology in Law Enforcement and Security: Overview," *International Journal for Research in Applied Science and Engineering Technology* 12, no. 6 (June 30, 2024): 1301–5, https://doi.org/10.22214/IJRASET.2024.63301.

[13] Christoph Van der Elst and Anne Lafarre, "Blockchain and Smart Contracting for the Shareholder Community," *European Business Organization Law Review* 20, no. 1 (2019): 111–37, https://doi.org/10.1007/s40804-019-00136-0.

into forensic auditing.[14] On the regulatory side, Annunziata (2023) assessed the European Union's Markets in Crypto-Assets Regulation (MiCAR), which marks a step forward in blockchain governance. However, it still leaves room for further development of blockchain-based corporate criminal law frameworks.[15]

Despite the significant contributions of these prior studies, the present research addresses a unique urgency by positioning blockchain not merely as a financial or technological tool but as a catalyst for comprehensive corporate criminal law reform. The novelty of this study lies in its holistic approach, combining technological analysis, legal theory, comparative perspectives, and a futuristic outlook to construct a legal framework responsive to the digital age. Therefore, this research is vital not only for legal development in Indonesia but also for addressing the increasingly complex and transnational nature of corporate crime globally.

Method

This study employs a normative legal research method[16], focusing on legal analysis as a system of norms that regulate corporate criminal liability in the context of blockchain technology implementation. The normative legal method is chosen as it allows for a systematic examination of the applicable legal framework, relevant legal principles, and regulatory developments related to corporate accountability in the digital era.[17] This research adopts a descriptive-prescriptive approach, meaning it not only aims to describe the existing legal conditions but also provides

---

[14] Teichmann, Boticiu, and Sergi, "Wirecard Scandal. A Commentary on the Biggest Accounting Fraud in Germany's Post-War History."

[15] Filippo Annunziata, "An Overview of the Markets in Crypto-Assets Regulation (MiCAR).," *SSRN Electronic Journal*, December 11, 2023, 1–72, https://doi.org/10.2139/SSRN.4660379.

[16] Kiki Kristanto et al., "The Convergence of Drug Trafficking and Terrorism: Uncovering the Dynamics of Narco-Terrorism," *Yustisia* 13, no. 3 (2024): 261–82, https://doi.org/10.20961/yustisia.v13i3.81599.

[17] 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.

recommendations for legal reforms necessary to integrate blockchain effectively into the corporate criminal liability system. To ensure a comprehensive analysis, this study utilizes four legal approaches: the statutory approach, the conceptual approach, the comparative approach, and the futuristic approach. The statutory approach involves examining various regulations related to corporate criminal liability and the use of blockchain technology, both at the national and international levels. Key regulations analyzed in this research include Indonesia's latest Criminal Code (KUHP), the Anti-Corruption Law (UU Tipikor), and anti-money laundering (AML) regulations. Additionally, this study assesses blockchain regulations in Indonesia, such as the Commodity Futures Trading Supervisory Agency (Bappebti) Regulation No. 5 of 2019 on Cryptocurrency Trading, as well as international legal instruments like the United Nations Convention Against Corruption (UNCAC), the Financial Action Task Force (FATF) guidelines on AML, and the OECD Guidelines on Corporate Governance of State-Owned Enterprises. The analysis of these regulations aims to understand how the current legal framework governs corporate accountability and how blockchain can be accommodated within the legal system. The conceptual approach is applied to explore legal theories underlying corporate criminal liability, good corporate governance, and how blockchain can contribute to enhancing legal transparency and accountability. This approach delves into various concepts in criminal law, corporate law, and technology law, examining how these principles can be adapted in the digital era to address emerging challenges brought about by blockchain technology. Furthermore, the conceptual analysis reviews concepts such as smart contracts, decentralized ledgers, and automated compliance mechanisms, which have the potential to prevent corporate crimes. Next, the comparative approach is utilized to compare blockchain regulations and corporate criminal liability frameworks across different jurisdictions. This comparative study covers countries that have pioneered blockchain regulations within their legal systems, such as the European Union with the Markets in Crypto-Assets Regulation (MiCA), the United States with the Securities and Exchange Commission (SEC) policies on digital assets, and Singapore, which has integrated blockchain into its financial and banking regulatory framework. This approach aims to identify best practices in blockchain

regulation and corporate accountability that can serve as a reference for Indonesia in developing more adaptive legal policies in response to technological advancements. Additionally, this study employs a futuristic approach to explore the future direction of legal reforms in addressing challenges posed by blockchain technology developments. This approach examines global trends in blockchain regulation, including the potential application of Artificial Intelligence (AI) in corporate governance, the use of regulatory sandboxes for testing new legal policies, and how the judicial system can adapt to the digital era in enforcing laws against corporate crimes facilitated by technology. The data for this study were collected through a literature review, encompassing legal document analysis, academic journals, reports from international organizations, and regulatory frameworks from various countries. The collected data is then analyzed using content analysis to identify regulatory gaps, legal challenges, and potential legal reforms. Through these approaches, this study aims to provide both academic and practical contributions to understanding the role of blockchain in enhancing transparency, accountability, and legal reform in corporate criminal liability.[18]

Result and Discussion

A. Regulatory Gaps in the Use of Blockchain for Corporate Criminal Liability

Blockchain is a decentralized data recording technology where each transaction or piece of information is stored in interconnected blocks, forming a chain.[19] This technology employs cryptography to secure each block, making the recorded data difficult to alter or counterfeit. Each block in the blockchain contains a set of verified

[18] Emelia Kontesa and Zico Junius Fernando, "Reclaiming Our Roots: Agrarian Law's Battle Against Land Grabbing," *Lex Scientia Law Review* 8, no. 2 (November 30, 2024): 1–10, https://doi.org/10.15294/LSLR.V8I2.10681.

[19] D Arora et al., "Blockchain-Based Security Solutions to Preserve Data Privacy And Integrity," in *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2019, 468–72, https://doi.org/10.1109/ICCCIS48478.2019.8974503.

transactions, which are authenticated by a network of computers.[20] This verification process is carried out by network participants known as nodes, who operate independently to ensure the validity and integrity of the data before it is added to the chain.[21]

Since no central authority controls the data, this system provides high transparency and trust for its users. Blockchain is also known for its immutability, meaning that once a transaction is recorded, it cannot be changed or deleted without the approval of the majority of the network. This feature offers strong security guarantees and prevents data manipulation, making it highly useful in various applications such as financial record-keeping, logistics, and supply chain management.[22]

Moreover, blockchain operates as a decentralized system, where data is stored and managed collectively by multiple parties. This differs from traditional systems that rely on a single central entity, thereby reducing the risk of system failures and enhancing resilience against cyberattacks. This technology has laid the foundation for various innovations, particularly in the world of cryptocurrency, but its applications are expanding into other sectors such as banking, government, and public administration.[23]

Blockchain has emerged as a disruptive technology with the potential to revolutionize various sectors, including corporate governance and corporate criminal law systems. With its decentralized,

---

[20] Joseph Migga Kizza, "Blockchains, Cryptocurrency, and Smart Contracts Technology: Security Considerations BT - Guide to Computer Network Security," ed. Joseph Migga Kizza (Cham: Springer International Publishing, 2020), 533–58, https://doi.org/10.1007/978-3-030-38141-7_25.

[21] M M Taha and M Alanezi, "Cryptocurrencies in Blockchains Environment: The Verification Trip," in *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)*, 2022, 159–64, https://doi.org/10.1109/ICCRESA57091.2022.10352512.

[22] Shiva Sumanth Reddy, Jahnavi S, and Manjunath D R, "Enhancing Data Security and Traceability in Supply Chain Management Using Blockchain Technology," *Journal of Cyber Security in Computer System* 3, no. 3 (September 3, 2024): 11–24, https://matjournals.net/engineering/index.php/JCSCS/article/view/899.

[23] Monika Juneja, "Blockchain Technology: Benefits, Challenges, Applications and Future Direction," *IJFMR - International Journal For Multidisciplinary Research* 6, no. 6 (December 2, 2024): 1–21, https://doi.org/10.36948/IJFMR.2024.V06I06.32265.

immutable, and transparent nature, blockchain promises to enhance accountability in business transactions, mitigate corruption risks, and optimize audit mechanisms. However, the application of blockchain in corporate criminal liability still faces significant challenges, particularly in terms of regulation.[24] Many countries have yet to establish a specific legal framework governing how blockchain can be utilized in financial oversight, corporate compliance systems, and law enforcement against corporate crimes. As a result, this technology has not been fully leveraged to close gaps in tax evasion, money laundering, and financial statement manipulation by corporations.

The rapid development of blockchain has also created a gap between technological innovation and legal regulation. Some countries have begun drafting blockchain regulations, but the approaches taken remain highly varied, leading to disharmony in international legal standards. Furthermore, the lack of specific regulations in many countries allows corporations to continue exploiting this technology to evade legal obligations. Therefore, regulatory gaps in the use of blockchain for corporate criminal liability present a significant challenge that requires further study, particularly regarding differences in legal approaches between countries, loopholes that corporations may exploit, and the implications of insufficient legal harmonization in overseeing blockchain-based transactions.

Most legal systems worldwide still rely on conventional oversight mechanisms for enforcing corporate criminal law. These mechanisms include manual audits, compliance reporting systems, and centralized financial supervision. Manual audits are typically conducted by regulators or independent auditors who review corporate financial documents to ensure compliance with the law. Compliance reporting systems depend on companies to self-report their financial and operational activities. In contrast, state authorities or financial institutions carry out centralized financial supervision to monitor transactions within the traditional banking system.

---

[24] Henry Dianto P. Sinaga and Andhy H. Bolifaar, "Blockchain Adoption for Plea Bargaining of Corporate Crime in Indonesia," in *ACM International Conference Proceeding Series* (Association for Computing Machinery, 2020), 115–19, https://doi.org/10.1145/3390566.3391680.

However, these approaches face growing challenges in keeping up with the evolution of digital transactions and blockchain-based financial systems. Blockchain's decentralized and anonymous nature makes financial transactions more difficult to trace compared to conventional banking systems. The absence of intermediaries such as banks or financial institutions in some blockchain-based transactions also reduces the effectiveness of oversight typically conducted by financial regulators.

For example, the FTX scandal in 2022 demonstrated these challenges. FTX, one of the largest cryptocurrency exchanges at the time, went bankrupt after it was revealed that the company had diverted customer funds into various crypto wallets without adequate oversight.[25] U.S. financial authorities struggled to track the flow of funds because transactions were conducted through blockchain networks, enabling rapid and anonymous asset transfers. In this system, transactions can be obscured using techniques such as mixing services or multiple digital wallets, making investigations more difficult. The FTX scandal illustrates how blockchain can be used in non-transparent financial transactions when there are no clear regulations governing its oversight mechanisms. The decentralized structure that makes blockchain advantageous can also pose challenges for legal authorities in uncovering corporate misconduct. Difficulties in accessing transaction data and identifying digital wallet owners slow down legal processes and the recovery of funds for affected victims.

In the European Union, regulations on digital assets and blockchain technology are still in development. The Markets in Crypto-Assets Regulation (MiCA) is a key step in establishing a legal framework for the crypto ecosystem.[26] This regulation aims to provide legal certainty for crypto market participants, including requirements for digital token issuers, crypto asset service providers, and consumer protection mechanisms. MiCA also addresses aspects such as financial stability and risk mitigation in the crypto market.

However, MiCA is primarily focused on regulating the crypto asset market rather than overseeing the use of blockchain in corporate

---

[25] Ledoux and Smaili, "Cryptocurrency Fauds: The FTX Story."

[26] Annunziata, "An Overview of the Markets in Crypto-Assets Regulation (MiCAR)."

criminal law and legal compliance systems. The regulation does not specifically address how blockchain can improve accountability and transparency in corporate transactions or how control mechanisms can be applied to prevent the misuse of this technology for illegal activities.

As a result, regulatory loopholes allow companies to use blockchain technology to process transactions anonymously and conceal assets from tax authorities and financial regulators. In an unregulated and decentralized blockchain system, companies can conduct transactions through unidentifiable digital wallets, use techniques like mixing services (tumblers) to obscure fund flows, and leverage smart contracts to automate transactions that are difficult to trace.

The absence of regulations specifically governing the use of blockchain for legal compliance has led to the technology being used more frequently as a financial manipulation tool rather than as an instrument for transparency and accountability. Although blockchain has enormous potential to enhance financial transparency through permanent and distributed ledger recording, without adequate regulations, it can also be exploited for the opposite purposes, such as money laundering, tax evasion, and unauthorized asset transfers.

In the context of corporate criminal law, the biggest challenge is developing oversight mechanisms that are compatible with blockchain's decentralized nature while still providing legal protection for legitimate asset holders. The European Union is still in the early stages of designing broader regulations to address the potential misuse of blockchain in business and financial transactions.

In the United States, the Financial Crimes Enforcement Network (FinCEN) has developed regulations concerning Know Your Customer (KYC) and Anti-Money Laundering (AML) in blockchain-based transactions to ensure that companies operating in the digital asset sector, such as cryptocurrency exchanges and blockchain service providers, comply with applicable financial laws.[27] KYC regulations require companies to collect user identity information before they can conduct

[27] Sarah Jane Hughes, "'Gatekeepers' Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes As Permission-Less Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money,'" *SSRN Electronic Journal*, August 21, 2019, 1–40, https://doi.org/10.2139/SSRN.3436098.

transactions, including full name, address, date of birth, and supporting documents such as passports or identity cards. After collecting the data, companies must verify the information against official databases or other supporting systems to ensure that users are legitimate individuals and not anonymous entities potentially engaging in illegal activities. This KYC policy is also applied to cryptocurrency exchanges, which must ensure that every user has undergone a verification process before being allowed to buy, sell, or trade digital assets.

Additionally, AML regulations are designed to detect and prevent money laundering practices that use digital assets as a means to conceal illicit funds. In implementation, companies in this sector are required to report suspicious transactions to FinCEN, particularly if transactions exceed certain thresholds or display patterns deemed unusual. Monitoring focuses on high-risk activities, such as large fund transfers, repeated transactions in a short period, or dealings with entities in countries with high money laundering risks. Companies that fail to comply with AML regulations may face severe penalties, including substantial fines and the revocation of their operating licenses. AML compliance also involves collaboration with financial regulators and law enforcement agencies to ensure that blockchain systems and digital assets are not misused for financial crimes. Through KYC and AML regulations, FinCEN seeks to create a more transparent, accountable, and effectively monitored digital asset ecosystem to reduce the risk of blockchain technology being exploited for illicit activities.

However, implementing these regulations still faces various challenges, particularly because many blockchain-based companies choose to operate in jurisdictions with looser or less stringent regulations than the United States. Due to the decentralized and anonymous structure that characterizes blockchain technology, companies can easily relocate their operations to countries that do not enforce strict KYC and AML standards. Consequently, FinCEN's oversight efforts are less effective in closing regulatory loopholes that enable companies to evade compliance obligations.

A concrete example is the Binance case, in which, in 2023, the company was accused of facilitating illegal transactions worth billions of dollars through a system that was not subject to U.S. financial regulators. Investigations revealed that Binance failed to implement strict KYC and

AML policies, allowing individuals and entities to conduct large transactions without undergoing adequate identity verification. Reports also indicated that Binance had become a platform for criminal groups and individuals looking to conceal the origin of their funds, including through stablecoins and mixing services to obscure transaction trails.

The Binance case highlights that while KYC and AML regulations have been implemented, their effectiveness depends on industry compliance and law enforcement mechanisms. With many companies operating across borders and using technologies that enable transaction anonymity, FinCEN and other regulators still face significant challenges in ensuring that existing regulations comprehensively oversee blockchain-based financial activities.

Furthermore, differences in regulations between countries create regulatory arbitrage, where companies can exploit legal loopholes by choosing more permissive jurisdictions. This underscores the importance of international cooperation in designing more coordinated regulations to address blockchain technology misuse in the context of financial crimes.

From a juridical perspective, the implementation of blockchain technology aims to strengthen legal evidentiary systems, improve the efficiency of law enforcement, and ensure greater accountability and transparency in corporate activities. Due to its immutable nature, blockchain allows for the permanent recording of transactions that can be audited in real-time, thereby enhancing the credibility and reliability of digital evidence in legal proceedings. Juridically, blockchain also serves to fill regulatory gaps and reinforce the legal framework so that it can respond to the challenges posed by modern, technologically sophisticated crimes committed by corporations. From a philosophical standpoint, blockchain embodies the pursuit of substantive justice and upholds core legal values such as honesty, transparency, and responsibility. This technology provides an opportunity to align legal practice with moral principles by ensuring that no individual or corporate entity can evade legal responsibility through data manipulation or the erasure of transactional records. By decentralizing data control and reducing the dominance of a single authority, blockchain promotes the philosophical ideal of egalitarianism within the law, ensuring equal access to information and justice for all stakeholders.

From a sociological angle, blockchain seeks to foster public trust in legal and financial institutions, reduce social disparities resulting from unequal access to information, and promote a more resilient and equitable social system. In a digitized and globalized society, blockchain can serve as a social tool to empower public oversight of corporate misconduct. By integrating transparent and traceable technologies into legal systems, the public gains a sense of security, knowing that economic transactions, contracts, and corporate conduct are being recorded honestly and accessibly. This, in turn, reinforces social cohesion, legal legitimacy, and collective confidence in regulatory institutions.

B. The Role of Blockchain in Preventing and Detecting Corporate Crimes

Blockchain has emerged as a promising technology for enhancing transparency and reducing the risks of corporate crimes, including fraud, money laundering, tax evasion, and financial statement manipulation.[28] With its immutability, decentralized ledger, and automation capabilities through smart contracts, blockchain can serve as a powerful tool to strengthen oversight and detect suspicious financial activities in corporate transactions. However, despite its significant potential, challenges related to regulation, legal acceptance, and technical limitations remain significant obstacles to its adoption as an instrument in corporate criminal law. Therefore, it is crucial to understand how blockchain can be utilized to enhance transparency, the extent to which smart contracts can aid corporate legal compliance, and the barriers that hinder its adoption within the legal system.

One of blockchain's key features that makes it effective in preventing corporate crimes is immutability, meaning that any recorded transaction cannot be altered or deleted.[29] This ensures that every

---

[28] Opeyemi E. Aro et al., "Blockchain Technology as a Tool for Corporate Governance and Transparency," *International Journal of Science and Research Archive* 13, no. 1 (October 30, 2024): 2479–93, https://doi.org/10.30574/IJSRA.2024.13.1.1971.

[29] Pvheanushaa Patmanathan et al., "The Effectiveness of Blockchain Technology in Preventing Financial Cybercrime," in *E3S Web of Conferences*, vol. 389 (EDP Sciences, 2023), 1–25, https://doi.org/10.1051/E3SCONF/202338907022.

modification or transaction within a company's financial system can be audited in real time, reducing the likelihood of data manipulation, which often plays a significant role in major financial scandals. For instance, in the Enron (2001) and Wirecard (2020) cases, these companies manipulated financial statements by falsifying balance sheets and internal transactions, causing investors and regulators to fail in detecting the fraud before the companies collapsed. If blockchain-based financial audits had been implemented, regulators could have accessed all transactions transparently, preventing such scandals at an early stage.

Additionally, blockchain enables real-time tracking in corporate financial systems, allowing transactions to be monitored by both internal and external auditors. In the financial sector, banks such as JPMorgan Chase and HSBC have begun utilizing blockchain-based systems to track interbank transactions and detect anomalies indicative of fraudulent activities. This technology allows companies to identify suspicious transactions much faster compared to traditional methods, which still rely on manual reporting and paper-based audit systems.

In the trade and supply chain sectors, blockchain has also been leveraged to prevent fraud in business transaction records. For example, in the food and pharmaceutical industries, blockchain has been implemented in product tracking systems to ensure that goods sold do not pass through illegal distribution channels. IBM Food Trust, for instance, has developed a program that allows companies to record their entire supply chain cycle on the blockchain, thereby reducing the risks of counterfeit products and illicit trade practices. In the context of corporate criminal law enforcement, such systems could be applied to detect and prevent corruption in corporate supply chains, as well as mitigate the risks of bribery in business contracts. However, despite blockchain's ability to enhance transparency, its application within legal systems remains limited due to the lack of regulations governing the admissibility of blockchain-based data as legal evidence. In many jurisdictions, legal systems still rely more on transaction records provided by conventional banking systems, which are often vulnerable to manipulation. Therefore, for blockchain to be widely utilized in preventing and detecting corporate crimes, legal reforms are needed to grant blockchain-generated data the same legal standing as other official corporate documents.

One of the primary features of blockchain that makes it effective in preventing corporate crime is immutability, where every transaction recorded on the blockchain cannot be altered or deleted. This means that any changes or transactions within a company's financial system can be audited in real-time, reducing the likelihood of data manipulation, which frequently occurs in major financial scandals. For example, in the cases of Enron (2001) and Wirecard (2020), these companies manipulated financial statements by falsifying balance sheets and internal transactions, causing investors and regulators to fail to detect fraud before the companies went bankrupt. If a blockchain system were implemented in corporate financial audits, regulators could transparently monitor all transactions, preventing such scandals at an earlier stage.

Additionally, blockchain enables real-time tracking within corporate financial systems, where both internal and external auditors can monitor every transaction. In the financial sector, several banks, such as JPMorgan Chase and HSBC, have begun using blockchain-based systems to track interbank transactions and detect anomalies indicating fraudulent activities. This technology allows companies to identify suspicious transactions more quickly compared to traditional methods, which still rely on manual reports and paper-based audit systems.

In the trade and supply chain sector, blockchain has also been utilized to prevent fraud in business transaction records. For instance, in the food and pharmaceutical industries, blockchain has been implemented in product tracking systems to ensure that goods sold do not pass through illegal distribution channels. A notable example is the IBM Food Trust program, which allows companies to record their entire supply chain cycle on the blockchain, thereby reducing the risk of product counterfeiting and illegal trade practices. In the context of corporate criminal law enforcement, such a system could be applied to detect and prevent corruption practices within corporate supply chains and reduce the risk of bribery in business contracts.

However, although blockchain can enhance transparency, its use in legal systems remains limited due to the lack of regulations governing the validity of blockchain-based data as legal evidence. In many jurisdictions, legal systems still rely more on transaction evidence provided by conventional banking systems, which are often susceptible

to manipulation. Therefore, for blockchain to be more widely adopted in the prevention and detection of corporate crime, legal reforms are needed to grant blockchain-generated data the same legal standing as other official corporate documents.

Although blockchain holds significant potential in increasing transparency and preventing corporate crime, various technical and legal barriers hinder its implementation within law enforcement systems. One of the biggest challenges is the lack of global regulatory standards governing the use of blockchain as a tool in legal compliance and corporate criminal law.

In many countries, there are no regulations explicitly requiring companies to use blockchain in their financial reporting, allowing many corporations to continue using conventional accounting systems that are more prone to manipulation. Additionally, there is still international disagreement on how blockchain-based transactions should be regulated, particularly in terms of data privacy and user protection. In the European Union, for example, the General Data Protection Regulation (GDPR) restricts the storage of personal data on blockchain due to its immutable nature, which conflicts with users' rights to request the deletion of their data in digital systems.[30]

Apart from regulatory challenges, technical issues also pose significant obstacles to the adoption of blockchain in legal systems. While blockchain offers high security, its slower transaction speed compared to conventional systems can be problematic in managing large-scale transactions. Moreover, implementing blockchain requires a strong digital infrastructure and high development costs, making it less incentivizing for companies to adopt this technology for legal compliance.

Given these challenges, the adoption of blockchain in corporate criminal law systems requires a more strategic approach, including the development of clearer regulations and enhanced international cooperation to create global standards that ensure this technology can

[30] Alexander Wodi, "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review," *SSRN Electronic Journal*, 2023, 1–22, https://doi.org/10.2139/SSRN.4601142.

effectively increase corporate transparency and accountability on a global scale.

In Indonesia, the regulation of blockchain technology is still in its early stages. It primarily focuses on the regulation of digital assets and financial transactions, without addressing broader aspects related to their use in corporate governance and corporate criminal liability. The existing regulations have not yet specifically outlined how blockchain can be utilized as a legal instrument in the prevention and detection of corporate crime, despite its significant potential to enhance transparency and accountability within the legal system. One of the main regulations governing blockchain aspects in Indonesia is the Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No. 5 of 2019 on Crypto Asset Trading, which stipulates that blockchain-based digital assets can be traded as commodities regulated by Bappebti under the Ministry of Trade. However, this regulation solely focuses on the legality of crypto trading and does not cover how blockchain can be applied in financial audits, business transparency, or corporate legal compliance systems.

Additionally, the Financial Services Authority (OJK) and Bank Indonesia (BI) have issued several policies related to blockchain-based digital transactions. Bank Indonesia, for instance, has prohibited the use of crypto assets as a means of payment but remains open to the development of blockchain technology within the national financial system. In the context of financial regulation, OJK has implemented OJK Regulation No. 12/POJK.01/2017 on Anti-Money Laundering and Counter-Terrorism Financing, which requires financial institutions to implement Know Your Customer (KYC) systems and monitor financial transactions.[31] Although blockchain has the potential to serve as an effective tool for detecting suspicious transactions in real-time, the existing regulations have yet to accommodate its use as part of law enforcement mechanisms in the financial industry. As a result, many companies and financial institutions in Indonesia continue to rely on

[31] Miftahul Fauzi, "Dampak Dan Regulasi Fintech Terhadap Inklusi Keuangan Di Indonesia," *SANTRI : Jurnal Ekonomi Dan Keuangan Islam* 2, no. 6 (December 4, 2024): 143–54, https://doi.org/10.61132/SANTRI.V2I6.1028.

conventional financial monitoring systems, which are more vulnerable to data manipulation and corporate crime.

In the latest Criminal Code (Law No. 1 of 2023 on the Criminal Code), provisions regarding corporate criminal liability are stipulated in several articles, affirming that corporations can be held criminally responsible if specific criteria are met.[32] Article 45 of the Criminal Code states that a corporation may be held criminally liable if the offense is committed within the scope of corporate activities, for the benefit of the corporation, and with the order or knowledge of an authorized executive within the corporation. In the context of specific offenses such as corruption and money laundering, the Criminal Code provides a framework for corporate liability by adjusting the penalties that may be imposed. Article 46 stipulates that sanctions against corporations may include fines, which can be significantly higher than those imposed on individuals. Furthermore, Articles 47 and 48 regulate additional penalties that can be imposed on corporations, including corporate dissolution, confiscation of profits obtained from the criminal offense, and specific prohibitions that may restrict corporate business activities. The Criminal Code also accommodates more specific sentencing mechanisms for economic and financial crimes committed by corporations. In the case of money laundering, the Criminal Code refers to Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering, which mandates that suspicious financial transactions must be reported and may serve as the basis for investigations by relevant authorities. However, in practice, the system used in money laundering investigations still relies on conventional audit mechanisms, which often have limitations in tracking complex and cross-border transactions.

The Criminal Code does not explicitly regulate the use of blockchain technology in corporate crime investigations and law enforcement.[33] However, blockchain's characteristics of permanently, transparently, and immutably recording every transaction have the potential to enhance the effectiveness of financial transaction oversight,

---

[32] Rusli Rusli and Firman Halawa, "Corporate Criminal Liability As An Insurance Crime Perpetrator Based On Law Number 1 Of 2023 On Criminal Law," *International Journal Of Humanities Education and Social Sciences* 3, no. 4 (February 27, 2024): 2111–17, https://doi.org/10.55227/IJHESS.V3I4.908.

[33] Kesarkar, "Blockchain Technology in Law Enforcement and Security: Overview."

including those related to money laundering and financial manipulation by corporations. Blockchain can serve as a transaction recording tool that enables legal and financial authorities to trace fund flows more accurately and efficiently compared to traditional systems, which are more susceptible to concealment or deletion of transaction traces.

Beyond financial and criminal regulations, Blockchain also holds potential in corporate governance and business transparency. However, Indonesia has yet to establish specific regulations that encourage its adoption in corporate governance. Law No. 40 of 2007 on Limited Liability Companies (UU PT) outlines financial reporting mechanisms and corporate transparency. Still, it does not accommodate the use of decentralized ledgers as part of a more transparent financial reporting system.[34] If blockchain were integrated into corporate reporting systems, practices such as tax evasion, fraudulent financial statements, and asset concealment would become more difficult, as every transaction would be permanently recorded and auditable by regulators in real time. Unfortunately, there are currently no regulations in Indonesia mandating companies to implement blockchain in their financial reporting or business transparency systems.

In Indonesia's financial and digital startup industries, some companies have begun adopting blockchain technology in their operations, albeit on a limited scale. Several fintech companies and digital banks have started utilizing blockchain to enhance transaction security and payment system efficiency. However, there is currently no legal mandate requiring the use of blockchain as part of corporate legal compliance systems.

Many companies in Indonesia remain reluctant to adopt this technology due to the absence of regulations that provide incentives or encourage its application in auditing and business oversight. As a result, while blockchain holds significant potential for improving corporate transparency and accountability, its adoption remains limited due to the lack of regulatory requirements for integrating it into corporate legal

---

[34] Dian Kusuma Wardhani, Tjiptohadi Sawarjuwono, and Sasongko Budisusetyo, "Blockchain in Capital Markets: A Revolution of the Trading System in Stock Exchange," *The Indonesian Accounting Review* 12, no. 1 (January 7, 2022): 1–16, https://doi.org/10.14414/TIAR.V12I1.2437.

frameworks. Overall, blockchain regulation in Indonesia remains minimal, primarily focusing on digital asset trading. At the same time, other aspects such as its use in financial auditing, corporate governance, and corporate criminal law enforcement are not yet adequately accommodated. To fully leverage the benefits of this technology, Indonesia needs to develop more comprehensive regulations, including provisions governing the use of blockchain in corporate reporting systems, legal compliance, and corporate crime investigations.[35] Such regulations would strengthen corporate accountability and help prevent illicit practices that harm both the state and society.

C. Legal Reforms for Integrating Blockchain in Corporate Criminal Liability

Legal reforms are necessary to integrate blockchain technology into corporate regulations and the judicial system, enabling the widespread adoption of blockchain within the legal system.[36] These reforms aim to ensure that blockchain can be legally used as an instrument of transparency and accountability in corporate criminal law while providing a clear legal framework for its implementation. Many countries have begun experimenting with technology-based regulations, such as regulatory sandboxes, technology-driven legal policies, and collaborations between the public and private sectors, to create more flexible regulations.

Regulatory sandboxes have become an approach used by various countries, including Singapore and the United Kingdom, to allow companies and regulators to test the legal impact of blockchain implementation before adopting it in full-scale policies.[37] This model provides a controlled legal environment where companies can develop

---

[35] Suyanto et al, "Exploring Blockchain Technology for Transparency and Efficiency in Indonesia's Financial Sector," *Nomico* 1, no. 10 (November 30, 2024): 36–45, https://doi.org/10.62872/36J2SM39.

[36] Harshit Jain et al., "Towards Transparent Justice: Promoting Integrity and Efficiency in the Judicial System with Blockchain," *SSRN Electronic Journal*, May 29, 2024, 1–7, https://doi.org/10.2139/SSRN.4847643.

[37] Victor Dostov, Pavel Shoust, and Ekaterina Ryabkova, "Regulatory Sandboxes as a Support Tool for Financial Innovations," *Journal of Digital Banking* 2, no. 2 (September 1, 2017): 179–88, https://doi.org/10.69554/UHEK4572.

and test blockchain-based solutions without having to comply with all existing regulations immediately. This approach enables direct supervision by regulators, allowing for regulatory adjustments based on findings during the trial phase. Thus, regulatory sandboxes serve as flexible legal instruments that support technological innovation while ensuring that their implementation considers relevant legal aspects.

In Singapore, the Monetary Authority of Singapore (MAS) has launched the Financial Technology Regulatory Sandbox to accommodate the testing of various blockchain-based financial technologies, particularly those related to digital payments, smart contracts, and financial transaction transparency.[38] Through this sandbox, companies operating in the financial sector can test blockchain-based business models under more flexible regulatory requirements before transitioning to stricter full-scale regulations. One example is the use of blockchain in cross-border payment systems, which several Singaporean fintech companies tested in the regulatory sandbox before obtaining an official license to operate. However, the implementation of the regulatory sandbox in Singapore remains highly focused on the financial sector and does not yet cover corporate criminal law and corporate liability comprehensively. As a result, the application of blockchain in legal compliance remains in an experimental zone, without concrete obligations for companies to use it in their audit systems and legal transparency mechanisms.

In the United Kingdom, the Financial Conduct Authority (FCA) has also developed a regulatory sandbox that allows companies to test blockchain technology within the financial system.[39] One of FCA's main focuses is examining how blockchain can be used to enhance transparency in financial transactions and ensure that this technology can help detect and prevent money laundering and illegal financial transactions. This program allows companies to develop blockchain-based systems for compliance with financial regulations, but remains

---

[38] Christopher Chen, "Rethinking the Regulatory Sandbox for Financial Innovation: An Assessment of the UK and Singapore," *Perspectives in Law, Business and Innovation*, 2020, 11–30, https://doi.org/10.1007/978-981-15-5819-1_2.

[39] Jon Truby, "Fintech and The City: Sandbox 2.0 Policy and Regulatory Reform Proposals," *International Review of Law, Computers & Technology* 34, no. 3 (September 1, 2020): 277–309, https://doi.org/10.1080/13600869.2018.1546542.

limited to the banking and investment sectors. A concrete example of this implementation is the use of blockchain in automatic financial transaction reporting, where every transaction conducted by a company is recorded directly in a system that regulators can audit in real-time. However, similar to Singapore, the regulatory sandbox in the United Kingdom has not yet addressed corporate criminal law aspects, meaning companies are not yet required to use blockchain as part of their legal compliance and accountability systems. Therefore, legal reforms must not only support technological innovation but also ensure legal protection, justice, and legal certainty in the application of blockchain for corporate compliance and law enforcement.

One of the main challenges in legal reform is ensuring that blockchain can be legally recognized as a valid tool within corporate criminal law. To achieve this, blockchain must be acknowledged as a legitimate instrument for legal evidence, financial audits, and corporate transaction monitoring systems. Several countries have started implementing blockchain technology in governmental administration systems and business records, with the primary goal of improving transparency, data security, and efficiency in both public governance and the business sector. Estonia and Switzerland are two leading countries in blockchain adoption at a national scale, each developing blockchain-based systems to strengthen government data integrity, enhance corporate accountability, and facilitate compliance with financial regulations and corporate law.

In Estonia, blockchain technology has been part of the national digital transformation strategy since early 2008, making it one of the first countries in the world to implement blockchain in public administration systems.[40] The Estonian government developed X-Road, a national data infrastructure that enables various government agencies to exchange information securely and efficiently. One key feature of this system is the use of blockchain technology to secure administrative records, including

[40] 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 26, 2022): 386–401, https://doi.org/10.1093/POLSOC/PUAC014.

civil registration documents, tax records, medical documents, and even electronic voting systems.[41]

A tangible example is the e-Residency system in Estonia, which allows individuals and businesses worldwide to register their companies online and access Estonian administrative services without physically being in the country. Blockchain technology is used in this system to ensure that the identities and business transactions conducted by e-Residents cannot be forged or manipulated. With a decentralized ledger, all business records registered by e-Residents can be verified transparently and securely. Additionally, this system enables business registration within minutes, compared to traditional processes that can take days or even weeks. Blockchain is also used in Estonia's judicial administration system, particularly in protecting the integrity of legal documents and court decisions. With this technology, any changes or access to legal documents can be directly traced, thereby reducing the risk of document manipulation by unauthorized parties. This enhances security and accountability within the judicial system while also expediting legal processes that are often hindered by administrative bureaucracy.

Meanwhile, in Switzerland, blockchain has been widely used in the financial sector, government administration, and business registration. The Swiss government has developed the Swiss Blockchain Act, which provides a clear legal framework for blockchain applications across various sectors, including digital asset trading, innovative contract systems, and business record-keeping based on distributed ledger technology.[42] One of the significant steps taken by Switzerland in adopting blockchain is implementing this technology in the corporate registration system in the canton of Zug, known as Crypto Valley. The canton of Zug serves as a prime example of how blockchain can be utilized for company registration and business transactions with higher transparency. In this system, registered companies can use smart

---

[41] Alexander Mechitov and Helen Moshkovich, "Estonia - A Small Giant of E-Government," *Journal of Academy of Business and Economics* 21, no. 3 (October 1, 2021): 43–53, https://doi.org/10.18374/JABE-21-3.4.

[42] Fabian O. Zehnder, "An Analysis of the Adaptability of Switzerland's Financial Regulatory Framework to Blockchain and Digital Currency Innovations," *Frontiers in Management Science* 3, no. 5 (October 24, 2024): 47–55, https://doi.org/10.56397/FMS.2024.10.05.

contracts to record business agreements, manage share ownership, and facilitate shareholder voting digitally.[43] By using blockchain, every transaction or change in a company's structure is immediately recorded in a distributed ledger, ensuring that no manipulation or alterations occur without the knowledge of the relevant authorities. Additionally, Switzerland has also implemented blockchain in its digital identity system, allowing citizens and residents to access government services with enhanced security. This system is designed to mitigate the risks of identity theft and document fraud, which are common issues in traditional government administration. For example, in business licensing or civil documentation processes, blockchain enables automatic identity verification, eliminating the need for individuals to submit physical documents that are prone to forgery or loss.

In the financial sector, Switzerland has become one of the first countries to recognize blockchain-based digital assets as legitimate financial instruments. This allows banks and financial institutions to utilize this technology in transaction recording, tax reporting, and compliance monitoring with anti-money laundering (AML) regulations. This provides a more transparent legal framework for companies seeking to integrate blockchain into their compliance systems while also increasing investor and stakeholder confidence in the security of blockchain-based transactions.

In the context of corporate criminal law, the validity of evidence generated through blockchain remains a complex issue, primarily because many judicial systems have yet to recognize blockchain-based transactions as admissible legal evidence. Most jurisdictions still rely on physical documents, conventional financial reports, and transaction records from traditional banking systems, which are vulnerable to manipulation or forgery. Blockchain, with its immutability and distributed ledger characteristics, could actually serve as a stronger tool for ensuring transaction validity and reducing the risk of data misuse. However, due to its anonymity and encryption features, many legal systems still lack mechanisms to assess the authenticity and ownership of blockchain data in criminal investigations.

---

[43] Van der Elst and Lafarre, "Blockchain and Smart Contracting for the Shareholder Community."

For blockchain to be accepted as legitimate evidence, judicial systems need to adopt new legal standards that establish digital forensic mechanisms. This would enable courts to use blockchain-based transactions as evidence in corporate criminal cases. Legal reforms in this area must also include regulations on how regulators and law enforcement agencies can access data within blockchain systems without violating corporate privacy rights and data protection regulations at the national and international levels.

One potential approach is a verification mechanism through an independent authority that acts as a third party in ensuring the authenticity of blockchain transactions submitted as evidence in criminal investigations. Additionally, there must be a legal framework governing regulators' access rights to blockchain data, including apparent limitations on the information that can be accessed, procedures for data seizure, and encryption methods used to balance law enforcement efforts with corporate privacy protection.

Legal reforms in corporate criminal law must ensure that blockchain regulations can be adapted to existing legal mechanisms, allowing this technology to function as a tool for enhancing accountability and transparency in corporate legal compliance. Most corporate criminal law systems still use a traditional approach, relying on periodic financial reports, external audits, and transaction monitoring through financial institutions such as banks and tax authorities. This system has various weaknesses, particularly in detecting suspicious transactions, identifying money laundering practices, and preventing financial report manipulation, which often plays a role in corporate crimes. With blockchain technology, this monitoring system can be significantly improved through the implementation of decentralized ledgers, enabling transactions to be monitored in real time by regulatory authorities and external auditors.

One of the main benefits of implementing blockchain in corporate legal compliance systems is its ability to create immutable transaction records, reducing the risk of data manipulation and financial fraud by companies. In conventional audit systems, auditors often rely on financial reports provided by the companies themselves, which can easily be manipulated to hide assets or evade tax obligations. For example, in the Enron scandal (2001) and Wirecard scandal (2020), these companies

managed to falsify their financial reports for years without detection by regulatory authorities. If a blockchain system were implemented, every transaction conducted by a company would be automatically recorded in a system that can be verified by multiple parties, significantly reducing the potential for manipulation.[44]

Additionally, blockchain can enable regulators and law enforcement agencies to have direct access to company transaction data without needing to go through banking intermediaries, which often slow down corporate crime investigations. In traditional systems, legal authorities must submit formal requests to banks or financial institutions to obtain transaction data, a process that often takes months and can even be hindered by privacy regulations or differing jurisdictions. With a blockchain-based system, every transaction can be monitored in real-time (real-time monitoring), allowing regulators to detect indications of corporate crime more quickly.

However, for blockchain to function effectively in corporate criminal law, existing regulations must be updated to accommodate this technology within corporate accountability systems, particularly in the context of anti-money laundering (AML) and tax compliance. Currently, most AML regulations still rely on financial transaction reporting through traditional banking systems, which have many limitations in tracking blockchain-based financial activities. With the rise of smart contracts and digital assets, AML regulations must be expanded to detect and prevent money laundering practices conducted through decentralized blockchain systems. The European Union has begun adopting this approach through the Markets in Crypto-Assets Regulation (MiCA), which aims to enhance transparency in digital asset transactions and ensure that blockchain-based service providers comply with AML standards and investor protection.[45] However, this regulation is still in its early stages. It focuses more on controlling the digital asset

---

[44] Hoje Jo et al., "Corporate Governance and Financial Fraud of Wirecard," *European Journal of Business and Management Research* 6, no. 2 (March 25, 2021): 96–106, https://doi.org/10.24018/EJBMR.2021.6.2.708.

[45] Neal Christiansen et al., "AML for a Blockchain Age," *Journal of Financial Compliance* 7, no. 2 (December 1, 2023): 148, https://doi.org/10.69554/MJHT4148.

market rather than on how blockchain can be used in forensic auditing and corporate crime investigations.

Therefore, broader legal reforms must address the misuse of blockchain, particularly in cases where companies use this technology to hide assets or manipulate finances. One of the main challenges in this regard is companies' ability to exploit blockchain's anonymity features, making it difficult for authorities to trace illicit sources of funds or detect illegal financial activities. Additionally, the legal system must develop mechanisms that allow law enforcement agencies to access blockchain transaction records without violating corporate privacy rights and data protection principles applicable in various jurisdictions. If blockchain regulations are not carefully developed, companies may exploit legal loopholes by using blockchain to create layers of transactions that are difficult to trace, further complicating law enforcement efforts in corporate criminal cases.

To develop blockchain regulations that enhance corporate accountability, governments and regulators must take strategic steps that encompass various legal and technological aspects. First, governments need to establish a clear and adaptive regulatory framework that accommodates blockchain within legal compliance systems without hindering industrial innovation. These regulations must set standards for blockchain-based audits, real-time transaction monitoring mechanisms, and requirements for companies to record their transactions in an automatically auditable system. Second, regulators need to strengthen collaboration with the blockchain industry and community to ensure that the regulations created can be effectively implemented in the business world. Models such as regulatory sandboxes, which allow technology testing in a controlled legal environment, could be a solution to address regulatory uncertainty before full-scale rules are enforced.

Third, law enforcement agencies and auditors must be equipped with the necessary capacity to understand and utilize blockchain technology in overseeing and investigating corporate crimes. Without an adequate understanding of how blockchain works, existing regulations will not be effectively implemented. Fourth, governments must promote international cooperation in harmonizing blockchain regulations, as corporate crimes often involve cross-border transactions that require coordination between various legal jurisdictions.

In Indonesia, these strategic steps still need to be further developed, as existing blockchain regulations are currently limited to digital asset trading and do not yet cover corporate criminal accountability. Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No. 5 of 2019, which governs cryptocurrency trading, does not address how blockchain can be used in corporate audit and legal compliance systems. The Financial Services Authority (OJK) and Bank Indonesia (BI) also lack specific regulations requiring companies to use blockchain in financial reporting or business transparency systems.

To address this issue, Indonesia needs to adopt policies similar to those of countries that have advanced in blockchain regulation by introducing regulations that allow blockchain to be used as a legitimate legal compliance tool. Furthermore, strengthening regulations in corporate criminal law is also necessary so that blockchain can serve as an effective tool in preventing financial crimes and enhancing corporate accountability.

Proper legal reforms will balance protecting corporate rights and privacy rights with the need for transparency and accountability in corporate criminal law. By adopting more flexible and technology-based regulations, blockchain can be widely used as an instrument for legal compliance and corporate crime prevention, thus creating a more modern, transparent, and effective legal system to address the challenges of the digital era.

Conclusion

Blockchain has emerged as an innovative technology with the potential to revolutionize corporate criminal liability, particularly in enhancing transparency, security, and accountability in transactions and corporate legal compliance. With its decentralized nature, immutability, and real-time auditing capabilities, blockchain can serve as an effective tool for detecting fraud, preventing financial report manipulation, and strengthening both internal and external audit systems. Several countries have adopted this technology across various aspects of legal and corporate regulations, each employing different approaches to accommodate blockchain within corporate criminal law. Estonia has integrated

blockchain into government administration and business registration systems to improve corporate compliance oversight. The Estonian government utilizes this technology in its e-Residency system and tax records, ensuring that every corporate transaction and legal document is automatically verified and cannot be altered, thereby reducing the risk of data manipulation. In Switzerland, the Swiss Blockchain Act has established a regulatory framework that enables blockchain-based business registration and the use of smart contracts in financial transactions and corporate governance. This legal foundation strengthens the use of blockchain as a compliance tool, particularly in preventing money laundering and fraud in financial reports. Singapore, through the Monetary Authority of Singapore (MAS), has implemented regulatory sandboxes that allow companies to test blockchain-based compliance mechanisms before widespread implementation. This approach provides flexibility in adapting corporate criminal law regulations to accommodate increasingly complex digital transactions. Meanwhile, the European Union has begun integrating blockchain into its Markets in Crypto-Assets Regulation (MiCA) policy as part of its anti-money laundering (AML) strategy. However, its application in corporate criminal law enforcement remains in the early stages. Unlike these countries, Indonesia still faces challenges in adopting blockchain as an instrument for corporate criminal liability. Existing regulations, such as Bappebti Regulation No. 5 of 2019, remain limited to digital asset trading and do not regulate how blockchain can be utilized in financial audits, business transparency, and corporate transaction monitoring systems. The absence of binding regulations regarding the validity of blockchain as legal evidence in corporate criminal cases further hinders its implementation in Indonesia. To integrate blockchain into Indonesia's corporate criminal law system, legal reforms are necessary, including the standardization of blockchain use in corporate financial reporting, verification mechanisms for decentralized ledger-based transactions, and policies that allow law enforcement to access blockchain data without violating corporate privacy rights. More adaptive regulations and harmonization with global standards are also needed to ensure that blockchain functions as a legitimate legal instrument in securing corporate accountability and enhancing the

effectiveness of law enforcement against increasingly complex corporate crimes in the digital era.

References

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.

Annunziata, Filippo. "An Overview of the Markets in Crypto-Assets Regulation (MiCAR)." *SSRN Electronic Journal*, December 11, 2023, 1–72. https://doi.org/10.2139/SSRN.4660379.

Aro, Opeyemi E., Michael Nweze, Eli Kofi Avickson, Opeyemi E. Aro, Michael Nweze, and Eli Kofi Avickson. "Blockchain Technology as a Tool for Corporate Governance and Transparency." *International Journal of Science and Research Archive* 13, no. 1 (October 30, 2024): 2479–93. https://doi.org/10.30574/IJSRA.2024.13.1.1971.

———. "Blockchain Technology as a Tool for Corporate Governance and Transparency." *International Journal of Science and Research Archive* 13, no. 1 (October 30, 2024): 2479–93. https://doi.org/10.30574/IJSRA.2024.13.1.1971.

Arora, D, S Gautham, H Gupta, and B Bhushan. "Blockchain-Based Security Solutions to Preserve Data Privacy And Integrity." In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 468–72, 2019. https://doi.org/10.1109/ICCCIS48478.2019.8974503.

Bem Machado, Andreia de, Silvana Secinaro, Davide Calandra, and Federico Lanzalonga. "Knowledge Management and Digital Transformation for Industry 4.0: A Structured Literature Review." *Knowledge Management Research & Practice* 20, no. 2 (March 4, 2022): 320–38.

https://doi.org/10.1080/14778238.2021.2015261.

Chen, Christopher. "Rethinking the Regulatory Sandbox for Financial Innovation: An Assessment of the UK and Singapore." *Perspectives in Law, Business and Innovation*, 2020, 11–30. https://doi.org/10.1007/978-981-15-5819-1_2.

Christiansen, Neal, Valerie-Leila Jaber, Grant Rabenn, and Melissa Strait. "AML for a Blockchain Age." *Journal of Financial Compliance* 7, no. 2 (December 1, 2023): 148. https://doi.org/10.69554/MJHT4148.

Dostov, Victor, Pavel Shoust, and Ekaterina Ryabkova. "Regulatory Sandboxes as a Support Tool for Financial Innovations." *Journal of Digital Banking* 2, no. 2 (September 1, 2017): 179–88. https://doi.org/10.69554/UHEK4572.

Elst, Christoph Van der, and Anne Lafarre. "Blockchain and Smart Contracting for the Shareholder Community." *European Business Organization Law Review* 20, no. 1 (2019): 111–37. https://doi.org/10.1007/s40804-019-00136-0.

Erica, Archa, Silva Wulandari, and Riya Widayanti. "Data Security Transformation: The Significant Role of Blockchain Technology." *Blockchain Frontier Technology* 3, no. 2 (January 31, 2024): 107–12. https://doi.org/10.34306/BFRONT.V3I2.466.

Fauzi, Miftahul. "Dampak Dan Regulasi Fintech Terhadap Inklusi Keuangan Di Indonesia." *SANTRI : Jurnal Ekonomi Dan Keuangan Islam* 2, no. 6 (December 4, 2024): 143–54. https://doi.org/10.61132/SANTRI.V2I6.1028.

Feldman, Robert. "Enron." In *Professionalism and Values in Law Practice*, 54–63. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2020. https://doi.org/10.4324/9780429244704-12.

Hughes, Sarah Jane. "'Gatekeepers' Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes As Permission-Less Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money.'" *SSRN Electronic*

Journal, August 21, 2019, 1–40. https://doi.org/10.2139/SSRN.3436098.

Jahja, Nathan Junino, Nor Farizal Mohammed, and Norziana Lokman. "Corruption Cases in Relation to State-Owned Enterprise in Indonesia." *Proceedings of the International Conference in Technology, Humanities and Management (ICTHM 2023), 12-13 June 2023, Istanbul, Turkey* 131 (November 15, 2023): 533–43. https://doi.org/10.15405/EPSBS.2023.11.46.

Jain, Harshit, Khushi Jain, Vaibhav Paliwal, Chahat Begmal, and Palak Girdhar. "Towards Transparent Justice: Promoting Integrity and Efficiency in the Judicial System with Blockchain." *SSRN Electronic Journal*, May 29, 2024, 1–7. https://doi.org/10.2139/SSRN.4847643.

Jo, Hoje, Annie Hsu, Rosamaria Llanos-Popolizio, and Jorge Vergara-Vega. "Corporate Governance and Financial Fraud of Wirecard." *European Journal of Business and Management Research* 6, no. 2 (March 25, 2021): 96–106. https://doi.org/10.24018/EJBMR.2021.6.2.708.

Kesarkar, Tejal. "Blockchain Technology in Law Enforcement and Security: Overview." *International Journal for Research in Applied Science and Engineering Technology* 12, no. 6 (June 30, 2024): 1301–5. https://doi.org/10.22214/IJRASET.2024.63301.

Kizza, Joseph Migga. "Blockchains, Cryptocurrency, and Smart Contracts Technology: Security Considerations BT - Guide to Computer Network Security." edited by Joseph Migga Kizza, 533–58. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-38141-7_25.

Kontesa, Emelia, and Zico Junius Fernando. "Reclaiming Our Roots: Agrarian Law's Battle Against Land Grabbing." *Lex Scientia Law Review* 8, no. 2 (November 30, 2024): 1–10. https://doi.org/10.15294/LSLR.V8I2.10681.

Kristanto, Kiki, Zico Junius Fernando, Ridwan Arifin, and Anis

Widyawati. "The Convergence of Drug Trafficking and Terrorism: Uncovering the Dynamics of Narco-Terrorism." *Yustisia* 13, no. 3 (2024): 261–82. https://doi.org/10.20961/yustisia.v13i3.81599.

Ledoux, Esther Lea, and Nadia Smaili. "Cryptocurrency Fauds: The FTX Story." *Journal of Financial Crime*, 2024, 1–7. https://doi.org/10.1108/JFC-01-2024-0022/FULL/XML.

Lynch, Luann J., Cameron Cutro, and Elizabeth Bird. "The Volkswagen Emissions Scandal." *SSRN Electronic Journal*, November 10, 2021, 1–17. https://doi.org/10.2139/SSRN.2975251.

Mandayam, Rashmi. "The Role of Digital Forensics in Corporate Fraud Investigations." *IJIRMPS - International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences* 12, no. 6 (December 13, 2024): 1–4. https://doi.org/10.37082/IJIRMPS.V12.I6.231752.

Mechitov, Alexander, and Helen Moshkovich. "Estonia - A Small Giant of E-Government." *Journal of the Academy of Business and Economics* 21, no. 3 (October 1, 2021): 43–53. https://doi.org/10.18374/JABE-21-3.4.

Monika Juneja. "Blockchain Technology: Benefits, Challenges, Applications and Future Direction." *IJFMR - International Journal For Multidisciplinary Research* 6, no. 6 (December 2, 2024): 1–21. https://doi.org/10.36948/IJFMR.2024.V06I06.32265.

Patmanathan, Pvheanushaa, Kavitha Arunasalam, Kahyahthri Suppiah, and Dhamayanthi Arumugam. "The Effectiveness of Blockchain Technology in Preventing Financial Cybercrime." In *E3S Web of Conferences*, 389:1 25. EDP Sciences, 2023. https://doi.org/10.1051/E3SCONF/202338907022.

Reddy, Shiva Sumanth, Jahnavi S, and Manjunath D R. "Enhancing Data Security and Traceability in Supply Chain Management Using Blockchain Technology." *Journal of Cyber Security in*

Computer Systems 3, no. 3 (September 3, 2024): 11–24. https://matjournals.net/engineering/index.php/JCSCS/article/view/899.

Ross, James, and Giles Swan. "The Markets in Crypto Assets Regulation: What Should Firms Be Doing Now?" *Journal of Financial Compliance* 7, no. 4 (May 1, 2024): 302–8. https://doi.org/10.69554/ISTO4753.

Rusli, Rusli, and Firman Halawa. "Corporate Criminal Liability As An Insurance Crime Perpetrator Based On Law Number 1 Of 2023 On Criminal Law." *International Journal of Humanities Education and Social Sciences* 3, no. 4 (February 27, 2024): 2111–17. https://doi.org/10.55227/IJHESS.V3I4.908.

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 26, 2022): 386–401. https://doi.org/10.1093/POLSOC/PUAC014.

Sinaga, Henry Dianto P., and Andhy H. Bolifaar. "Blockchain Adoption for Plea Bargaining of Corporate Crime in Indonesia." In *ACM International Conference Proceeding Series*, 115–19. Association for Computing Machinery, 2020. https://doi.org/10.1145/3390566.3391680.

Suyanto et al. "Exploring Blockchain Technology for Transparency and Efficiency in Indonesia's Financial Sector." *Nomico* 1, no. 10 (November 30, 2024): 36–45. https://doi.org/10.62872/36J2SM39.

Taha, M M, and M Alanezi. "Cryptocurrencies in Blockchain Environment: The Verification Trip." In *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)*, 159–64, 2022. https://doi.org/10.1109/ICCRESA57091.2022.10352512.

Teichmann, Fabian Maximilian Johannes, Sonia Ruxandra Boticiu, and Bruno S. Sergi. "Wirecard Scandal. A Commentary on the Biggest

Accounting Fraud in Germany's Post-War History." *Journal of Financial Crime* 31, no. 5 (October 16, 2023): 1166–73. https://doi.org/10.1108/JFC-12-2022-0301/FULL/XML.

Truby, Jon. "Fintech and The City: Sandbox 2.0 Policy and Regulatory Reform Proposals." *International Review of Law, Computers & Technology* 34, no. 3 (September 1, 2020): 277–309. https://doi.org/10.1080/13600869.2018.1546542.

Wardhani, Dian Kusuma, Tjiptohadi Sawarjuwono, and Sasongko Budisusetyo. "Blockchain in Capital Markets: A Revolution of the Trading System in Stock Exchange." *The Indonesian Accounting Review* 12, no. 1 (January 7, 2022): 1–16. https://doi.org/10.14414/TIAR.V12I1.2437.

Wiggins, Rosalind Z., and Andrew Metrick. "The Lehman Brothers Bankruptcy H: The Global Contagion." *SSRN Electronic Journal*, April 8, 2015, 1–26. https://doi.org/10.2139/SSRN.2593081.

Wodi, Alexander. "The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review." *SSRN Electronic Journal*, 2023, 1–22. https://doi.org/10.2139/SSRN.4601142.

Zehnder, Fabian O. "An Analysis of the Adaptability of Switzerland's Financial Regulatory Framework to Blockchain and Digital Currency Innovations." *Frontiers in Management Science* 3, no. 5 (October 24, 2024): 47–55. https://doi.org/10.56397/FMS.2024.10.05.

Acknowledgment

We extend our heartfelt appreciation to all individuals and institutions whose invaluable support and contributions have played a crucial role in the completion of this article. We are equally grateful to the authors of books, journal articles, and other scholarly resources that have provided essential perspectives and a strong foundation for our analysis. Acknowledging that academic work is a continuous process of refinement, we warmly welcome feedback and constructive criticism from readers. This openness reflects our commitment to enhancing the quality and relevance of our research. We sincerely hope that this article serves as a meaningful resource for scholars, practitioners, and the broader community in navigating and addressing complex legal issues in everyday life.

Funding Information

None.

Conflicting Interest Statement

There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

In an effort to ensure the academic integrity and authenticity of published works, we are firmly committed to the principles of publishing ethics and material authenticity. Every work we publish undergoes a rigorous process of authenticity checking to prevent plagiarism and ensure that all sources are appropriately acknowledged and adhere to applicable standards of research ethics. We emphasize that each author is responsible for providing work that is not only innovative and contributes to existing knowledge but also upholds academic integrity. Violations of these principles will be taken seriously, and necessary steps will be taken to correct any errors or discrepancies. With this, we are committed to promoting an ethical and responsible academic environment where the originality and integrity of the work are placed at the highest level.