# "ORGANISATIONAL CHALLENGES IN IMPLEMENTING CRYPTOCURRENCY TRANSACTION MONITORING: AN ANALYSIS OF TRADITIONAL BANKING AND FINANCIAL INSTITUTIONS"

*Research Paper*

George Antoine Helou, Swiss School of Business and Management, Geneva, Switzerland, georgehelou@mail.com

## “Abstract“

*This paper provides a critical analysis of the organisational challenges associated with implementing cryptocurrency-based transaction monitoring in traditional banks. Despite blockchain and AI technologies having the potential to introduce greater transparency and detect anomalies in real time, the fragmentation of organisations, a lack of staff expertise and a lack of resources pose a bottleneck to the efficiency of these technologies. Comparative studies have shown that organisational inertia is often the cause of compliance failure, rather than technological incompetence. Suggested models include compliance by design, continuous human resource training and selective adoption of highly governed hybrid AI-blockchain frameworks. In combination with regulatory co-evolution, these approaches will be required to balance efficiency, accountability, and systemic stability in a rapidly evolving digital financial ecosystem.*

*Keywords: Cryptocurrency, Transaction monitoring, Organisational challenges, Banking, AML/CFT*

## 1 Introduction

### 1.1 Background on cryptocurrency integration in banking

The emergence of cryptocurrencies has caused significant disruption to the established financial system, putting pressure on current anti-money laundering (AML) frameworks. Their decentralised and pseudonymous nature not only enables legitimate breakthroughs, but also illegal ones (Almeida et al., 2023; Albrecht et al., 2019). The Financial Action Task Force (2021) and the European Commission (2024) have emphasised the urgent need for regulatory change due to the increasing tendency of criminals to use crypto assets to evade detection. Against this backdrop, traditional banks are under increasing pressure to align their compliance frameworks with the technological landscape, as traditional monitoring tools often prove ineffective (Campbell-Verduyn, 2018; Dupuis and Gleason, 2020).

## 1.2 Research problem

Despite regulatory efforts, banks face difficulties in operationalising effective cryptocurrency transaction monitoring. Dark silos of compliance, legacy infrastructures and a lack of integration with emerging technologies pose a barrier to robust implementation (Desmond et al., 2019; Zavoli and King, 2021). This issue is exacerbated by concerns regarding privacy, transparency and regulatory responsibility (Pocher and Mater, 2023). Consequently, there has been little discussion about the organisational aspects, namely how banks are structured, governed, and adapt to crypto-compliance.

## 1.3 Aim and objectives

The overarching research question that will guide this study is as follows: What organisational issues do traditional banks encounter when adopting effective cryptocurrency transaction monitoring, and how can these issues be resolved through technological and regulatory adaptation?

The threefold objective is as follows:

1. Critically assess the organisational and governance obstacles that impede the integration of crypto-monitoring by banks.

2. To assess opportunities and constraints of blockchain and AI-based compliance technology in institutions.

3. To give a strategic organisational response to ensure a balance between innovation, cost and regulatory expectations.

## 1.4 Significance

The significance of this question is that it shifts the debate elsewhere into the purely technical remedies and to the organisational conditioning that enables sustainable compliance. Institutional unpreparedness to implement technologies can result in minimal or even counterproductive outcomes, as demonstrated by Zavoli and King (2021) and Ferri (2024a). By placing crypto-monitoring within a broader framework of governance, training and resource distribution issues, this work contributes to our overall understanding of compliance capacity. Theoretically, it sheds light on the role of organisational design as a mediator of technical efficacy; practically, it informs banks and regulators on how to develop resilient strategies. In this way, the research positions organisational adaptation as a creator of AML/CFT objectives in the cryptocurrency era, rather than a peripheral concern.

# 2 Literature review

## 2.1 Current approaches to crypto transaction monitoring

Cryptocurrencies contribute to money laundering while also remaining open to surveillance. They are used for money laundering due to a lack of transparency and the ability to transfer money across borders, an area which is receiving increased research attention (Brenig, Accorsi and Müller, 2015; Albrecht et al., 2019). According to Dupuis and Gleason (2020), regulation has continued to lag behind innovation, which keeps banks in a reactive compliance trap. By contrast, Achebe, Ilori and Isibor (2023) view the irrevocable audit trails offered by blockchain as the future of AML work, an aspect that determines its potential utility. This contradiction highlights the paradox that cryptocurrencies facilitate money laundering (Barone and Masciandaro, 2019; Boyko, Dotscenko and Dolia, 2022) while also enabling the tracing of funds (Gabbiadini, Gobbi and Rubera, 2025). This discussion suggests that the quality of technology alone cannot be used to determine the monitoring strategies at the organisational level. Instead, the organisational capacity and readiness for governance must be taken into account when evaluating these strategies.

Artificial intelligence poses threats to efficiency and has dual uses. Iguodala and Oyiborhoro (2025) state that AI is better at spotting fraud thanks to its ability to detect tiny differences, while Liang et al. (2025a; 2025b) suggest using a combination of AI and blockchain technology to eliminate flaws in pseudonymity. However, there is also the issue of vulnerability: Ehi Esoimeme (2024) reminds us that AI tools can be misused, and Pettersson Ruiz and Angelis (2021) demonstrate that supervised learning can be exploited. In addition to technological considerations, scholars debate the systemic effects.

Ahmed et al. (2025) discuss systemic surveillance and Joshi (2025) presents a form of macroprudential risk referred to as crypto-integration, which generates stability-related responses. Conversely, Kader (2020) and Haykov (2024) argue that crypto and banking can coexist with effective governance. These conflicting views demonstrate the disparity between compliance and resilience, emphasising the necessity for organisational responses that incorporate technical tools into broader stability models.

## 2.2 Organisational implementation challenges

Organisational factors are crucial in determining the efficacy of cryptocurrency transaction monitoring. Zavoli and King (2021) empirically demonstrate that compliance is impeded by fragmented accountability and interdepartmental silos. These issues are supported by Aidoo (2025a) in their case studies and are found to positively correlate with weak organisational cultures and repeated AML failures. Trozze, Davies, and Kleinberg (2022) expand upon this finding, showing that the outcome of prosecuting crypto crimes is more dependent on institutional alignment regarding evidence handling and compliance reporting than on technological advancement.

However, Adesemoye et al. (2024) present a more optimistic view in their article, suggesting that organisational inertia can be mitigated by integrating digital currencies into the banking system with a carefully planned change management strategy. Together, these studies imply that institutional design is not merely a backdrop, but rather a determinant of whether novel monitoring technologies enhance or impede compliance effectiveness.

Another critical theme is the focus on human capital and resource allocation. While Indonesian banks view crypto monitoring as a complement to staff expertise, as demonstrated by Rolando (2025), Aidoo (2025b) emphasises that the compliance potential of blockchains relies on efficient training structures. Conversely, Subashi (2024) highlights the opacity of money laundering techniques as a key source of knowledge asymmetry that can only be mitigated through employee training.

These gaps are exacerbated by financial constraints. Ahmed et al. (2025) and Aghiad and Al-Dandachi (2024) found that banks were unable to modernise due to cost barriers, while Verma (2024) discovered that institutions with thin margins tended to view compliance as a regulatory liability. However, Achebe et al. (2023) argue that RegTech automation can restructure the long-term efficiency-generating compliance process. According to the literature, it is therefore important to reframe compliance as a strategic investment coupled with capability building in order to overcome organisational inertia.

### 2.3 Regulatory compliance requirements

One of the key issues in the literature is the regulatory environment for monitoring cryptocurrency transactions. According to the FATF (2021), new technologies present both opportunities and risks in relation to AML/CFT, necessitating the adoption of new analytics, albeit with enforcement remaining a challenge. The BIS (Aldasoro et al., 2025) has proposed institutional schemes to coordinate AML compliance across crypto-assets. However, critics argue that these schemes underestimate national regulatory diversity. Amponsah and Amponsah (2025), on the other hand, argue that the adoption of crypto regulations in Africa is uneven and that global frameworks have failed when applied to loose institutional settings.

The regulatory environment also complicates the monitoring strategies of banks, particularly in Europe and the United States. The European Commission (2024) favours integrated compliance with its AML/CFT package. Meanwhile, Pocher and Mater (2023) maintain that contradictions between anonymity and transparency are inherent in EU frameworks. Packin and Volovelsky (2023) demonstrate how NFTs are enforced in the US, highlighting the general tendency of regulators to apply the same AML strategies to new assets. However, Pocher (2025) cautions that excessive regulation could jeopardise the operational capacity of banks. Cross-jurisdictional research identifies these tensions as international standards are inconsistent (Yepes, 2011). Anggriawan and Susila (2024) highlight regulatory loopholes in the fight against terrorist financing in Indonesian banks, where the country's AML legislation is also flawed (Wardani, Ali and Barkhuizen, 2022). Futhermore, Von Hafe et al. (2025) reveal that fragmentation undermines not only the effective implementation of AML measures, but also stifles innovation, creating uncertainty within organisations.

## 3 Research methodology

### 3.1 Research design

The qualitative and exploratory research design employed in this study is most suitable for investigating the evolving and controversial nature of cryptocurrency regulation and compliance frameworks. As Huang (2021) and Campbell-Verduyn (2018) observe, cryptocurrencies present technical and socio-political challenges that require an interpretative approach to understand organisational responses. A case-based and thematic approach allows us to understand the various perspectives of scholars on anti-money laundering, blockchain and financial governance (Kolachala et al., 2021; Dupuis and Gleason, 2020). This approach does not rely on econometric analysis because similar data is still immature in different jurisdictions, which favours a discourse-based evaluation (Meszka, 2023; Desmond et al., 2019).

### 3.2 Data collection and sources

This study only employs secondary data, drawing on 66 academic sources such as journal articles, regulatory reports and policy papers. These sources will provide insight into both the conceptual discussion and practical case analyses of AML compliance in relation to cryptocurrencies (Almeida et al., 2023; Albrecht et al., 2019). International policy can be drawn from regulatory reports such as those from the FATF (2021), the European Commission (2024) and the BIS (Aldasoro et al., 2025), while empirical research (Johari et al., 2020; Zavoli and King, 2021) can demonstrate institutional implementation issues. The incorporation of studies spanning various jurisdictions:

Indonesian (Rolando, 2025; Wardani et al., 2022) and African settings (Amponsah and Amponsah,

2025), provides a basis for valuable comparisons. Sources were selected based on their focus on technical innovations (Liang et al., 2025a; Adedokun, 2025), legal frameworks (Pocher, 2025; von Hafe et al., 2025) and critical governance debates (Ferri, 2024a; Cassella, 2024).

### 3.3 Analytical framework

A critical literature synthesis was used to assess organisational challenges from three perspectives: structural, technological and regulatory. Concerns such as compliance silos and fragmented governance have been identified in relation to evidence of systemic flaws (Desmond et al., 2019; Zavoli and King, 2021). The potential and risks of convergence between blockchain and AI were discussed, with references to literature focusing on innovation (Adedokun, 2025; Iguodala and Oyiborhoro, 2025) as well as drawing attention to potential abuses (Ehi Esoimeme, 2024). Regulatory issues concerning the tension between transparency and privacy were considered based on sources such as the FATF (2021), Pocher and Mater (2023), and Soana and Arruda (2024). This framework enables the systematic assessment of organisational preparedness for the successful implementation of monitoring systems. Considering both positive (Achebe et al., 2023; Liang et al., 2025b) and critical (Subashi, 2024; Cassella, 2024) perspectives, this approach enables a balanced analysis of institutional constraints and generates new opportunities.

## 4 Results and findings

### 4.1 Organisational challenges

The literature consistently highlights organisational fragmentation as a significant challenge in monitoring cryptocurrencies within banking institutions. Johari et al. (2020) state that successful customer due diligence in the era of cryptocurrency requires unhindered coordination between the compliance, IT and operations teams. However, siloed organisational structures can hinder information sharing. Ibrahim (2019) also notes that the fragmentation of roles has reduced the ability of banks to identify terrorism financing risks associated with cryptocurrencies. Carlisle (2017), however, argues that regulatory supervision can drive institutional change by requiring departments to coordinate with each other. Nevertheless, this underestimates institutional inertia. Wardani, Ali, and Barkhuizen (2022) provide empirical evidence that legal frameworks requiring interdepartmental collaboration are impractical because resource asymmetry between units leads to further dysfunction.

A second obstacle relates to the shortage of skilled personnel. According to Hamilton (2024), the transformative potential of cryptocurrencies is compromised by personnel's inability to understand blockchain technology. Furthermore, Haykov (2024) highlights the issue of governance arising from the reliance of banks on external consultants. These shortcomings are evidenced by comparative research: Oana Florea and Nitu (2020) demonstrate the repeated failures of Romanian banks, while Pocher (2025) identifies similar issues within European institutions. These findings collectively suggest that organisational silos and a lack of technical knowledge prevent theoretical compliance ambitions from translating into operational practice.

## 4.2 Implementation barriers

The inability to transform legacy banking systems by adopting new technologies is directly linked to implementation challenges. While Knezevic (2018) recognises blockchain as a revolutionary technology, he also highlights that the existing infrastructure is outdated, preventing banks from fully leveraging its transparency. Leuprecht, Jenkins and Hamilton (2022) further support this view, demonstrating how institutional weaknesses, particularly outdated IT systems, create blind spots that are exploited by criminals. Some optimists, such as Rane, Choudhary and Rane (2023), suggest that the convergence of AI and blockchain is a viable integration trajectory, but this assumes that there is sufficient capital and technical investment to enable rapid technological upgrades. However, Aghiad and Al-Dandachi (2024) find that innovation is mostly theoretical, as many traditional banks remain stagnant due to bureaucratic processes and regulatory reluctance.

These barriers are exacerbated by issues with resource allocation. Joshi (2025) asserts that high monitoring costs are prohibitive at institutional levels and that crypto is viewed as a macroprudential threat. Verma (2024) asserts that banks view AML investment as a regulatory burden rather than a strategic asset, resulting in low compliance. By contrast, Iguodala and Oyiborhoro (2025) suggest that AI-powered fraud detection could enhance capacity and efficiency by reducing false positives. However, Dupuis and Gleason (2020) warn that regulatory dialectics guarantee increasing expenses despite cost savings. While these views differ on other aspects, they all agree that the ability of banks to adopt technological solutions is constrained by financial and strategic factors.

## 4.3 Strategic responses

Despite the remaining obstacles, the literature recognises a number of adaptive strategies. One such strategy is the public–private partnership: Packin and Volovelsky (2023) argue that these partnerships facilitate the exchange of information between banks, regulators and technology providers. However, Pocher and Mater (2023) warn that collaboration could result in a loss of accountability. The effectiveness of collaboration also depends on the jurisdiction, as Amponsah and Amponsah (2025) demonstrate by showing that it was more effective in Africa. In this context, they found that collaboration increased compliance, implying jurisdictional dependence.

Another strategic response is the introduction of hybrid compliance frameworks. Adedokun (2025) and Liang et al. (2025a; 2025b) emphasise the potential of AI–blockchain convergence for real-time monitoring and proactive detection. However, due to a lack of algorithmic transparency and poorly regulated systems, the use of algorithms remains problematic. Ehi Esoimeme (2024) reinforces this criticism by showing that AI tools can be used to circumvent protection, highlighting the dual-use aspect of innovation.

Technology is essential, as is regulatory adaptation. Soana and Arruda (2024) define the new privacy–traceability trade-offs with which central banks will have to deal when managing clients. Meanwhile, Von Hafe et al. (2025) show that fragmented European structures stifle innovation and create uncertainty. Yepes (2011) presents comparative evidence showing that harmonised international standards reduce compliance differences. All this evidence suggests that effective monitoring requires a combination of technology and laws that evolve together to strike a better balance between innovation and regulation.

| Theme | Key Findings | Implications for Banks |
|---|---|---|
| Cross-departmental Coordination | Organisational silos hinder collaboration across compliance, IT, and operations (Johari et al., 2020; Ibrahim, 2019). | Need to restructure responsibilities and create cross-functional compliance teams. |
| Knowledge & Capability Gap | Compliance staff lack blockchain expertise; reliance on external consultants undermines autonomy (Hamilton, 2024; Haykov, 2024; Oana Florea and Nitu, 2020). | Investment in staff training and in-house expertise is critical for sustainability. |
| Legacy System Integration | Legacy infrastructures prevent full use of blockchain transparency; outdated IT systems create vulnerabilities (Knezevic, 2018; Leuprecht et al., 2022). | Modernisation of IT infrastructure required to enable advanced monitoring integration. |
| Cost & Resource Allocation | Banks perceive compliance as a burden; constraints slow adoption of monitoring systems (Joshi, 2025; Verma, 2024; Dupuis and Gleason, 2020). | Reframe compliance costs as strategic investment in resilience, not sunk costs. |
| Public–Private Partnerships | Partnerships offer adaptive responses but raise accountability concerns (Packin and Volovelsky, 2023; Pocher and Mater, 2023). | Engage selectively in partnerships, balancing efficiency with clear accountability. |
| Hybrid AI–Blockchain Compliance | Convergence enhances detection but risks opacity and misuse (Adedokun, 2025; Liang et al., 2025a; Ehi Esoimeme, 2024). | Adopt hybrid monitoring frameworks with transparent governance safeguards. |
| Regulatory Adaptation | Legal fragmentation undermines strategies; harmonisation improves compliance but remains aspirational (Soana and Arruda, 2024; Von Hafe et al., 2025). | Advocate for harmonised regulations while adapting strategies to local contexts. |

*Table 1: Summary of Key Findings*

# 5 Recommendations

## 5.1 Capacitance and organisational integration

One of the key suggestions in the literature is the adoption of pragmatic organisational structures that integrate compliance into the broader business strategy. Ferri (2024a; 2024b) argues that AML strategies cannot function as standalone checklists and must be integrated into governance frameworks. Zavoli and King (2021) provide empirical evidence that accountability fragmentation hinders success.

Consequently, there is a proposal for compliance by design, in which regulation is considered an integral part of operations. However, the slow pace of cultural change in the banking industry restricts the feasibility of this approach.

In addition to structural changes, there is also a need for staff training. Aidoo (2025b) emphasises that blockchain is effective when operated by trained professionals, while Rolando (2025) demonstrates that investing in employee skill development enabled Indonesian banks to introduce monitoring as an extension of traditional banking practices. However, Subashi (2024) cautions that knowledge asymmetries will arise with transparency, and that knowledge must be developed continuously, not periodically.

## 5.2 Selective adoption and hybrid compliance models

Another suggestion relates to hybrid AI-blockchain monitoring models. Adedokun (2025) and Liang et al. (2025a; 2025b) recommend convergence technologies for real-time anomaly detection, offering a significant improvement on old systems. However, Ehi Esoimeme (2024) warns that this technology could be exploited to bypass security measures, highlighting the dual-use threat of innovation. This demonstrates how technology adoption cannot be complete without effective governance. Amponsah and Amponsah (2025) advocate a selective adoption approach, whereby banks implement convergence systems alongside human controls in close collaboration with regulators. This middle ground strikes a balance between efficiency and accountability, minimising the risks posed by technological opacity while capitalising on its advantages. Together, the literature emphasises that sustainable monitoring requires a dual commitment to institutional integration and the adaptive use of technological tools within rigorous administrative oversight structures.

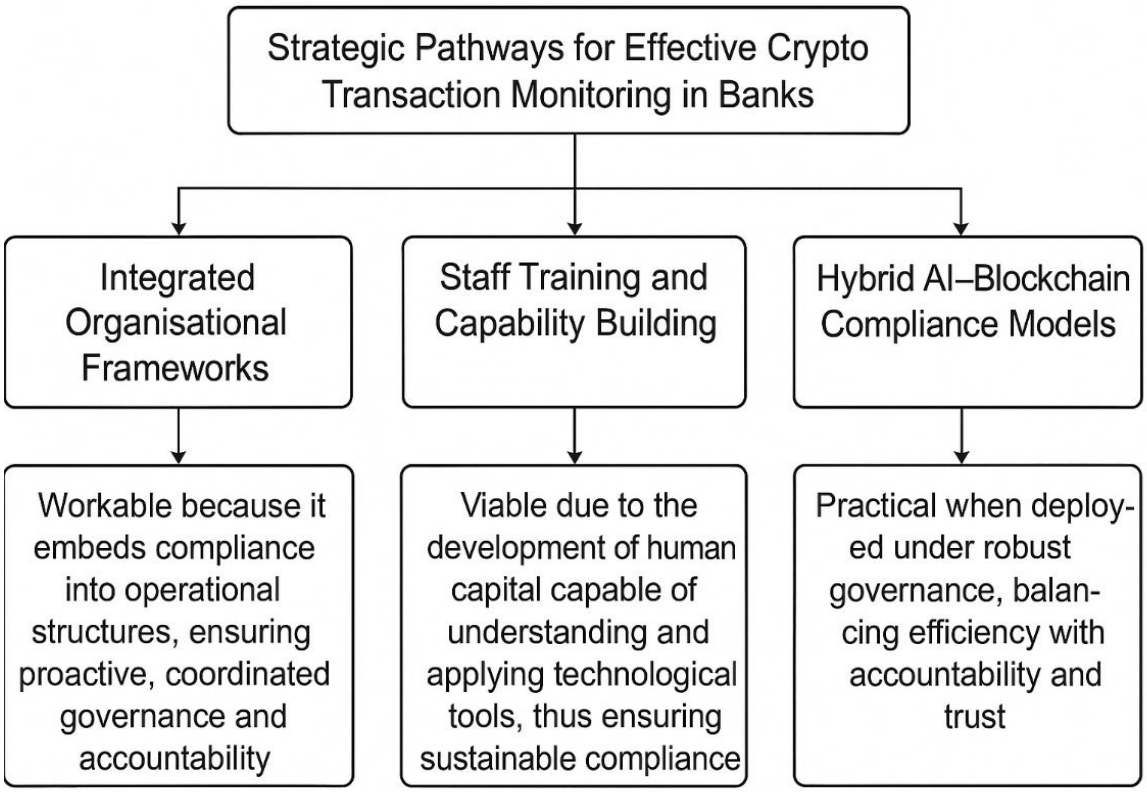


*Figure 1: Strategic recommendations*

## 6 Conclusion and future research

The present research has critically examined the organisational challenges faced by traditional banks when implementing cryptocurrency transaction monitoring, emphasising the interplay between compliance, governance, and technology. While the results demonstrate the potential of blockchain and AI technologies to increase transparency and efficiency (Adedokun, 2025; Liang et al., 2025a), they are constrained by organisational silos, expertise gaps, and existing infrastructures (Johari et al., 2020; Knezevic, 2018). Therefore, pragmatic approaches are required to ensure compliance is integrated into operational structures rather than being perceived as an ancillary benefit (Ferri, 2024a; Zavoli and King, 2021).

The analysis also emphasised the importance of human capital as the main determinant of compliance effectiveness, underscoring the importance of training staff to fill knowledge gaps within institutions (Aidoo, 2025b; Rolando, 2025). Similarly, hybrid monitoring models have potential, but require the ability to strike the right balance between efficiency, governance, and regulatory control (Ehi Esoimeme, 2024; Soana and Arruda, 2024). These results contribute to the discussion on how banks can balance innovation and compliance without impacting stability.

As identified by von Hafe et al. (2025) and Yepes (2011), future studies must extend these findings through comparative cross-jurisdictional research designs in order to understand how regulation can be used to inform organisational strategies. In addition, primary data based on interview methods with compliance experts might reinforce the secondary findings and remove the constraints identified in the specified study (Trozze et al., 2022). These recommendations will facilitate a more comprehensive understanding of the relationships between regulatory, technological and organisational forces, ensuring that financial institutions remain compliant in the rapidly evolving cryptocurrency ecosystem.

## References


Achebe, V.C., Ilori, O. and Isibor, N.J. (2023) 'Next-generation AML compliance: Leveraging blockchain innovations to disrupt money laundering networks', *International Journal of Multidisciplinary Research and Growth Evaluation*, 4(2), pp. 741–753.

Adedokun, T. (2025) 'Smart compliance: Opportunities and pitfalls in deploying AI-blockchain systems for real-time AML monitoring'.

Adesemoye, O., Chukwuma-Eke, E., Comfort, I., Lawal, Isibor, N., Akintobi, A. and Ezeh, F. (2024) 'Integrating digital currencies into traditional banking to streamline transactions and compliance', *International Journal of Advanced Multidisciplinary Research Studies*, 4(6), pp. 1942–1961.

Aghiad, A. and Al-Dandachi (2024) 'Impact of cryptocurrency on traditional banking systems', *Journal of University Studies for Inclusive Research*, 5, pp. 14393–14415.

Ahmed, B., Abrar, A., Ullah, M., Dawood, M.N. and Waheed, M. (2025) 'Cryptocurrency and traditional financial systems: Exploring the impact of cryptocurrencies on traditional banking systems, financial regulations, and monetary policies', *International Journal of Business and Management Sciences*, 6(1), pp. 587–609.

Aidoo, S. (2025a) 'Case studies of AML compliance failures: Lessons learned and national interest implications'.

Aidoo, S. (2025b) 'The role of blockchain in AML compliance: Potential applications and limitations'.

Albrecht, C., Duffin, K.M., Hawkins, S. and Morales Rocha, V.M. (2019) 'The use of cryptocurrencies in the money laundering process', *Journal of Money Laundering Control*, 22(2), pp. 210–216.

Aldasoro, I., Frost, J., Lim, S., Perez-Cruz, F. and Shin, H. (2025) 'BIS Bulletin No 111: An approach to anti-money laundering compliance for cryptoassets'.

Alkadri, S. (2018) 'Defining and regulating cryptocurrency: Fake internet money or legitimate medium of exchange?'.

Almeida, H., Pinto, P. and Fernández Vilas, A. (2023) 'A review on cryptocurrency transaction methods for money laundering', *arXiv*.

Amponsah, A.A. and Amponsah, A.A. (2025) 'Global crypto and digital asset regulations: African focus and worldwide outlook', *SSRN Electronic Journal*.

Anggriawan, R. and Susila, M.E. (2024) 'Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations', *Novum Jus*, 18(2), pp. 249–277.

Barone, R. and Masciandaro, D. (2019) 'Cryptocurrency or usury? Crime and alternative money laundering techniques', *European Journal of Law and Economics*, 47(2), pp. 233–254.

Boyko, A., Dotscenko, T. and Dolia, Y. (2022) 'Patterns of financial crimes using cryptocurrencies', *Socio-economic Relations in the Digital Society*, 2(44), pp. 23–28.

Brenig, C., Accorsi, R. and Müller, G. (2015) 'Economic analysis of cryptocurrency backed money laundering', *ECIS 2015 Completed Research Papers*.

Campbell-Verduyn, M. (2018) 'Bitcoin, crypto-coins, and global anti-money laundering governance', *Crime, Law and Social Change*, 69(2), pp. 283–305.

Carlisle, D. (2017) 'Virtual currencies and financial crime: Challenges and opportunities'.

Cassella, S. (2024) 'Editorial: Cryptocurrency and crime: Old crimes committed in new ways, or a new order of challenges for law enforcement?', *Journal of Financial Crime*, 31(5), pp. 1049–1051.

Desmond, D.B., Lacey, D. and Salmon, P. (2019) 'Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review', *Journal of Money Laundering Control*, 22(3).

Dülger, M.V. (2025) 'The use of crypto assets in money laundering and the measures to be taken against it', *SSRN Electronic Journal*.

Dupuis, D. and Gleason, K. (2020) 'Money laundering with cryptocurrency: Open doors and the regulatory dialectic', *Journal of Financial Crime*, 28(1), pp. 60–74.

Esoimeme, E. (2024) 'Examining the potential misuse of artificial intelligence to circumvent technology-based processes for AML/CFT compliance in the cryptocurrency ecosystem'.

European Commission (2024) 'Questions and answers: Anti-money laundering and countering financing of terrorism (AML/CFT)'.

FATF (2021) 'Opportunities and challenges of new technologies for AML/CFT'.

Ferri, C. (2024a) 'New approaches to old problems? Thinking about a new design of the AML/CFT strategy', *arXiv*.

Ferri, C. (2024b) 'New approaches to old problems? Thinking about a new design of the AML/CFT strategy', *arXiv*.

Gabbiadini, R., Gobbi, L. and Rubera, E. (2025) 'Money laundering and blockchain technology: Can you follow the trail of cryptocurrency transactions?', *SSRN Electronic Journal*.

Guidara, A. (2022) 'Cryptocurrency and money laundering: A literature review', *Corporate Law and Governance Review*, 4(2), pp. 36–41.

Hajj, M.E. and Farran, I. (2024) 'The cryptocurrencies in emerging markets: Enhancing financial inclusion and economic empowerment', *Journal of Risk and Financial Management*, 17(10), p. 467.

Hamilton, C. (2024) 'Money is morphing - Cryptocurrency can morph to be an environmentally and financially sustainable alternative to traditional banking', *Digital Commons@DePaul*.

Haykov, J.M. (2024) 'The evolution of currency: Bridging traditional banking and cryptocurrency with TNT', *Journal of Critical Realism in Socio-Economics (JOCRISE)*, 2(04), pp. 389–405.

Huang, S. (2021) *Cryptocurrency and crime*. Routledge eBooks, pp. 125–143.

Ibrahim, S.A. (2019) 'Regulating cryptocurrencies to combat terrorism-financing and money laundering', *Stratagem*, 2(1).

Iguodala, O.D. and Oyiborhoro, A. (2025) 'AI-powered anti-money laundering (AML) and fraud detection: Enhancing financial security through intelligent fraud detection', *World Journal of Advanced Research and Reviews*, 26(2), pp. 3702–3714.

Jaffery, H., Mehmood, S., Ahmed, M.S. and Gul, H. (2025) 'Study the role of blockchain in financial services: The impact of cryptocurrencies on traditional banking system and regulatory challenges', *Review of Applied Management and Social Sciences*, 8(1), pp. 251–262.

Johari, R.J., Zul, N.B., Talib, N. and Hussin, S.A.H.S. (2020) 'Money laundering: Customer due diligence in the era of cryptocurrencies'.

Joshi, P. (2025) 'Cryptocurrency vs traditional banking: A financial stability perspective'.

Kader, A. (2020) 'Cryptocurrency and traditional banking – A comparative economic analysis', *International Journal of Integrated Research and Practice*, pp. 85–97.

Knezevic, D. (2018) 'Impact of blockchain technology platform in changing the financial sector and other industries', *Montenegrin Journal of Economics*, 14(1), pp. 109–120.

Kolachala, K., Simsek, E., Ababneh, M. and Vishwanathan, R. (2021) 'SoK: Money laundering in cryptocurrencies', *The 16th International Conference on Availability, Reliability and Security*.

Lee, J. and Darbellay, A. (2025) *A research agenda for financial law and regulation*. Edward Elgar Publishing.

Leuprecht, C., Jenkins, C. and Hamilton, R. (2022) 'Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency', *Journal of Financial Crime*, 30(4).

Liang, W., Mary, B.J., Farinu Hamzah, Adedokun Taofeek and John, B. (2025a) 'AI and blockchain for AML: A policy and technology convergence to combat crypto-enabled financial crimes'.

Liang, W., Mary, B.J., Farinu Hamzah and Oluremi, D. (2025b) 'Next-Gen AML technologies and financial crime: The role of AI and blockchain in regulating cryptocurrency', *ResearchGate*.

Meszka, J. (2023) 'On modern crime – Money laundering and cryptocurrencies', *Ius et Administratio*, 45(2-4), pp. 5–17.

Oana Florea, I. and Nitu, M. (2020) 'Money laundering through cryptocurrencies'.

Ozili, P.K. (2022) 'CBDC, fintech and cryptocurrency for financial inclusion and financial stability', *Digital Policy, Regulation and Governance*, 25(1).

Packin, N.G. and Volovelsky, U. (2023) 'Digital assets, anti-money laundering and counter financing of terrorism: An analysis of evolving regulations and enforcement in the era of NFTs'.

Pettersson Ruiz, E. and Angelis, J. (2021) 'Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges', *Journal of Money Laundering Control*, ahead-of-print.

Pocher, N. (2020) 'The open legal challenges of pursuing AML/CFT accountability within privacy-enhanced IoM ecosystems'.

Pocher, N. (2025) *Crypto-asset ecosystems and the EU anti-money laundering framework*. Law, Governance and Technology Series. Springer International Publishing.

Pocher, N. and Mater, A. (2023) 'Distributed ledger technologies between anonymity and transparency: AML/CFT regulation of cryptocurrency ecosystems in the EU'.

Rane, N., Choudhary, S. and Rane, J. (2023) 'Blockchain and artificial intelligence (AI) integration for revolutionizing security and transparency in finance', *Social Science Research Network*.

Rolando, B. (2025) 'The impact of cryptocurrency on the traditional banking system in Indonesia: A threat or complement', *Jurnal Akuntansi dan Bisnis*, 5(1), pp. 15–28.

Saha, S., Ahmed Rizvan Hasan, Mahmud, A., Ahmed, N., Parvin, N. and Karmakar, H. (2024) 'Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda', *Multidisciplinary Reviews*, 7(8), pp. 2024168–2024168.

Soana, G. and Arruda, T. de (2024) 'Central bank digital currencies and financial integrity: Finding a new trade-off between privacy and traceability within a changing financial architecture', *Journal of Banking Regulation*.

Stefan, C. (2018) 'Tales from the crypt: Might cryptocurrencies spell the death of traditional money? – A quantitative analysis', *Proceedings of the International Conference on Business Excellence*, 12(1), pp. 918–930.

Subashi, R. (2024) 'Cryptocurrencies and money laundering', *Balkan Journal of Interdisciplinary Research*, 10(1), pp. 55–62.

Trozze, A., Davies, T. and Kleinberg, B. (2022) 'Explaining prosecution outcomes for cryptocurrency-based financial crimes', *Journal of Money Laundering Control*.

Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies, T. and Johnson, S.D. (2022) 'Cryptocurrencies and future financial crime', *Crime Science*, 11(1).

Verma, H. (2024) 'The impact of cryptocurrency on money laundering practices', *African Journal of Commercial Studies*, 5(2), pp. 51–60.

Von Hafe, F., Wagle, Y., Guede-Fernández, F., Giordano, A.P., Silva, L. and Azevedo, S. (2025) 'Legal frameworks for blockchain applications: A comparative study with implications for innovation in Europe', *Frontiers in Blockchain*, 8.

Wardani, A., Ali, M. and Barkhuizen, J. (2022) 'Money laundering through cryptocurrency and its arrangements in Indonesian Money Laundering Act', *Lex Publica*, 9(2), pp. 49–66.

Yepes, C. (2011) 'Compliance with the AML/CFT international standard: Lessons from a cross-country analysis'.

Zavoli, I. and King, C. (2021) 'The challenges of implementing anti-money laundering regulation: An empirical analysis', *The Modern Law Review*, 84(4), pp. 740–771.