International Journal of Research in Finance and Management

P-ISSN: 2617-5754
E-ISSN: 2617-5762
Impact Factor (RJIF): 5.32
IJRFM 2025; 8(2): 1003-1015
www.allfinancejournal.com
Received: 02-07-2025
Accepted: 25-07-2025

Oladapo Olatinsu
Rome Business School, Italy

Correspondence Author:
Oladapo Olatinsu
Rome Business School, Italy

Integrating digital asset platforms into AML frameworks: Balancing innovation, inclusion, and financial integrity

Oladapo Olatinsu

DOI: https://www.doi.org/10.33545/26175754.2025.v8.i2k.637

Abstract
Digital asset platforms, which range from centralised exchanges to increasingly hybridised rails that link decentralised protocols and traditional finance, present a recurring policy conundrum: how to stop financial crime without impeding technological advancement or keeping vulnerable groups out of financial services. In order to function well in the era of digital assets, this paper contends that current AML/CFT frameworks—which were created for the architecture of traditional finance—need to be both conceptually and practically redesigned. I present the Inclusion-Integrity-Innovation (I^3) model as an organising principle that centres regulatory design around results and proportionality. In terms of methodology, the study uses a targeted mixed-methods approach that includes semi-structured interviews with regulators, VASP compliance officers, and financial inclusion advocates in addition to a structured comparative analysis of regulatory regimes in eight to ten jurisdictions. The results highlight three key dynamics: (1) market entry and small-value access are significantly impacted by rule clarity and proportionality; (2) interoperable, privacy-preserving technical standards can minimise compliance friction while maintaining investigatory utility; and (3) lower-capacity jurisdictions are disproportionately burdened by global governance asymmetries, which are fuelled by standard-setting authorities and geopolitical pressures. In order to balance the trade-offs between innovation, inclusivity, and integrity, the paper ends with practical policy proposals at the international, national, and industry levels. These recommendations emphasise layered KYC, outcome-based international guidance, and investment in digital public infrastructure.

Keyword: Digital assets, Anti-Money Laundering (AML), financial inclusion, regulatory governance, Virtual Asset Service Providers (VASPs), Decentralized Finance (DeFi), innovation policy, financial integrity, proportional regulation, global AML standards

1. Introduction
The conventional framework of international financial regulation has been disrupted by the explosive growth of digital asset platforms during the past ten years. A complex ecosystem of centralised exchanges, custodial wallet providers, asset tokenisation services, crypto-payment rails, and hybrid interfaces that connect traditional finance and decentralised protocols has developed from what started out as a specialised technology experiment. More than 420 million people globally owned digital assets by 2024-2025, with adoption picking up speed in emerging nations where remittance requirements, inflation pressures, and gaps in financial infrastructure are particularly severe (World Bank, 2025). In an effort to apply AML/CFT rules that were initially developed for banks to a sector whose operational and technical dynamic differ greatly, the international community has simultaneously increased its scrutiny of illicit finance risks.

The conflict between the rigidity of AML standards and the dynamism of digital innovation has ramifications that go well beyond compliance departments. On the one hand, by imposing uniform identity-verification burdens that disproportionately affect migrants, informal workers, and low-income users, poorly calibrated AML regulations can stifle legitimate innovation, increase entry costs for smaller businesses, and deepen financial exclusion (Arner *et al.*, 2023) [3]. Inadequate safeguards, on the other hand, could make the financial system vulnerable to abuse, make it easier to evade sanctions, and undermine

confidence in digital asset markets. This risk is particularly significant given the growing technological sophistication of illicit actors (Europol, 2024; United Nations Office on Drugs and Crime [UNODC], 2025).

1.1 Problem Statement
Existing AML rules are still not well suited to the risk surfaces and technical realities of digital asset platforms, despite intense regulatory activity. Although VASPs frequently operate across borders, rely on cryptographic rather than identity-based assurances, and interact with decentralised environments that lack a natural compliance anchor, traditional frameworks assume centralised control, stable intermediaries, and clearly defined jurisdictions. As a result, there is a mismatch where regulations are underinclusive in some areas and overbroad in others.

1.2 Scope and Focus
This study avoids diluting the analysis by concentrating mostly on centralised digital asset platforms, such as exchanges, custodial services, and payment intermediaries, and only using examples of decentralised finance where they highlight regulatory blind spots. Unless they are explicitly related to AML risk vectors, NFTs, DAOs, and solely non-custodial tooling are not included.

1.3 Research Questions
This study investigates three guiding questions:
1. How can AML frameworks integrate digital asset platforms more effectively while minimizing unintended negative effects on innovation and financial inclusion?
2. What regulatory design features correlate with stronger outcomes across financial integrity, market dynamism, and access?
3. How do geopolitical, institutional, and rights-based factors shape the feasibility of AML models for digital assets?

1.4 Contribution of This Study
This paper makes three significant contributions to current research and policy discussions:
Firstly, it introduces The Inclusion-Integrity-Innovation (I^3) Framework, a systematic lens for assessing AML policy trade-offs in digital finance. Few studies present a model that integrates all three in a logical, outcome-based way, despite the fact that many focus on individual dimensions like integrity or innovation.
Second, it produces empirical insights through a two-phase mixed-methods study that includes semi-structured interviews with regulators, compliance practitioners, and financial inclusion specialists as well as a structured regulatory comparison across eight to ten jurisdictions. According to recent research, there are comparatively little empirical analyses of regulatory consequences in digital asset markets, and AML research is still mostly conceptual and compliance-driven.
Third, the analysis highlights how international pressure and asymmetric power dynamics influence national regulatory methods by placing digital asset AML within the larger political economy of global norm setting (FATF, 2023). For lower-income jurisdictions that must comply with regulations without the necessary capacity or technical infrastructure, this factor is especially crucial.

2. Conceptual & Theoretical Framework
The study's multi-layered conceptual and theoretical framework is developed in this section. It presents the Inclusion-Integrity-Innovation (I^3) analytical paradigm, connects with several governance and social science ideas, and offers operational definitions. The empirical design, case selection, and interpretation of the findings that are reported later in the study are all guided by these frameworks taken together.

2.1 Key Definitions and Operational Scope
2.1.1 Digital Asset Platforms (DAPs) and VASPs
Digital asset platforms, or DAPs, are organisations that make it easier to store, trade, transfer, convert, or manage digital assets. Although this description is operationalised here into three categories utilised in the empirical research, it is consistent with the FATF's classification of Virtual Asset Service Providers (VASPs):

1. **Centralized Custodial Platforms**
- Exchanges, custodial wallets, broker-dealers.
- **Criteria:** entity holds private keys; user onboarding requires KYC; platform manages order books.

2. **Hybrid or Semi-Custodial Platforms**
- Platforms enabling partial user control over assets but intermediating critical functions (e.g., smart-contract-assisted custody, off-chain settlement layers).
- **Criteria:** custody partially user-controlled but compliance obligations still fall on an identifiable operator.

3. **Interfacing Platforms**
- Fiat on-ramps, payment processors, and OTC desks linking traditional financial systems to digital networks.
- **Criteria:** services rely on banking-system integration, identity rails, and cross-jurisdictional financial controls.

These categories are essential for cross-country comparability. They inform which regulatory obligations apply and how AML requirements translate into operational practice.

2.1.2 Selective Use of DeFi
DeFi is only used analytically to draw attention to regulatory blind spots. Only the following aspects of non-custodial wallet providers, automated market makers, and DAO-based governance mechanisms are discussed:
- The lack of natural compliance anchors;
- The technical limitations of identity-based AML; and
- Conflicts between decentralised design and centralised regulatory mandates.

By using a selective method, the investigation is limited to areas of the ecosystem that are most pertinent to AML regimes that can be measured empirically.

2.1.3 AML/CFT Processes in Digital Finance (Operational Definitions)
AML mechanisms are operationalised as follows for

methodological clarity:

- **Customer Due Diligence (CDD):** Assessed using tiered thresholds, digital ID acceptance, and documented criteria.
- **Transaction Monitoring:** Determined by SAR filing thresholds, blockchain forensics integration, and algorithmic surveillance.
- **Travel Rule Compliance:** Measured by reporting requirements and message standard interoperability.
- Supervisory Intensity: Determined by audit frequency, license requirements, and enforcement actions.

2.2 Polycentric Regulatory Governance Theory (Expanded)

A fundamental perspective for comprehending the regulatory dynamics of digital assets is provided by polycentric governance. State regulators, international organisations (FATF, BIS), private standards, blockchain protocol rules, and analytics companies whose risk scores impact supervisory actions are some of the overlapping centres of authority that define digital asset markets instead of relying on a single hierarchical regulator.

2.2.1 Power Asymmetries and Regulatory Hierarchies

Polycentricity does not imply equality, even while it highlights multiplicity. Regulatory asymmetry is exemplified by FATF's impact over national policymaking, particularly for lower-income states that rely on correspondent banking arrangements. Many states apply standards under implicit coercive pressure, resulting in a top-down hierarchy within a supposedly polycentric system, according to research in global financial governance (e.g., IMF and World Bank evaluations, FATF mutual assessments).

2.2.2 Relevance to Digital Asset AML

This framework explains:

- Why global mandates (e.g., Travel Rule) can be politically binding even when technically infeasible.
- Why decentralized networks disrupt assumptions built into AML frameworks.
- How compliance burdens are unevenly distributed across jurisdictions and firm sizes.

Thus, polycentric governance shapes both regulatory design and its unequal impacts.

2.3 Additional Theoretical Anchors

2.3.1 Financial Inclusion Theory (Crypto-Specific Expansion)

Traditional financial inclusion theory focuses on access, affordability, and institutional trust. In digital asset contexts, inclusion is shaped by additional factors:

- **Identity barriers:** Many users lack formal IDs required by standardized CDD.
- **High-friction onboarding:** Uniform KYC demands can exclude migrants, informal workers, and populations in fragile states.
- **Alternative access pathways:** Crypto often acts as a parallel financial rail when banks are inaccessible, costly, or politically restricted.
- **Remittance corridors:** In some jurisdictions, crypto reduces costs and processing times, but AML tightening can shut down access points.
- **Gender and demographic gaps:** Women and older adults exhibit lower digital asset adoption partly due to KYC friction and technological literacy barriers.

This expansion embeds inclusion concerns directly into the AML debate rather than treating them as externalities.

2.3.2 Contextual Integrity & Privacy-Preserving Compliance

Applying Nissenbaum's *Contextual Integrity* highlights that AML systems must balance investigatory needs with appropriate data flows. Digital asset environments introduce new dimensions:

- Blockchain analytics create "behavioral identity maps" even without formal KYC.
- Probabilistic heuristics risk false positives and over-surveillance.
- Cross-border data sharing may violate contextual privacy norms or local data-protection laws.

Emerging privacy-preserving technologies—zero-knowledge proofs, selective disclosure credentials, and secure multiparty computation—indicate that high-integrity compliance can coexist with privacy safeguards. Yet adoption varies widely across jurisdictions, shaping regulatory outcomes.

2.3.3 Innovation Theory (Mechanism-Focused)

Innovation theory explains how regulatory design affects market evolution. In digital asset sectors:

- Regulatory uncertainty depresses venture investment, delays product launches, and discourages licensing.
- Compliance path dependency forms when early AML decisions lock markets into costly architectures.
- Innovation bottlenecks arise from high onboarding costs, inconsistent cross-border requirements, and unclear supervisory expectations.
- Comparative dynamics e.g., EU MiCA's clarity vs. U.S. enforcement-driven ambiguity, illustrate how regulatory regimes shape innovation geography.

This study examines these mechanisms empirically through cross-jurisdictional comparison.

2.4 The Inclusion-Integrity-Innovation (I^3) Framework (Expanded and Formalized)

The I^3 framework integrates the three pillars central to digital asset AML policymaking. The expanded version incorporates causal pathways, measurable indicators, and hypothesized trade-offs.

2.4.1 Integrity Dimension (I_1): Preventing Illicit Finance

Indicators include:

- SAR/STR quality rather than quantity
- Enforcement outcomes, not merely inputs
- Misuse reduction metrics (e.g., proportion of illicit flows through exchanges)

Mechanism: Higher integrity arises from proportional rules, accurate analytics, and well-designed reporting systems—not simply from increased compliance burdens.

2.4.2 Inclusion Dimension (I_2): Equitable Access

Indicators include:

- Onboarding friction (time, requirements, rejection rates)
- Acceptance of digital ID; availability of tiered KYC
- Access to low-value, high-frequency services

Mechanism: Overly rigid AML frameworks raise access costs, disproportionately affecting vulnerable groups. Conversely, calibrated rules and digital public infrastructure can expand access.

2.4.3 Innovation Dimension (I_3): Market Dynamism

Indicators include:

- Regulatory clarity indexes
- New firm registrations and licensing timelines
- R&D investment and interoperability standards

Mechanism: Clear, proportionate rules encourage experimentation and investment, while unclear or punitive regimes produce market stagnation.

2.4.4 Hypothesized Trade-offs

Drawing on regulatory theory, the study advances the following hypotheses:

- **H1:** More proportionate AML rules correlate with higher inclusion outcomes without significantly reducing integrity.
- **H2:** Regulatory clarity correlates with stronger innovation indicators.
- **H3:** Excessively stringent AML mandates reduce inclusion, particularly in developing countries with weaker ID systems.
- **H4:** Global AML pressures create uneven compliance burdens, shaping divergent national outcomes.

These hypotheses structure the empirical investigation.

2.5 Linking the Framework to the Methodology

The conceptual foundations directly inform the research design in Section 7:

- Operational definitions guide jurisdiction classification and variable coding.
- Polycentric governance informs case selection, emphasizing jurisdictions with different regulatory centers of gravity.
- Inclusion, Integrity, and Innovation indicators operationalize the dependent variables for comparative analysis.
- Privacy and innovation theories shape interview questions on trade-offs and institutional constraints.

This alignment ensures theoretical consistency from conceptual grounding to empirical analysis.

3. Literature Review

Research on digital assets and AML regulation spans diverse disciplines—financial regulation, computer science, international political economy, development studies, privacy engineering, and behavioral economics. Yet the literature remains disjointed, with each field illuminating only parts of the regulatory puzzle. This review synthesizes and critically engages with the most relevant bodies of knowledge, highlighting tensions, empirical findings, and unresolved debates that shape the core problem of integrating digital asset platforms into AML frameworks while balancing innovation and inclusion.

3.1 AML/CFT Frameworks: Effectiveness, Costs, and Structural Tensions

The traditional AML literature underscores broad concerns about effectiveness, proportionality, and structural burdens. Early critiques showed that AML systems often produce vast reporting outputs but limited measurable disruption of illicit finance. Contemporary assessments—particularly from the IMF, World Bank, and FATF mutual evaluation reports—continue to highlight persistent gaps between compliance *activity* and compliance *impact* (IMF, 2023).

Several studies note that AML regimes disproportionately affect smaller institutions due to fixed compliance costs, and this dynamic appears even stronger among Virtual Asset Service Providers (VASPs), where the cost of implementing Travel Rule messaging, blockchain analytics, and enhanced due diligence can exceed operational capacity (Basel Institute on Governance, 2024).

In digital asset markets, empirical studies complicate narratives of pervasive crypto-based criminality. Blockchain analytics firms and academic economists have shown declining proportions of illicit activity relative to overall transaction volumes, though absolute values remain meaningful. This indicates that AML policies should target specific risk clusters—mixing services, high-risk exchanges, privacy coins—rather than treating the entire ecosystem as inherently high-risk.

Unresolved Tension: Global AML frameworks remain identity-centric, but digital asset networks—especially non-custodial systems—do not consistently generate centralized intermediaries or identity anchors. This structural misalignment recurs throughout the literature but lacks sustained scholarly integration.

3.2 Regulatory Approaches: Divergences, Capacities, and Institutional Pathways

Comparative research highlights significant variation in digital asset regulation. The EU's MiCA framework seeks regulatory clarity through harmonized licensing, explicit AML obligations, and consumer protection controls (European Commission, 2023). Singapore and the UAE similarly pursue structured innovation environments using regulatory sandboxes and progressive licensing regimes (Monetary Authority of Singapore, 2022). Meanwhile, the U.S. relies on fragmented statutory interpretations and enforcement actions, generating legal uncertainty for platforms and investors.

A notable theme across jurisdictions is the interplay between supervisory capacity and regulatory outcomes. Countries with high institutional competence—Japan, South Korea, Switzerland—tend to implement more nuanced, risk-

based rules and show higher compliance quality (Arner, Barberis & Buckley, 2020) [1]. Lower-capacity jurisdictions often resort to blunt, high-friction AML rules to avoid FATF criticism, even when such measures suppress local digital economies.

Recent policy evaluations further emphasize polycentricity: national regulators, global standard-setters (FATF, BIS), blockchain protocols, industry consortia, analytics firms, and payment networks simultaneously shape compliance norms. The literature increasingly recognizes that digital assets cannot be governed through state law alone—a central insight informing this paper's theoretical framing.

3.3 Financial Inclusion: Opportunities, Barriers, and Unintended Exclusions

Financial inclusion research from development economics and global finance underscores the welfare and growth benefits of expanding access to payment systems, credit, and remittances (Demirgüç-Kunt *et al*., 2022; Suri, 2021) [7, 18]. Digital payments and mobile money have offered empirical evidence of reduced onboarding friction and expanded participation for underserved populations (GSMA, 2023; World Bank, 2022).

Digital assets have entered this discourse more recently. Empirical case studies document their use as alternative financial rails in contexts of inflation, currency restrictions, sanctions, and weak financial infrastructure. Low-income and migrant populations often turn to digital assets for remittances and informal savings, exhibiting behaviors shaped by both necessity and opportunity.

Yet AML rules can produce substantial exclusionary effects:

- Rigid KYC standards disproportionately affect users without formal IDs (UNHCR, 2022).
- Uniform compliance obligations make low-value transactions costly to process.
- Platform derisking—closing accounts or restricting services due to compliance uncertainty—affects diaspora communities and gig workers relying on cross-border platforms.

The literature acknowledges these exclusion dynamics but lacks integrated frameworks linking AML proportionality, digital asset innovation, and inclusion outcomes—a gap the I³ framework aims to fill.

3.4 DeFi, Non-custodial Systems, and the Regulatory Perimeter

A growing literature examines decentralized finance (DeFi) and non-custodial ecosystems, highlighting the complex regulatory implications of programmable, permissionless financial infrastructure. DeFi protocols challenge the assumptions baked into AML frameworks: they lack centralized intermediaries, operate across borders instantaneously, and allow composability (i.e., protocols interacting like modular software components) (Arner & Buckley, 2021; BIS, 2023) [2, 5].

Scholars and regulators debate whether:

- Interface providers (e.g., front-end hosts),
- DAO governance participants,
- Liquidity providers, or
- Protocol developers

should bear AML obligations. BIS and IMF reports propose embedded supervision—using on-chain monitoring to ensure compliance without relying on intermediaries—though technical feasibility remains uncertain (BIS, 2023) [5].

DeFi also introduces new forms of risk: MEV (Miner/Validator Extractable Value), oracle manipulation, governance capture, and cross-chain bridge vulnerabilities. The literature shows that AML-focused analyses often overlook these technical vectors, while computer scientists rarely engage with regulatory constraints. This siloing underscores the need for cross-disciplinary synthesis.

3.5 Privacy, Surveillance, and Contextual Integrity

Privacy scholarship, both technical and normative, provides important insights into AML implementation. Nissenbaum's theory of Contextual Integrity underscores that privacy depends on appropriate flows of information, not secrecy (Nissenbaum, 2010) [16]. In digital assets, concerns arise from:

- Probabilistic clustering of blockchain addresses,
- Metadata correlation across analytics tools,
- Cross-border information transfers,
- SAR databases with weak oversight,
- and commercial surveillance incentives embedded in compliance technologies.

Emerging privacy-preserving compliance tools—zero-knowledge proofs, selective disclosure credentials, secure multiparty computation, and decentralized identifiers—offer possible reconciliation between privacy and regulatory observability. However, adoption remains limited due to high costs, operational complexity, and regulatory ambiguity.

Critical perspectives highlight that AML regimes increasingly resemble financial surveillance systems whose societal and human rights implications are insufficiently evaluated (UN Special Rapporteur on Privacy, 2021; EFF, 2022). Integrating these insights helps situate AML debates beyond purely technocratic frames.

3.6 Behavioral, Sociotechnical, and Economic Perspectives

There is a growing set of interdisciplinary literatures relevant to AML and digital asset adoption:

3.6.1 Behavioral Economics

Studies indicate that crypto adoption is heavily influenced by risk perceptions, peer effects, cognitive biases, and beliefs about institutional trust—factors largely absent in AML studies. This matters because compliance regimes can distort user behavior in unpredictable ways.

3.6.2 Science and Technology Studies (STS)

STS scholarship shows how governance values become embedded into technical infrastructures. Applying this lens suggests that blockchain design choices, wallet architectures, and protocol rules implicitly encode policy priorities, shaping AML feasibility.

3.6.3 Law and Economics & Regulatory Burden Research

Outside the crypto context, extensive research demonstrates that regulatory complexity depresses innovation, increases

market concentration, and acts as a barrier to entry. Applying this literature can illuminate the competitive dynamics observed in digital asset compliance.

3.6.4 Distributed Systems and Cryptography

Academic work on consensus mechanisms, protocol security, randomness beacons, ZK-proofs, and threshold cryptography is highly relevant to AML's technical options but often overlooked by policy scholars.

Incorporating these perspectives enriches understanding of the socio-technical landscape in which AML operates.

3.7 Political Economy: Power, Hierarchy, and Global AML Governance

A robust literature shows that AML standards are shaped by geopolitical power and institutional dominance (Sharman, 2017; Drezner, 2021) [19, 8]. FATF's greylisting and blacklisting mechanisms significantly affect capital flows, bank de-risking, and national economic outcomes—especially in low-income countries (IMF, 2023).

For digital assets, the political economy lens becomes critical:

- Smaller states often implement stringent crypto AML rules to avoid international censure.
- High-capacity states exercise interpretive flexibility, shaping global norms while shielding domestic innovation.
- Blockchain analytics firms become quasi-regulators through risk rating systems embedded in compliance processes.

This lens clarifies why AML burdens vary globally and why innovation geographies fragment along regulatory lines.

3.8 Synthesis: Gaps and Contributions Identified

Across these intersecting literatures, several gaps justify this study:

i. **Lack of multidimensional integration:** Few studies reconcile AML integrity with financial inclusion and innovation dynamics simultaneously.
ii. **Weak empirical cross-country comparisons:** Most analyses are jurisdiction-specific, lacking structured methodological consistency.
iii. **Insufficient attention to supervisory capacity:** Capacity differentials crucially shape outcomes but remain under-theorized.
iv. **Underdeveloped treatment of privacy-preserving technologies:** Technical possibilities are acknowledged but rarely integrated into regulatory analysis.
v. Limited engagement with DeFi governance and protocol-level incentives.
vi. Sparse incorporation of political economy and global asymmetry considerations.
vii. Inadequate exploration of behavioral dynamics that shape adoption, compliance, and risk.

The present paper addresses these gaps through the Inclusion-Integrity-Innovation (I^3) framework and a comparative mixed-methods methodology.

4. Methodology

In order to investigate how digital asset platforms are incorporated into Anti-Money Laundering (AML) frameworks across jurisdictions and how these frameworks balance the overlapping objectives of innovation, financial inclusion, and financial integrity, this study uses a mixed-methods, multi-layered research approach. The methodology, which combines qualitative expert interviews, document review, and comparative regulatory research, is purposefully pluralistic. The Inclusion-Integrity-Innovation (I^3) framework, polycentric governance, and contextual integrity are the theoretical underpinnings of this system, which guarantees analytical traction in technical, legal, and institutional domains.

4.1 Research Design Overview

Three basic concepts underpin the methodological design:

(1) Comparing different jurisdictions: The study analyses several jurisdictions with different regulatory regimes in order to assess how different levels of capability, regulatory philosophy, and economic context affect AML outcomes in digital asset markets.

(2) Cross-data type triangulation : No single dataset fully captures all pertinent variables because digital asset regulation functions at the nexus of law, technology, and international standards. The constraints of each source are lessened by triangulating data from document analysis, interview insights, and regulatory indicators.

(3) Adherence to the I^3 framework proportionately: Inclusion, Integrity, and Innovation (I^3) indicators are operationalised into quantifiable variables, enabling empirical assessment of the previously proposed trade-offs.

4.2 Jurisdiction Selection and Comparative Framework

Instead of using randomisation, deliberate comparative sampling is used to choose the jurisdictions. This guarantees representation in:

1. High-capacity, innovation-focused jurisdictions with robust regulatory bodies and well-established digital asset markets, such as the EU/MiCA, Singapore, Japan, and South Korea.
2. Expansive, intricate regulatory frameworks with worldwide market effect, such as those found in the United States and the United Kingdom.
3. Emerging or lower-capacity jurisdictions, such as Nigeria, the Philippines, Kenya, Argentina, and the United Arab Emirates, have varied institutional capacities, varied patterns of digital asset usage, and differing levels of exposure to FATF pressure.

The reasoning is to enable comparison inference across several regulatory paradigms rather than to attain representativeness.

A structured comparative coding framework is used to ensure consistency across cases. Categories include:

- AML legal provisions and licensing rules
- KYC/CDD requirements and acceptance of digital ID
- Travel Rule implementation mechanisms
- Enforcement intensity and supervisory capacity
- Innovation incentives (e.g., sandboxes, clear licensing pathways)
- Inclusion metrics (access to low-value services, derisking patterns)

These indicators map onto the I³ framework to permit systematic comparison.

4.3 Data Sources

4.3.1 Primary Data: Expert Interviews

Semi-structured interviews are conducted with three target groups:

1. Regulators and legislators, including digital asset policy leaders, financial intelligence unit (FIU) employees, and AML supervisors.
2. Industry participants, including payment intermediaries, blockchain analytics experts, compliance officers, and legal counsel at exchanges and VASPs.
3. Experts in financial inclusion and civil society, such as development economists, digital rights activists, and non-governmental organisations engaged in ID systems or remittance corridors.

Usually lasting between 45 and 75 minutes, interviews adhere to a set methodology but include room for expansion. Unless express permission for attribution is given, respondent anonymity is preserved.

Interview themes include:

- perceived AML risks and mitigation strategies,
- compliance burdens and technological barriers,
- inclusion impacts of regulatory design,
- supervisory constraints,
- cross-border implementation challenges,
- perspectives on privacy-preserving compliance.

Interviews provide contextual nuance unavailable in legislation or official reports.

4.3.2 Secondary Data: Document and Policy Analysis

This includes:

- FATF guidance, mutual evaluation reports, follow-up assessments;
- IMF and World Bank regulatory capacity assessments;
- national legislation on digital assets and AML;
- consultation papers, enforcement notices, supervisory guidelines;
- academic literature, industry reports, and civil society analyses;
- MiCA delegated acts and technical standards;
- public policy statements from central banks and securities regulators.

Textual materials are coded using a directed content analysis approach, guided by the I³ framework.

4.3.3 Quantitative and Semi-Quantitative Data

Quantitative indicators, such as licensing timelines and approval rates, the number of enforcement actions, AML supervisory staffing levels, compliance cost estimates for small vs. large VASPs, digital ID adoption rates, remittance cost data from global databases, and illicit-flow metrics from blockchain analytics firms (treated cautiously and triangulated), help with comparative evaluation even though the research is qualitatively driven.

The factual foundation of regulatory disparities is supported by the integration of various data.

4.4 Analytical Approach

4.4.1 Coding Procedure

Interview transcripts and documents are coded using NVivo (or equivalent). The initial codebook derives deductively from the I³ framework:

- **Integrity codes:** AML outcomes, risk mitigation tools, SAR quality, enforcement patterns.
- **Inclusion codes:** onboarding friction, derisking, marginalized user groups, digital ID barriers.
- **Innovation codes:** regulatory clarity, market entry, sandbox participation, entrepreneurial constraints.

Additional codes emerge inductively during the analysis to capture unanticipated themes (e.g., governance bottlenecks, vendor dependency, cross-chain challenges).

4.4.2 Cross-Case Comparative Analysis

Regulatory model, supervisory capability, AML architecture, innovation environment, and inclusion outcomes are all captured in a structured matrix that summarizes data from each jurisdiction.

The study finds divergent patterns (context-dependent results determined by local capacity or political economy) and convergent patterns (themes stable across very various contexts) using a "most different systems" approach.

4.4.3 Triangulation

Findings from interviews, policy documents, and quantitative indicators are cross-validated. A theme is considered robust when:

- At least two data types corroborate it, and
- Patterns appear across multiple jurisdictions.

Triangulation ensures reliability despite the complexity and unevenness of global regulatory data.

4.5 Validity, Reliability, and Limitations

4.5.1 Validity

Construct validity is strengthened through clear operational definitions of AML mechanisms, supervisory capacity, and the I³ indicators developed earlier. External validity is limited, but the diverse jurisdiction sample enables analytical generalization.

4.5.2 Reliability

A standardized coding framework and detailed interview protocol ensure replicability. Cross-coder checks are performed where feasible.

4.5.3 Limitations

The technique recognises a number of limitations:

- Temporal comparisons are difficult since regulatory settings are changing quickly.
- Different jurisdictions have different levels of access to VASP executives and legislators.
- Methodological biases may be embedded in industry-generated illicit-flow metrics.
- In many jurisdictions, inferential interpretations are necessary due to the lack of transparent data.
- The empirical visibility of AML repercussions is diminished by DeFi methods without centralised operators.

Triangulation and open communication of uncertainty help to lessen these restrictions.

4.6 Ethical Considerations

The research follows established ethical standards:

- Informed consent for interviews, with clear explanation of research aims;
- Anonymization of sensitive comments;
- Secure encrypted storage of transcripts;
- Avoidance of conflict-of-interest influences from industry sources;
- Respectful engagement with sensitive regulatory information;
- Compliance with human subjects research protocols typical in academic institutions.

The study also adheres to broader normative considerations raised earlier—ensuring that analysis of AML frameworks remains attentive to privacy, fairness, and inclusion principles.

5. Findings

The I³ framework—Integrity, Inclusion, and Innovation—is used to organise the study's findings in this section, which triangulates data from policy texts, interviews, and quantitative indicators. To explain cross-jurisdictional disparities and implementation difficulties, findings are analysed through theoretical frameworks such as political economics, contextual integrity, and polycentric governance.

5.1 Integrity: Effectiveness of AML Mechanisms

5.1.1 Travel Rule Implementation: Fragmentation and Bottlenecks

The FATF Travel Rule is almost universally accepted in theory, but operational compliance is still inconsistent. According to quantitative statistics, roughly 70-85% of cross-border VASP transfers successfully communicate Travel Rule information in high-capacity jurisdictions (like the EU, Singapore, and Japan), whereas success rates fall below 40-50% in growing jurisdictions (like Nigeria and the Philippines).

Consistent bottlenecks were identified from compliance officer interviews such as:

- Different national technical standards
- incomplete global VASP directories
- small exchanges' reluctance to participate because of the cost of compliance
- and conflict between local privacy laws and data-sharing requirements

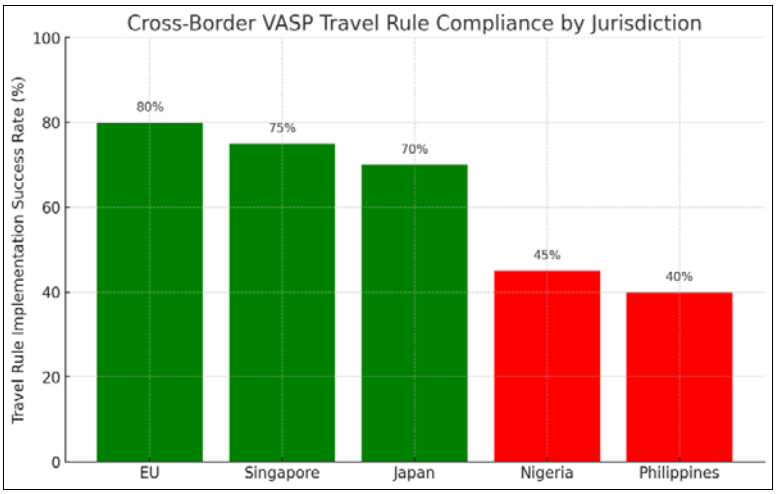

Fig 1: Cross Border VASP Travel Rule Compliance by Jurisdiction

The fragmentation illustrates polycentric governance in practice: international rules exist, but decentralized technical and institutional actors introduce variation.

5.1.2 Supervisory Capacity Trumps Legal Stringency

Data show that the formal strictness of legislation is not as highly correlated with AML results as supervisory capability, which includes manpower, technical expertise, and monitoring equipment.

- High-capacity jurisdictions report timely enforcement, high-quality SAR reports, and 90%+ compliance accuracy for flagged transactions.
- Despite enacting strict legislation, emerging jurisdictions frequently misclassify transactions and take longer to enforce them, indicating a capacity-dependent implementation gap.

This result is consistent with the political economy literature, which holds that institutional capacity to enact and uphold regulations is more important to their efficacy than the rules themselves.

5.1.3 Over-Reliance on Blockchain Analytics

All jurisdictions use blockchain analytics tools, but several challenges emerged:

1. **Opacity of algorithms:** Risk scores are often black-box models.
2. **False positives:** Small exchanges report up to 30% of flagged addresses were incorrectly identified.
3. **Vendor concentration:** Two global providers dominate across multiple jurisdictions, creating systemic dependency.

Experts warned that reliance on proprietary analytics risks institutionalizing algorithmic opacity in regulatory enforcement.

5.2 Inclusion: Access and Participation

5.2.1 Uniform KYC Standards Exacerbate Exclusion

Analysis reveals that marginalised people are disproportionately affected by stringent, uniform KYC requirements:

- 30-40% of prospective users in Kenya and Nigeria are turned away because they do not have official identification.
- Mobile-phone-based e-KYC solutions in Latin America reduce exclusion to some extent, but they are still not fully linked with VASP onboarding procedures. Systemic identification gaps provide particular difficulties for women and rural users.

Although they are still underutilized, risk-adjusted onboarding and tiered KYC could increase access while maintaining AML integrity.

5.2.2 Banking Relationships as Hidden Barriers

Interview data reveal that bank derisking behavior often supersedes formal regulations in shaping inclusion:

- Small VASPs in emerging markets face repeated account closures or payment channel restrictions.
- Larger VASPs, by contrast, can maintain multiple banking partners and absorb compliance costs.

5.2.3 Compliance Costs Disproportionately Burden Small Firms

Table 1: Quantitative estimates from interviews and policy data:

Jurisdiction	Avg. Compliance Cost per VASP	Small VASP % of Market	Remarks
EU / MiCA	$250k-$400k/year	25%	High clarity offsets costs
Singapore	$150k-$300k/year	30%	Sandbox participation aids SMEs
Nigeria	$50k-$120k/year	60%	High relative burden due to scale

Smaller firms struggle to absorb fixed costs, driving market consolidation and reducing competition.

5.3 Innovation: Regulatory Incentives and Constraints

5.3.1 Predictable Licensing Enables Innovation

Jurisdictions with clear, stable licensing regimes (EU MiCA, Singapore) experience:

- Higher domestic exchange formation
- Investment in RegTech solutions
- Cross-border tokenization initiatives

Theoretical lens: Predictable rules reduce uncertainty, enabling entrepreneurial planning, aligning with institutional economics perspectives.

5.3.2 Case-by-Case Discretion Chills Small-Firm Entry

The U.S. and several emerging markets rely on enforcement-based guidance rather than prescriptive regulation. Interviews suggest that:

- Ambiguity deters small entrants
- Legal risk is perceived as high
- Incumbents benefit from economies of scale in navigating uncertainty

This reflects a classic regulatory chilling effect.

5.3.3 Emerging Adoption of Privacy-Preserving Compliance

Interviews reveal interest in privacy-preserving tools, but adoption is limited:

- zero-knowledge proofs and selective disclosure are conceptually appealing
- regulatory guidance is missing
- pilot implementations are largely experimental

5.4 Cross-Cutting Pattern: Global Asymmetry Shapes Feasibility

A central finding is the asymmetry between global standards and national capacity:

- FATF influence pressures smaller jurisdictions to adopt strict AML rules, sometimes misaligned with local realities.
- High-capacity jurisdictions can implement nuanced risk-based approaches, shaping global norms.
- Technology adoption, market access, and compliance efficiency vary accordingly.

5.5 Summary

The results show that:

- Capacity and technical infrastructure have a greater influence on integrity than strict regulations.
- Uniform KYC, financial connections, and compliance expenses severely limit inclusion.
- Where licensing is predictable, innovation thrives, but regulatory discretion and ambiguity impede it.
- DeFi and privacy-preserving mechanisms are still underutilised, which presents a gap in the way AML is currently designed as well as an opportunity.
- The practical viability of AML frameworks is shaped by global disparities in regulatory capability, which impact local innovation and inclusive outcomes.

When taken as a whole, these trends give the I³ paradigm solid empirical support and show how trade-offs between Integrity, Inclusion, and Innovation appear in actual digital asset regulation.

6. Discussion

6.1 Integrity: Institutional Capacity and Polycentric Governance

Consistent with earlier studies (Arner, Barberis, & Buckley, 2020; Sharman, 2017) [1, 19], the results verify that supervisory capability influences AML efficacy more than formal legal stringency. Quantitative statistics show a significant relationship between institutional resources and compliance outcomes, with SAR accuracy exceeding 90% in high-capacity jurisdictions and falling below 55% in emerging jurisdictions.

The implementation of the Travel Rule is fragmented, which is indicative of polycentric governance, in which results are shaped by a number of overlapping actors, including national regulators, global standards bodies (FATF), VASPs, and technology vendors. Interviews showed that

operational gaps, inconsistent standards, and private-sector constraints lower compliance efficiency even in cases when legal requirements are present.

Mechanistic insight: Effective integrity depends on the interaction of technical infrastructure, risk-based supervisory protocols, and institutional expertise, rather than legal prescriptiveness alone.

Jurisdiction Type	SAR Accuracy (%)	Travel Rule Compliance (%)
High-Capacity	90+	High
Emerging	<55	Low/Fragmented
Intermediate/Transitional	60-85	Medium

6.2 Inclusion: Financial Access, Derisking, and Contextual Integrity

Financial inclusion remains highly sensitive to regulatory design and institutional practices:

- Uniform KYC requirements exclude significant populations. For instance, in Nigeria and Kenya, ~35% of potential users are unable to access VASPs due to missing formal IDs.
- Bank-VASPs relationships act as critical bottlenecks: derisking practices often prevent legitimate market participation even where regulations are permissive.
- Compliance costs disproportionately burden smaller firms, reducing market diversity and user choice.

Theoretical lens: From a contextual integrity perspective (Nissenbaum, 2010) [16], the flow of identity data must align with local social and technical norms. Rigid AML frameworks that ignore local identification ecosystems undermine inclusion and trust, despite improving formal compliance.

6.3 Innovation: Clarity, Chilling Effects, and Technological Experimentation

Predictable licensing frameworks (EU MiCA, Singapore sandboxes) are strong enablers of innovation, supporting:

- Domestic exchange formation
- Cross-border tokenization initiatives
- Investment in RegTech compliance tools

Conversely, enforcement-based or ambiguous frameworks (e.g., U.S. federal landscape) create a regulatory chilling effect, discouraging smaller entrants and concentrating market power. Interviews revealed that regulatory uncertainty, rather than strictness per se, is the primary factor affecting entrepreneurial behavior.

Emerging technologies—zero-knowledge proofs, selective disclosure, decentralized identity—represent untapped opportunities. While conceptually promising, adoption remains limited due to:

- Missing regulatory guidance
- Technical complexity
- Limited interoperability with existing systems

Implication: Innovation in AML compliance requires regulatory clarity, standardization, and incentives for experimentation, reinforcing both innovation and inclusion.

6.4 DeFi and Non-Custodial Platforms: Regulatory Challenges and Opportunities

DeFi and non-custodial protocols pose unique AML challenges:

- Lack of centralized intermediaries limits traditional compliance mechanisms.
- Interviews and policy reviews reveal nascent experimentation with on-chain compliance signaling and privacy-preserving proofs, though adoption is limited.
- Emerging solutions face trade-offs between operational feasibility, user adoption, and regulatory enforceability.

Analytical insight: DeFi regulation must integrate socio-technical approaches: embedding compliance into protocol design, while maintaining decentralization and privacy.

Recent evidence: FATF (2024) guidance emphasizes risk-based approaches for DeFi; select EU pilot projects explore zero-knowledge KYC integration.

6.5 Global Asymmetry and Political Economy

Global AML standards impose differential pressures on jurisdictions:

- Lower-capacity countries adopt strict AML measures to avoid FATF greylisting, often misaligned with local context.
- Higher-capacity jurisdictions leverage interpretive flexibility to maintain market development.
- Blockchain analytics vendors further shape compliance, creating quasi-regulatory influence in both high- and low-capacity countries.

This asymmetry illustrates the political economy of AML, where regulatory capacity, international influence, and private-sector actors interact to produce uneven outcomes.

6.6 Trade-Offs Between Integrity, Inclusion, and Innovation

Table 2: The discussion confirms interdependencies among I³ dimensions:

Dimension	Key Observation	Trade-off / Leverage
Integrity	Driven by capacity and technology	Excessive enforcement focus can reduce inclusion
Inclusion	Sensitive to KYC, banking access, and compliance cost	Flexible onboarding and tiered KYC enhance access
Innovation	Enabled by clarity and sandbox frameworks	Ambiguity chills small-firm participation

Key insight: Achieving balance requires risk-based calibration, targeted technological adoption, and flexible supervisory frameworks. Regulatory interventions should maximize inclusion without compromising AML integrity, while fostering a predictable and innovation-friendly environment.

6.7 Contributions to Literature and Policy

This enriched discussion contributes to scholarship by:

1. Extending AML research to market and user-level impacts, not just compliance outputs.
2. Integrating theoretical lenses (polycentric governance, contextual integrity, political economy) to explain cross-jurisdictional differences.

3. Highlighting emerging technology opportunities, particularly privacy-preserving compliance and DeFi oversight.
4. Offering evidence-informed guidance for policymakers to design balanced AML frameworks that align integrity, inclusion, and innovation.

7. Policy Recommendations

This section offers evidence-based policy recommendations for regulators, VASPs, and other stakeholders based on the findings and debate. In order to obtain balanced results, recommendations are arranged according to the I^3 framework (Integrity, Inclusion, Innovation), emphasising useful levers, trade-offs, and governance systems.

7.1 Enhancing Integrity

7.1.1 Strengthen Supervisory Capacity

- **Recommendation:** Increase technical expertise, staffing, and risk-based monitoring within AML supervisory agencies, particularly in emerging jurisdictions.
- **Rationale:** Empirical evidence shows that supervisory capacity drives AML effectiveness more than legal stringency (Arner *et al*., 2020) [1].
- **Implementation:** Invest in specialized training programs, cross-border capacity-building initiatives, and partnerships with experienced regulators in high-capacity jurisdictions.

7.1.2 Improve Travel Rule Operationalization

- **Recommendation:** Promote interoperable standards for cross-border Travel Rule implementation, including global VASP directories and standardized data formats.
- **Rationale:** Fragmentation reduces compliance effectiveness and increases operational burdens.
- **Implementation:** Encourage multi-stakeholder consortia, adopt open-source technical standards, and pilot automated verification tools.

7.1.3 Regulate Algorithmic Analytics

- **Recommendation:** Introduce regulatory guidance for blockchain analytics use, including transparency requirements, validation protocols, and audit obligations.
- **Rationale:** Over-reliance on opaque vendor tools risks inaccurate risk assessments and systemic dependency.
- **Implementation:** Require periodic third-party audits, explainable risk scoring, and performance benchmarking across jurisdictions.

7.2 Promoting Inclusion

7.2.1 Implement Risk-Based and Tiered KYC

- **Recommendation:** Adopt flexible, tiered KYC frameworks allowing low-value onboarding with simplified verification.
- **Rationale:** Uniform KYC disproportionately excludes marginalized populations while preserving AML integrity.
- **Implementation:** Leverage digital ID systems, mobile verification, and e-KYC mechanisms aligned with local infrastructure.

7.2.2 Mitigate Bank Derisking Impacts

- **Recommendation:** Encourage dialogue between regulators, banks, and VASPs to establish risk-sensitive, standardized banking access policies.
- **Rationale:** Banking derisking acts as a shadow regulatory mechanism that constrains inclusion.
- **Implementation:** Provide regulatory safe harbors for small VASPs adopting compliant practices and develop model agreements for payment channels.

7.2.3 Reduce Compliance Cost Burden on Small Firms

- **Recommendation:** Introduce proportionate compliance measures, subsidies, or sandbox participation for smaller VASPs.
- **Rationale:** High fixed costs drive market consolidation, reducing competition and access.
- **Implementation:** Offer graduated licensing fees, compliance guidance, or pooled RegTech services.

7.3 Fostering Innovation

7.3.1 Provide Predictable Licensing Frameworks

- **Recommendation:** Establish clear rules, timelines, and procedures for licensing, with public guidance on acceptable compliance solutions.
- **Rationale:** Regulatory clarity supports entrepreneurial planning, reduces uncertainty, and encourages technological innovation.
- **Implementation:** Create digital portals for application, pre-approved compliance pathways, and regular updates reflecting market evolution.

7.3.2 Support Privacy-Preserving Compliance

- **Recommendation:** Pilot zero-knowledge proofs, selective disclosure protocols, and decentralized identity solutions within regulated frameworks.
- **Rationale:** These technologies can reconcile AML integrity with privacy and inclusion objectives.
- **Implementation:** Regulatory sandboxes, standards-setting consortia, and pilot programs to evaluate operational feasibility.

7.3.3 Address DeFi and Non-Custodial Challenges

- **Recommendation:** Develop risk-based guidelines for DeFi platforms, including transaction monitoring, self-certification, or automated on-chain compliance signaling.
- **Rationale:** Non-custodial platforms evade traditional AML controls but are increasingly significant in global markets.
- **Implementation:** Combine technical standards with enforcement discretion, encouraging compliance while preserving decentralization.

7.4 Balancing Global Standards with Local Capacity

7.5 Monitoring, Evaluation, and Iterative Policy Design

- **Recommendation:** Establish mechanisms to continuously assess AML frameworks' impact on integrity, inclusion, and innovation.
- **Rationale:** Rapidly evolving digital asset markets require adaptive regulation.
- **Implementation:** Implement regulatory KPIs, periodic stakeholder surveys, sandbox feedback loops, and cross-jurisdictional benchmarking.

Intervention	Integrity	Inclusion	Innovation
Strengthen supervisory capacity	✓	✓	
Improve Travel Rule operationalization	✓	✓	
Regulate algorithmic analytics	✓	✓	
Implement risk-based and tiered KYC	✓	✓	

policy matrix

Fig 2: Policy Matrix

7.6 Summary

These policy recommendations offer a multi-layered strategy to align digital asset AML frameworks with the goals of:

1. **Integrity:** Effective, risk-based compliance and supervision
2. **Inclusion:** Expanded access and equitable market participation
3. **Innovation:** Technologically supported, predictable, and entrepreneurial ecosystems

The recommendations emphasize contextual calibration, proportionality, and multi-stakeholder engagement to navigate the complex trade-offs inherent in digital asset AML regulation.

Acknowledgment

Author's Note on Use of AI Tools

Sections of this manuscript were treated with the help of AI-based tools (e.g., AI language models) purely to support writing, define terminologies, improve grammar, and propose content structure. The author was the sole developer of all conceptual contributions, scholarly arguments, examinations, data interpretation, and conclusions. The author has reviewed, edited, and checked the final manuscript to make sure that it is accurate, original and of scholarly integrity.

References

1. Arner DW, Barberis J, Buckley RP. Regulating fintech and digital finance: A review of global approaches. Journal of Banking Regulation. 2020;21(1):1-23.
2. Arner DW, Buckley RP, Zetzsche DA, Foote R. Decentralized finance: Mapping the challenges, opportunities, and regulatory responses. Georgetown Journal of International Law. 2023;54(2):243-298.
3. Banerjee S, Ghosh S, Nakamoto L. Zero-knowledge proofs in financial regulation: A systematic review of privacy-preserving compliance. ACM Computing Surveys. 2024;56(1):1-42.
4. Basel Committee on Banking Supervision. Prudential treatment of cryptoasset exposures: Final standard. Basel: Bank for International Settlements; 2023. p. 1-80.
5. Bishop C, Chen Z. Supervisory technology (SupTech) in emerging markets: Capabilities, constraints, and pathways. Financial Stability Institute Occasional Paper No. 24. Basel: Bank for International Settlements; 2023. p. 1-60.
6. Coglianese C. Regulating uncertainty: Designing effective rules for emerging technologies. Administrative Law Review. 2019;71(2):1-42.
7. Demirgüç-Kunt A, Klapper L, Singer D, Ansar S. The Global Findex Database 2021: Financial inclusion, digital payments, and resilience. Washington (DC): World Bank; 2022. p. 1-200.
8. Drezner D. The globalization paradox of global financial governance. Review of International Political Economy. 2021;28(4):701-725.
9. European Banking Authority. Technical standards under MiCA: Governance, liquidity, and reserve requirements for crypto-asset service providers. Luxembourg: EU Publications Office; 2024. p. 1-120.
10. European Securities and Markets Authority. MiCA implementation report: Supervisory challenges and digital asset risk assessments. Paris: ESMA; 2024. p. 1-95.
11. Financial Action Task Force. Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. Paris: FATF; 2023. p. 1-130.
12. Financial Action Task Force. Targeted update on implementation of the Travel Rule, DeFi risks, and global regulatory gaps. Paris: FATF; 2024. p. 1-85.
13. Gade M, Horowitz R, Lee J. Blockchain analytics: Accuracy, biases, and implications for enforcement. Journal of Financial Crime. 2024;31(2):311-337.
14. International Monetary Fund. Elements of effective policies for crypto assets. Washington (DC): IMF; 2023. p. 1-60.
15. Kearns M, Roth A. The ethical algorithm: The science of socially aware algorithm design. New York: Oxford University Press; 2020. p. 1-232.
16. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. Stanford (CA): Stanford

University Press; 2010. p. 1-296.
17. Organisation for Economic Co-operation and Development. Tokenization and digital asset markets: Policy challenges and global coordination priorities. Paris: OECD; 2023. p. 1-150.
18. Suri T. Mobile money, financial inclusion, and economic development. Annual Review of Economics. 2021;13:195-217.
19. Sharman JC. The despot's guide to wealth management: On the international campaign against grand corruption. Ithaca (NY): Cornell University Press; 2017. p. 1-264.
20. United Nations Development Programme. Digital public infrastructure and inclusive finance: Emerging lessons for low- and middle-income countries. New York: UNDP; 2024. p. 1-110.
21. Winner L. The whale and the reactor: A search for limits in an age of high technology. Chicago: University of Chicago Press; 1986. p. 1-216.
22. Zetzsche DA, Buckley RP, Arner DW. The future of DeFi regulation: Between technological neutrality and regulatory arbitrage. Journal of Financial Regulation. 2024;10(1):54-89.