Decrypting Crypto: Supervision, Intelligence, and Recovery in the Virtual Assets Era



A Reference for Latin America and the Caribbean Financial Intelligence Units and Regulators

IDB

FINANCIAL INTEGRITY SERIES

Authors

Chapter 1 — José Ángel Arias (IDB Consultant)
Chapter 2 — Guillermo Lagarda (IDB), Paulina Verástegui (IDB Consultant)
Chapter 3 — TRM Labs
Chapter 4 — José Ángel Arias (IDB Consultant)
Chapter 5 — John Grajales (OAS)
Chapters 6 and 7 — Nicolás Dassen (IDB), Marcela Duque (IDB Consultant)
Chapter 8 — Kamal Anwar (UNOCT)

JEL Codes: G28, G18, K24, O38, F65

Keywords: Cryptoassets, Financial Integrity, AML/CFT Regulation, Blockchain Analytics, Virtual Asset Service Providers (VASPs)

http://www.iadb.org

Copyright © 2026 Inter-American Development Bank (IDB). This work is subject to a Creative Commons Attribution 4.0 International Public License CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/legalcode). The terms and conditions indicated in the URL link must be met and the respective recognition must be granted to the IDB.

Any and all disputes arising under this license that cannot be settled amicably shall be resolved in accordance with the following procedure. Pursuant to a notice of mediation communicated by reasonable means by either you or the licensor to the other, the dispute shall be submitted to non-binding mediation conducted in accordance with the World Intellectual Property Organization (WIPO) Mediation Rules. Any dispute that cannot be settled amicably shall be submitted to arbitration pursuant to the United Nations Commission on International Trade Law (UNCITRAL) rules. The use of the IDB name for any purpose other than the respective recognition and the use of the IDB logo are not authorized by this license and require an additional license agreement.

Note that the URL link includes terms and conditions that are an integral part of this license.



Cover image generated using artificial intelligence.

Table of Contents

How to Use This Guide 7

Introduction 8

Why This Publication Matters 10

Building the Foundations: Understanding the Technology and the Types of Virtual Assets 11

From Understanding to Action: Regional Evidence and Regulatory Design 11

Operational Effectiveness: From Myths to Measurable Results 12

From Fragmented Compliance to Effective Governance 13

From Knowledge to Implementation: The Road Ahead 13

Chapter 1: The Technology Behind Cryptocurrencies and Virtual Assets 15

Introduction 16

Distributed Ledgers: Foundations of Trust 16

How Transactions Work: From Wallets to Blocks 16

Consensus Mechanisms: Ensuring Integrity 17

The Role of Technology for VASPs in AML/CFT/CPF 17

Opportunities and Risks for AML/CFT/CPF Frameworks 18

Resource and Sustainability Challenges 20

Implications for Financial Intelligence Units 21

Conclusion 21

Chapter 2: Understanding Cryptocurrencies and Virtual Assets 23

Introduction 24

Defining Virtual Assets and Service Providers 24

Major Categories of Virtual Assets 24

Cryptocurrencies 24

Stablecoins 24

Privacy Coins 25

Utility and Governance Tokens 26

Non-Fungible Tokens (NFTs) 26

Institutional Design: Who Should Regulate and Supervise? 26

Comparative Regulatory Approaches 27

Typologies and Misuse Cases 28

Supervisory Challenges and Policy Implications 29

Conclusion 29

Chapter 3: Cryptoasset Adoption in Latin America and Illicit Finance Risks 31

Introduction 32

A Region Transformed by Digital Migration 32

Current Trends in Adoption in LAC 33

Illicit Finance Risks in Latin America and the Caribbean 34

Beyond Cartels: From SIM Swapping to Money Laundering 36

Conclusion 38

Chapter 4: Customer Identification, Beneficial Ownership, and Traceability in Virtual Assets: Definitions, Challenges, and Implementation of a Balanced Regulatory Framework 40

Introduction 41

The Regulatory Imperative for Transparency in Digital Finance 41

Technology and the Traceability Challenge 42

FATF Recommendations 10, 15, 24, and 25 in the Virtual-Asset Context 44

Insights from the VASP Survey 45

Gaps in Customer Identification, Beneficial Ownership Verification, and Traceability 46

Toward a Balanced and Effective Regulatory Framework 47

Conclusion: Transparency as the Foundation of Trust 48

Chapter 5: Toward Standardized Threshold-Based Transaction Reporting Requirements for Virtual Asset Service Providers 49

Introduction 50

The Spectrum of Data Collection and National Disparities 50

Operational and Strategic Value of CTR and VASP Data 51

Challenges to Effective Analysis 51

The Case for Risk-Based and Context-Sensitive Reporting Frameworks 52

Conclusion 53

Chapter 6: Debunking Myths: Anonymity, Attribution, and Recovery of Cryptoassets and Virtual Assets 54

Introduction 55

Myth #1: Cryptocurrencies Provide Complete Anonymity 55

From Anonymity to Pseudonymity 55

Wallet Attribution, Customer Identification, and Beneficial Ownership 56

Analytical Tools and De-Pseudonymization Techniques 56

Challenges in Wallet Attribution and Identifying Relevant Beneficial Owners 57

Myth #2: Cryptoasset Recovery Is Too Complex 57

Reassessing the Myth 59

Conclusion 61

Chapter 7: Practical Considerations for FIUs in Cryptoasset and Virtual Asset Investigations and Recovery 62

Introduction 63

Technical Challenges in Cryptoasset Investigations 63

Accessing Private Keys and Seed Phrases 63

The Diversity of Wallet Types and Their Investigative Implications 64
Legal and Procedural Challenges 64
Warrants and Seizure Orders for Virtual Assets 64
Jurisdictional Complexities in Cross-Border Cases 65
MLATs and International Cooperation Frameworks 65
Operational Challenges and Capacity Requirements 65
Post-Recovery Management of Seized Cryptoassets 66
Conclusion 66
Chapter 8: Cross-Country Experiences and Best Practices in Public Policy and Regulation 68
Introduction 69
The Good — Effective Policies, Institutions, and Partnerships 70
The Bad — Regulatory Gaps and Implementation Asymmetries 72
The Ugly — When Policy and Practice Diverge 73
Lessons and Opportunities for Regional and Global Cooperation 74
Information Sharing and Joint Enforcement 74
Capacity Building and Tailored Assistance 74
Knowledge Products and Guidance 75
Public–Private Partnerships (PPPs) 75
Balancing Integrity and Inclusion 75
Conclusion — From Global Mandate to Regional Action 76
References 78

How to Use This Guide

This publication addresses multiple audiences across the AML/CFT/CPF ecosystem. While it is designed to be read as a whole, each chapter is also self-contained. The following reading paths may help readers prioritize content:

- **FIU analysts and investigators** seeking to build or strengthen cryptoasset investigation capabilities should begin with Chapters 1 and 2 for technological and taxonomic foundations, then move to Chapters 6 and 7 for operational procedures on tracing, freezing, and recovery.
- **Supervisors and regulators** designing or refining VASP oversight frameworks should focus on Chapters 4, 5, and 8, which address beneficial ownership, reporting thresholds, and cross-country regulatory experiences respectively.
- **Policymakers and senior officials** preparing for FATF mutual evaluations or developing national strategies should read the Introduction for the strategic framing and priorities, Chapter 3 for regional risk context, and Chapter 8 for governance and institutional design.
- **All readers** may benefit from Chapter 3's regional evidence base and Chapter 6's myth-busting analysis, which ground the publication's findings in documented LAC cases and operational realities.

Cross-references between chapters are provided throughout to facilitate navigation across related topics.

INTRODUCTION

Introduction

1. The rapid expansion of cryptoassets and their underlying blockchain technologies is reshaping the traditional financial landscape, creating unprecedented opportunities for innovation, inclusion, and transparency while also increasing the risks of illicit finance. As adoption across private-sector economic activities accelerates, a critical question arises: are countries and private-sector actors identifying, assessing and mitigating the ML/TF risks of new products, business practices, and technologies before they are launched or used, as contemplated under FATF Recommendation 15, or is adoption moving faster than the understanding of the underlying technologies, their scope, potential, and limitations?

2. Across Latin America and the Caribbean (LAC), private-sector actors have moved quickly to adopt virtual assets.[1] In parallel, Financial Intelligence Units (FIUs) have strengthened their institutional and analytical capacities, and supervisory authorities have begun to modernize their approaches. However, the growing adoption of cryptoassets adds an additional layer of complexity. Their growing use across a wide range of private-sector activities increases the burden on regulators and supervisors. The novelty of the underlying technologies, the challenges associated with tracing on-chain transaction data, and the diversity of virtual assets that can be issued or exchanged through these systems together create a regulatory and supervisory environment fundamentally different from that of traditional financial institutions.

3. This creates a structural gap: while technology evolves at high speed, risk-based regulatory and supervisory systems adapt far more slowly. As a result, many countries face a sequential implementation challenge: they must first bring VAs and VASPs within the AML/CFT framework through technical compliance with the FATF Standards, and then translate that formal coverage into effective implementation through secondary rules, supervision, resources, expertise, and inter-agency coordination. Addressing these challenges requires developing a solid understanding of the technology, identifying the specific risks relevant to each jurisdiction, and building a shared vision for effective coordination and collaboration, supported by common guidance and digital public goods that enable countries to benefit from economies of scale and accelerate learning across the region.

4. At the same time, it is essential for countries to develop and implement risk-based regulations grounded in relevant international standards while taking into account their own circumstances, institutional contexts, and domestic risk profiles. Under FATF Recommendation 15, countries are expected to regulate and supervise VASP activities for AML/CFT purposes where those activities are permitted; countries may prohibit such activities, but prohibition does not remove the need to identify and mitigate related risks, including activity by offshore or non-compliant providers. Rather than rushing to issue regulations solely to demonstrate compliance, countries must develop a solid understanding of the factors that underpin effective oversight—namely, the required skills, the necessary technological resources, and appropriate regulatory frameworks. This includes not only determining which institution should supervise virtual-asset activities, but also defining the substantive perimeter of regulation: which activities must be licensed or registered where permitted, which may be restricted or prohibited, and which should be reported or subject to enhanced controls. Only by grounding reforms in this knowledge can countries avoid creating unnecessary burdens or generating unintended consequences.

5. This publication, *Decrypting Crypto: Supervision, Intelligence, and Recovery in the Virtual Assets Era*, aims to help close that gap. It consolidates technical, regulatory, and operational knowledge on cryptoassets, particularly on virtual assets, into an accessible framework tailored to the needs of FIUs and supervisory bodies. Each chapter contributes a distinct analytical or operational building block—from understanding the technology itself to designing proportionate regulation for risk-based supervision, identifying and tracing illicit transactions, and ultimately developing effective cryptoasset recovery frameworks. Together, these elements provide a roadmap for strengthening the region's resilience against money laundering, terrorist financing, proliferation financing, and other forms of financial crime in the cryptoassets era.

6. This guide does not seek to replace existing FATF standards, regional risk assessments, or technical typology reports. Rather, it translates them into an integrated, operational reference for FIUs, supervisors, regulators, and policymakers. Existing materials often focus on specific components of the virtual-asset ecosystem—such as the risk-based approach, the Travel Rule,

[1] Throughout this publication, "virtual asset" is used in the FATF sense: a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes (FATF Recommendations, Glossary). "Cryptoasset" is used as a broad umbrella term for digital assets based on cryptography and distributed ledger technology (DLT) that may or may not fall within the FATF definition of a virtual asset. When discussing regulatory frameworks and FATF standards, "virtual assets" is the preferred technical term.

stablecoins, typologies, and asset recovery. This publication brings those elements together in a single practical roadmap that links technological understanding, regulatory design, reporting frameworks, investigative techniques, and recovery procedures.

7. Although grounded in the experience of Latin America and the Caribbean, the guide's contribution is of broader relevance. Many jurisdictions outside the region face the same implementation challenge: they understand that virtual assets and VASPs must be regulated and supervised, but lack a concise operational framework for determining where to begin, how to sequence reforms, and how to connect supervision, intelligence, and enforcement. By combining regional evidence, international standards, and practical implementation guidance, this publication offers a tool that can support capacity building not only in LAC but also in other jurisdictions confronting similar gaps in knowledge, technology, coordination, and enforcement.

Why This Publication Matters

8. The global anti-money laundering, countering the financing of terrorism, and counter-proliferation financing (AML/CFT/CPF)[2] system is at a critical moment in discussions about the future of transactions involving different types of virtual assets, including cryptoassets. The Financial Action Task Force (FATF) updated Recommendation 15 in 2018 and its Interpretive Note in 2019 to address the risks of virtual assets and Virtual Asset Service Providers (VASPs), yet implementation remains uneven—a situation referred to as the "Sunrise Issue." The FATF's 2026 Targeted Update on Virtual Assets and VASPs found that 86 percent of responding jurisdictions reported having conducted a VA/VASP risk assessment (124 of 145), and 73 percent of respondents that do not prohibit or plan to prohibit VASPs entirely reported requiring VASPs to be licensed or registered (95 of 130), but only 58 percent reported having licensed or registered a VASP in practice (76 of 130 Travel Rule implementation has also advanced, with 83 percent of relevant respondents reporting that they have passed legislation implementing it (91 of 109), yet 60 percent of those jurisdictions had not yet taken Travel Rule-related supervisory or enforcement action (55 of 91) (FATF, 2026a).

9. The FATF's March 2026 Targeted Report on Stablecoins and Unhosted Wallets further underscores the urgency of these challenges. With stablecoin market capitalization exceeding USD 316 billion and daily trading volumes surpassing those of Bitcoin, stablecoins now account for an estimated 84 percent of illicit virtual-asset transaction volume (Chainalysis, 2026). The report identifies programmable compliance controls—such as allow-listing and deny-listing through smart contracts, freeze-and-burn capabilities, and transaction limits—as emerging good practices that stablecoin issuers and jurisdictions can deploy to mitigate risks in secondary markets and peer-to-peer (P2P) transactions via unhosted wallets. It also provides a detailed annex of risk indicators specific to stablecoin misuse, which are directly relevant to the reporting and supervisory frameworks discussed in Chapters 5 and 8 of this guide.

10. At the regional level, the July 2025 Evaluación Sectorial de Riesgos de Activos Virtuales y Proveedores de Servicios de Activos Virtuales (ESR) published by GAFILAT provides the authoritative baseline for understanding ML/TF risks across its 18 member countries. The ESR concludes that the region faces a very high risk of money laundering through virtual assets associated with fraud and scams, cyberattacks, and drug trafficking; a high risk associated with human trafficking; and a medium risk associated with terrorist financing. Its five principal vulnerabilities—lack of knowledge and training, insufficient legal frameworks, limited investigative capacity, inadequate technological infrastructure, and gaps in VASP licensing and supervision—directly inform the building blocks addressed in each chapter of this guide.

11. Within the LAC region, the challenge is compounded by institutional asymmetries. Some jurisdictions—Brazil, Mexico, and Chile—have developed fintech ecosystems that, to some extent, include virtual-asset frameworks; others remain in the early stages of legal or supervisory design. FIUs report challenges accessing identification data and beneficial-ownership information for virtual-asset accounts, obtaining cooperation from offshore or unlicensed VASPs that provide services into their jurisdictions—a challenge highlighted in FATF's 2026 report on offshore VASPs—and retaining specialized analysts capable of interpreting complex blockchain data. These constraints directly affect countries'

[2] The FATF now uses the tripartite formulation "AML/CFT/CPF" to encompass anti-money laundering, countering the financing of terrorism, and counter-proliferation financing. This reflects the growing importance of proliferation-financing risks in the virtual-asset ecosystem, as documented in the FATF's 2025 Targeted Update and 2026 Stablecoins Report, particularly with respect to actors linked to the DPRK and Iran. This guide adopts this formulation in all formal and regulatory contexts.

ability to meet FATF standards, particularly those related to effectiveness—namely, FATF Immediate Outcomes 3, 6, 7, and 8[3]—which serve as benchmarks for supervision, financial intelligence, money-laundering investigations, and the confiscation of illicit proceeds, and which in turn have cross-cutting implications for the effective implementation of other Immediate Outcomes.

12. Closing this gap requires more than a solid regulatory framework: it demands a deeper technical understanding of how these systems function, what types of risks they entail, and how public–private partnerships (PPPs) that include VASPs alongside traditional financial institutions can be institutionalized to strengthen the collaboration and dialogue essential for the effective prevention and disruption of illicit activities linked to virtual asset transactions. The chapters that follow address each of these needs systematically.

Building the Foundations: Understanding the Technology and the Types of Virtual Assets

13. **Chapter 1**, *The Technology Behind Cryptocurrencies and Virtual Assets*, establishes the technical foundations upon which effective oversight must rest. It demystifies how blockchain and distributed ledger technologies (DLTs) work—how transactions are created, validated, and permanently recorded—and explains why this transparency can become a powerful ally for FIUs. The chapter translates technical concepts such as consensus mechanisms, smart contracts, and cryptographic validation into operational knowledge for investigators and supervisors. By clarifying the distinction between pseudonymity and anonymity, it helps institutions accurately interpret blockchain data, integrate it into suspicious transaction-reporting systems, and identify typologies specific to cryptoasset-enabled money laundering.

14. In doing so, Chapter 1 helps close a critical knowledge gap: the nascent technological literacy related to cryptoassets among AML/CFT/CPF authorities. Understanding how value is transferred on a blockchain is the first step toward designing proportionate controls and conducting meaningful investigations.

15. **Chapter 2**, *Understanding Cryptocurrencies and Virtual Assets*, complements this technical foundation by providing a clear taxonomy of the asset classes involved—cryptocurrencies, stablecoins, privacy coins, utility and governance tokens, and non-fungible tokens (NFTs). It explains how these instruments are issued, valued, and exchanged, and compares the regulatory approaches adopted in the United States, the European Union, the United Kingdom, and major LAC jurisdictions. Drawing on the FATF's 2026 classification of stablecoin types—asset-backed, virtual-asset-backed (VA-backed), and algorithmic—the chapter maps the risk profiles associated with each category. For FIUs, this classification is essential: different asset types imply distinct risk profiles, reporting obligations, and enforcement challenges.

16. By providing a comparative lens, the chapter allows regulators to benchmark their frameworks against international standards and adapt institutional design accordingly. It thereby helps close the conceptual gap between global norms and national implementation, guiding policymakers and regulatory designers in aligning domestic definitions with FATF Recommendation 15 and its Interpretive Note.

From Understanding to Action: Regional Evidence and Regulatory Design

17. **Chapter 3**, *Cryptoasset Adoption in Latin America and Illicit Finance Risks*, anchors the discussion in empirical evidence. Drawing on transaction data, case studies, and typologies—including the risk levels identified in the GAFILAT 2025 ESR—it maps the region's crypto ecosystem: its scale, drivers, and vulnerabilities. Countries such as Argentina, Brazil, Mexico, Venezuela, and El Salvador illustrate how economic volatility, dependence on remittance, and technological innovation have spurred adoption. At the same time, the chapter documents how organized-crime groups, including drug cartels, transnational laundering networks, and state-linked cyber actors, exploit regulatory gaps to move illicit funds through crypto channels.

[3] Although not specific to VAs/VASPs, IO3, IO6, IO7, and IO8 are particularly relevant where VAs/VASPs constitute a material ML/TF/PF risk. In such cases, IO3 assesses whether supervisors effectively regulate and supervise VASPs and whether VASPs implement AML/CFT preventive measures. IO6 examines the extent to which information obtained from VASPs, including customer and transaction records, contributes to financial intelligence and investigations. IO7 considers whether money laundering cases involving virtual assets are effectively investigated, prosecuted, and sanctioned. IO8 evaluates whether authorities can successfully identify, trace, seize, and confiscate illicit virtual assets and related criminal proceeds. Together, these outcomes provide an indication of the effectiveness of a jurisdiction's AML/CFT framework in addressing risks arising from virtual asset activities where such risks are present.

18. For FIUs, this analysis provides both situational awareness and risk prioritization. By identifying common money-laundering typologies—from trade-based schemes involving East Asian underground banks to cryptoasset-enabled sanctions evasion—it transforms abstract risk assessments into concrete investigative leads. The regional lens also underscores that effective regulation, supervision, and intelligence cannot rely solely on national efforts; cross-border coordination through FATF-Style Regional Bodies (FSRBs), such as the Caribbean Financial Action Task Force (CFATF) and the Grupo de Acción Financiera de Latinoamérica (GAFILAT), as well as through the Egmont Group, remains indispensable.

19. **Chapter 4**, *Customer Identification, Beneficial Ownership, and Traceability in Virtual Assets*, addresses three related but distinct transparency challenges: identifying the customer or person controlling a virtual-asset account or wallet; tracing transactions across blockchain networks; and, where legal persons or legal arrangements are involved, identifying and verifying their beneficial owners under FATF Recommendations 24 and 25. The chapter draws on an original survey of VASPs across six LAC countries to assess how these requirements are implemented in practice and where gaps remain.

20. Its findings reveal fragmentation—divergent thresholds, inconsistent documentation standards, and limited interoperability between national BO registries and VASP systems. The chapter proposes a balanced framework centered on clarity, proportionality, and cooperation, advocating for systems that use interoperable supervisory application programming interfaces (APIs) between registries and VASPs, proportional compliance requirements for smaller entities, and institutionalized public–private information-sharing channels.

21. **Chapter 5**, *Toward Standardized Threshold-Based Transaction Reporting Requirements for Virtual Asset Service Providers*, explains the distinct but complementary roles of suspicious transaction reports (STRs), currency transaction reports (CTRs), and large virtual currency transaction reports (LVCTRs) in the cryptoasset context. It shows how divergent reporting thresholds and data fields across countries can create blind spots and opportunities for regulatory arbitrage, and it proposes practical options for designing risk-based, technology-neutral CTR and LVCTR reporting regimes for VASPs. The chapter highlights how high-quality bulk reporting data from VASPs can strengthen both operational analysis and strategic intelligence within FIUs, while remaining sensitive to capacity constraints and proportionality considerations in Latin America and the Caribbean.

Operational Effectiveness: From Myths to Measurable Results

22. **Chapter 6**, *Debunking Myths: Anonymity, Attribution, and Recovery of Cryptoassets and Virtual Assets*, confronts two misconceptions that often distort policy debates: that cryptoassets guarantee anonymity and that their recovery is impossible. It distinguishes the investigative task of attributing pseudonymous blockchain activity to real-world persons from beneficial ownership identification where legal persons or legal arrangements are involved, and demonstrates how blockchain transparency, when coupled with appropriate legal and analytical tools, can support tracing and recovery.

23. It outlines how modern blockchain analytics platforms, cross-chain tracing techniques, and the implementation of the FATF Travel Rule collectively enable investigators to link pseudonymous addresses to real-world identities. The chapter also examines the investigative implications of P2P transactions involving unhosted wallets, including the challenges they create for attribution when no obliged intermediary is present. Equally important, it documents successful recovery operations in Argentina, Brazil, and Caribbean countries, showing that virtual assets can be frozen, seized, confiscated or forfeited, and liquidated through existing legal mechanisms.

24. **Chapter 7**, *Practical Considerations for FIUs in Cryptoasset and Virtual Asset Investigations and Recovery*, operationalizes these insights by translating them into concrete procedures that FIUs can implement. Whereas Chapter 6 demonstrates that recovery is possible, Chapter 7 explains how recovery actually happens in practice. It details how investigators identify cryptoasset evidence, secure private keys, apply digital forensics techniques, and draft seizure orders that expressly cover cryptographic materials. The chapter also addresses cross-border coordination challenges, the limitations of Mutual Legal Assistance Treaties (MLATs), and the need for rapid-response mechanisms tailored to the speed of cryptoasset and other types of virtual-asset transfers. Together, Chapters 6 and 7 form a comprehensive operational pathway, moving from myth-busting to the achievement of measurable, real-world results.

From Fragmented Compliance to Effective Governance

25. Chapter 8, *Cross-Country Experiences and Best Practices in Public Policy and Regulation*, synthesizes global and regional identifies four enablers of sustainable regulation—clarity, cooperation, capacity, and continuity. It also incorporates the FATF's 2026 recommended actions for jurisdictions on stablecoin oversight, including supervisory colleges for cross-border stablecoin arrangements, structured public–private partnerships, and the establishment of regulatory sandboxes (FATF, 2026b). The chapter cautions against common pitfalls: fragmented mandates, slow enforcement, and the unintended consequences of over-regulation, such as de-risking and financial exclusion.

From Knowledge to Implementation: The Road Ahead

26. Taken together, the eight chapters chart a coherent path for modernizing AML/CFT/CPF systems in the digital era. They demonstrate that cryptoassets and other types of virtual assets are not inherently threats to financial integrity; rather, the risks stem from institutional inertia—from insufficient knowledge and the failure to adapt supervision, investigation, and cooperation mechanisms to technologies that record every transaction transparently and permanently.

27. The lessons distilled in this publication converge on seven actionable priorities for FIUs and policymakers across Latin America and the Caribbean:

- **Ensure continuous learning about underlying technologies.** FIUs and supervisory agencies must maintain risk-based, up-to-date knowledge of the technologies underlying virtual assets, prioritizing the products, services, and use cases most relevant to their domestic risk profile—for example, stablecoin activity in jurisdictions where stablecoins are materially used in remittance corridors. This knowledge is essential not only to understand and leverage these technologies for effective supervision, but also to recognize when their misuse may threaten the integrity of risk-based oversight systems.

- **Monitor exposure to risks arising from the use of cryptoassets and other virtual assets, including stablecoins.** Shifts in socioeconomic conditions and country-specific dynamics (e.g., crime, trade, immigration) can increase the use of virtual assets for cross-border commerce, payments, and remittances. The growing role of stablecoins in illicit virtual-asset transaction volume—as distinct from their debated role in legitimate payment use cases—requires particular attention to P2P transactions via unhosted wallets and the adequacy of risk mitigation measures. FIUs must keep their risk assessments current to anticipate these changes and respond more effectively.

- **Modernize legal frameworks based on technological and risk-related knowledge.** Update laws governing seizure, forfeiture, and evidentiary procedures to explicitly include virtual assets and cryptographic materials, ensuring that enforcement actions meet applicable standards of due process and procedural legitimacy. Where stablecoin issuance is permitted, countries should consider requiring stablecoin issuers to maintain and deploy technical capabilities to freeze, burn, and withdraw stablecoins in secondary markets, in line with FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets.

- **Invest in analytical capacity.** Establish specialized cryptoasset investigation and supervisory capacity, including teams equipped with blockchain analytics tools, sustainable training programs, and talent-retention mechanisms to ensure lasting institutional expertise.

- **Institutionalize cooperation.** Complement formal mutual assistance mechanisms, which are generally slow and fragmented, with standing memoranda of understanding (MOUs) and secure, real-time data exchange protocols among FIUs, VASPs, and regional and international bodies. Jurisdictions should also fully implement the FATF principles of information sharing and cooperation among VASP supervisors. Consider establishing multinational supervisory colleges to supervise stablecoin issuers and other entities involved in cross-border stablecoin arrangements.

- **Embed transparency in asset management.** Develop auditable custodial and liquidation procedures for forfeited cryptoassets to ensure accountability, safeguard value, and maintain public trust.
- **Balance integrity and inclusion.** Promote regulatory approaches that strengthen oversight without excluding small or emerging VASPs, thereby reducing the migration of users toward unregulated or informal markets.

28. As Latin America and the Caribbean prepare for the Fifth Round of FATF Mutual Evaluations, the insights offered in this volume provide a foundation for measurable progress. By combining technological understanding, regulatory clarity, and institutional cooperation, the region can transform cryptoassets from a perceived threat into a catalyst for greater transparency, integrity, and trust in financial systems.

CHAPTER 1:

The Technology Behind Cryptocurrencies and Virtual Assets

Chapter 1: The Technology Behind Cryptocurrencies and Virtual Assets

Introduction

29. Understanding the technology that powers cryptoassets and virtual assets is essential for authorities that regulate, supervise, and investigate related financial activity. Although cryptoassets have evolved from a niche innovation into a global phenomenon, the blockchain technology and other distributed ledger technologies (DLT) that underpin them remain widely misunderstood or oversimplified. GAFILAT's 2025 *Evaluación Sectorial de Riesgos* identified "lack of knowledge and training" and "insufficient technological infrastructure" as two of the five principal vulnerabilities affecting AML/CFT/CPF effectiveness in the region's virtual asset sector (GAFILAT, 2025). For FIUs, understanding these systems is not merely a theoretical concern but a fundamental prerequisite for distinguishing between legitimate innovation and high-risk or illicit uses that threaten financial integrity.

30. This chapter provides a concise and comprehensive overview of how blockchain technology and DLTs function, how transactions are validated and secured, and the implications these mechanisms hold for AML/CFT/CPF frameworks. It also discusses the human and technological resources that FIUs require to monitor and investigate activities involving cryptoassets effectively and sustainably.[4]

Distributed Ledgers: Foundations of Trust

31. At the core of many virtual assets is a distributed ledger—a decentralized database replicated across multiple computers, or nodes. Each node maintains a synchronized copy of the ledger, allowing transactions to be recorded without relying on a central intermediary such as a bank or clearinghouse. Updates occur through consensus mechanisms, which are rule-based protocols ensuring that all participants agree on the validity and sequence of transactions.

32. Public, or permissionless, blockchains such as Bitcoin and Ethereum are open networks where anyone who meets basic technical requirements can participate, view transactions, and validate activity. They maximize transparency but permit pseudonymity: users are identified by cryptographic addresses rather than legal names, creating challenges for identifying beneficial owners. Private, or permissioned, blockchains restrict participation to approved entities, a structure favored by banks, central banks, and corporate consortia. Platforms such as Hyperledger Fabric and R3 Corda exemplify this approach, providing efficiency and enabling regulatory oversight through controlled access.

33. Blockchain's core innovation replaces reliance on intermediaries with reliance on code, cryptography, and consensus mechanisms. This architecture makes transactions resilient to single points of failure and resistant to tampering, yet it also introduces a jurisdictional gap because decentralized networks often operate beyond the jurisdiction of any single regulator.

How Transactions Work: From Wallets to Blocks

34. Every transaction on a blockchain begins with a digital wallet, a software or hardware interface that stores the cryptographic keys authorizing asset transfers. Wallets do not hold the assets themselves; rather, they store the private keys that enable the transfer of tokens recorded on the ledger.

35. A transaction starts when a sender creates a digital instruction specifying the amount, the recipient's address, and any associated network fees. The sender's private key cryptographically signs this instruction, ensuring authenticity and non-repudiation. The signed message is then broadcast across the network, where it awaits validation by network participants.

36. Validation ensures that the sender possesses sufficient funds and that the transaction complies with network rules. Depending on the blockchain, different consensus mechanisms—such as Proof of Work (PoW) or Proof of Stake (PoS)—determine which transactions will be added to the next block. Once validated, transactions are grouped into a block, timestamped, cryptographically linked to the previous block, and distributed across the network. When consensus is reached, the new block becomes an immutable part of the ledger.

[4] For an updated supervisory primer on consensus mechanisms, including Layer 2 protocols and emerging consensus designs, see Bains (2025).

37. This process establishes an auditable chain of custody, which means that every transaction is visible on public blockchains, enabling law enforcement authorities to reconstruct transaction flows and identify patterns consistent with illicit behavior. However, because blockchain identities are pseudonymous rather than anonymous, effective investigation requires combining on-chain data (transaction flows) with off-chain intelligence (exchange records, subpoenaed information or IP data obtained through PPPs) to link addresses to the real individuals behind them. on-chain data (transaction flows) with off-chain intelligence (exchange records, subpoenaed information or IP data obtained through PPPs) to link addresses to the real individuals behind them.

38. Not all wallets operate within the regulated perimeter. The FATF distinguishes between **hosted wallets**—managed by a VASP or other intermediary that holds the private keys on behalf of the user and is subject to AML/CFT/CPF obligations—and **unhosted wallets** (also referred to as self-hosted or non-custodial wallets), defined as "virtual asset wallets that are not hosted or managed by a third-party service provider and where the user maintains exclusive control over the access keys" (FATF, 2026b). Transfers between two unhosted wallets, conducted without the involvement of a VASP or other obliged entity, are known as **peer-to-peer (P2P)** transactions. While all transactions on public blockchains remain visible and traceable, P2P transfers via unhosted wallets present heightened illicit-finance risks because they fall outside the direct scope of AML/CFT/CPF obligations typically imposed on intermediaries and can break the chain of Travel Rule information: the last VASP involved may retain originator information, but it will not transmit that information to a beneficiary's unhosted wallet. The investigative implications of this distinction are examined in detail in Chapter 6.

Consensus Mechanisms: Ensuring Integrity

39. Bitcoin's PoW model secures the network by requiring participants—"miners"—to solve computational puzzles. The cost of falsifying data is intentionally prohibitive: altering one block would require redoing the computation for all subsequent blocks. The drawback is the enormous energy consumption this model entails, which has concentrated mining activity in jurisdictions with low electricity costs and created additional challenges for financial investigations.

40. An alternative, PoS, replaces energy consumption with financial commitment. Validators lock up a portion of their tokens as collateral; the protocol then selects them in proportion to their holdings to confirm transactions. Ethereum's 2022 "Merge" transitioned the network to PoS, dramatically reducing its energy consumption. While more sustainable, PoS raises governance concerns because large stakeholders may exercise disproportionate influence over transaction validation.

41. Hybrid systems such as Delegated Proof of Stake (DPoS), Proof of Authority (PoA), or Proof of Space and Time (PoST) attempt to combine efficiency, decentralization, and security. Many central bank digital currency pilots rely on permissioned DLTs where only vetted institutions may validate transactions, an approach that preserves regulatory oversight while benefiting from the efficiencies of distributed systems.

The Role of Technology for VASPs in AML/CFT/CPF

42. The key link between the pseudonymous world of blockchain and the regulated financial system is the VASP. Under the FATF Standards (Interpretive Note to Recommendation 15; FATF, 2021 Updated Guidance), a VASP is any natural or legal person that, as a business, conducts one or more of the following activities for or on behalf of another person: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) custody or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer's offer or sale of a virtual asset. Cryptocurrency exchanges and wallet custodians generally fall within this category when conducting covered activities and are therefore subject to AML/CFT/CPF obligations. A DeFi application, meaning the software itself, is not a VASP under the FATF Standards, as the Standards do not apply to underlying technology. However, creators, owners, operators, or other persons who maintain control or sufficient influence over a DeFi arrangement may meet the VASP definition and be subject to the same obligations, even where the arrangement describes itself as decentralized.

43. A critical regulatory requirement for VASPs is the implementation of the FATF Travel Rule, which requires VASPs to obtain, hold, and transmit originator and beneficiary information securely and on a timely basis in connection with covered VA

transfers.[5] For FIUs, the Travel Rule is vital because it converts a pseudonymous on-chain transfer into an identifiable financial transaction, providing the crucial off-chain data necessary for intelligence analysis and investigation.

44. Because the core blockchain protocol does not transmit personally identifiable information (PII), the industry is developing DLT-based messaging protocols to achieve Travel Rule compliance. These protocols leverage the cryptographic features of the underlying technology to address the Travel Rule's data-sharing challenge:

- **Secure Messaging Layers:** VASPs use standardized, secure messaging protocols (like TRISA or OpenVASP) that operate off chain. These systems are designed to identify the counterparty VASP using the public wallet address and then securely transmit the Travel Rule data (e.g., name, address, account information) through end-to-end encryption. This ensures that the data is transmitted securely only between the relevant regulated entities, without being exposed on the public ledger. However, FATF's 2025 Best Practices in Travel Rule Supervision paper notes that interoperability remains a practical challenge, and VASPs may need to maintain more than one Travel Rule solution to reach counterparties across markets (FATF, 2025a).

- **Smart Contract Automation:** Smart contracts can be used to automate compliance controls. For example, a smart contract can be programmed to verify that a counterparty VASP has been approved before a transaction is executed, or to flag or suspend a transfer until the required Travel Rule data has been exchanged.

- **Verifiable Credentials and Digital Identity:** Emerging decentralized identity (DID) solutions built on DLTs are key enabling technology. These systems allow users to prove their identity and ownership of a wallet address to a VASP through cryptographic proofs, which the VASP can then use to satisfy the Travel Rule's verification requirements without repeatedly handling or exposing sensitive know-your-customer (KYC) documentation.

45. By implementing these DLT-based solutions, VASPs create an auditable and encrypted link between the immutable on-chain transaction record (the public address and transfer amount) and the required off-chain identifying information (Travel Rule data, which must be submitted before or when the VA transfer is conducted rather than ex post), thereby strengthening compliance and providing FIUs with a clear pathway for identifying illicit actors.

Opportunities and Risks for AML/CFT/CPF Frameworks

46. For AML/CFT/CPF authorities, blockchain technology presents both opportunities and challenges. On the opportunity side, public blockchains provide exceptional transparency. Because every transaction is recorded and time-stamped, investigators can trace funds from origin to destination with a degree of precision that is often difficult to achieve in traditional banking systems. Specialized blockchain analytics tools—such as Chainalysis, TRM Labs, and Elliptic—apply heuristics and machine-learning models to link wallet addresses to real-world entities, identify suspicious clusters, and detect red-flag typologies, but their outputs should be interpreted cautiously because attribution may be probabilistic, costs can be substantial, and precision may be insufficient for certain supervisory or enforcement uses.

47. The immutable nature of the blockchain creates a permanent audit trail that can support judicial proceedings and help maintain the integrity of seized digital evidence. Beyond enforcement, distributed ledgers can also foster innovation in compliance: smart contracts are capable of embedding AML/CFT/CPF rules directly into financial logic, automatically enforcing transaction limits or Travel Rule data requirements. Emerging digital identity systems based on blockchain could enhance customer due diligence (CDD) processes while protecting user privacy through selective disclosure mechanisms.

48. An increasingly important application of smart contract technology is **programmable compliance**—the embedding of AML/CFT/CPF controls directly into the smart contracts that govern how virtual assets operate on the blockchain. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets identifies several programmable controls that stablecoin issuers can deploy to mitigate risks in both primary and secondary markets:

[5] In June 2025, FATF updated Recommendation 16 on payment transparency to ensure that the standard remains technology-neutral and future-proof. The revisions clarify responsibilities within the payment chain, standardize certain information requirements, and introduce requirements for tools to protect against fraud and error, including alignment or validation checks such as pre-validation, post-validation, or holistic monitoring. The revised requirements are expected to be implemented by the end of 2030 and will apply to VASPs through Recommendation 15.

- **Allow-listing (whitelisting):** Issuers can restrict transactions to pre-approved wallet addresses only. If a wallet address is not included on the access-control list embedded in the smart contract, the transaction is automatically rejected. CDD requirements can be integrated into the pre-approval process, ensuring that only identified users can transact in the stablecoin (FATF, 2026b).

- **Deny-listing (blacklisting):** Issuers can embed a deny control list in the smart contract that blocks specific wallet addresses from holding, receiving, or transferring stablecoins. The criteria for adding addresses may be informed by blockchain analytics, law enforcement data, or sanctions lists. While more reactive than allow-listing, deny-listing enables issuers or competent authorities, as permitted by the applicable legal and governance framework, to freeze wallet addresses with a stablecoin balance (FATF, 2026b).

- **Block, freeze, and withdraw capabilities:** Issuers can program smart contracts to block specific transactions, freeze entire wallet addresses, or withdraw (through the burning and reissuance of tokens) stablecoins when authorized under applicable legal or governance arrangements. These capabilities enable issuers to comply with orders from competent authorities, such as confiscation orders from law enforcement (FATF, 2026b).

- **Transaction limits:** Smart contracts can enforce per-transaction or daily aggregate limits on the amount transferred by wallet addresses, complementing allow-listing or deny-listing to reduce the risk of circumvention (FATF, 2026b).

49. These programmable controls represent a significant shift in how compliance can be operationalized within the virtual-asset ecosystem. Unlike traditional finance, where compliance depends on human processes and post-hoc monitoring, smart-contract-based controls can enforce predefined rules at the point of transaction execution—automatically and in real time. For FIUs and supervisors, understanding these capabilities is essential for assessing whether stablecoin issuers and intermediaries in their jurisdiction have deployed adequate technical safeguards. Several jurisdictions have already adopted elements of these approaches, including Japan (which applies CDD at issuance and redemption and leverages information from blockchain analytics firms and investigative authorities to assess risks), Switzerland (where a stablecoin issuer has implemented allow-listing via smart contracts for Swiss franc-denominated stablecoins), and Hong Kong, China (which requires stablecoin licensing applicants to assess risks associated with unhosted wallets and submit medium-to-long-term mitigation plans) (FATF, 2026b).

50. The same technological features that enable innovation and programmable compliance can also limit or circumvent regulatory strategies when activity moves outside identifiable intermediaries or issuer-controlled environments. The challenge for regulators is therefore to understand how these technological features affect the effectiveness of existing controls:

- **Privacy Coins:** Certain cryptoassets, such as Monero (XMR) and Zcash (ZEC), employ advanced cryptographic techniques to conceal senders, recipients, and transaction amounts. Monero uses ring signatures and stealth addresses to combine the true sender's input with decoy inputs, making it extremely difficult to identify the true source of funds. Zcash uses zk-SNARKs (zero-knowledge proofs) to verify that a transaction is valid without revealing the underlying transaction data, significantly complicating conventional transaction tracing.

- **Mixing and Obfuscation Services:** Centralized and decentralized mixing services, including privacy "tumblers", pool and redistribute funds to break the direct link between source and destination, a practice that FATF has explicitly identified as a money-laundering red flag.

- **DeFi Layering:** DeFi platforms pose a challenge because automated protocols replace traditional intermediaries. Criminal actors may exploit these platforms to conduct rapid and complex layering activities entirely on-chain:

    a. **Cross-Chain Bridges and Interoperability Risks:** Bridges are used to move assets between different blockchains (e.g., from Ethereum to Solana), fragmenting the transaction trail across multiple protocols and jurisdictions—a practice known as "chain-hopping." The FATF's 2026 report highlights that stablecoins face heightened cross-chain risks because blockchain developers increasingly prioritize interoperability for stablecoins compared to other virtual assets. This interoperability, while facilitating legitimate remittances and

financial activity, may also be exploited by illicit actors to obscure transaction flows. A particularly significant risk arises when centrally issued stablecoins circulate on other blockchains in the form of newly created, or "wrapped" tokens: the issuer's ability to freeze or deny-list the original asset may not extend to the wrapped version, weakening a key compliance control (FATF, 2026b).

b. **Liquidity Pools and DEXs:** Funds may be rapidly swapped for different tokens (e.g., Ether to stablecoins) and routed through various decentralized exchanges, often within a single complex transaction to obscure the original source of funds.

- **Cross-Border Complexity:** A single transaction may involve a wallet in one jurisdiction, validators in several others, and a VASP or exchange registered offshore. FATF's 2026 oVASP report notes that such activity can create regulatory blind spots; complicate supervision, mutual legal assistance processes, and international cooperation; and increase opportunities for regulatory arbitrage (FATF, 2026c).

51. These arrangements, products, and services have not displaced regulated VASPs or mainstream stablecoins because they often involve higher transaction costs, lower liquidity, greater technical complexity, weaker consumer protection, greater sanctions and enforcement risk, and limited usefulness for ordinary users who require reliable fiat on- and off-ramps. Legitimate users generally have strong incentives to remain within more liquid, user-friendly, and compliant platforms. Illicit actors, by contrast, may accept higher costs or technical complexity when those tools enhance anonymity or impede traceability. Regulators can respond by focusing on the points where these channels intersect with identifiable actors: requiring enhanced due diligence and blockchain analytics-based risk assessment by VASPs, imposing targeted restrictions or delisting requirements on products that significantly impair traceability, supervising stablecoin issuers' programmable controls, treating persons who exercise control or sufficient influence over DeFi arrangements as VASPs where the FATF definition is met. FATF's 2026 Targeted Report on Regulatory Challenges from Decentralised Finance reinforces this functional and risk-based approach and identifies on-chain and off-chain indicators of control that jurisdictions can use when assessing whether persons exercise control or sufficient influence over a DeFi arrangement (FATF, 2026d). Regulators should also strengthen monitoring of bridges and wrapped tokens, and improving cooperation with foreign supervisors, issuers, and blockchain-intelligence providers.

Resource and Sustainability Challenges

52. Supervising and investigating cryptoasset activity demands a blend of technological infrastructure, specialized human expertise, and inter-agency coordination. FIUs require personnel who can interpret blockchain data, understand typologies, and collaborate effectively with regulated VASPs and forensic specialists. FIUs such as FinCEN, TRACFIN, and Chile's UAF have established specialized cryptoasset units that combine data scientists, financial analysts, and investigators to manage these complexities.

53. Technological investment is equally critical. Agencies need access to fit-for-purpose blockchain analytics platforms capable of tracing transactions and assessing counterparty risk, as well as systems that integrate blockchain data into existing STR frameworks. However, these tools should be used with appropriate safeguards, since their attribution outputs may be insufficiently precise on their own to support supervisory sanctions or enforcement action. Secure digital-evidence management systems are necessary to maintain the chain of custody for seized assets. The cost of commercial analytics solutions can be substantial, though open-source tools offer lower-cost alternatives; in practice, FIUs can begin with general-purpose data-science ecosystems such as Python or R, used with Jupyter notebooks, open blockchain APIs, and graph-analytics libraries, which, while less user-friendly than commercial platforms, can significantly expand analytical capacity at relatively low cost.

54. Sustainability extends beyond funding. Retaining skilled personnel, ensuring continuous training, and maintaining inter-agency cooperation are ongoing challenges. For developing economies, partnerships with multilateral institutions—including the IDB, United Nations Office on Drugs and Crime (UNODC), and the Egmont Group—help pool resources, standardize approaches, and lower entry costs.

Implications for Financial Intelligence Units

55. The evolving crypto ecosystem requires FIUs to adapt both their analytical frameworks and institutional mindset. Building an informed understanding of national risk profiles is the first step: mapping the scale of peer-to-peer activity, identifying local VASPs, and quantifying exposure to cross-border flows. Collaboration with VASPs and blockchain intelligence providers can improve the quality of information contained in STRs and provide early-warning indicators of illicit behavior.

56. Integrating blockchain-derived information into existing financial intelligence processes enhances the ability to detect complex money-laundering and asset-laundering schemes. Indicators such as wallet clustering, transaction velocity, and counterparty exposure can be incorporated into risk-scoring models. Because crypto transactions transcend borders, regional cooperation becomes indispensable. Within the Americas, organizations such as the CFATF and GAFILAT play a key role in fostering information sharing, joint typology exercises, and coordinated investigations. At the international level, the Egmont Group's Secure Web (ESW) provides a secure platform for collaboration and information sharing among FIUs.

57. Continuous training and professional development are essential. As blockchain technologies evolve—introducing new asset types, privacy features, and cross-chain mechanisms—AML/CFT/CPF professionals must keep pace. FIUs that institutionalize continuous learning and invest in multidisciplinary teams will be better positioned to meet the demands of a rapidly evolving financial landscape.

Conclusion

58. Blockchain technologies and DLTs have redefined how value is recorded and transferred, offering both transparency and new vulnerabilities. For FIUs and supervisory bodies, understanding these technologies is no longer optional but a core operational requirement. Effective AML/CFT/CPF oversight depends on the ability to trace digital transactions, understand the underlying code-based logic, and translate complex data into actionable intelligence. The emergence of programmable compliance controls—including allow-listing, deny-listing, freeze-and-burn capabilities, and transaction limits embedded in smart contracts—adds a new dimension that supervisors must understand and assess when evaluating the adequacy of stablecoin issuers' risk mitigation measures.

59. The task for policymakers is to balance innovation and integrity. Countries that invest in digital literacy, analytical capabilities, and international cooperation will be better positioned to reduce their exposure to illicit finance while harnessing blockchain's potential to strengthen transparency and public trust. In this sense, technology is not merely a risk to be mitigated but a tool to be understood, governed, and leveraged effectively.

Key Actions for FIUs and Supervisors — Chapter 1

- **Build foundational blockchain literacy across investigative, analytical, and supervisory teams.** Prioritize understanding how wallets, transactions, consensus mechanisms, hosted and unhosted wallets, and P2P transactions operate, so that staff can interpret on-chain evidence, understand which transfers fall within or outside the regulated AML/CFT/CPF perimeter, and assess VASP compliance.
- **Assess programmable compliance controls for stablecoins.** Where stablecoin issuance is permitted, FIUs should coordinate with supervisors and other competent authorities to assess whether stablecoin issuers operating in or serving the jurisdiction have deployed appropriate programmable controls (e.g., allow-listing, deny-listing, freeze-and-burn capabilities, and transaction limits). Where gaps exist, supervisors and regulators should consider whether supervisory guidance, expectations, or regulatory requirements should address them.
- **Invest in fit-for-purpose blockchain analytics and integrate on-chain data into existing STR and supervisory workflows.** Open-source tools (e.g., Python, R, open blockchain APIs, and graph analytics libraries) can offer lower-cost entry points, while commercial platforms may provide more advanced attribution and risk-scoring capabilities. Outputs should be interpreted cautiously and combined with off-chain information, since attribution may not be sufficient on its own.
- **Develop awareness of cross-chain and offshore risks.** Understand how bridge protocols, wrapped tokens, and offshore or unlicensed VASPs can fragment transaction trails, weaken issuer-level controls such as freezing or deny-listing mechanisms, and complicate supervision, international cooperation, and asset tracing.

CHAPTER 2:

Understanding Cryptocurrencies and Virtual Assets

Chapter 2: Understanding Cryptocurrencies and Virtual Assets

Introduction

60. For FIUs, a nuanced understanding of what constitutes a cryptoasset—and how different categories of virtual assets function—is essential for designing effective measures to combat money-laundering, terrorist financing, proliferation financing, and related financial crimes. The rapid evolution of these instruments, ranging from decentralized cryptocurrencies and stablecoins to NFTs and DeFi instruments, has outpaced most regulatory frameworks. This chapter explains how major categories of digital assets are created, exchanged, and valued; how regulatory regimes in key jurisdictions have responded; and what typologies reveal about their misuse. The aim is to equip FIUs with a practical understanding of the technologies they monitor, the economic logic underlying them, and their implications for financial integrity.

Defining Virtual Assets and Service Providers

61. The FATF defines a virtual asset (VA) as a "digital representation of value that can be digitally traded, transferred, or used for payment or investment purposes" (FATF Recommendations, Glossary; FATF, 2021 Updated Guidance). Entities engaged in exchanging, safeguarding, or transferring such assets are VASPs, as defined under Recommendation 15 and its Interpretive Note (see Chapter 1, para. 42 for the full five-limb definition). The FATF Recommendations require countries to identify, license, and supervise these providers under a risk-based approach.

62. This functional definition deliberately distinguishes virtual assets from other digital instruments. Central bank digital currencies (CBDCs) are considered sovereign money in digital form and therefore fall outside FATF's definition of virtual assets. Similarly, closed-loop tokens used in gaming or loyalty programs are generally exempt, as they lack transferability or market value. The key criterion is whether the instrument can serve as a medium of exchange or a store of value independent of a central issuer.

63. While the FATF's approach ensures technological neutrality, national interpretations vary widely. Some jurisdictions treat cryptoassets as securities, others as commodities, and still others as payment instruments or a combination thereof. This fragmentation complicates supervision and cross-border enforcement, making international cooperation indispensable for FIUs.

Major Categories of Virtual Assets

64. Although thousands of tokens circulate globally, most fall into a limited number of categories whose creation processes and underlying logic shape their risk profiles and AML/CFT/CPF relevance.

Cryptocurrencies

65. Cryptocurrencies such as Bitcoin and Litecoin are decentralized digital assets that operate on public blockchains without a central issuer. They are created through mining or minting, depending on the consensus mechanism. In PoW systems, miners validate transactions by solving cryptographic puzzles; the first to solve one adds the new block and earns newly created coins. In PoS systems, participants stake existing tokens as collateral; validators are chosen in proportion to their holdings and receive newly minted tokens as rewards. Because issuance is algorithmic rather than asset-backed, the value of most cryptocurrencies is driven primarily by market expectations and scarcity, making them largely speculative assets. Their pseudonymous nature, global reach, and liquidity make them attractive for both legitimate innovation and illicit activity. Bitcoin remains widely used in ransomware payments and darknet-market transactions, although stablecoins have now overtaken it as the dominant virtual asset in illicit on-chain transactions (Chainalysis, 2026).

Stablecoins

66. Stablecoins are virtual assets that generally incorporate a stabilization mechanism and are used as a means of payment or store of value. The FATF recognizes that stablecoins are not a legal or technical category and that the use of this term is

not intended to endorse any stability claims (FATF, 2026b). As of mid-2025, more than 259 stablecoins were in circulation, with total market capitalization exceeding USD 316 billion and daily trading volumes surpassing those of Bitcoin. Stablecoins represent approximately 30 per cent of all on-chain virtual asset transaction volume (FATF, 2026b). Fiat-backed stablecoins dominate the market (95 per cent of total market capitalization), with U.S. dollar-referenced stablecoins accounting for 97 per cent of that category.

67. The FATF's 2026 Targeted Report on Stablecoins classifies them into three types based on their stabilization mechanisms:

- **Asset-backed stablecoins** are backed by financial assets, such as fiat currencies or government bonds. Issuers typically commit to redeeming stablecoins for the backing asset on a 1:1 basis. They generally have centralized governance structures managed by the issuer. USDC and USDT are the dominant examples. For AML/CFT purposes, transparency over the issuer, reserve assets, custodians, and redemption channels helps supervisors identify accountable entities and key fiat on- and off-ramps; weak disclosure can obscure accountability and complicate risk assessment.

- **VA-backed stablecoins** are issued using other virtual assets and tokenized financial instruments as collateral. Due to price volatility concerns, these arrangements typically require over-collateralization. Issuance, redemption, and collateral management are often conducted through autonomous smart contracts, and in some cases users may issue stablecoins directly without relying on centralized governing entities or intermediaries (FATF, 2026b).

- **Algorithmic stablecoins** maintain price stability by adjusting supply through smart contracts or algorithms without relying on reserve-backed assets. They do not typically offer redemption into fiat currency but instead seek to stabilize prices through mechanisms such as token swaps or token burns. The collapse of TerraUSD (UST) in 2022, which erased more than USD 40 billion in value, demonstrated how opaque algorithmic stabilization mechanisms can generate significant systemic risk (FATF, 2026b).

68. Stablecoins' link to traditional finance—through bank accounts, custodians, and reserve assets—creates both opportunities for supervision and potential vulnerabilities when cross-jurisdictional oversight is fragmented. Stablecoins have also become the virtual asset most commonly used in illicit transactions, accounting for an estimated 84 per cent of the USD 154 billion in illicit virtual asset transaction volume in 2025 (Chainalysis, 2026). Their price stability, high liquidity, and interoperability make them attractive to illicit actors, particularly for P2P transfers via unhosted wallets and conversion into fiat currency through OTC brokers (see Chapter 3 for regional typologies).

69. A distinctive feature of many centrally governed stablecoins is the issuer's ability to embed programmable compliance controls in smart contracts—including allow-listing, deny-listing, freeze-and-burn capabilities, and transaction limits—as detailed in Chapter 1. These technical measures represent an emerging set of tools that issuers and supervisors can use to mitigate risks in secondary markets and P2P transactions where direct issuer-level AML/CFT controls may otherwise be more limited.

70. In the United States, the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act, enacted on July 18, 2025, establishes a federal framework for payment stablecoins. For AML/CFT purposes, the key point is that clearer issuer authorization, reserve, and supervisory requirements may facilitate institutional adoption while also adding an additional layer of regulatory accountability for payment stablecoins offered within the U.S. financial system.[6]

Privacy Coins

71. Privacy coins, including Monero (XMR) and Zcash (ZEC), may be mined or staked, depending on their underlying protocol, and incorporate cryptographic techniques such as ring signatures and zero-knowledge proofs that conceal transaction origins and amounts. These features enhance user privacy but significantly reduce transaction transparency and traceability. The FATF (2021; 2025) and the International Monetary Fund (2023) identify privacy-enhancing assets as presenting higher ML/TF/PF risks. Several jurisdictions—including Japan, South Korea, and the United Kingdom—have banned or delisted them from licensed exchanges to preserve compliance standards.

[6] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, §§ 4(a)(1)(A), 20, 139 Stat. 419, 425–26, 465 (2025).

Utility and Governance Tokens

72. Utility and governance tokens are commonly created through initial coin offerings (ICOs) or token generation events. Developers may mint a fixed or variable supply of tokens and distribute them to users or investors in exchange for fiat currency or other cryptoassets. These tokens often grant access to digital services or voting rights within decentralized protocols rather than representing ownership interests in tangible assets. Their issuance is often analogous to distributing digital membership rights, although many ICOs have functioned primarily as speculative fundraising mechanisms. The U.S. Securities and Exchange Commission (SEC) has repeatedly determined that such offerings constitute unregistered securities offerings when they are marketed as investments with an expectation of profit.

Non-Fungible Tokens (NFTs)

73. NFTs represent unique digital assets recorded on a blockchain. Each NFT is minted by attaching a distinct identifier and metadata to a token, linking it—sometimes loosely—to a digital file such as artwork, music, or a certificate. NFTs can represent intangible creative works or tokenized rights to real-world assets. Their subjective valuation, rapid price volatility, and peer-to-peer transferability have already contributed to cases of wash trading and price manipulation resembling forms of art-market laundering (OECD, 2023).

74. Understanding how each category is generated is critical for FIUs. Assets created algorithmically without reserves (e.g., Bitcoin) derive value from network trust and market sentiment; those issued against real assets (e.g., fiat-backed stablecoins) depend on the credibility of custodians; and those issued through fundraising events (e.g., ICOs and certain NFT offerings) raise investor-protection and disclosure concerns. Each model implies different red-flag indicators, enforcement strategies, and regulatory obligations.

Institutional Design: Who Should Regulate and Supervise?

75. Regulatory design encompasses both substantive rules and institutional architecture. A fundamental question concerns which authority should oversee virtual asset activity and how its mandate aligns with the function and risks of the activities being supervised. Around the world, three main models have emerged, each with distinct advantages and risks.

76. In many countries, central banks have assumed a leading role because cryptoassets intersect with monetary policy, payment systems, and financial stability. This approach allows close monitoring of systemic effects and interaction with cross-border payment infrastructures. Brazil's Central Bank, for instance, supervises VASPs under the country's Virtual Asset Law and integrates them into the national payment ecosystem alongside the DREX digital currency project. Yet central bank leadership can also blur the boundary between prudential oversight and market conduct, stretching mandates originally designed for sovereign money rather than privately issued tokens.

77. Other jurisdictions entrust oversight to financial sector supervisors or bank regulation agencies, reflecting the view that VASPs operate much like financial intermediaries. The United Kingdom's Financial Conduct Authority (FCA) and several European Union (EU) member states operating under MiCA follow this model. Locating supervision within existing prudential authorities facilitates consistency with customer protection and AML rules already applied to banks and securities firms. However, traditional supervisors may lack the technical expertise and agility required to engage effectively with decentralized protocols, smart contracts, and algorithmic stablecoins.

78. A third model relies on specialized or hybrid agencies dedicated to digital assets. The U.S. approach, involving multiple regulators—SEC, CFTC, FinCEN, and state licensing authorities—reflects this hybrid logic but also illustrates its coordination challenges. Some jurisdictions, including India, have assigned or concentrated VASP-related AML/CFT supervisory functions within FIUs or dedicated cryptoasset/fintech units to bridge the expertise gap while maintaining cross-sector coordination.

79. Choosing among these options is not merely an administrative decision—it determines how effectively AML/CFT/CPF obligations can be enforced, how innovation is treated, and how accountability is distributed across the state. Cryptoasset regulation is best understood as a matching exercise among the activity, the associated risks, and the supervisory

capabilities required to address them. Where virtual assets are used as payment or settlement tools, regulation should focus on payment-system integrity, reserve management, redemption rights, operational resilience, sanctions compliance, and issuer-level controls. Where tokens resemble investment products, disclosure, market conduct, custody, conflicts of interest, and investor protection become central. Where VASPs provide exchange, transfer, or custody services, licensing or registration, CDD, Travel Rule implementation, suspicious transaction reporting, and supervisory access to data are foundational. For privacy-enhancing products and obfuscation services, the regulatory question is whether and under what conditions they should be permitted, restricted, prohibited, or subject to enhanced mitigating measures, given the vulnerabilities they create for traceability. For DeFi arrangements and cross-chain bridges, the question is more complex: whether identifiable persons exercise control or sufficient influence, and where risk-mitigation measures can be imposed—on VASPs, issuers, front-end operators, custodians, or fiat on- and off-ramps.

80. These choices involve important tradeoffs. Centralized models can promote coherence and reduce gaps between agencies but they may create risks of institutional overload or insufficient sector-specific expertise. Dispersed or sectoral models can draw on specialized knowledge and foster expertise, but they require strong domestic coordination mechanisms —consistent with FATF Recommendations 2 and 31—to avoid fragmented oversight, duplicated efforts, and opportunities for regulatory arbitrage. Prohibition models may reduce domestic exposure to specific risks, but they can also push activity toward offshore or informal channels. Moreover, they are not a substitute for identifying, assessing, and mitigating VA/VASP risks, including activity by offshore, unlicensed, or non-compliant providers that may continue to serve users in the jurisdiction. Conversely, frameworks that permit VA activities while promoting AML-by-design—consistent with the obligation under Recommendation 15 to identify, assess, and mitigate risks before launch or use—can support responsible innovation and financial inclusion, but they may leave important supervisory gaps if not accompanied by effective licensing or registration, supervision, and enforcement. Comprehensive, risk-based licensing or registration regimes for VASPs and stablecoin-related intermediaries can provide clarity and market discipline, but they may also increase compliance costs, particularly for smaller or emerging providers, making proportionality an essential design principle. For Latin America and the Caribbean, where regulatory capacity and market maturity vary widely, institutional design should align with existing financial supervision structures while ensuring that cryptoasset oversight integrates effectively into national AML/CFT/CPF frameworks. Policymakers must consider where the necessary powers, data-access authorities, and enforcement tools already reside—and how best to adapt them to a digital–asset ecosystem that transcends traditional sectoral boundaries. The jurisdictional examples below should therefore be read not as a ranking of regulatory models, but as illustrations of how countries allocate responsibilities and define regulatory requirements in response to different cryptoasset-related challenges.

Comparative Regulatory Approaches

81. The global regulatory landscape reflects divergent philosophies regarding innovation, risk management, and market integrity.

82. In the **United States**, cryptoassets are regulated through a fragmented framework involving multiple sectoral authorities. The SEC and Commodity Futures Trading Commission (CFTC) share jurisdiction, while FinCEN has required VASPs to register as money service businesses since 2013. Proposed bills such as the Financial Innovation and Technology for the 21st Century (FIT21) and the Clarity for Payment Stablecoins Act aim to clarify responsibilities and establish uniform consumer protections. Enforcement actions—including the USD 4.3 billion settlement reached with Binance Holdings Ltd. in 2023 for AML-related violations—illustrate a shift toward greater accountability under existing financial-crime laws.

83. **The European Union's** Markets in Crypto-Assets (MiCA) Regulation, adopted in 2023, provides one of the world's most comprehensive regulatory frameworks for cryptoassets. MiCA harmonizes authorization, governance, and disclosure requirements across EU member states, while the Transfer of Funds Regulation (TFR) extends Travel Rule obligations to cryptoasset transfers. This coordinated approach exemplifies the EU's "same activity, same risk, same rules" philosophy. Notably, MiCA classifies stablecoins into two distinct regulatory categories: E-Money Tokens (EMTs), which are linked to a single fiat currency and are issued by authorized credit institutions or electronic money institutions subject to AML/CFT obligations; and Asset-Referenced Tokens (ARTs), which purport to maintain a stable value by

referencing another value, right, or asset, or a combination thereof. While ART issuers are not themselves AML/CFT obliged entities, competent authorities consider ML/TF risks when granting or refusing authorization, and exchange, custody, or distribution services involving ARTs require authorization as a Crypto-Asset Service Provider (CASP) with full AML/CFT/CPF obligations (FATF, 2026b). For issuers of significant ARTs and EMTs, the European Banking Authority establishes and chairs supervisory colleges to coordinate oversight across member states (FATF, 2026b).

84. The **United Kingdom** integrated cryptoassets into the Financial Services and Markets Act 2023, granting the Financial Conduct Authority (FCA) authority to supervise VASPs. The FCA maintains a public registry of authorized firms and enforces stringent requirements for custody, client fund segregation, and anti-promotion rules, reinforcing investor confidence.

85. In **Latin America**, Brazil's Virtual Asset Law No. 14,478/2022 established a regulatory perimeter and criminalized virtual asset fraud. The Central Bank of Brazil, responsible for oversight, is also piloting its own permissioned DLT-based digital currency, DREX, balancing innovation and control. Mexico's Fintech Law (2018) recognizes virtual assets as means of payment under the Bank of Mexico's supervision, but restricts their use within regulated financial institutions. El Salvador's 2021 Bitcoin Law, which made Bitcoin legal tender, remains one of the most prominent experiments in state-level adoption—boosting tourism but raising concerns regarding fiscal exposure and AML/CFT supervision (IMF, 2022). In early 2025, the law was amended to make Bitcoin acceptance voluntary as part of an agreement with the IMF, though El Salvador remains committed to positioning itself as a digital asset hub through the Digital Asset Issuance Law and a robust licensing regime.

86. These models highlight the global tension between promoting innovation and preserving financial integrity. For FIUs, they underscore the importance of understanding foreign regulatory regimes, which often determine data-sharing channels and the enforceability of cross-border cooperation requests.

Typologies and Misuse Cases

87. Illicit use of cryptoassets often mirrors the traditional money-laundering cycle of placement, layering, and integration, but each stage is executed digitally and at much greater speed.

88. In the **placement stage**, criminals convert cash into cryptoassets through informal brokers, ATMs, or over-the-counter (OTC) traders. Investigations in Latin America show that small retail exchanges frequently serve as entry points for drug-trade proceeds, especially where KYC controls are weak.

89. During **layering**, offenders exploit pseudonymity and the borderless nature of virtual asset transfers to obscure the origins of funds. Assets may pass through multiple wallets, move across blockchains via bridges, or be routed through mixing services. The Tornado Cash case illustrates this risk: sanctioned by the U.S. Office of Foreign Assets Control (OFAC) in 2022, the decentralized protocol allegedly laundered more than USD 7 billion, including funds linked to North Korean cyberattacks (U.S. Treasury, 2022).

90. The scale of state-linked virtual asset theft has reached unprecedented levels. In February 2025, DPRK-affiliated actors conducted the largest single theft of virtual assets in history, stealing approximately USD 1.46 billion from the VASP ByBit. The attackers used social-engineering techniques and malicious code to access wallet infrastructure and manipulate transaction data. The stolen funds were subsequently laundered through mixers, cross-chain bridges, and over 125,000 Ethereum wallets, before being converted into USDT on the TRON blockchain and off-ramped through OTC brokers and peer-to-peer platforms (FATF, 2025c). As of mid-2025, only 3.8 per cent of the stolen funds had been recovered, highlighting the need for enhanced public–private partnerships and more rapid international cooperation mechanisms (FATF, 2025c). The DPRK's 221 General Bureau has also been assessed as using USDT in transactions involving the sale and transfer of military equipment and raw materials used in munitions production, indicating efforts to operationalize stablecoins in WMD-related procurement (FATF, 2026b).

91. During the **integration stage**, laundered assets re-enter the formal economy through conversion to fiat or investment in real estate, luxury goods, or NFTs. NFT marketplaces have exhibited patterns of self-trading designed to inflate prices, effectively "cleaning" illicit funds under the guise of art sales.

92. Governance failures can also generate AML/CFT/CPF vulnerabilities. The FTX collapse in 2022 revealed how the absence of segregation between customer and corporate funds can compromise an exchange's integrity, prompting calls for stricter custodial rules. Meanwhile, attempts to evade sanctions—notably increased ruble-to-cryptoasset conversions following Russia's invasion of Ukraine—demonstrated both the agility of digital markets and the limits of large-scale evasion, given blockchain transparency and improved VASP compliance.

93. These typologies demonstrate that the same attributes driving financial innovation—speed, global reach, and pseudonymity—can also be exploited for concealment when regulatory frameworks are weak.

Supervisory Challenges and Policy Implications

94. For FIUs, supervising this ecosystem requires both technical and institutional adaptation, as well as sustained analytical capacity. Effective oversight depends on linking on-chain evidence with off-chain intelligence—including exchange records, IP addresses, and banking relationships—to interpret transactions meaningfully.

95. Licensing and registration remain foundational elements of an effective supervisory framework. The FATF's 2026 Targeted Update on VAs and VASPs shows modest progress in technical compliance with Recommendation 15: 34 percent of 149 assessed jurisdictions were largely compliant, up from 29 percent in 2025, but only one jurisdiction was fully compliant. Licensing and registration gaps remain significant: only 40 percent of assessed jurisdictions (59 of 149) satisfactorily require VASPs to be licensed or registered, while survey data show that 73 percent of relevant respondents require licensing or registration but only 58 percent have licensed or registered a VASP in practice. DeFi also remains a supervisory challenge: 31 percent of responding jurisdictions (44 of 142) reported that their risk-mitigation measures apply to DeFi arrangements, but only four have imposed licensing or registration requirements and only two have actually licensed or registered such arrangements in practice (FATF, 2026a). Even where regulatory frameworks exist, supervisory authorities often face limited technical expertise and technological capacity. Integrating blockchain analytics into STR systems requires interoperable data infrastructure and clear legal gateways for information exchange.

96. Regional initiatives such as the Financial Intelligence Data Labs under development in Latin America with IDB support demonstrate how partnerships can strengthen analytical capacity and standardize methodologies.

97. A persistent policy challenge involves balancing transparency with privacy. While blockchain transparency enhances traceability, expanded monitoring of unhosted wallets and DeFi platforms also raises legitimate concerns regarding surveillance and proportionality. Innovative approaches—such as privacy-preserving compliance tools based on zero-knowledge proofs—suggest that technology can help reconcile these objectives.

98. Finally, capacity building must extend beyond FIUs to prosecutors, judges, and law enforcement authorities. Understanding how assets are minted, traced, seized, and valued helps ensure that financial intelligence leads to enforceable judicial outcomes and successful asset recovery.

Conclusion

99. Understanding how digital assets are generated, valued, and governed is fundamental to safeguarding financial integrity. The mechanisms of minting, backing, and trading determine whether a cryptoasset functions as a payment instrument, a speculative vehicle, or a conduit for illicit finance. For FIUs, distinguishing among these dimensions transforms abstract technology into actionable intelligence. The rapid growth of stablecoins—now the dominant virtual asset class both by trading volume and by share of illicit on-chain activity—makes understanding their three-tier classification (asset-backed, VA-backed, algorithmic) and the programmable compliance tools available to issuers particularly important.

100. In Latin America and the Caribbean—where cryptoasset adoption intersects with remittance flows and macroeconomic volatility—the challenge lies in designing proportionate regulation while leveraging blockchain's transparency. Lessons from the United States, European Union, and United Kingdom demonstrate that clear rules, robust supervision of VASPs, and sustained investment in analytical capabilities can foster innovation without compromising financial integrity. Ultimately, the impact of these technologies will depend not on code alone but on the institutions that develop the capacity to govern them effectively.

Key Actions for FIUs and Supervisors — Chapter 2

- **Understand the FATF's three-tier stablecoin classification** (asset-backed, VA-backed, and algorithmic) with particular attention to asset-backed and fiat-referenced stablecoins, given their market dominance and their distinct risk profiles, governance structures, reserve, and supervisory implications.
- **Monitor developments in stablecoin market within your jurisdiction**, prioritizing the volume and nature of asset-backed or fiat-referenced stablecoin transactions, the role of OTC brokers, and the prevalence of P2P transfers via unhosted wallets.
- **Benchmark your jurisdiction's regulatory framework against MiCA's EMT and ART classifications** and the FATF 2026 recommended actions for stablecoin oversight, including supervisory colleges for cross-border arrangements.
- **Keep risk assessments up to date by reflecting that stablecoins are now estimated to account for a majority of illicit virtual asset transaction volume**. Incorporate the DPRK ByBit case and proliferation-financing typologies into institutional threat assessments where relevant to the domestic risk profile.
- **Ensure that your jurisdiction's VASP licensing or registration framework encompasses stablecoin issuers and relevant intermediaries,** clearly delineates AML/CFT/CPF obligations for each participant in the stablecoin ecosystem (issuers, reserve custodians, intermediary VASPs, payment providers), and supports risk-based requirements for secondary-market activity.

CHAPTER 3:

Cryptoasset Adoption in Latin America and Illicit Finance Risks

Chapter 3: Cryptoasset Adoption in Latin America and Illicit Finance Risks

Introduction

101. Cryptoasset adoption has expanded rapidly across Latin America in recent years, driven by economic pressures such as inflation, the need for greater financial inclusion, and reliance on remittances. This growth in legitimate use has been accompanied by increasing illicit finance risks, as criminal actors increasingly exploit digital assets for money laundering, terrorist financing, proliferation financing, fraud schemes, and sanctions evasion.

102. The region's policymakers now face the dual challenge of fostering financial innovation while safeguarding integrity. Blockchain intelligence solutions are becoming increasingly important for strengthening oversight—equipping law enforcement authorities and regulators with tools to trace illicit cryptoasset transactions and enforce regulatory requirements in the digital-asset ecosystem.

103. This chapter examines current cryptoasset adoption trends in Latin America, the associated illicit finance threats, and the existing regulatory frameworks, and proposes policy and regulatory strategies—including enhanced VASP oversight, implementation of global AML/CFT/CPF standards, investment in blockchain-intelligence capabilities, and PPPs—to balance innovation with security.

A Region Transformed by Digital Migration

104. The digital migration underway in Latin America and the Caribbean reflects the convergence of structural economic pressures and technological opportunities. Over the past five years, the region has experienced one of the fastest increases in cryptocurrency activity worldwide. A regional analysis of transaction data from 2019 to 2024 shows sustained exponential growth. Transaction volume in the region surpassed USD 500 billion in 2024, contributing significantly to the global total of USD 10.6 trillion, a 56 per cent increase from the previous year.[7] Inflationary pressures, limited access to banking services, and the high cost of cross-border remittances remain the principal drivers.

105. Economic instability has long shaped the region's financial behavior. In countries experiencing repeated currency crises and strict capital controls, confidence in domestic currencies has often eroded significantly. For households facing annual inflation rates exceeding 100 per cent, digital dollars—particularly stablecoins pegged to the U.S. dollar—offer a parallel store of value. Another important driver is the region's dependence on remittances. In 2023, LAC received more than USD 155 billion in remittances, equivalent to 5 per cent of regional GDP (World Bank, 2023). The COVID-19 pandemic further accelerated this digital shift. Lockdowns, limited physical banking access, and the rise of online commerce pushed new users toward digital wallets, embedding cryptoassets into everyday financial behavior.[8]

106. However, the rise of cryptocurrencies in Latin America also brings significant challenges. Like any financial instrument, cryptoassets can be exploited by illicit actors to evade sanctions and launder funds. Cybercriminals have used digital assets to perpetrate investment fraud schemes and facilitate darknet market transactions, and have even created proprietary exchanges and tokens to facilitate illicit activities.

107. This evolving threat landscape has exposed gaps in regulatory frameworks. Across Latin America, regulatory responses have been uneven, with some countries proactively developing cryptoasset oversight frameworks while others lag behind or prohibit certain forms of crypto activity. Brazil, the region's largest economy, has developed a regulatory framework that addresses consumer protection, anti-fraud safeguards, and AML/CFT/CPF obligations, while Mexico continues to refine its cryptoasset regulations; meanwhile, countries such as Bolivia have prohibited cryptocurrency use entirely.

[7] Blockchain intelligence analysis (2025).
[8] For example, stablecoins may allow an Argentine shopkeeper to protect savings against hyperinflation, while a migrant worker in the United States may send money to family members in Mexico at a fraction of the cost of traditional remittance channels. These factors have fueled a grassroots adoption of cryptoassets as a means of economic empowerment and financial inclusion.

Current Trends in Adoption in LAC

108. Cryptoasset adoption in Latin America and the Caribbean continues on a robust upward trajectory, positioning the region as one of the fastest-growing crypto markets worldwide. In 2024, Latin America accounted for a substantial share of the USD 10.6 trillio in global crypto transactions. Brazil, Mexico, and Argentina, in particular, show high adoption rates, placing 9th, 16th, and 19th, respectively, in TRM's 2024 Global Crypto Adoption Index. Their high levels of participation reflect both consumer interest and economic necessity. A closer look at country-level trends illustrates the diverse drivers of crypto uptake across the region:

109. Argentina. Amid a long history of high inflation and capital controls, many Argentinians have embraced cryptoassets as a tool for financial adaptation such as hedging against inflation and preserving financial independence. This pattern is visible in transaction data: Chainalysis estimates that Argentina received approximately USD 91.1 billion in cryptoasset value between July 2023 and June 2024, the highest figure in Latin America for that period. Stablecoins are central to this activity, accounting for an estimated 61.8 per cent of Argentina's cryptoasset transaction volume, above both Brazil's 59.8 per cent and the global average of 44.7 per cent. Argentine users frequently turn to USD-pegged stablecoins to safeguard savings from peso devaluation and to transact in a more stable unit of value. For risk-assessment purposes, these figures suggest that authorities should monitor not only overall adoption, but also product-level indicators such as stablecoin transaction volumes, VASP customer data, STR trends, and blockchain-analytics indicators.

110. Brazil. With the region's largest cryptoasset market, Brazil has benefited from a tech-savvy population and supportive fintech infrastructure. Chainalysis (2024b) estimates that Brazil received approximately USD 90.3 billion in cryptoasset value between July 2023 and June 2024, while institutional-sized transaction activity increased by approximately 29.2 per cent between the last two quarters of 2023 and 48.4 per cent between Q4 2023 and Q1 2024. At the same time, Brazil's broader digital-payments landscape is dominated by Pix: the Banco Central do Brasil (2025) reports that Pix processed 63 billion transactions totaling BRL 26.4 trillion in 2024, demonstrating an openness to digital finance innovations. The government is also piloting a central bank digital currency (the Digital Real, or Drex), indicating an institutional push alongside grassroots adoption. Brazil's experience illustrates how a combination of need (e.g., alternative investment opportunities during periods of low yields) and digital infrastructure (efficient payment rails) can accelerate cryptoasset adoption.

111. Mexico. Cryptoasset adoption in Mexico is driven by both domestic needs and the large volume of remittances from abroad. Millions of unbanked or underbanked Mexicans view cryptoassets as a means of accessing financial services beyond traditional banking channels. Mexican families receiving remittances have begun to rely—often without being aware of the underlying infrastructure—on cross-border providers that use cryptoassets behind the scenes to transfer funds from the United States more quickly and at lower cost. On the policy front, Mexico has taken a leadership role by assuming the presidency of the FATF with an agenda focused on financial inclusion and improving the implementation of related FATF standards in lower-capacity jurisdictions.

112. Venezuela. While not formally ranked in the Crypto Adoption Index, Venezuela is often cited for its high level of grassroots cryptoasset adoption under challenging macroeconomic conditions. During the period of hyperinflation and strict capital controls between 2017 and 2021, Venezuelans turned to cryptocurrencies (especially stablecoins like Tether, better known as USDT) as an alternative store of value and medium of exchange, a practice that has persisted because of continuing macroeconomic instability. Cryptoassets facilitate day-to-day transactions and the receipt of remittances or aid from abroad, bypassing the physical bolívar. At the same time, the same features that make crypto useful—speed, pseudonymity, and operating outside traditional intermediaries—also contribute to the development of a sizable grey market, facilitating tax evasion and a range of illicit activities amid limited oversight and transparency. The government itself launched a national cryptocurrency (the Petro) as part of broader efforts to facilitate international transactions under sanctions. Although reliable data remain limited, Venezuela exemplifies how crypto adoption can be spurred by severe currency collapse and international isolation.

113. El Salvador. As the first country to adopt Bitcoin as legal tender in September 2021, El Salvador has sought to establish a comprehensive regulatory framework designed to foster innovation while maintaining financial integrity. The country's approach to digital assets includes robust licensing, compliance, and AML/CFT/CPF measures, overseen by the Comisión Nacional de Activos Digitales (CNAD). Initially, the Bitcoin Law required businesses to accept Bitcoin as payment, alongside the US dollar, but in early 2025, the law was amended to make Bitcoin acceptance voluntary as part of an agreement

with the International Monetary Fund (IMF). Despite these modifications, El Salvador remains committed to positioning itself as a global hub for crypto businesses through the Digital Asset Issuance Law (DAI Law), a strong licensing regime, and international regulatory cooperation with countries such as Argentina and Paraguay. The legal framework has attracted major industry players, with Tether announcing plans to relocate its headquarters to El Salvador in early 2025 after securing a DASP licence.

114. Overall, Latin America's virtual asset landscape is characterized by both opportunity and necessity. Individuals are increasingly using cryptoassets to access financial services in new ways—including protecting savings against inflation, facilitating cross-border commerce and remittances, and participating in the digital economy. TRM's *A Digital Migration* report observed that the pandemic catalyzed an online migration in Latin America, bringing many users into the cryptocurrency ecosystem as traditional brick-and-mortar services faltered. Cryptoassets are increasingly viewed not merely as a speculative investment, but as a practical tool for everyday finance in the region. These adoption trends set the stage for policymakers: the challenge is to support financial innovation while addressing the vulnerabilities that accompany it.

Illicit Finance Risks in Latin America and the Caribbean

115. The other side of Latin America and the Caribbean's rapid cryptoasset expansion is the growing misuse of cryptocurrencies by illicit actors. Globally, illicit cryptoasset activity remains a small fraction of total transactions (about 0.4 per cent in 2024) but still amounted to roughly USD 45 billion in value (TRM, 2025). The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets further notes that stablecoins, particularly when used in peer-to-peer transfers involving unhosted wallets, have become the most common virtual asset used in illicit transactions, accounting for 84 per cent of USD 154 billion in illicit virtual-asset transaction volume in 2025 (Chainalysis, 2026).

116. GAFILAT's July 2025 *Evaluación Sectorial de Riesgos* provides the authoritative baseline for understanding these risks across the 18 GAFILAT member countries. The ESR concludes that, at the regional level, virtual assets and VASPs present a **very high risk** of money laundering from fraud and scams, cyberattacks, and drug trafficking; **high risk** from human trafficking; and **medium risk** from tax fraud, corruption, illicit use of mixers and dark web commerce, and terrorist financing (GAFILAT, 2025). The principal threats identified by the ESR—cyberattacks, illicit use of mixers and the dark web, fraud and investment scams, drug trafficking, human trafficking, tax fraud, corruption, and terrorist financing—are consistent with the typologies documented by the FATF at the global level and are illustrated by the case studies presented in this chapter.

117. The dominance of stablecoins in illicit virtual asset activity reflects several characteristics that increase their attractiveness to threat actors. Their price stability allows criminals to move proceeds without exposure to the volatility of assets like Bitcoin or Ether. Their high liquidity and interoperability across multiple blockchain networks—including Tron, Ethereum, Solana, and Avalanche—enable rapid cross-border transfers. And their ease of conversion to fiat currency through OTC brokers makes them a preferred medium for the final cash-out stage of laundering schemes. The FATF 's 2026 Targeted Report on Stablecoins and Unhosted Wallets notes that the majority of illicit stablecoin activity occurs in the secondary market, while FATF's 2026 report on offshore VASPs underscores a broader, cross-product vulnerability: threat actors commonly rely on offshore, unlicensed, or unregistered VASPs—including OTC brokers and peer-to-peer platforms—located in jurisdictions without AML/CFT/CPF controls or that fail to comply with existing obligations (FATF, 2026b; FATF, 2026c).

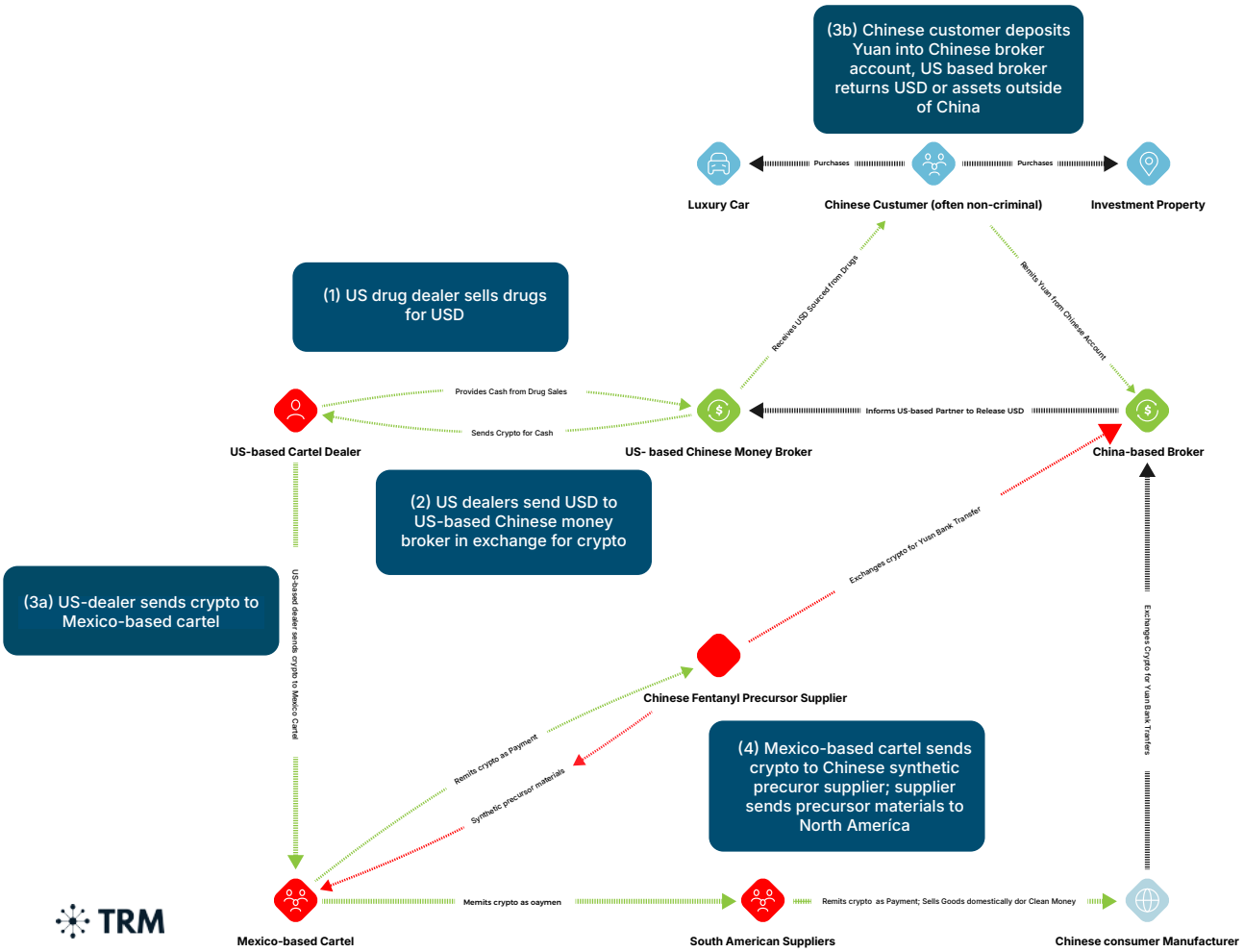
118. Within that illicit activity, some of the principal drivers are sanctions evasion, fraud schemes, and scams. Illicit actors are attracted by many of the same features that appeal to legitimate users—the speed, pseudonymity, and cross-border nature of cryptoassets—to facilitate crimes such as ML/TF/PF. Latin America is no exception: as cryptocurrency adoption increases, so too have instances of crypto-based crime in the region. Organized crime groups and fraud actors in Latin America have rapidly adopted cryptoassets to hide their activities and profits. Law enforcement agencies across the region report that drug cartels, cybercrime rings, and sanctioned entities are incorporating digital assets into their operations, exploiting regulatory gaps and the inherently borderless nature of cryptoassets.

119. Drug cartel-linked laundering provides a notable example. A recent study highlighted how drug cartels exploit East Asian underground banking networks and cryptocurrencies to launder drug proceeds, creating a rapid, discreet, and largely unregulated financial pipeline (TRM, 2025). Cartels sell U.S. dollars earned from drug sales at a discount to brokers in East Asia, who then use cryptocurrencies to transfer value across borders, avoiding traditional banking scrutiny. These funds are often converted into yuan in black markets, where they may be used to purchase precursor chemicals for illicit drugs, which are then

shipped to Latin America and the United States for drug manufacturing. This crypto-enabled trade-based money-laundering (TBML) scheme allows both cartels and global brokers to circumvent financial controls, evade law enforcement detection, and operate across borders with minimal risk. Figure 3.1 illustrates this scheme.

120. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets highlights that drug trafficking organizations are increasingly leveraging stablecoins, particularly USDT on TRON and USDC on Ethereum, for paying overseas suppliers of synthetic drug precursors, settling drug transactions, and laundering proceeds. The laundering schemes often involve the use of money mules, OTC brokers, and peer-to-peer platforms, and rapid virtual asset transfers across multiple blockchain networks, complicating detection and disruption efforts. Drug trafficking organizations also exploit high-volume online gambling platforms and merchant-refund loops, where goods are purchased using stolen identities and returned for refunds in stablecoins to third-party wallets (FATF, 2026b).

Figure 3.1. TRM Graph Visualizer with Explanatory Notes Illustrating How Cartels and Chinese Brokers Use Cryptocurrencies to Launder Drug Proceeds



Source: TRM Labs (2025), Shadow Bankers.

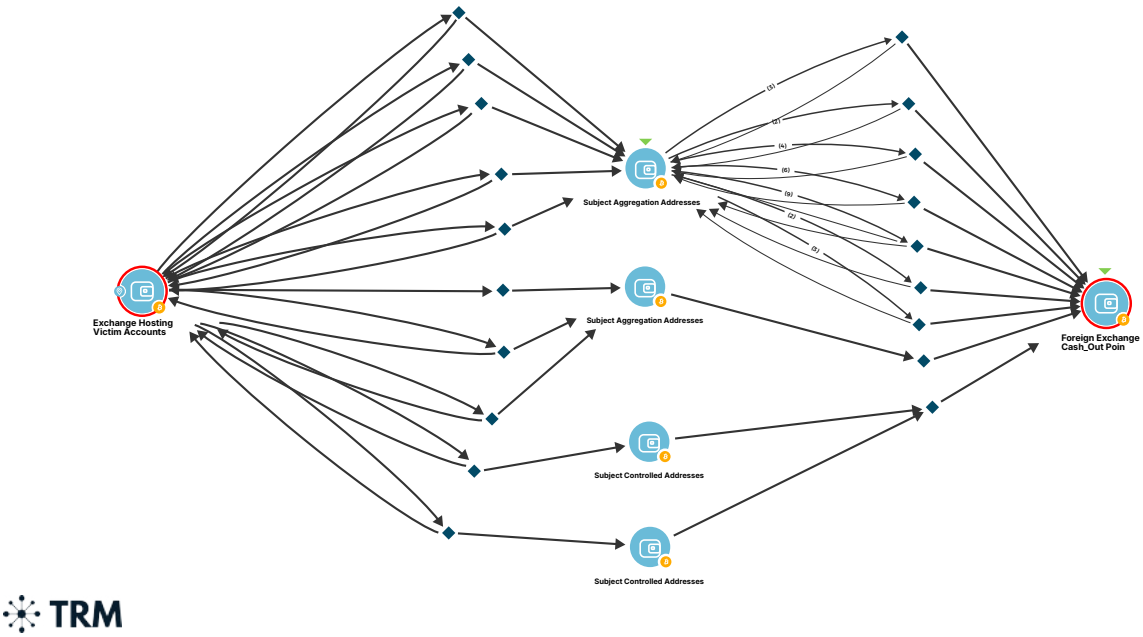
121. Terrorist organizations using virtual assets increasingly favor stablecoins over Bitcoin for many of the same reasons identified in money-laundering typologies. ISIL (Da'esh), its regional affiliates, and Al-Qaeda have been reported to solicit donations in stablecoins via encrypted platforms and social media, providing rotating wallet addresses through which they receive virtual assets from supporters worldwide. They have been observed breaking larger sums into numerous smaller transfers that pass through multiple VASPs to lower the risk of detection, and combining stablecoin transactions with DeFi aggregators, coin-swap exchanges, and anonymity-enhancing tools. Transaction patterns typically involve dense multi-hop transfers, micro-splitting of funds, and re-aggregation before conversion into fiat currency through off-ramping, often through OTC brokers that advertise minimal or no CDD requirements (FATF, 2026b). While virtual assets are more commonly used in combination with traditional TF methods, and the exact scale of virtual asset use for terrorist financing remains difficult to measure, the GAFILAT ESR assesses the risk of terrorist financing through virtual assets at a medium level for the LAC region (GAFILAT, 2025).

Beyond Cartels: From SIM Swapping to Money Laundering

122. To illustrate the spectrum of illicit cryptoasset risks emerging in Latin America, the following case studies highlight recent documented incidents:

123. Argentina — SIM-Swap Fraud and the Country's First Cryptoasset Seizure. In June 2023, Argentine authorities achieved a significant milestone in cybercrime enforcement by dismantling a criminal organization engaged in SIM-swapping and, for the first time in the country, seizing cryptoassets as part of the investigation. The organization had hijacked victims' mobile phone numbers via phishing and SIM-swap techniques to gain access to their financial accounts, including cryptoasset wallets. During the searches, the Prosecutors' Unit Specializing in Cybercrime Investigations (UFEIC) recovered digital wallets and seized the crypto assets they contained. Investigators used blockchain analytics and tracing tools to map out the criminal network through its on-chain transactions, identifying additional victims, money mules, and co-conspirators beyond the initial six suspects arrested. This case not only disrupted a sophisticated fraud scheme but also established an important legal precedent in Argentina for treating cryptoassets as seizable property in criminal investigations.

Figure 3.2. SIM-Swap Fraud Scheme in Argentina



Source: TRM Labs (2025).

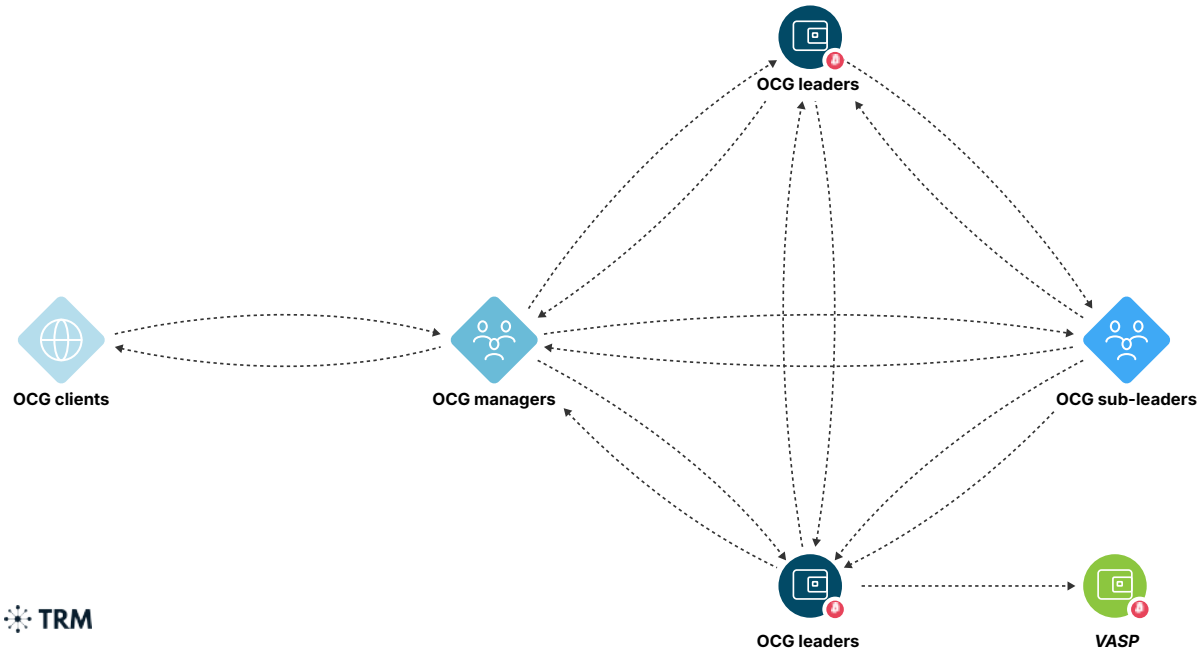
124. Brazil — Cryptoasset-Based Money Laundering Operations. In July 2023, Brazil's Federal Police dismantled two major money laundering operations that had collectively laundered approximately USD 400 million (over BRL 2 billion) in illicit funds since 2017. These criminal enterprises, linked to drug trafficking organizations, created their own cryptoasset exchange in Rio de Janeiro, along with a network of more than 20 shell companies. They used this infrastructure to convert drug proceeds from cash into cryptoassets and back into fiat currency, thereby obscuring the trail of funds between the traditional financial system and the blockchain networks. In a large-scale operation conducted across four states, Brazilian authorities executed nearly 30 search and seizure warrants, arrested 11 individuals, and confiscated more than USD 400,000 in cash along with other assets. The inclusion of an in-house cryptoasset exchange within the laundering network illustrates the evolving sophistication of organized crime in Latin America.[9]

125. Venezuela — Virtual Assets in a Sanctions Environment. In the context of international sanctions, cryptoassets have been used to facilitate certain cross-border transactions and access to foreign currency. In these cases, crypto transactions—when conducted outside proper regulation or through unlicensed intermediaries or exchanges—have functioned alongside traditional financial channels rather than replacing them. One widely discussed example is the 2018 launch of the Petro, a state-backed cryptocurrency presented as a tool to support trade and financing in a constrained sanctions environment. Most recently, reports indicate that stablecoins—particularly USDT—have been used by Venezuela's state-owned oil company for oil transactions, and have also functioned as a de facto exchange-rate policy instrument through their role in foreign-currency access and conversion channels. Separately, the transnational criminal group known as Tren de Aragua has been identified by international authorities as using cryptoassets for money-laundering activities, leading to targeted U.S. Department of the Treasury sanctions on its members in 2023. These patterns underscore how digital assets can appear in sanctions-related and organized-crime schemes and present a complex challenge for regulators, requiring vigilance that extends beyond domestic law into the broader domains of international finance and security.

126. Spain and the T3 Task Force — Disrupting a Latin American Crime Syndicate. In January 2025, Spanish authorities (Guardia Civil) in partnership with the T3 Financial Crime Unit—a private-sector alliance of blockchain industry participants, including TRON, Tether, and TRM Labs—froze USD 26.4 million in cryptocurrency linked to a sprawling money laundering network. The targeted organization, with ties spanning from Europe to Latin America, provided cash-to-crypto laundering services for criminal enterprises, effectively operating as an underground "crypto bank" serving illicit actors. This enforcement action, codenamed Operation T3, is notable for its scale and coordination: it represented the largest asset freeze conducted by the T3 Financial Crime Unit since its establishment. By tracing blockchain addresses associated with the syndicate and leveraging exchange records, investigators identified and froze illicit funds before they could be converted into fiat currency. Spanish officials credited the public–private collaboration for giving law enforcement unprecedented reach into crypto corridors used by the syndicate. This case highlights both the transnational nature of crypto crime (where a Latin American gang can launder money through Europe using digital assets) and the effectiveness of innovative partnerships in countering it.

[9] For an additional case study from Brazil, see https://www.trmlabs.com/resources/case-studies/from-swiping-right-to-exposing-a-crypto-theft-ring-in-brazil

Figure 3.3. TRM Graph Visualizer Illustrating the Hierarchical Flow of Funds Within the Criminal Enterprise as Exposed by Spanish Authorities



Source: TRM Labs (2025).

127. These cases demonstrate the range of illicit finance risks tied to cryptoassets in Latin America, from relatively small-scale fraud rings to massive laundering operations and even nation-state evasion of sanctions. They also illustrate an encouraging trend: law enforcement is adapting. With the aid of specialized blockchain intelligence tools and international cooperation, authorities in and beyond Latin America have begun to disrupt cryptoasset-enabled crime. Nonetheless, the prevalence of scams, darknet markets, and criminal cryptoasset hubs in the region calls for sustained vigilance. It reinforces the need for robust regulatory measures and intelligence-driven enforcement to prevent Latin America's cryptoasset economy from being undermined by illicit activity.

Conclusion

128. Latin America and the Caribbean's rapid adoption of cryptoassets reflects both the region's structural economic pressures and its growing digital sophistication. Stablecoins, in particular, have become integral to the region's financial landscape—serving as stores of value, remittance instruments, and tools for financial access in economies marked by inflation and limited banking infrastructure. At the same time, the same features that drive legitimate adoption—speed, pseudonymity, cross-border reach, and the ability to operate outside traditional intermediaries—have made cryptoassets—and stablecoins in particular—attractive to illicit actors across the full spectrum of financial crime.

129. The GAFILAT's 2025 Evaluación Sectorial de Riesgos confirms that the region faces very high risk from fraud, cyberattacks, and drug trafficking through virtual assets, alongside high risk from human trafficking and medium risk from terrorist financing. These assessments are consistent with the typologies documented by the FATF at the global level and are illustrated by the case studies in this chapter—from Argentina's first cryptoasset seizure to Spain's T3 Task Force partnership that froze USD 26.4 million in cartel-linked stablecoins.

130. For FIUs and policymakers, the evidence presented in this chapter underscores three key imperatives. First, risk assessments must be continuously updated to reflect changes in the virtual-asset threat environment, including the growing role of stablecoins in illicit transaction flows, multi-chain layering, OTC-broker cash-out networks, offshore or non-compliant VASPs, and DeFi-related exposure. FATF's 2026 work on virtual assets reinforces the need for a functional and risk-based approach: jurisdictions should assess these products, services, and arrangements according to their actual domestic exposure rather than treating them as uniform risk categories. In the case of DeFi, this includes identifying persons who may exercise control or sufficient influence over an arrangement and assessing the risks arising from interactions between DeFi arrangements and regulated financial institutions or VASPs (FATF, 2026d). Second, the regional case studies demonstrate that effective enforcement is possible when institutions invest in blockchain-analytics capabilities, establish specialized investigation units, and develop structured public–private partnerships. Third, no country can address these risks in isolation: the cross-border and multi-jurisdictional nature of virtual-asset crime demands coordinated action through FSRBs such as CFATF and GAFILAT, the Egmont Group, and bilateral cooperation mechanisms.

131. The chapters that follow address the institutional and regulatory building blocks needed to translate this situational awareness into effective policy and operational action—beginning with beneficial ownership transparency (Chapter 4) and standardized transaction reporting frameworks (Chapter 5) which together form the data foundation for intelligence-driven oversight of the region's growing virtual asset ecosystem.

Key Actions for FIUs and Supervisors — Chapter 3

- **Update national and sectoral risk assessments** to incorporate the GAFILAT 2025 ESR's risk-level findings and the FATF 's 2026 VA/VASP materials, including typologies related to stablecoins and unhosted wallets, offshore VASP risks, and DeFi-related vulnerabilities where relevant to the domestic risk profile. Ensure stablecoins, unhosted wallets, P2P transactions, oVASPs, and DeFi arrangements are explicitly assessed according to domestic exposure.
- **Map your jurisdiction's cryptoasset ecosystem:** identify local and offshore VASPs serving domestic users, including licensed, registered, unlicensed, or non-compliant providers; estimate the volume and nature of stablecoin transactions; assess reliance on OTC brokers; and quantify exposure to cross-border flows.
- **Integrate stablecoin-specific typologies** into STR analysis workflows—particularly drug precursor procurement via USDT/USDC, stablecoin-facilitated gambling-platform laundering, and micro-split TF donation campaigns.
- **Invest in public–private partnerships covering VA-related actors and risks.** Drawing on example cases,[10] explore partnerships that bring together competent authorities, law enforcement, VASPs, stablecoin issuers, and blockchain-intelligence firms to share risk indicators and support rapid tracing, freezing, and disruption of illicit stablecoin flows before their conversion into fiat currency.
- **Strengthen cross-border cooperation mechanisms through** CFATF, GAFILAT, the Egmont Group, and bilateral channels to enable rapid tracing and freezing of virtual assets, as well as information exchange in multi-jurisdictional laundering schemes.

[10] Such as Operation T3 Financial Crime Unit.

CHAPTER 4:

Customer Identification, Beneficial Ownership, and Traceability in Virtual Assets: Definitions, Challenges, and Implementation of a Balanced Regulatory Framework

Chapter 4: Customer Identification, Beneficial Ownership, and Traceability in Virtual Assets: Definitions, Challenges, and Implementation of a Balanced Regulatory Framework

Introduction

132. Virtual assets have transformed financial systems in Latin America and the Caribbean, creating both new opportunities and new vulnerabilities for those responsible for safeguarding financial integrity. In this environment, three related but distinct transparency questions arise: identifying the customer or person controlling a virtual-asset account or wallet; tracing transactions across blockchain networks; and, where legal persons or legal arrangements are involved, identifying and verifying their beneficial owners. These concepts interact operationally, but they should not be treated as interchangeable.

133. This chapter examines how countries across the region are addressing these challenges within virtual-asset ecosystems. It distinguishes customer due diligence and customer identification obligations—principally relevant through FATF Recommendations 10 and 15—from beneficial ownership transparency under Recommendations 24 and 25. It then considers how blockchain traceability, VASP records, registries, and other information sources can be combined to support both functions. Drawing on a survey of VASPs in six Latin American countries, the chapter identifies progress and persistent fragmentation and proposes a pathway toward a more balanced, coherent, and effective framework.

The Regulatory Imperative for Transparency in Digital Finance

134. FATF Recommendations 24 and 25 require countries to ensure that adequate, accurate, and up-to-date beneficial ownership information is available for legal persons and legal arrangements. In the virtual-asset context, these obligations do not mean that a wallet, blockchain address, smart contract, or virtual asset itself has a 'beneficial owner' in the R.24/R.25 sense. Rather, beneficial ownership becomes relevant where a VASP, its customer, or another relevant participant is a legal person or legal arrangement. Separately, FATF Recommendations 10 and 15 require applicable customer due diligence and other preventive measures by obliged entities. Blockchain pseudonymity and the use of unhosted wallets can make customer attribution and transaction tracing more difficult, which in turn may impair authorities' ability to connect virtual-asset activity to the relevant legal persons, arrangements, and beneficial owners.

135. In Latin America, the uneven adoption of regulatory frameworks for VASPs exacerbates these challenges. The GAFILAT's 2025 Evaluación Sectorial de Riesgos identifies "insufficient legal frameworks" and "lack of effective PSAV licensing/registration and supervision" as two of the five principal vulnerabilities affecting the region's AML/CFT/CPF effectiveness in the virtual asset sector (GAFILAT, 2025). Some countries—such as Brazil, Mexico, and Argentina—host relatively mature fintech ecosystems with dozens of licensed providers. Others are still in the early stages of designing legal frameworks and building supervisory capacity. This asymmetry creates opportunities for regulatory arbitrage, as firms migrate to jurisdictions with lighter oversight or unclear definitions of virtual asset obligations. Figure 4.1 illustrates this uneven landscape by classifying selected LAC jurisdictions according to whether they combine VASP licensing with Travel Rule enforcement, have partial frameworks, remain undefined, or are not classified.

Figure 4.1. LAC VASP Regulatory Maturity



Note: Categories reflect the status of each jurisdiction's VASP AML/CFT framework as of September 2026. "VASP licensing/registration + Travel Rule implementation" means that binding requirements are in force for VASP licensing or registration and for the FATF Travel Rule, with evidence of supervisory implementation. "Partial" refers to jurisdictions where relevant requirements exist but the framework remains incomplete, transitional, recently enacted, or subject to limited implementation or enforcement. "Undefined" indicates that no clear and comprehensive enforceable framework covering both VASP licensing/registration and the Travel Rule could be identified. "Not classified" indicates insufficient current public information to assign a category reliably.

Source: Own elaboration with data from the FATF (2026a), GAFILAT (2025), and publicly available national legislation and regulatory sources.

Technology and the Traceability Challenge

136. Understanding these distinctions requires a brief review of how blockchain systems record value. Public blockchains are generally transparent and immutable but pseudonymous: transactions are associated with alphanumeric addresses rather than verified legal identities. This allows transaction flows to be traced on-chain, but does not by itself establish the identity of the person controlling a wallet.

137. The first challenge is therefore one of attribution. Linking a blockchain address to a natural or legal person generally requires combining on-chain information with off-chain information such as VASP customer records, payment information, device or network data, and other investigative sources. Beneficial ownership is a separate question that arises where the attributed customer or relevant participant is a legal person or legal arrangement. Evidence that a person controls a private key or wallet may establish wallet control, but it does not substitute for CDD or for identifying and verifying the beneficial owner of a legal-person or legal-arrangement customer where required.

Figure 4.2. Traditional Finance vs. Decentralized Systems

Dimension	Traditional Finance	Decentralized Finance (Blockchain-Based Systems)	Why it matters
Record of ownership	Linear, documented legal title in registries and account contracts	On-chain balances at pseudonymous addresses; legal title, if any, resides off-chain	Visibility of title vs. visibility of addresses
Link to identity	Accounts tied to verified persons/entities (KYC/KYB)	Identity is external—linked only via VASPs, the Travel Rule, or analytics	Actors may be unknown even when flows are known
Control over assets	Exercised through legal/corporate rights (beneficial owners, signatories, board members)	Distributed and dynamic: private keys, multisig signers, admins/upgraders, protocol governance	"Controller" may differ from "owner," and may change without filings
Supervisory visibility	Data via registries and intermediaries	Public ledger shows transactions, but identity hinges on off-chain linkage	Regulatory blind spot: economic actors can remain invisible despite public records

Source: own elaboration.

138. Smart contracts and decentralized applications raise a related but distinct challenge. They do not have beneficial owners in the same way as legal persons or legal arrangements. The relevant AML/CFT question is whether identifiable persons—such as owners, operators, administrators, upgraders, multi-signature key holders, or front-end operators—exercise control or sufficient influence over the arrangement, such that the activity may fall within the VASP perimeter under Recommendation 15. Where VASPs provide services to legal-person customers that use these arrangements, they must still apply CDD and identify and verify the beneficial owners of those customers; information on smart contract governance and control can support risk assessment, but it is not a substitute for CDD or BO verification.

139. Stablecoins introduce related CDD and traceability challenges arising from the structure of their ecosystem. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets distinguishes between **primary market** participants (typically VASPs or institutional clients who purchase or redeem stablecoins directly from the issuer and are therefore subject to CDD requirements) and **secondary market** holders, who may use hosted wallets subject to VASP obligations or unhosted wallets with no obliged intermediary. While stablecoin issuers can monitor on-chain circulation and balances at the level of blockchain addresses, they cannot directly observe the identities of all corresponding holders. Where stablecoins are held with a VASP, customer identity information may be available to competent authorities through existing AML/CFT frameworks and powers. Where stablecoins are held in unhosted wallets, only the pseudonymous blockchain address is observable, and no underlying CDD information is available (FATF, 2026b). The AML/CFT vulnerability is especially relevant at redemption or cash-out: holders may avoid official redemption channels to convert stablecoins into fiat currency and instead use informal channels or non-compliant service providers, including OTC brokers and P2P platforms, which can impede identification of the person controlling the wallet or the underlying legal-person customer (FATF, 2026b).

140. Given the rapid growth in the use of USD-pegged stablecoins for cross-border payments, supervisors should anticipate higher volumes of VASP-to-VASP transfers and prioritize Travel Rule implementation, interoperability, supervision, and enforcement across these payment corridors.

FATF Recommendations 10, 15, 24, and 25 in the Virtual-Asset Context

141. FATF Recommendation 24 requires countries to ensure that competent authorities have timely access to adequate, accurate, and up-to-date information on the beneficial ownership of legal persons. Recommendation 25 extends these requirements to legal arrangements, including trusts and similar legal structures. For VASPs, the operational entry point is customer due diligence: under Recommendation 10, as applied to VASPs through Recommendation 15, VASPs must identify and verify the beneficial owners of legal-person customers and the relevant legal arrangements they service. Effective implementation therefore depends both on VASPs' CDD controls and on the availability of reliable BO information generated by domestic R.24 and R.25 frameworks.

142. The challenge is therefore not to apply BO requirements to blockchain networks themselves, but to ensure that VASPs can identify and verify customers and beneficial owners when legal persons or legal arrangements interact with wallets, smart contracts, or DeFi-related services. Ownership thresholds and control tests vary across jurisdictions, often in the 10–25 percent range, but a risk-based approach should not rely solely on shareholding; it should also consider effective control through voting rights, appointment powers, contractual rights, debt instruments, or other means of control. Although many VASPs voluntarily adopt stricter internal thresholds, legal definitions and reporting requirements remain inconsistent.

143. In blockchain-based systems, Travel Rule implementation can support transparency for covered virtual-asset transfers by linking transfer information to VASP customer records. It does not replace CDD or beneficial ownership obligations, and it does not, on its own, identify the beneficial owners of legal-person customers. Its value lies in preserving originator and beneficiary information across VASP-to-VASP transfers and making that information available to competent authorities where needed, subject to effective implementation, interoperability, supervision, and enforcement.

144. Following FATF's multi-pronged approach, VASPs CDD, including verification, should draw on three complementary sources: (i) information on legal persons held by VASPs (the identity and status of each BO, including the nature of the participation, voting or other control rights, and any intermediaries in the chain); (ii) national registry information (company registers, tax authorities records, notarial databases, or BO registries that provide adequate, accurate, and up-to-date information accessible to competent authorities); and (iii) alternative mechanisms that securely integrate or link datasets—for example, shared databases, credit bureau information, and blockchain analytics—to corroborate BO information where registry coverage is partial. Together, these channels support VASPs' CDD and BO verification obligations by helping corroborate the identity and status of legal-person customers, legal arrangements, and the natural persons who ultimately own or control them. Figure 4.3 maps these FATF expectations against observed LAC challenges, including inconsistent BO thresholds, limited registry interoperability, and fragmented legal gateways for information sharing.

Figure 4.3. FATF Standards vs. Observed LAC Challenges

Dimension	FATF Standards	Observed LAC Challenges
Information quality	Adequate, accurate, and up-to-date BO data; verification mechanisms	Pseudonymity and smart-contract governance obscure effective control; beneficial-ownership thresholds remain inconsistent (10–25%)
Availability	Timely access for competent authorities; standardized filings	Limited direct links or API access to national registries; manual processes create delays and increase costs
Access for FIUs/supervisors	Legal gateways and interoperable data sharing	Fragmented mandates and limited interoperability; safe-harbor uncertainty slows sharing

Source: Own elaboration with data from the FATF (2026a), GAFILAT (2025), and publicly available national legislation and regulatory sources.

Insights from the VASP Survey

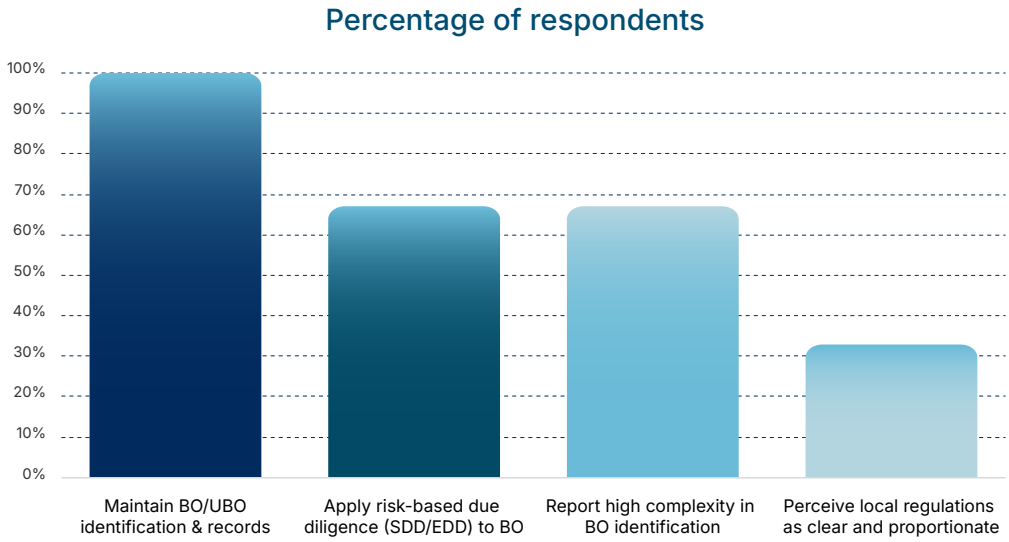
145. To complement this regulatory analysis, a regional survey of major VASPs was conducted for this publication across six jurisdictions—Mexico, Brazil, Argentina, Colombia, Peru, and Chile. The surveyed companies were established between 2014 and 2023, representing both early adopters and more recent entrants to the digital asset market. Respondents represented a broad range of business models, from business-to-consumer (B2C) platforms offering retail exchange and custody services to institutional providers facilitating treasury management, cross-border payments, and liquidity provision for corporate clients. Some specialized in technology infrastructure for regulatory compliance and blockchain integration.

146. Most respondents identified stablecoins as a transformative innovation for cross-border payments and remittances. By connecting to fiat on- and off-ramps that interface with national payment systems, these firms enable near-instant settlement while significantly reducing transaction costs, expanding access to international transfers for consumers and small businesses.

147. When asked about their KYC and KYB procedures, respondents described detailed onboarding protocols: collection of legal documentation, beneficial ownership declarations, where applicable, proof of address, and verification of directors and shareholders. Several firms also conduct enhanced due diligence (EDD) for high-risk customers, including politically exposed persons (PEPs), and require sworn statements identifying beneficial owners.

148. Despite these strong internal controls, participants cited considerable regulatory divergence across jurisdictions. Thresholds for identifying BOs, licensing requirements, and documentation standards differ between Brazil, Mexico, Argentina, and Colombia. For instance, while Brazil's Council for Financial Activities Control (COAF) mandates formal licensing and periodic reporting, Argentina's Financial Information Unit (UIF) has issued only general guidelines. This regulatory fragmentation increases compliance costs and complicates cross-border operations. Figure 4.4 summarizes the survey results, showing that while most respondents maintain BO/UBO records, fewer perceive local regulations as clear and proportionate.

Figure 4.4. Cryptoasset Service Providers Survey: BO Practices and Regulatory Clarity



Source: own elaboration with data from the VASP survey.

Gaps in Customer Identification, Beneficial Ownership Verification, and Traceability

149. The survey findings reveal several structural gaps affecting customer identification, beneficial ownership verification, and transaction traceability.

150. First, regulatory inconsistency leads to **uneven thresholds and documentation requirements.** Some jurisdictions define a beneficial owner by reference to a 10–25 percent ownership threshold, while others provide limited guidance on how BO and control tests should be applied to VASP customers that are legal persons or legal arrangements. A risk-based approach should consider not only shareholding but also effective control through differential voting rights, the power to appoint or remove senior management, debt or contractual rights, and other informal means; regimes focused solely on shareholding risk underidentifying beneficial owners.

151. Second, **access to national registries** remains limited in many jurisdictions. Many registries of legal persons or beneficial owners are not interoperable with VASP reporting systems (for example, because they lack APIs or standardized data formats), forcing manual verification processes that increase compliance costs and delay investigations.

152. Third, **smart contracts and decentralized applications** create challenges for identifying accountable persons and determining whether an activity falls within the VASP perimeter. FATF's analysis generally focuses on whether identifiable persons exercise control or sufficient influence over a DeFi arrangement, rather than treating the protocol itself as having beneficial ownership under Recommendations 24 and 25. VASPs participating in the survey reported that they currently avoid offering services involving smart contract deployment or DeFi-related activities because of these unresolved perimeter, control, and compliance risks.

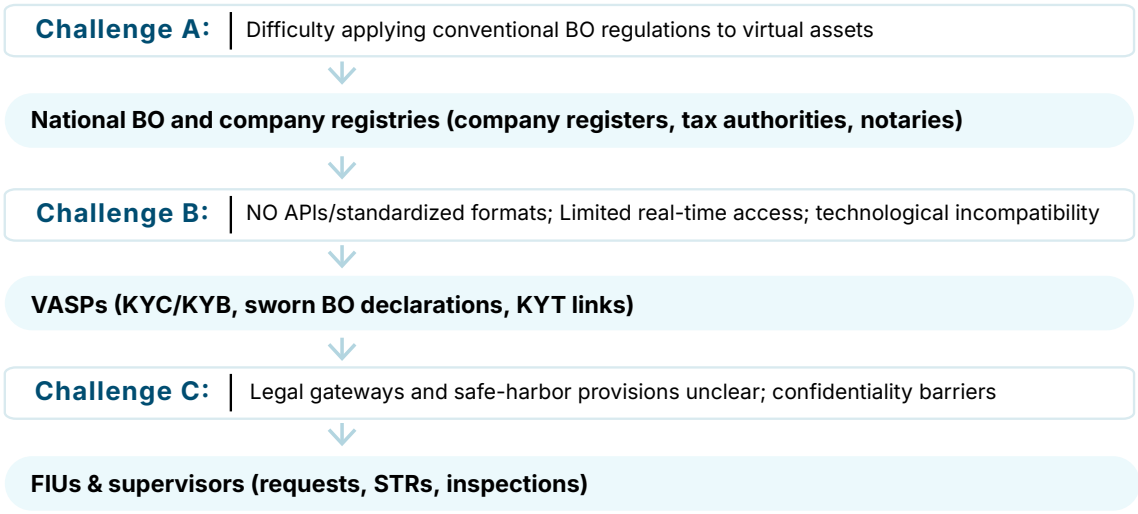
153. Fourth, **unhosted wallets and P2P transactions** create CDD, customer-identification, and transaction-monitoring challenges that can also affect BO transparency where legal-person customers or legal arrangements are involved. The FATF notes that P2P transactions conducted through unhosted wallets fall outside the scope of AML/CFT/CPF obligations because there is no intermediary to collect CDD information or file suspicious transaction reports (FATF, 2026b). Threat actors may transfer stablecoins through layered unhosted wallets that are transactionally distant from wallets subject to the Travel Rule, and the pseudonymous nature of blockchain addresses enables criminals to exploit additional layers of pseudonymity, particularly when they frequently generate new wallet addresses and discontinue the use of previously used addresses (FATF, 2026b). To mitigate these risks on a risk-sensitive basis, the FATF identifies several measures that jurisdictions and VASPs may consider: limiting the amount of funds that can be transferred to unhosted wallets, applying enhanced CDD for unhosted wallet transactions, using blockchain analytics to assess the risk profile of counterparties controlling unhosted wallets, and subjecting applying CDD measures at the points of issuance and redemption involving unhosted wallets (FATF, 2026b).

154. Fifth, **compliance-cost asymmetries** constitute a broader supervisory and implementation constraint rather than a beneficial-ownership vulnerability in themselves. Large exchanges may be able to sustain sophisticated customer-identification, BO-verification, transaction-monitoring, and blockchain-analytics systems, while smaller providers may face materially higher relative compliance costs. These asymmetries can weaken implementation across several AML/CFT/CPF controls if obligations are not calibrated according to risk. Proportionality should therefore reflect the nature, scale, complexity, customer base, products, services, and geographic exposure of the VASP rather than size alone.

155. Sixth, **offshore, unlicensed, or non-compliant VASPs** serving domestic customers can create broader gaps in customer identification, access to information, supervision, and enforcement. These gaps may also impair beneficial ownership verification where the customer is a legal person or legal arrangement, but the underlying vulnerability is wider: domestic authorities may have limited access to CDD and transaction records, limited supervisory reach, and slower cooperation channels. FATF's 2026 work on offshore VASPs reinforces the need for jurisdictions to assess these cross-border exposures and determine whether licensing or registration, supervisory cooperation, enforcement, or other risk-mitigation measures are appropriate (FATF, 2026c).

156. Finally, **information sharing between private firms and competent authorities** remains fragmented. FATF's 2026 global review of public–private information-sharing arrangements emphasizes that effective PPPs require a clear legal basis, defined objectives and governance, appropriate data-protection and confidentiality safeguards, and clear expectations regarding what information can be shared, by whom, and for what purpose (FATF, 2026e). Where these foundations are absent or unclear, firms may be reluctant to share suspicious activity indicators proactively, including relevant wallet addresses and emerging typologies.

Figure 4.5. Data Flow for BO Traceability



Source: own elaboration.

Toward a Balanced and Effective Regulatory Framework

157. Addressing these gaps requires a balanced regulatory framework that protects financial integrity without discouraging innovation. Participants in the VASP survey offered several recommendations that are consistent with emerging international best practices.

158. First, **public–private collaboration** should be institutionalized within a clear legal and governance framework. Competent authorities, FIUs, VASPs, financial institutions, and other relevant private-sector participants should have structured channels for sharing emerging typologies, risk indicators, and operational insights, including those related to virtual-asset transactions. Consistent with FATF's 2026 work on public–private information sharing, such arrangements should rest on a clear legal basis, defined objectives and governance, appropriate data-protection and confidentiality safeguards, and clear expectations regarding what information can be shared, by whom, and for what purpose (FATF, 2026e).

159. Second, **regulatory clarity and harmonization** are essential. Inconsistent domestic implementation of FATF's functional definition of VASPs, inconsistent beneficial ownership thresholds, and overlapping reporting requirements create compliance inefficiencies. Harmonized, risk-based rules would allow firms to operate more seamlessly across borders while maintaining consistency with FATF standards.

160. Third, **proportionality** is key. Supervisory obligations should be calibrated according to assessed risk, taking into account the nature, scale, complexity, products, services, customer base, and geographic exposure of the VASP. Smaller providers should not automatically face the same compliance burden as large international exchanges when their risk profile is lower, but reduced requirements should be justified by risk, not by size alone. Such differentiation encourages formalization and expands the perimeter of regulated activity.

161. Fourth, **risk-based supervision supported by technology** should guide implementation. Regulators may leverage data analytics and, where appropriate, artificial intelligence and machine learning tools to analyze transaction patterns, prioritize high-risk entities, and optimize the allocation of supervisory resources. Integrating KYT data with BO records enhances the detection of layered transactions and the rapid movement of illicit funds.

162. Fifth, **innovation and regulatory sandboxing** can support adaptive regulation. Regulatory sandboxes allow controlled experimentation with new products and compliance technologies, thereby fostering innovation while maintaining effective

supervisory oversight. The FATF's 2026 Recommended Actions encourage jurisdictions to consider establishing regulatory sandboxes with industry participants to develop standards and solutions that enable innovation while safeguarding against misuse (FATF, 2026, Recommended Actions for Jurisdictions, IX). As an implementation option, pilot programmes could test automated BO verification APIs or blockchain-based digital identity solutions that securely link wallet addresses to verified customers.

163. Finally, **interoperability** should be pursued at both the technological and institutional levels. Open-API frameworks can facilitate standardized KYB processes across jurisdictions, while regional data-sharing agreements can help FIUs overcome domestic capacity gaps.

Conclusion: Transparency as the Foundation of Trust

164. Beneficial ownership transparency and effective CDD remain core components of financial integrity. In the context of virtual assets, achieving them requires aligning technological design, regulatory intent, and institutional capacity. Latin American countries have made significant progress in expanding supervision of VASPs and enforcing AML/CFT/CPF standards, yet gaps persist in consistency, access, and coordination—particularly regarding unhosted wallets, offshore VASPs, and the stablecoin secondary market, where the absence of obliged intermediaries creates structural blind spots for customer identification, transaction monitoring, and BO transparency where legal persons or arrangements are involved.

165. The experience of surveyed VASPs demonstrates both willingness and constraint: they are eager to comply but hindered by fragmented regulation and costly reporting frameworks. A balanced approach—anchored in clarity, cooperation, and proportionality—can transform compliance into a predictable and proportionate pathway to market legitimacy.

166. For FIUs and supervisors, the path forward involves embracing blockchain's transparency as a tool rather than a threat. Building interoperable data systems, integrating blockchain analytics, and maintaining continuous dialogue with the private sector will enable regulators to illuminate previously opaque areas of digital finance.

167. Ultimately, effective customer identification, transaction traceability, and beneficial ownership transparency—where legal persons or legal arrangements are involved—are prerequisites for trust in the region's digital future. If Latin America and the Caribbean succeed in reconciling innovation with integrity, they can establish a global precedent for responsible digital transformation—one in which technology enhances, rather than erodes, the rule of law.

Key Actions for FIUs and Supervisors — Chapter 4

- **Assess whether your jurisdiction clearly distinguishes between BO transparency for VASPs as legal persons, CDD and BO verification obligations for VASP customers** that are legal persons or legal arrangements, and separate risk assessments for DeFi arrangements, smart contracts, and unhosted wallets. Avoid framing blockchain networks or smart contracts themselves as having beneficial owners.
- **Apply risk-based measures to mitigate P2P and unhosted-wallet risks,** including enhanced CDD where a VASP is involved, blockchain-analytics-based counterparty risk assessment, and appropriate transfer limits for VASP-to-unhosted-wallet transactions where warranted by the risk profile.
- **Evaluate whether offshore VASPs serving residents of your jurisdiction** are subject to appropriate licensing or registration, supervision, CDD obligations, enforcement mechanisms, and cooperation channels, in line with FATF's 2026 report on offshore VASPs.
- **Pursue interoperability between BO registries, CDD/KYB records, and VASP reporting systems** through Open API frameworks, standardized data formats, and regional data-sharing agreements under the auspices of CFATF or GAFILAT.
- **Institutionalize PPP information-sharing frameworks involving VASPs,** with clear legal gateways, governance, permitted purposes, confidentiality, and data-protection safeguards for the lawful exchange of operational indicators and emerging typologies.

CHAPTER 5:

Toward Standardized Threshold-Based Transaction Reporting Requirements for Virtual Asset Service Providers

Chapter 5: Toward Standardized Threshold-Based Transaction Reporting Requirements for Virtual Asset Service Providers

Introduction

168. Building on the preceding chapters—which describe the virtual asset ecosystem, the relevant regulatory frameworks, and the role of beneficial ownership and traceability—this chapter examines how FIUs collect and standardize transactional data from VASPs. It focuses in particular on cash transaction reports (CTRs) and their virtual asset-specific equivalents, including large virtual currency transaction reports (LVCTRs), and explores how these reporting tools can be designed to generate high-quality, actionable financial intelligence.

169. While preceding chapters emphasize customer due diligence, Travel Rule compliance, and supervisory engagement, FIUs also depend on systematic, threshold-based reporting from obliged entities. In the VASP context, however, reporting frameworks are often fragmented: thresholds vary widely across jurisdictions, data fields are not harmonized, and key virtual asset-specific elements—such as wallet addresses, transaction hashes, and protocol identifiers—are captured inconsistently. These gaps weaken the evidentiary value of the data, complicate cross-border analysis, and create opportunities for regulatory arbitrage.

170. The sections that follow describe the main reporting instruments used by FIUs—suspicious transaction reports (STRs), CTRs, and LVCTRs—highlight current disparities in reporting thresholds and coverage, and set out a practical proposal for standardized, risk-based CTR reporting requirements for VASPs in Latin America and the Caribbean. The chapter concludes with options for regional cooperation and technical implementation, and links these issues to the broader capacity-building agenda developed later in this publication.

The Spectrum of Data Collection and National Disparities

171. FIUs rely on VASPs to provide core transactional information that is essential for identifying illicit financial flows associated with transnational organized crime and other predicate offences within the virtual asset ecosystem. The foundational reporting mechanism within AML/CFT/CPF legal frameworks remains the STR. STRs are mandatory submissions triggered when VASP compliance systems detect unusual transactions and, following internal analysis, determine reasonable grounds to suspect ML/TF/PF, or other related illicit activities.

172. STRs are expected to include a detailed narrative explaining the red flags that triggered the review, how compliance officers gathered additional information, and how the activity deviated from the customer's expected transactional profile. When properly prepared, STRs provide FIUs with high-value investigative leads and strategic intelligence.

173. In parallel, many jurisdictions employ CTRs, traditionally applied to fiat currency transactions exceeding a defined monetary threshold. Historically, many national CTR regimes have used a USD 10,000 benchmark, but this is a domestic reporting threshold rather than a FATF threshold for VASP reporting. While several jurisdictions have since adjusted this benchmark to account for inflation or country-specific risk conditions, others have retained the same threshold without periodic review or adjustment. Within the VASP context, some jurisdictions have extended CTR obligations to cash-in and cash-out operations, exchange activities, and aggregated transactions.

174. Notably, Canada has pioneered the use of the LVCTR, which extends CTR principles to virtual asset transactions by capturing transfers above a specified value threshold and combining blockchain data with customer identification information. Additionally, some regulatory frameworks require the submission of KYC information and beneficial ownership data to further strengthen the linkage between off-chain identities and on-chain transactional evidence.

175. The FATF establishes a USD/EUR 1,000 threshold for CDD on occasional VA transactions; however, it is not a threshold for CTR/LVCTR reporting. Jurisdictions are expected to implement these standards taking into account factors such as sector-specific risk, institutional maturity, market structure, and supervisory capacity. As a result, reporting thresholds across the region differ markedly. For example, Colombia mandates reporting for virtual-asset transactions as low as USD 150 for single transactions or USD 450 for aggregated transactions involving individuals, whereas Mexico imposes reporting

obligations only for transactions exceeding approximately USD 73,000.[11] Other jurisdictions, such as Ecuador and Canada, maintain thresholds close to USD 10,000.

176. This divergence does not, by itself, explain VA/VASP regulatory arbitrage, but it can create structural inconsistencies that may enable criminal actors to shift their operations toward jurisdictions with weaker controls. At the same time, it may prevent FIUs from effectively comparing, aggregating, and jointly analyzing data at the regional level, thereby undermining cross-border financial intelligence efforts.

Operational and Strategic Value of CTR and VASP Data

177. The value of CTRs and LVCTRs lies not merely in their formal compliance function but in their capacity to generate operationally meaningful financial intelligence. FIUs rely on this data primarily for reactive investigative support, using off-chain identifiers provided by VASPs to associate pseudonymous on-chain activity with identifiable natural and legal persons. This linkage is indispensable in cryptography-based environments, where anonymity or pseudonymity is a defining feature.

178. Furthermore, CTR and LVCTR data support asset tracing and the process of freezing, seizure, and forfeiture processes by providing evidentiary foundations for reconstructing transaction flows. They also facilitate link analysis, allowing FIUs to identify money mules, facilitators, and organized-crime networks operating across platforms and jurisdictions.

179. Beyond supporting reactive intelligence, VASP-generated data plays a critical role in proactive analysis and risk assessment. FIUs use this information to conduct sector specific money-laundering risk assessments and to develop typology and red-flag reports relating to exchanges, over-the-counter (OTC) brokers, peer-to-peer platforms, and anonymity-enhancing services. Strategic analysis of these datasets informs policymaking, supervisory prioritization, and the early identification of emerging criminal methodologies, typologies, and sector-specific red flags. For example, anomalous transaction patterns—such as rapid token accumulation, high-frequency cash conversions, or unusual stablecoin flows—can be detected and addressed before they evolve into systemic vulnerabilities.

180. A particularly valuable resource for enhancing the analytical value of VASP reporting is the FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets, which includes a detailed annex of risk indicators specific to stablecoin misuse. The indicators are organized into three broad categories: **unusual transaction-related indicators** (17 items, including rapid cross-border stablecoin movements inconsistent with customer profiles, rapid conversions between fiat and stablecoins with no economic rationale, and the use of multiple accounts used for conversion transactions); **anonymity-related indicators** (15 items, including transfers involving unhosted wallets located multiple hops away from Travel Rule-covered wallets, cross-chain bridging across multiple blockchains in short periods, and stablecoins combined with mixers or privacy wallets); and **TF and PF-related indicators** (8 items, including numerous small donations to frequently changing wallets with shared artefacts, stablecoin payments to intermediaries near free trade zones for dual-use items, and off-ramping in jurisdictions with weak AML/CFT/CPF controls) (FATF, 2026b). FIUs should consider integrating these indicators into their CTR/LVCTR analytical frameworks and disseminating them to reporting entities as guidance for the preparation of STRs.

Challenges to Effective Analysis

181. Despite the clear benefits of VASP reporting, several challenges continue to limit the effectiveness of FIU analysis and dissemination, particularly where reporting requirements are not calibrated to assessed risk or supported by minimum data-quality expectations. First, differences in reporting thresholds, coverage, and data-field requirements can generate significant variations in the volume, quality, and granularity of reported data, creating analytical blind spots in cross-border cases. Second, persistent data quality issues—such as inaccurate wallet addresses, missing transaction hashes, or incomplete originator and beneficiary information—undermine the reliability of submissions and weaken Travel Rule compliance.

[11] Equivalent to 645 UMAs. Source: Operaciones con Activos Virtuales, Ministerio de Hacienda de México. Available at: https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/actividades/act_avi.pdf

182. Institutional fragmentation further complicates the landscape. Coordination among FIUs, central banks, securities regulators, and other supervisory authorities is often inconsistent, leading to overlapping mandates, duplicative reporting obligations, and, in some cases, contradictory regulatory guidance. Additionally, many VASPs perceive limited value in the reporting process due to insufficient feedback. This has led to the characterization of FIUs as "black holes," where information is submitted without visible analytical outputs, feedback, or sectoral guidance.

183. Capacity constraints within FIUs, particularly the limited availability of specialized blockchain analytics tools and adequately trained personnel, remain a significant obstacle. The GAFILAT's 2025 Evaluación Sectorial de Riesgos identifies "insufficient technological infrastructure and tools" as one of the five principal vulnerabilities affecting the region's AML/CFT/CPF effectiveness in the virtual asset sector (GAFILAT, 2025). Acquiring and maintaining these tools, as well as developing the necessary technical expertise, is often costly, and many available solutions are not specifically designed for FIU operational needs, resulting in the underutilization of potentially valuable CTR and LVCTR datasets.

184. A structural challenge specific to stablecoins concerns the reporting gap associated with P2P transactions conducted through unhosted wallets. Because these transactions occur without the involvement of a VASP or other obliged entity, no STR or CTR is generated by an obliged entity—leaving FIUs with no direct data source for a growing category of transactions. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets identifies this as a key vulnerability: the absence of a reporting obligation for P2P transactions means there is no obliged entity responsible for submitting suspicious transaction reports in respect of such transfers (FATF, 2026b). To partially address this gap, stablecoin issuers may play a complementary monitoring and reporting role: when requested by law enforcement authorities to freeze unhosted wallets suspected of containing misused stablecoins, issuers may monitor transactions associated with identified wallet addresses and, where appropriate, submit STRs to the FIU (FATF, 2026b). Jurisdictions should consider formalizing these complementary reporting arrangements alongside the VASP-focused CTR/LVCTR framework discussed in this chapter (see also Chapter 4, para. 153 on P2P risk mitigation measures).

The Case for Risk-Based and Context-Sensitive Reporting Frameworks

185. To overcome these limitations, jurisdictions should first assess the ML/TF/PF risks associated with VAs and VASPs, implement the relevant FATF Standards, and tailor reporting requirements to their specific risk environments. Where consistent with domestic risk and context, alignment of core data fields and definitions, including standardized CTR thresholds, can facilitate the exchange of comparable datasets, enhance the detection of cross-border typologies, and strengthen collective AML/CFT/CPF responses. The objective should not be standardization for its own sake, but effective, comparable, and risk-sensitive reporting.

186. However, any regional alignment must remain grounded in risk, context, and proportionality. Reporting thresholds and coverage should reflect assessed sectoral risks, transaction size distributions, the prevalence of cash-based conversion services, the role of OTC brokers, supervisory capacity, and the exposure of the jurisdiction to organized crime. A rigid, one-size-fits-all threshold would be impractical and potentially counterproductive. Instead, reporting frameworks should seek to mitigate regulatory arbitrage by reducing disparities that criminal networks can exploit while preserving sufficient flexibility to reflect domestic risk conditions, including lower-risk areas where simplified measures may be appropriate.

187. In this regard, conducting sector-specific ML/TF/PF risk assessments for the VASP sector, while retaining a VA/VASP dimension in the national risk assessment and other relevant assessment processes, is a critical prerequisite. Such assessments enable FIUs to identify specific vulnerabilities and adopt measures that are proportionate to the risks identified. This evidence-based approach supports sound policymaking while avoiding overregulation and the adoption of standards that are difficult to operationalize in practice. The GAFILAT 2025 ESR provides a regional starting point for this exercise, and jurisdictions should build upon its risk-level findings when calibrating their domestic CTR/LVCTR reporting thresholds and scope.

188. A standardized, risk-based CTR/LVCTR framework for VASPs should prioritize operational effectiveness over formal compliance. Key elements include a risk-based threshold model calibrated to particular risk conditions—including both single and aggregated transactions—together with sufficient regulatory flexibility to adjust thresholds in response to evolving risks or market volatility. Equally important are standardized reporting fields, including wallet addresses, transaction hashes, and chain identifiers, as well as consistent definitions of key concepts such as "transaction," "cash equivalent," and "virtual asset

transfer." The risk indicators in Annex A of FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets can also serve as context-sensitive, standardized red-flag guidance for reporting entities, particularly for transaction monitoring and STR preparation, and may inform CTR/LVCTR analysis where relevant to the jurisdiction's risk profile.

Conclusion

189. Strengthening the global AML/CFT/CPF framework for virtual assets requires more than isolated national reforms. Risk-based regional alignment on key elements of VASP reporting—particularly core data fields, definitions, and the treatment of cross-border flows—would significantly enhance the analytical value of CTR and LVCTR data for FIUs, supervisors, and law enforcement agencies, while preserving flexibility on thresholds and coverage. Technical working groups led by FIUs, supervisors, and central banks can serve as practical forums to agree on common templates, clarify definitions (for example, "transaction," "cash equivalent," and "virtual asset transfer"), and coordinate periodic reviews as markets evolve.

190. At the same time, jurisdictions must address the structural reporting gap for P2P stablecoin transactions via unhosted wallets, which currently fall outside the CTR/LVCTR framework entirely. Formalizing the complementary monitoring and reporting role of stablecoin issuers—alongside the VASP-focused obligations—is an important step toward closing this gap.

191. Risk-based reporting frameworks will only realize their full potential if FIUs possess the analytical, technological, and governance capacities to use the resulting data effectively. Subsequent chapters in this publication discuss in greater detail the development of specialized cryptoasset units, data-science tools, and institutional partnerships. From the perspective of reporting frameworks, the core message is simple: well-designed CTR and LVCTR obligations for VASPs, aligned with FATF standards, calibrated to local risks, and supported by consistent core data fields, can transform fragmented transactional records into a coherent cross-border intelligence asset that supports both day-to-day investigations and strategic oversight of the sector. The next chapter illustrates how these reporting data, combined with on-chain analytics and other sources of information, can be deployed in concrete investigative and asset-tracing scenarios.

Key Actions for FIUs and Supervisors — Chapter 5

- **Apply the risk indicators in Annex A of FATF's 2026 Targeted Report on Stablecoins using a context-sensitive approach.** These indicators are particularly useful for transaction monitoring and STR preparation, and may also inform CTR/LVCTR analytical workflows where relevant to the jurisdiction's risk profile. The Annex contains more than 40 risk indicators covering unusual transaction patterns, anonymity-related typologies, and TF/PF-specific red flags.
- **Assess the reporting gap associated with P2P transactions conducted through unhosted wallets in your jurisdiction.** Consider whether stablecoin issuers should be formalized as complementary reporting entities alongside VASPs, particularly for monitoring transactions involving wallet addresses identified by law enforcement authorities and, where appropriate, submitting STRs.
- **Pursue risk-based regional alignment of core CTR/LVCTR data fields, definitions, review methodologies, and reporting thresholds** through technical working groups under the auspices of CFATF or GAFILAT. Prioritize standardized wallet address, transaction hash, and chain identifier fields to enable cross-border data comparison, without assuming uniform thresholds across jurisdictions.
- **Calibrate domestic reporting thresholds and coverage** to the GAFILAT 2025 ESR, the national risk assessment, sector-specific VA/VASP risk assessments, and local market conditions (transaction size distributions, OTC broker prevalence, organized crime exposure). Avoid rigid one-size-fits-all thresholds that create compliance burden without generating proportionate intelligence value.
- **Establish structured feedback mechanisms for reporting VASPs** by publishing sectoral typology reports, red-flag guidance, and aggregated trend analysis to demonstrate the value of their submissions and improve STR and CTR quality over time.

CHAPTER 6:

Debunking Myths: Anonymity, Attribution, and Recovery of Cryptoassets and Virtual Assets

Chapter 6: Debunking Myths: Anonymity, Attribution, and Recovery of Cryptoassets and Virtual Assets

Introduction

192. The expansion of cryptoassets in Latin America and the Caribbean has reshaped how value is stored and transferred, creating both opportunities and new vulnerabilities for financial integrity. Yet public discourse and even some policy debates remain influenced by misconceptions about how these systems function. Two myths persist with particular force: that cryptocurrencies provide complete anonymity and that cryptoassets cannot be effectively recovered.

193. For FIUs, law enforcement agencies, and supervisory authorities, dispelling these myths is not an academic exercise but a practical necessity. Misunderstanding the transparency inherent in blockchain systems can lead to misplaced regulatory priorities or missed enforcement opportunities. Likewise, assuming that virtual assets cannot be recovered discourages investment in the technical expertise, analytical capabilities, and cooperation mechanisms necessary to make recovery possible. In this chapter, "recovery" refers to the process of identifying, tracing, evaluating, freezing, seizing, confiscating and enforcing a resulting order for, managing, and disposing of—including returning or sharing—criminal property and property of corresponding value, pursuant to judicial or other competent legal authority.

194. This chapter builds on the previous discussion of CDD, traceability, and ownership or control information to examine how FIUs and investigators can effectively identify, trace, and recover cryptoassets. It demonstrates that the transparency of distributed ledgers, when combined with robust legal frameworks, analytics tools, and international cooperation, can transform what was once perceived as an untraceable asset class into one of the most transparent and auditable forms of value transfer in modern finance. The chapter also links these operational advances to FATF Immediate Outcomes 7 and 8, which assess countries' effectiveness in investigating ML and confiscating illicit proceeds.

Myth #1: Cryptocurrencies Provide Complete Anonymity

From Anonymity to Pseudonymity

195. A persistent misconception holds that cryptoassets exist within an entirely anonymous environment, beyond the reach of identification or oversight. In reality, most blockchain networks, such as Bitcoin, Ethereum, or Tron, operate on public ledgers that record every transaction permanently and transparently. What users actually experience, however, is pseudonymity: while users are identified through alphanumeric blockchain addresses rather than legal names, all transfers remain publicly visible.

196. This pseudonymous design allows regulators, auditors, investigators, and any other observers to scrutinize transactions recorded on the blockchain in considerable detail. When competent authorities are appropriately equipped, distributed ledger technology can support the tracing of value flows and the identification of illicit activity with a level of granularity that may be difficult to achieve in some traditional finance contexts.

197. Although cryptoassets have at times been exploited for illicit financial activities, the belief that they provide complete anonymity is largely inaccurate in the case of most public blockchains. Recognizing this distinction is essential for understanding how financial investigators can effectively trace and attribute cryptoasset transactions—including those linked to criminal activity—thereby strengthening oversight and demonstrating that meaningful monitoring is achievable.[12] Recent data from TRM Labs is consistent with this progress: the share of cryptocurrency transaction volume associated with illicit activity declined by 51 per cent in 2024 compared to the previous year, reflecting, at least in part, improvements in tracing capabilities, compliance practices, and enforcement effectiveness.[13]

198. This distinction between pseudonymity and anonymity is crucial for understanding how investigators can attribute blockchain activity to natural or legal persons. When users conduct transactions across multiple blockchain addresses or interact with regulated service providers, they leave observable patterns of activity that can support customer attribution and

[12] In 2018, approximately 26 percent of Bitcoin users and 46 percent of Bitcoin transactions were associated with illicit activity (Foley, Karlsen, & Putniņš, 2018).
[13] According to TRM Labs (2024), the share of cryptocurrency transaction volume associated with illicit activity declined by 51 percent in 2024 compared with the previous year.

wallet-control analysis. Where legal persons or legal arrangements are involved, this information may support beneficial ownership inquiries, but it is not a substitute for CDD or BO verification.

Wallet Attribution, Customer Identification, and Beneficial Ownership

199. Under the FATF Standards, beneficial ownership refers to the natural person or persons who ultimately own or control a customer, or on whose behalf a transaction is conducted; in the context of legal persons and legal arrangements, it refers to the natural persons who ultimately own, control, or exercise ultimate effective control over them. In cryptoasset investigations, however, the immediate question is often attribution of wallet control rather than beneficial ownership in the R.24/R.25 sense. Evidence of control over private keys, transaction behaviors, and interactions with regulated intermediaries can support attribution and risk assessment, but it does not replace CDD or BO verification where legal persons or arrangements are involved.

200. Regulated VASPs—such as exchanges and custodians—are required under FATF Recommendation 15 to apply CDD and other AML/CFT preventive measures, and to comply with the Travel Rule requirements for covered VA transfers by obtaining, holding, and transmitting required originator and beneficiary information. This information, when combined with blockchain transaction data, enables investigators to connect pseudonymous wallets to real identities.

201. The critical distinction is therefore not between "traceable" and "untraceable" systems, but between regulated and unregulated transactional pathways. Transactions that pass through licensed or registered and effectively supervised VASPs are generally more accessible to competent authorities through customer records and lawful information requests. Transactions conducted solely through unhosted wallets present greater investigative challenges, but they nevertheless leave a permanent and auditable digital trail on the blockchain.

Analytical Tools and De-Pseudonymization Techniques

202. Over the past five years, blockchain analytics platforms such as TRM Labs, Chainalysis, and Elliptic have significantly enhanced the ability of FIUs to trace funds across blockchain networks and jurisdictions. These platforms apply heuristics and machine learning models to detect transactional patterns and attribute blockchain addresses to identifiable entities, including VASPs, exchanges, mixers, darknet marketplaces, and other services linked to illicit activity. Common techniques include:

- **Cluster analysis:** Identifies groups of wallet addresses likely controlled by the same entity based on co-spending patterns and transaction behavior.
- **Exchange attribution:** Identifies transaction flows involving regulated VASPs that maintain KYC information capable of linking blockchain addresses to real-world identities.
- **Cross-chain tracing:** Follows funds across decentralized exchanges and bridge protocols that connect different blockchains.
- **Risk profiling:** Assigns risk scores to wallets associated with darknet markets, ransomware, or sanctions evasion, or other illicit typologies.

203. Strengthening the capacity to implement virtual asset tracing and recovery techniques through appropriate analytical tools is a critical component of institutional capacity building aimed at improving effectiveness and measurable outcomes, but such investments should be guided by VA/VASP risk assessments so that resource-intensive tools and specialized personnel are targeted toward the activities, entities, and use cases that present the greatest ML/TF/PF risks. Jurisdictions responsible for regulating or supervising VASPs should undertake structured capability assessments that evaluate not only their regulatory and supervisory frameworks but also the availability of specialized personnel, talent-retention mechanisms, and the adequacy of their technological and analytical infrastructure. When these capacities are in place, improvements in effectiveness become increasingly measurable through operational outcomes. For instance, TRM Labs (2025) reports that illicit cryptocurrency transactions accounted for only 0.4 per cent of total transaction volume in 2024, representing a 51 per cent decline from 2023. Although multiple factors may explain this trend, it is consistent with improvements in blockchain analytics capabilities and more coordinated enforcement efforts across jurisdictions.

Challenges in Wallet Attribution and Identifying Relevant Beneficial Owners

204. Despite substantial advances in blockchain analytics, attributing cryptoasset activity to the natural or legal persons behind blockchain addresses remains a significant challenge for FIUs and law enforcement agencies. This attribution problem should be distinguished from beneficial ownership in the FATF Recommendations 24 and 25 sense. Where the person using a wallet is a natural person acting on their own behalf, the immediate issue is customer or wallet attribution. Where the relevant customer or participant is a legal person or legal arrangement, or legal arrangement, investigators may additionally need to identify and verify the natural persons who ultimately own or control that entity or arrangement. Both tasks can be complicated by the technical architecture of distributed ledger systems and by the cross-border nature of virtual-asset activity.

205. Hosted vs. Unhosted Wallets: Implications for Attribution and Traceability. As discussed in Chapters 1 and 4, the principal operational distinction between hosted and unhosted wallets is whether an obliged intermediary is present and therefore whether customer information may be available to competent authorities. For the purposes of attribution, this distinction has a direct investigative consequence: where a regulated VASP is involved, investigators may be able to connect on-chain activity with customer records and, where relevant, beneficial ownership information; where transactions occur exclusively through unhosted wallets, attribution depends more heavily on blockchain analytics, open-source intelligence, subsequent interaction with regulated entry or exit points, and international cooperation. The absence of an intermediary therefore makes attribution more difficult, but it does not make the underlying transaction untraceable.

206. Cross-Border Complexities and Jurisdictional Barriers. The borderless nature of virtual asset transactions adds another layer of complexity to beneficial ownership identification, as both regulatory frameworks and investigative tools vary significantly across jurisdictions:

- **Regulatory Fragmentation.** Countries differ widely in their implementation of FATF Recommendations 15 and, where legal persons or legal arrangements are involved, Recommendations 24 and 25. This results in uneven requirements for VASP oversight, customer identification, and beneficial ownership transparency, creating opportunities for regulatory arbitrage and allowing funds to migrate toward jurisdictions with weaker AML/CFT/CPF controls or more limited enforcement capacity.

- **VASP Location and Compliance Gaps.** When virtual assets transit through offshore, unlicensed, or non-compliant VASPs serving customers from another jurisdiction, obtaining customer, transaction, or BO information may become exceedingly difficult, even where suspicious activity has already been identified. This reflects the risks highlighted in FATF's 2026 work on offshore VASPs, including licensing or registration gaps, weak supervision, and limited cooperation channels.

- **Limitations of Traditional Cooperation Mechanisms.** MLATs and similar cooperation mechanisms, originally designed for conventional banking systems, are often too slow to support time-sensitive cryptoasset investigations spanning multiple jurisdictions. To address these challenges, FIUs increasingly rely on the ESW for intelligence exchange, the EU's FIU.net (hosted with Europol) for cross-matching among EU FIUs, Europol EC3 partnerships for operational support, and regional asset-recovery networks such as ARIN-CARIB for rapid tracing and freezing coordination (IMF, 2024).

207. Emerging frameworks such as the EU's MiCA Regulation and global Travel Rule compliance networks may help standardize information exchange between VASPs and reduce fragmentation in VA transfer information.

Myth #2: Cryptoasset Recovery is Too Complex

208. A persistent misconception suggests that recovering cryptoassets associated with illicit activity is inherently impracticable. This perception often stems from the technical nature of blockchain technology and from early cases where investigators lacked the tools, legal powers, or cooperation channels to pursue recovery effectively. In reality, cryptoasset recovery is achievable, but it remains operationally, legally, technologically, and cross-border intensive. The challenge lies not only in establishing lawful control over the assets—typically through seizure warrants, freezing orders, production orders directed to VASPs, or, where necessary, expedited mutual legal assistance requests—but also in preserving evidence, securing the assets, managing volatility, coordinating across jurisdictions, and enforcing confiscation or forfeiture orders. This is consistent with FATF's 2025 Asset Recovery guidance, which emphasizes the full recovery cycle from identification and tracing through freezing, seizure, confiscation, management, disposal, return, or sharing.

209. Once authorized access has been obtained, the operational recovery process can be highly efficient. Seized assets can often be transferred almost instantaneously to a government-controlled wallet, reducing the need for physical transportation or warehouse-style storage. Unlike physical cash or gold, cryptoassets do not deteriorate over time nor do they require physical storage, but they still require secure custody, valuation, volatility management, and liquidation in accordance with applicable judicial orders.

210. For centrally governed stablecoins, an additional recovery mechanism exists that is generally unavailable for decentralized virtual assets such as Bitcoin. **Stablecoin issuers** such as Tether (USDT) and Circle (USDC) maintain technical capabilities to freeze, burn, and deny-list wallet addresses through smart contract functions embedded in their stablecoins (see Chapter 1, paras. 48–49). Upon request from competent law enforcement authorities, issuers may freeze stablecoins associated with unhosted wallet addresses suspected of containing illicit funds, even where the identity of the wallet holder has not yet been established. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets notes that, notwithstanding the inability to identify the actual holder, where an address is determined to be linked to criminal activity, executing freezing functions remains feasible (FATF, 2026b). This capability represents an important complementary investigative tool because it can prevent the dissipation of assets while traditional investigative and international cooperation processes continue. The FATF further encourages stablecoin issuers to maintain a centralized law enforcement contact that is monitored 24/7 and capable of taking expeditious action to freeze stablecoins when legally appropriate (FATF, 2026, Recommended Actions for the Private Sector, IV).

211. Even when stablecoins are misused through unhosted wallets without the involvement of an obliged intermediary, investigators retain several important tools. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets identifies a structured investigative approach for pursuing illicit transactions involving unhosted wallets (FATF, 2026b):

- **Tracing transaction flows to exit points:** using commercial or open-source blockchain analytics tools to follow funds from a target address through intermediary addresses and protocols to potential cash-out or off-ramp points.
- **Setting up alerts:** monitoring identified wallet addresses for ongoing activity and behavior patterns indicative of additional illicit transactions.
- **Conducting open-source intelligence (OSINT):** increasing attribution strength by combining on-chain data with publicly available information.
- **Integrating on-chain with traditional investigative methods:** combining blockchain evidence with conventional law enforcement techniques to develop prosecutable cases.

Figure 6.1. Comparative Perspective: Traditional vs. Cryptoasset Recovery

Aspect	Traditional Asset Recovery	Cryptoasset Recovery	Key Challenges / Limitations
Visibility	Opaque; relies on bank secrecy waivers, intermediaries, and company registries	Public, permanent ledger records all transactions	Requires forensic tools and trained analysts to interpret blockchain data
Provenance	Requires documentation or expert valuation to establish ownership	Provenance is embedded in the transaction history	Privacy coins, mixers, and cross-chain swaps can obscure traceability
Seizure Process	Physical control or court orders are required to seize tangible assets	Digital control through private keys or VASP cooperation	Access to private keys may be impossible without suspect cooperation
Cross-Border Complexity	Relies on slow Mutual Legal Assistance Treaties (MLATs) and local court processes	Potential near real-time tracing and freezing via VASP cooperation	Many VASPs operate offshore or outside FATF-compliant jurisdictions
Custody and Disposition	Costly storage and depreciation risks for physical assets	Secure digital custody; direct liquidation or auction is possible	Legal frameworks for seized-cryptoasset management remain uneven

Source: own elaboration.

Reassessing the Myth

212. While cryptoassets introduce new technical and jurisdictional complexities, they also offer significant advantages in terms of transparency, auditability, and operational efficiency once lawful control over the assets has been established. Where the necessary tools, expertise, and lawful access are available, the immutable nature of blockchain records can facilitate detailed tracing and attribution, thereby supporting the objectives reflected in FATF Immediate Outcomes 7 (money laundering investigation and prosecution) and 8 (confiscation of criminal proceeds) (RUSI, 2024).

213. In this sense, the principal challenge of cryptoasset recovery is not purely technological; it is also legal, operational, institutional, and cross-border. Effective recovery depends on interagency coordination, timely international cooperation with VASPs and foreign competent authorities, appropriate legal powers, specialized forensic tools, and secure asset-management capacity. When these elements are in place, certain aspects of cryptoasset recovery may be faster, more transparent, and operationally more efficient than comparable traditional asset recovery processes. The availability of stablecoin issuer freeze mechanisms adds an additional dimension: for certain centrally governed stablecoins, recovery may begin before the wallet holder has been identified, through the freezing of the relevant wallet address.

214. Experience from a growing number of virtual asset recovery cases demonstrates that effective outcomes depend less on institutional reluctance toward new financial technologies than on developing the technical, legal, and investigative capacity required to trace, freeze, and recover such assets. Box 6.1 presents selected examples of successful freezing and recovery operations involving virtual assets. Chapter 7 builds on these findings by moving from demonstrated feasibility to the operational procedures required for investigation, freezing, seizure, cross-border cooperation, and post-recovery management.

Box 6.1. Regional and Global Experiences in Virtual Asset Recovery

Regional Enforcement Experience

Argentina – MPBA Operation (2023). The Public Ministry of Buenos Aires (MPBA) established a dedicated Cryptoassets Investigation Team that, in 2023, executed 27 coordinated raids targeting a phishing network operating across multiple jurisdictions. Investigators recovered Ether (ETH), Tron (TRX), and Binance Coin (BNB) tokens within six months of the operation's initiation. This case demonstrated how on-chain analytics and rapid coordination with exchanges can transform crypto investigations from intelligence to confiscation, reducing the traditional lag between detection and recovery.

Source: Ministerio Público de la Provincia de Buenos Aires, 2023; TRM Labs, 2024.

Brazil – Federal Police Operation (2023). Brazil's Federal Police dismantled a BRL 2 billion money-laundering network that used shell companies and a domestic exchange to conceal drug-trafficking proceeds. The operation resulted in multiple arrests and the confiscation of large digital holdings, reflecting the country's growing proficiency in financial-intelligence cooperation between the Federal Police, COAF (Financial Intelligence Unit), and the Securities Commission (CVM).

Source: Polícia Federal do Brasil, 2023; COAF Annual Report 2024.

Caribbean – CFATF Cooperation Model (2024). Recognizing regional constraints in forensic capacity, CFATF members launched a pilot Crypto Investigations Working Group in 2024. The initiative facilitates real-time intelligence exchange between Financial Intelligence Units (FIUs) and law-enforcement agencies, enabling coordinated tracing, freezing, and confiscation actions across jurisdictions. This model showcases how regional platforms can compensate for national resource gaps and aligns directly with FATF Immediate Outcome 8 on the confiscation of criminal proceeds.

Source: CFATF Secretariat, 2024.

Global Precedents

United States – Department of Justice (2023). The U.S. Department of Justice seized over USD 3 billion in Bitcoin connected to the Silk Road marketplace—the largest single cryptoasset seizure to date. Assets were transferred to a secure federal digital wallet under the U.S. Marshals Service, underscoring the maturity of custodial frameworks and inter-agency coordination.

Source: U.S. Department of Justice, "United States v. James Zhong," 2023; IMF Fintech Note 2023/04.

United Kingdom – National Crime Agency (NCA). The NCA has integrated crypto confiscations into its asset-recovery regime. In 2023, seized digital assets generated over GBP 300,000 in proceeds through regulated auctions conducted via the Asset Recovery Agency. The NCA's model highlights how clear custodial procedures and liquidation protocols can normalize crypto within standard asset-management frameworks.

Source: OECD, Crypto-Asset Tax and Enforcement Report, 2023; NCA Annual Review 2023.

Singapore – Monetary Authority of Singapore (MAS). Singapore incorporates crypto seizures into its anti-money-laundering enforcement under the Payment Services Act 2019. The MAS framework ensures that seized tokens meet evidentiary and custodial standards equivalent to traditional financial instruments, enabling their admissibility in court proceedings and reinforcing public confidence in digital enforcement.

Source: Monetary Authority of Singapore, 2023 Enforcement Report.

215. Experiences from LAC, together with those from other jurisdictions, provide several key policy lessons for strengthening cryptoasset supervision and recovery frameworks:

- **Invest in Analytical and Asset-Management Capacity.** Blockchain analytics tools and specialized personnel have become indispensable for effective financial investigations. FIUs, law enforcement agencies, prosecutors, and asset-management teams should have sustainable funding for technology, continuous training, secure custody arrangements, and the capacity to manage or hold virtual assets once restrained or seized. Equally important are mechanisms to attract and retain specialized talent; without them even the most advanced analytical tools are unlikely to achieve their full operational potential.

- **Modernize Legal Frameworks.** The supervision of financial technologies should not rely solely on the accumulation of regulatory requirements but should evolve toward risk-based and collaborative oversight, particularly through engagement with private-sector actors such as VASPs and wallet providers. At the same time, legal frameworks governing freezing, seizure, confiscation, forfeiture, management, and disposal should explicitly encompass virtual assets and cryptographic credentials, thereby ensuring procedural certainty in both civil and criminal proceedings. Jurisdictions should also consider, where stablecoin issuance is permitted and appropriate, requiring centrally governed stablecoin issuers to maintain technical capabilities to freeze, burn, or withdraw stablecoins, consistent with FATF's 2026 recommended actions.

- **Institutionalize Cooperation.** Establish expedited cooperation mechanisms with VASPs, custodians, stablecoin issuers, and regional FIUs to complement the often lengthy processes associated with mutual legal assistance requests. Structured MOUs and secure data-exchange protocols can substantially accelerate recovery operations. Stablecoin issuers should also maintain centralized law enforcement contact points available on a 24/7 basis to facilitate expeditious freezing.

- **Embed Transparency in Asset Management.** Develop public reporting and auditing standards for seized virtual assets to ensure transparency and public confidence in their custody, valuation, and ultimate disposition.

- **Measure Effectiveness.** Integrate virtual asset investigations and recovery outcomes into national risk assessments, supervisory strategies, and mutual evaluation preparation, using indicators aligned with FATF Immediate Outcomes 7 and 8 and calibrated to the jurisdiction's assessed VA/VASP risks.

Conclusion

216. The myths of complete anonymity and insurmountable recovery complexity no longer withstand careful scrutiny. With appropriate legal frameworks, institutional capacity, and analytical tools, cryptoassets can often be traced, frozen, and recovered with a degree of transparency that is difficult to achieve in many traditional finance systems. Public blockchains, once widely perceived as opaque, are increasingly proving to be valuable instruments of accountability when leveraged by capable institutions. For certain centrally governed stablecoins, issuer-level freeze mechanisms through smart contracts provide an additional enforcement tool that has no direct parallel in the traditional asset-recovery toolkit, subject to applicable legal authority and issuer capabilities.

217. For Latin American and Caribbean FIUs, the imperative is clear: invest in people, partnerships, and analytical platforms capable of transforming data into evidence and technology into institutional trust. Effective recovery of illicit cryptoassets strengthens not only AML/CFT/CPF effectiveness but also public confidence in the integrity and resilience of the financial system.

Key Actions for FIUs — Chapter 6

- **Use FATF's investigative-leads framework for cases involving unhosted wallets:** trace transactions to exit points, establish address alerts, conduct open-source intelligence (OSINT) to strengthen attribution, and integrate on-chain evidence with traditional investigative methods.
- **Measure and report virtual-asset recovery outcomes** using indicators aligned with FATF Immediate Outcomes 7 and 8 and calibrated to the jurisdiction's assessed VA/VASP risks, thereby demonstrating effectiveness and supporting sustained investment in blockchain analytics and asset-recovery capabilities.

CHAPTER 7:

Practical Considerations for FIUs in Cryptoasset and Virtual Asset Investigations and Recovery

Chapter 7: Practical Considerations for FIUs in Cryptoasset and Virtual Asset Investigations and Recovery

Introduction

218. The previous chapter established that the perceived anonymity and practical irrecoverability of cryptoassets are often overstated: public blockchain records, attribution techniques, cooperation with intermediaries and issuers, and documented recovery cases demonstrate that virtual assets can be traced, frozen, and recovered. This chapter does not revisit that case. Instead, it focuses on the operational question that follows: what must FIUs, prosecutors, and law enforcement authorities have in place to act effectively when a virtual asset is identified in an investigation? It therefore turns from feasibility to execution, addressing evidence identification, cryptographic access, seizure procedures, international cooperation, rapid response, and post-recovery asset management.

219. As the adoption of cryptoassets accelerates across economic activity, FIUs must navigate a rapidly evolving technical and operational environment. They operate in a landscape where technological change often outpaces regulatory adaptation, where illicit actors exploit cross-border digital ecosystems, and where effective recovery depends on specialized skills and coordinated institutional responses. Public blockchains have introduced unprecedented visibility into the movement of value; however, that transparency is accompanied by technical, procedural, and jurisdictional challenges that differ substantially from those encountered in traditional financial investigations. This chapter examines these challenges and distils practical considerations for FIUs, prosecutors, supervisors, and law enforcement agencies as they strengthen their capacity to trace, freeze, seize, and ultimately confiscate or forfeit virtual assets in accordance with international standards, including FATF Immediate Outcomes 6, 7, and 8.

Technical Challenges in Cryptoasset Investigations

220. One of the first challenges for investigators is determining whether a case involves cryptoassets at all. Traditional financial investigations focus primarily on bank accounts, real estate, cash, and physical assets. Cryptoassets, by contrast, often leave no immediate physical trace and may remain invisible unless investigators understand the types of evidence that point to their existence. Investigators increasingly encounter hardware wallets that resemble USB drives or compact electronic devices, paper records or handwritten seed phrases that may appear to be ordinary notes, and software artefacts on computers or mobile devices that indicate the installation of wallet applications. Transaction confirmations, exchange communications, screenshots, and application logs may also reveal involvement with VASPs.

221. FIUs benefit from standardized checklists and protocols that help identify potential cryptoasset indicators during searches and digital evidence reviews. In practice, this requires integrating cryptoasset-specific questions into investigative interviews, training officers to recognize devices capable of storing private keys, and systematically reviewing seized digital media for wallet-related applications and cryptographic materials. The September 2023 Comando Vermelho case in Argentina illustrates this point well: authorities recovered approximately USD 45,000 in cryptocurrency after discovering a seed phrase stored inside a safe. The seizure was possible only because investigators knew how to identify and secure cryptographic materials—demonstrating that the timely identification and preservation of cryptographic evidence is often the decisive factor determining whether virtual assets can ultimately be recovered.

Accessing Private Keys and Seed Phrases

222. Once cryptoassets are detected, FIUs confront the critical challenge of securing access to private keys or seed phrases. Unlike traditional assets, cryptoassets cannot be seized simply by physically removing an object or by freezing an account through a financial institution. Without access to the relevant private key, the asset remains inaccessible from a cryptographic standpoint. This creates unique investigative, legal, and operational questions that must be addressed early in any crypto-related case.

223. Access may be obtained through several methods. Digital forensic teams may recover cryptographic credentials stored on digital devices by examining browser extensions, wallet files, unencrypted storage, password managers, or system backups. Investigators acting under appropriate legal authority may search for physical notes or disguised documents

containing seed phrases. In some jurisdictions, courts can mandate key disclosure, although such mechanisms vary widely and raise complex questions regarding privacy, self-incrimination, and enforceability. In cases involving hosted wallets, FIUs may cooperate with VASPs that maintain custody of the relevant private keys on behalf of clients and can freeze or transfer the assets pursuant to legally valid orders.

224. For centralized stablecoins such as USDT and USDC, investigators may have an additional recovery pathway that does not require access to private keys at all. Because stablecoin issuers maintain the technical capabilities to freeze wallet addresses directly through smart contract functions (see Chapter 1, paras. 48–49, and Chapter 6, para. 210), competent authorities may request the issuer to immobilize the stablecoins at the target address—thereby preventing their transfer or conversion—even without identifying the wallet holder or obtaining the private key. This represents a significant operational advantage over decentralized cryptoassets such as Bitcoin, where recovery generally requires access to the relevant private key. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets recommends that stablecoin issuers maintain a centralized law enforcement contact point that is monitored 24/7 and able to take measures to expeditiously freeze stablecoins (FATF, 2026, Recommended Actions for the Private Sector, IV). Investigators should establish these contact channels proactively—before a case arises—and understand the evidentiary requirements that each issuer applies before executing a freeze.

225. These approaches illustrate why FIUs must foster close collaboration among investigative units, digital forensic specialists, prosecutors, and regulators. The speed of cryptoasset transactions means that delays in securing cryptographic credentials—or in requesting issuer-level freezes for centrally governed stablecoins—may render assets unrecoverable. Early identification and rapid interagency coordination are therefore essential for successful intervention.

The Diversity of Wallet Types and Their Investigative Implications

226. Cryptoasset storage methods have diversified significantly, creating distinct investigative and operational challenges. Hardware wallets store cryptographic credentials offline and require specific forensic techniques; software wallets installed on mobile devices may be protected by biometric authentication; paper wallets, often disguised as ordinary documents, may be located anywhere in a residence or workplace; and brain wallets, which rely entirely on a memorized passphrase, may leave little or no physical trace. Multisignature wallets introduce additional layers of complexity by requiring multiple private keys to authorize transactions, potentially involving multiple individuals across different jurisdictions.

227. FIUs must understand the operational implications of each wallet type. For example, hardware wallets may require careful handling to avoid tampering with embedded secure elements, while mobile wallets may require immediate preservation measures to prevent remote wiping. Multisignature arrangements require investigators to identify all key holders and obtain cooperation or legal mandates from each one before the assets can be lawfully accessed or transferred. Familiarity with these technical nuances supports more effective investigations and increases the likelihood of successful asset recovery.

Legal and Procedural Challenges

Warrants and Seizure Orders for Virtual Assets

228. Traditional warrants often fail to reflect the specific characteristics of cryptoassets. Effective seizure orders should explicitly authorize the capture of digital and cryptographic materials, including seed phrases, hardware wallets, recovery devices, and encrypted backups. Orders should include language permitting law enforcement to access, transfer, or secure cryptoassets in government-controlled wallets once they are lawfully accessed. They should also address the possibility that devices may be password-protected or encrypted, requiring specialized procedures to unlock or duplicate data without compromising evidentiary integrity.

229. FIUs benefit significantly from proactively collaborating with prosecutors and judicial authorities to develop standardized templates for cryptoasset-related warrants. These templates help ensure that seizures comply with procedural requirements and reduce the risk of legal challenges that could invalidate investigative actions.

Jurisdictional Complexities in Cross-Border Cases

230. Cryptoasset transactions are inherently borderless in their practical operation. Differences in national regulatory frameworks create substantial barriers to effective recovery. Jurisdictions vary in their definitions of virtual assets, their licensing requirements for VASPs, their implementation of the FATF Travel Rule, and their levels of enforcement capacity. These discrepancies create opportunities for regulatory arbitrage, allowing illicit actors to route transactions through jurisdictions where oversight is weaker or cooperation mechanisms are slower.

231. FIUs should therefore maintain up-to-date country risk assessments that account for regulatory divergences. Understanding where VASPs are registered, how enforcement frameworks operate in each jurisdiction, and which cooperation channels enable investigators to anticipate obstacles when pursuing cross-border cases.

MLATs and International Cooperation Frameworks

232. MLATs remain a cornerstone of international cooperation, but their traditional timelines are often incompatible with the speed of cryptoasset and other virtual asset transactions. Cryptoassets can be transferred across the globe within minutes; an MLAT request may take weeks or months to process. This temporal mismatch represents one of the most significant barriers to successful asset recovery. To address this gap, jurisdictions are increasingly establishing expedited cooperation channels, direct communication networks among specialized investigation units, and standardized protocols for requesting VASP data.

233. Regional cooperation networks dedicated to cryptoasset investigations—whether through the guidance and support provided by FATF-style regional bodies, the Egmont Group, or through bilateral agreements—can significantly improve response times. Likewise, joint training initiatives and technical liaison officers embedded in partner jurisdictions can facilitate faster information exchanges and preserve assets before they can be dissipated or further laundered.

234. The FATF's 2026 Recommended Actions reinforce this imperative: jurisdictions should ensure that competent authorities are provided with the necessary tools to cooperate swiftly with domestic and international counterparts, including through established channels, MOUs, and legal provisions that enable the prompt exchange of information on stablecoin arrangements (FATF, 2026, Recommended Actions for Jurisdictions, V). Jurisdictions should also consider establishing **multinational supervisory colleges** to supervise stablecoin issuers and other entities involved in cross-border stablecoin arrangements, when necessary (FATF, 2026, Recommended Actions for Jurisdictions, IV). These institutional mechanisms can provide a faster and more structured complement to ad hoc MLAT processes, particularly in cases involving cross-border stablecoin arrangements.

Operational Challenges and Capacity Requirements

235. Operational readiness is fundamental to successful cryptoasset investigations. FIUs must invest in training programmes that build proficiency in blockchain analytics, digital forensics, cryptographic evidence handling, and the integration of on-chain and off-chain intelligence. Experience from countries such as Argentina demonstrates the value of establishing specialized cryptoasset investigation teams that combine investigators, data scientists, and compliance specialists. These units typically achieve higher recovery rates because they can respond more rapidly and interpret blockchain data more effectively.

236. Beyond general training, effective cryptoasset recovery requires specialized technical knowledge. Investigators should understand consensus mechanisms, token standards, smart contract behavior, wallet architectures, and the compliance frameworks under which VASPs operate. Multidisciplinary expertise is increasingly necessary as criminals exploit DeFi, cross-chain bridges, privacy-enhancing technologies, and obfuscation tools. FIUs that institutionalize specialized cryptoasset roles are better positioned to adapt to evolving risks and technologies developments.

237. Timing represents one of the most significant operational constraints. Cryptoassets can be transferred across multiple chains and jurisdictions in minutes. Mixing services and automated DeFi protocols can fragment transaction trails within seconds. Exchanges may retain logs for limited periods, and devices used to store keys may be remotely wiped if not secured quickly. In the light of these operational challenges, FIUs should develop rapid-response procedures that allow investigators to seek emergency preservation orders, engage promptly with VASPs, and coordinate real-time operational actions with law enforcement and supervisory partners.

238. Investigators should also recognize that the issuer-level freeze mechanism for centrally governed stablecoins has important limitations in cross-chain environments. When centrally issued stablecoins circulate on other blockchains in the form of newly created ("wrapped") tokens, the issuer's ability to freeze or deny-list the original asset may not extend to its wrapped representation (FATF, 2026b). For example, freezing USDT on the Tron blockchain does not automatically freeze wrapped USDT that has been bridged to Ethereum or Solana. Investigators must therefore determine whether target stablecoins have been bridged to secondary blockchains and, if so, identify the relevant bridge protocol and any intermediary entities that may assist in implementing freezing measures on the destination chain.

Post-Recovery Management of Seized Cryptoassets

239. Recovering virtual assets is only part of the challenge; their secure and transparent management is equally important. Once seized, cryptoassets must be secured, valued, stored, managed, and ultimately disposed of in a manner that complies with national law and preserves public trust. Jurisdictions have adopted different approaches reflecting their legal frameworks and institutional capacities. Finland requires seized virtual assets to be held in cold in cold storage to mitigate the risk of unauthorized transfers. The United Kingdom has adopted the use of public auctions, with proceeds deposited into state accounts, demonstrating that cryptoassets can be handled transparently within traditional asset recovery regimes. The United States has adopted a broader strategic approach, establishing a Strategic Bitcoin Reserve and Digital Asset Stockpile that retains certain seized assets as part of broader sovereign digital asset management policy.

240. PPPs play a crucial role in effective post-recovery management. Government agencies often lack the technical infrastructure or specialized expertise to maintain secure cold-storage wallets, implement multi-signature custody arrangements, track chain-of-custody integrity, or liquidate assets under controlled conditions. Partnerships with regulated custodians, cybersecurity firms, and blockchain-intelligence providers can fill these gaps. The U.S. Marshals Service, for instance, relies on private custodial firms to manage and auction seized cryptoassets, ensuring security and compliance throughout the process. Similar models have adopted across Europe and Asia, highlighting the growing acceptance of hybrid public–private approaches to cryptoasset custody.

Conclusion

241. For FIUs across Latin America and the Caribbean, the lessons outlined in this chapter have direct operational and strategic implications. Strengthening technical and institutional capacity remains essential—not only through the acquisition of blockchain analytics tools, but also by cultivating the specialized human expertise required to use them effectively. The stablecoin ecosystem also introduces a powerful operational tool—issuer-level freezing through smart contract functionality—that can secure assets even before private keys are obtained or beneficial owners identified, although investigators must also understand the limitations of this mechanism in cross-chain environments. As cryptoasset transactions increasingly transcend borders, international cooperation mechanisms must evolve accordingly, with faster, more coordinated channels for information exchange and joint investigative action, including through multinational supervisory colleges and structured MOUs. Equally important is the establishment of robust post-seizure asset-management protocols to ensure that recovered virtual assets are securely stored, properly accounted for, and ultimately disposed of in a transparent and fully auditable manner. FATF mutual evaluations increasingly emphasize measurable effectiveness in tracing and recovering illicit proceeds. By embracing blockchain transparency, investing in analytical and forensic capabilities, and institutionalizing cooperation with domestic and international partners—including stablecoin issuers—FIUs will be better positioned to meet these standards and strengthen their ability to combat financial crime in the digital era.

Key Actions for FIUs, Prosecutors, and Law Enforcement Authorities — Chapter 7

- **Establish proactive communication channels with major stablecoin issuers (e.g., Tether and Circle)** before cases arise. Understand each issuer's procedures, evidentiary requirements, and expected response times for freeze requests. Maintain a up-to-date directory of 24/7 law enforcement contact points.
- **Develop standardized seizure warrant templates** that explicitly cover seed phrases, hardware wallets, encrypted backups, and authorize the transfer of virtual assets to government-controlled wallets. Work with prosecutors and judicial authorities to validate these templates in advance.
- **Build institutional capacity for cross-chain investigation:** recognize that freezing stablecoins on one blockchain does not automatically affect wrapped versions on other blockchains. Train investigators to trace bridge protocols and identify relevant intermediary entities on destination blockchains.
- **Establish rapid-response procedures** for cryptoasset-related cases: emergency preservation orders, protocols for the immediate engagement of VASPs, and real-time coordination with law enforcement partners. Timely action is often the single most critical operational factor.
- **Establish or participate in regional cooperation networks** dedicated to cryptoasset investigations through CFATF, GAFILAT, the Egmont Group, or bilateral agreements. Consider participating in multinational supervisory colleges for the oversight of cross-border stablecoin arrangements.

CHAPTER 8:

Cross-Country Experiences and Best Practices in Public Policy and Regulation

Chapter 8: Cross-Country Experiences and Best Practices in Public Policy and Regulation

Introduction

242. The past decade has witnessed an extraordinary expansion of virtual asset activity. Cryptocurrencies, stablecoins, and DeFi platforms now facilitate transaction volumes once associated primarily with the global banking system. Alongside these innovations have emerged new channels for money laundering, terrorist financing, proliferation financing, and sanctions evasion. The FATF has responded by refining standards, while Multilateral Development Banks (MDBs) and international organizations continue to provide technical assistance and promote convergence around shared principles of financial integrity, inclusion, and innovation.

243. The United Nations framework for countering the misuse of emerging financial technologies has gained renewed momentum in recent years. Security Council Resolution 2462 (2019) called upon Member States to strengthen domestic regulation of financial systems—including emerging digital financial instruments—and to criminalize the willful provision or collection of funds for terrorist purposes. In January 2025, the Security Council Counter-Terrorism Committee adopted the **Algeria Guiding Principles** (S/2025/22)—a set of non-binding guiding principles on preventing, detecting, and disrupting the use of new and emerging financial technologies for terrorist purposes, prepared in accordance with the 2022 Delhi Declaration. The Algeria Guiding Principles highlight the importance of a comprehensive and risk-based approach to countering the financing of terrorism, and specifically address VAs and VASPs, PPPs, and the use of blockchain analytics—themes that are directly relevant to the regulatory and supervisory challenges examined throughout this guide.

244. In parallel, the establishment of a global UN programme dedicated to CFT, led by UNOCT through its United Nations Counter-Terrorism Centre (UNCCT), created a coordinated mechanism for strengthening national capacity. Between 2019 and 2024, this initiative trained more than 11,000 officials across 86 countries, developed a Handbook on Countering the Misuse of Virtual Assets and Virtual Asset Service Providers for Terrorism Financing Purposes (2024), and supported the development of digital tools that assist financial investigators in tracing suspicious digital transactions. The Handbook, developed jointly with the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), a FATF-style regional body (FSRB), and based on EAG practices, is now being implemented through regional workshops—including a three-day workshop with the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), also an FSRB, in Addis Ababa (June 2025), and a practical webinar with the Middle East and North Africa Financial Action Task Force (MENAFATF), another FSRB, in February 2026—with an addendum to the Handbook currently under development to incorporate experiences from additional regions. A similar workshop focused on LAC, potentially in partnership with CFATF, GAFILAT, and the IDB, would represent a logical next step for extending these operational lessons to the countries of the Americas.

245. These global efforts coincide with the continued evolution of FATF's work on virtual assets. Rather than constituting a separate regulatory architecture, the FATF's 2026 virtual-asset work programme—including the Seventh Targeted Update, the Targeted Report on Stablecoins and Unhosted Wallets, the report on offshore VASPs, and the Targeted Report on Regulatory Challenges from Decentralised Finance—reinforces the implementation of Recommendation 15 through a risk-based approach. Across this package, the central challenge is the transition from formal frameworks to effective implementation, particularly in risk assessment, licensing or registration, supervision and enforcement, Travel Rule implementation, offshore and cross-border activity, P2P transactions involving unhosted wallets, and DeFi arrangements (FATF, 2026a–d).

246. Latin America and the Caribbean reflect this global diversity. Brazil, Mexico, and Chile have enacted comprehensive fintech legislation that includes provisions relating to AML/CFT/CPF frameworks for virtual assets; whereas others are still developing foundational legislative frameworks. Some Caribbean states rely on sectoral guidance, while others, such as Jamaica and Barbados, are integrating cryptoasset oversight into their national AML/CFT/CPF strategies. The region accounts for a significant share of global cryptoasset activity, yet the implementation of compliance frameworks continues to lag. The GAFILAT's 2025 Evaluación Sectorial de Riesgos identifies five principal vulnerabilities affecting the region: lack of knowledge and training, insufficient legal frameworks, limited investigative capacity, inadequate technological infrastructure, and gaps in VASP licensing and supervision (GAFILAT, 2025). This fragmentation creates opportunities for innovation and experimentation but also for regulatory arbitrage.

Figure 8.1. Selected FATF Technical Compliance and Effectiveness Ratings in LAC



Note: In this map, "Technical Compliance" is defined as achieving at least six ratings of Compliant (C) or Largely Compliant (LC) across the following nine Recommendations: R9 – Financial institution secrecy laws; R15 – New technologies; R16 – Payment transparency; R23 – DNFBPs: other measures; R24 – Transparency and beneficial ownership of legal persons; R25 – Transparency and beneficial ownership of legal arrangements; R26 – Regulation and supervision of financial institutions; R28 – Regulation and supervision of DNFBPs; and R40 – Other forms of international cooperation. "Effectiveness" is defined as achieving at least five ratings of High (HE) or Substantial (SE) effectiveness across the following seven Immediate Outcomes: IO1 – Risk, policy and coordination; IO2 – Supervision; IO3 – Preventive measures; IO4 – Legal persons and arrangements; IO5 – Financial intelligence; IO6 – Money laundering investigation and prosecution; and IO8 – Confiscation. Classifications are based solely on this subset.

Source: Own elaboration with data from the latest FATF/FSRB mutual evaluation and follow-up data available as of September 2026.

The Good — Effective Policies, Institutions, and Partnerships

247. Several jurisdictions and multilateral initiatives demonstrate that balanced governance of digital finance is achievable. Their experiences suggest that effective regulation depends on three key factors: clarity of rules, cooperation among institutions, and sustained institutional and technical capacity building.

248. Brazil provides one of the most developed regulatory models in Latin America. Law No. 14,478 of 2022 designates the Central Bank as the primary authority responsible for VASP supervision, facilitates the integration of virtual asset service providers into the national payment system, and mandates segregation of customer funds. The framework combines prudential oversight with innovation: the DREX pilot explores programmable payments under strict AML/CFT/CPF controls. Crucially, Brazil's COAF plays a central coordinating role, through formal MOUs and dedicated interagency working groups to facilitate the systematic exchange of supervisory information between the Central Bank, risk assessments functions, and investigative authorities. This approach exemplifies proportionate, dialogue-based regulation—collaborative and risk-based oversight rather than adversarial supervision.

249. Singapore provides a complementary example from outside the region. Its Payment Services Act establishes a tiered licensing system that calibrates obligations to institutional risk levels. The Monetary Authority of Singapore (MAS) maintains continuous consultation with industry through public papers, risk advisories, and working groups. This continuous feedback loop has contributed to a high-compliance environment while preserving space for innovation.

250. In the **European Union**, the 2023 MiCA and the revised Transfer of Funds Regulation (TFR) together represent the first comprehensive supranational framework for the regulation and supervision of cryptoassets. MiCA harmonizes definitions, licensing requirements, and disclosure obligations across the European Union (27 member states), while the

revised TFR requires originator and beneficiary information to accompany covered cryptoasset transfers. Notably, MiCA classifies stablecoins into E-Money Tokens (EMTs) and Asset-Referenced Tokens (ARTs), with distinct regulatory obligations for each. For issuers of significant ARTs and EMTs, as defined under MiCA, the European Banking Authority establishes and chairs supervisory colleges to coordinate oversight across member states—a model that the FATF's 2026 recommended actions encourage other jurisdictions to consider for cross-border stablecoin arrangements (FATF, 2026b). For emerging and developing jurisdictions, the EU model demonstrates that regulatory coherence across borders is achievable when principles are standardized and institutions share infrastructure.

251. At the regional level, **Jamaica and Barbados**, both active members of the CFATF, illustrate how small jurisdictions can leverage regional cooperation to strengthen supervisory capacity. Jamaica's Financial Investigations Division has begun integrating advance analytics tools into its AML/CFT/CPF processes, while Barbados has introduced targeted AML/CFT/CPF compliance training for exchanges and financial intermediaries.

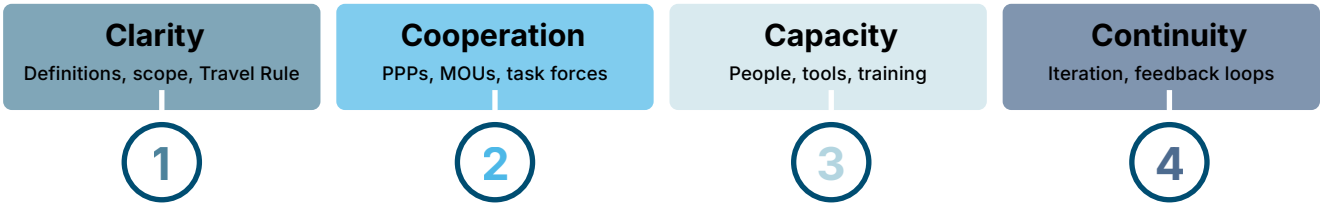
252. Beyond national efforts, multilateral programming has emerged as a key driver of progress. The UNOCT-led CFT Programme exemplifies how capacity-building can scale effectively. Since 2019, it has delivered tailored mentoring and technical assistance to more than 80 jurisdictions, helping them assess risk, develop legislation, and implement FATF-aligned measures. Its PPP model convenes FIUs, regulators, and private-sector VASPs to share typologies and develop coordinated supervisory and enforcement approaches. The 2024 Handbook on Countering the Misuse of Virtual Assets consolidates these experiences into practical operational guidance, and the Algeria Guiding Principles provide an overarching normative framework within which such efforts can be anchored. The IDB's own technical-assistance programming in the LAC region, including support for Financial Intelligence Data Labs and regional training initiatives, complements these global efforts by providing context-specific and demand-driven support to national institutions.

253. The FATF's 2026 Targeted Report on Stablecoins and Unhosted Wallets provides an additional layer of actionable guidance for jurisdictions and the private sector. Its recommended actions include:

- **Requiring stablecoin issuers to maintain and execute the technical capability to freeze, burn, and withdraw stablecoins circulating in secondary markets**, apply CDD at the redemption stage, and implement allow-lists and deny-lists using a risk-based approach (FATF, 2026, Recommended Actions II).
- **Establishing multinational supervisory colleges** to coordinate oversight of stablecoin issuers and other entities involved in cross-border stablecoin arrangements (FATF, 2026, Recommended Actions IV).
- **Establishing regulatory sandboxes in collaboration with industry participants** to develop standards and solutions that enable innovation while safeguarding against misuse, such as through smart contract monitoring, blockchain forensics, or automated sanctions screening (FATF, 2026, Recommended Actions IX).
- **Institutionalizing structured public–private partnerships** to strengthen cooperation on typologies, risk indicators, and emerging threats, including operational partnerships supporting investigations involving off-chain transactions or the freezing of stablecoins (FATF, 2026, Recommended Actions VIII).

254. Taken together, these experiences underscore four core enablers of success—Clarity, Cooperation, Capacity, and Continuity—which can be understood as the four pillars of sustainable and effective regulation. They demonstrate that regulation is not a static exercise but an adaptive process of continuous learning, in which trust between public and private stakeholders is both a prerequisite for and an outcome of effective governance.

Figure 8.2. Four Pillars of Effective Crypto Regulation



Source: own elaboration.

The Bad — Regulatory Gaps and Implementation Asymmetries

255. Despite significant progress, uneven implementation remains one of the principal weaknesses of the global AML/CFT/CPF response to virtual-asset risks. The most common challenges include legal ambiguity, institutional fragmentation, uneven enforcement, and emerging gaps in the oversight of DeFi.

256. Legal ambiguity persists in many jurisdictions that have yet to establish consistent definitions and regulatory classifications for cryptoassets. When similar tokens are classified differently as securities, commodities, or payment instruments, supervisory authorities may face difficulties coordinating their respective mandates. This uncertainty can discourage legitimate innovation and create opportunities for regulatory arbitrage, as firms seek jurisdictions with less burdensome or less clearly defined regulatory requirements. In Latin America, differing interpretations among central banks and securities regulators have occasionally resulted in overlapping or inconsistent licensing frameworks. The GAFILAT's 2025 ESR confirms that "insufficient legal frameworks" remain one of the five principal vulnerabilities across the region (GAFILAT, 2025). This regulatory confusion also impedes the adoption of essential countermeasures such as the FATF Travel Rule, as small, regional VASPs face high costs and unclear technical requirements for implementation.

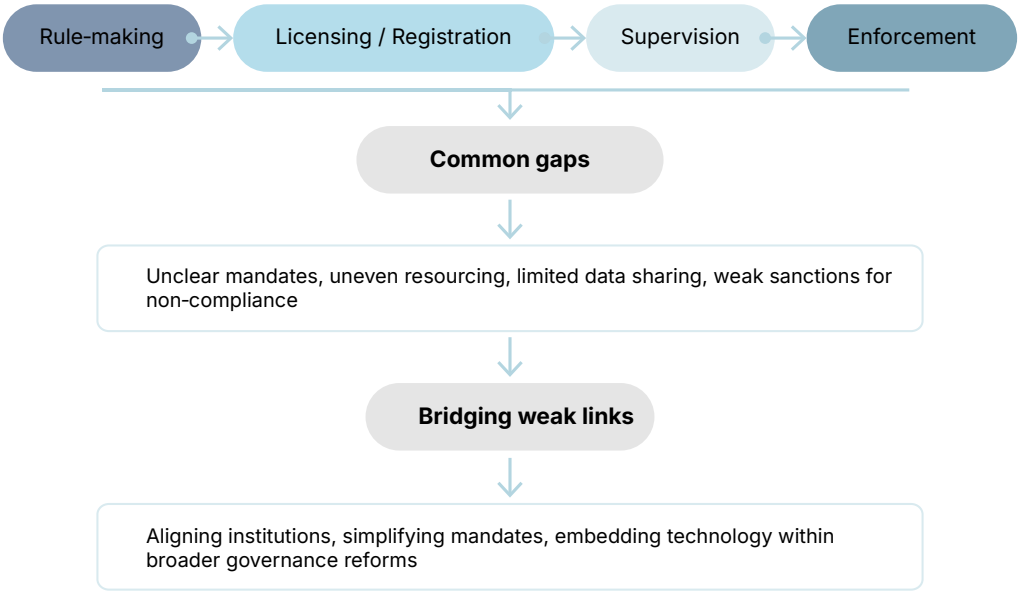
257. Institutional fragmentation can also undermine effective supervision and enforcement. In some countries, separate agencies oversee tax compliance, prudential soundness, and AML/CFT/CPF obligations, often without effective information-sharing mechanisms. One regional example involves exchanges licensed for consumer protection but unsupervised for AML/CFT/CPF purposes, creating supervisory gaps that may be exploited by illicit actors. Similar coordination challenges can arise even in advanced economies: in the United States, overlapping mandates among agencies such as the SEC, CFTC, and FinCEN continue to create coordination challenges; in Europe, implementation of MiCA across Member States will continue to require significant coordination efforts.

258. Enforcement asymmetries further compound these challenges. The FATF's 2025 Targeted Update found that, while most jurisdictions had introduced VASP registration, supervisory and enforcement activity remains limited. Among the 85 jurisdictions that have passed Travel Rule legislation, 59 per cent (50 of 85) have not yet issued findings or directives, nor undertaken enforcement actions focused on Travel Rule compliance (FATF, 2025). In several jurisdiction across Latin America and the Caribbean, fewer than 30 percent of registered exchanges had filed a STR within two years of licensing. These supervisory and compliance gaps may be exploited by transnational organized crime (TOC), particularly those involved in drug trafficking and illegal mining, who use non-compliant VASPs to layer illicit proceeds before reintroducing them into the formal financial system. Without credible supervision and enforcement, regulatory frameworks risk becoming largely symbolic.

259. Decentralized finance (DeFi) remains a particularly important implementation challenge. FATF's 2026 work on virtual assets, including its Seventh Targeted Update and Targeted Report on Regulatory Challenges from Decentralised Finance, shows that formal implementation remains limited and emphasizes a functional and risk-based approach rather than regulation based on labels or technology alone. The relevant question is whether natural or legal persons exercise control or sufficient influence over an arrangement and, more broadly, how regulated financial institutions and VASPs interact with DeFi activities. Jurisdictions should therefore assess the scale and nature of their domestic DeFi exposure, identify arrangements or persons that may fall within the applicable regulatory perimeter, and calibrate supervisory resources to the level of identified ML/TF/PF risk (FATF, 2026a; FATF, 2026d).

260. Similar lessons emerge from multilateral technical-assistance programmes. The UNOCT CFT Programme notes that technology transfers that are not accompanied by tailored implementation strategies rarely produce sustainable results. Countries that adopt advanced analytics without parallel investment in human capacity or legislative reform often struggle to integrate those tools into routine supervisory and investigative practices. Conversely, nations that embed training, mentorship, and inter-agency coordination into implementation are more likely to achieve measurable improvements in effectiveness. This evidence reinforces a central lesson: sustainable compliance cannot be outsourced solely through technology; it must be embedded within institutions, processes, and human capabilities.

Figure 8.3. The Compliance Chain



Source: Own elaboration.

The Ugly — When Policy and Practice Diverge

261. Even well-intentioned reforms can generate unintended consequences when regulatory ambition outpaces institutional capacity or market readiness. Comparative experience across jurisdictions suggests that three risks commonly emerge under such conditions: de-risking, consumer vulnerability, and coordination breakdowns.

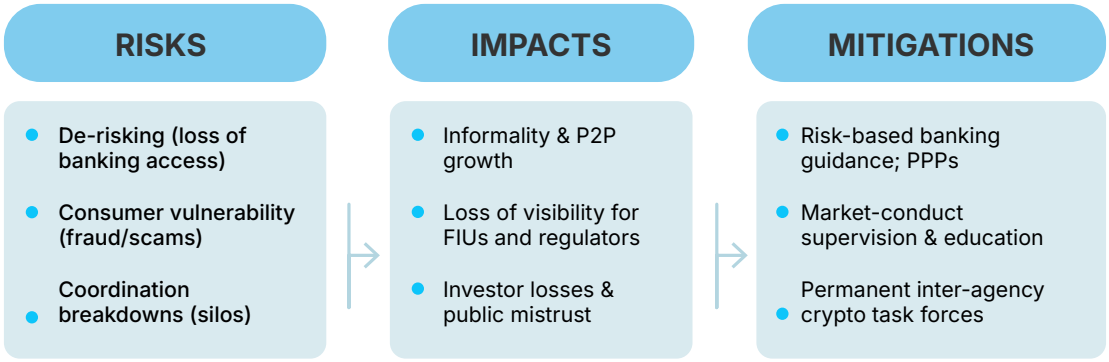
262. De-risking remains one of the most visible unintended consequences. International financial institutions, seeking to reduce perceived compliance and reputational risks, may terminate correspondent banking relationships with smaller financial institutions and crypto exchanges. In parts of Central America and the Caribbean, compliant VASPs and remittance service providers have, in some cases, lost access to banking services despite maintaining AML/CFT/CPF controls. When applied indiscriminately, de-risking measures may encourage the migration of legitimate activity toward less transparent channels, including informal P2P markets, thereby reducing the effectiveness of risk-based oversight. This can reduce visibility for FIUs and other competent authorities. FATF and World Bank analyses have consistently highlighted that excessive de-risking can undermine financial inclusion, increase market concentration, and weaken regional competitiveness.

263. Consumer vulnerability represents a second significant policy concern. In jurisdictions where retail participation in cryptoasset markets has expanded more rapidly than regulatory literacy, fraudulent schemes tend to proliferate. Between 2020 and 2023, several pyramid operations in Brazil, Colombia, and Peru disguised themselves as "AI trading bots" or "mining pools," generating substantial losses for retail investors. These cases demonstrate that AML/CFT/CPF measures alone are insufficient to protect consumers; consumer education, market-conduct supervision, and swift judicial recourse are equally critical.

264. A third concern relates to weaknesses in institutional coordination. Where central banks, securities commissions, and FIUs operate in silos, oversight may become reactive rather than preventive. Jurisdictions that have established permanent inter-agency cryptoasset task forces—Brazil, Singapore, and the United Kingdom among them—demonstrate that structured inter-agency coordination can improve response times and strengthen policy coherence. Conversely, when mandates overlap or data are compartmentalized, investigations may be delayed and public confidence may be weakened.

265. Finally, international experience suggests that technology deployed without adequate institutional context can be counterproductive. The experience of multilateral programmes delivering digital-forensics and analytical tools—whether UNODC's goAML platform or UNOCT's capacity-building initiatives—demonstrates that technology investments are most effective when accompanied by tailored training, enabling legal frameworks, and sustainable maintenance arrangements, and should be adapted to member states' resource constraints and priorities rather than relying on one-size-fits-all implementation models. Otherwise, systems risk becoming underutilized once external funding concludes. Sustainable innovation requires strong national ownership and integration into existing investigative workflows, a lesson as applicable to blockchain analytics as to any other technology deployed in service of financial integrity.

Figure 8.4. When Policy and Practice Diverge



Source: Own elaboration.

Lessons and Opportunities for Regional and Global Cooperation

266. Despite these challenges, the accumulated experience of national authorities and multilateral institutions points to a clear set of priorities for moving from fragmented compliance toward effective governance.

Information Sharing and Joint Enforcement

267. Cross-border collaboration has become indispensable. Joint investigations conducted under CFATF and GAFILAT auspices have demonstrated that tracing illicit cryptoasset flows across jurisdictions is feasible when FIUs share typologies, wallet identifiers, and related intelligence through secure and standardized channels. Establishing regional memoranda of understanding aligned with Egmont Group principles would help institutionalize these practices. Blockchain-intelligence cooperation—linking regional data labs, law-enforcement cyber units, and VASP compliance teams—can support the development of early-warning indicators of coordinated money-laundering networks. The FATF's 2026 recommended action on multinational supervisory colleges (Recommended Actions IV) provides an institutional model for formalizing cooperation in cross-border stablecoin-related cases.

Capacity Building and Tailored Assistance

268. The UNOCT-led CFT Programme, UNODC's goAML deployments, and parallel IDB technical-assistance initiatives demonstrate the value of sustained and integrated capacity-building efforts. Beyond stand-alone training events, effective programming combines training, legislative support, and peer review. Regional training hubs could help standardize and consolidate curricula on the Travel Rule, beneficial-ownership verification, and the seizure of virtual assets. Digital tools developed by the UN system—notably UNODC's **goAML platform**, which is now used by more than 70 member states and is being enhanced to incorporate advanced financial intelligence analysis capabilities, building on the analytical functions

previously developed under UNOCT's goFintel initiative in partnership with the Netherlands FIU—illustrate how scalable and evolving technology can support FIUs in conducting risk assessments and managing investigative workflows. Embedding the regional use of such platforms could accelerate institutional learning and reduce duplication of effort. The GAFILAT's 2025 ESR should serve as a foundational reference for prioritizing capacity-building investments, given its identification of knowledge gaps and infrastructure deficiencies as the region's top vulnerabilities.

269. UNOCT's regional delivery model—as demonstrated through the ESAAMLG workshop in Addis Ababa (June 2025) and the MENAFATF practical webinar (February 2026), both focused on operationalizing the 2024 Handbook on Virtual Assets—provides a useful model for engagement in the LAC region. A forthcoming addendum to the Handbook, currently incorporating experiences from MENAFATF members, may further enrich the available body of operational knowledge. A similar LAC-focused workshop, delivered in partnership with CFATF, GAFILAT, UNOCT, and the IDB, would help disseminate both the operational guidance contained in the Handbook and the normative principles reflected in the Algeria Guiding Principles to the region's FIUs and supervisors.

Knowledge Products and Guidance

270. Addressing emerging risks also requires the development of standardized manuals and typology reports. The 2024 UNOCT Handbook distills good practices from multiple regions. Adapted to the regional context of the Americas, such materials could serve as the foundation for a regional compendium of cryptoasset typologies, updated on a regular basis in partnership with CFATF, GAFILAT, and the IDB. The FATF's 2026 stablecoin risk indicators (Annex A) provide a ready-made starting point for this exercise. Furthermore, regional discussions must begin to address DeFi, which currently sits largely outside VASP regulatory perimeters. Proactive risk assessments of DeFi platforms are necessary to prevent the next wave of regulatory arbitrage and illicit activity.

Public–Private Partnerships (PPPs)

271. Collaborative mechanisms linking competent authorities, FIUs, financial institutions, VASPs, and other relevant private-sector actors can strengthen the speed and quality of financial intelligence. Models such as the United Kingdom's Joint Money Laundering Intelligence Taskforce (JMLIT) and the Australia's Fintell Alliance illustrate how structured public–private arrangements can facilitate the exchange of operational insights within defined legal boundaries. FATF's 2026 global review of public–private information-sharing arrangements reinforces this approach, emphasizing that effective PPPs require a clear legal basis, defined governance and objectives, appropriate data-protection safeguards, and sustained trust among participants. For the virtual-asset ecosystem, such mechanisms can bring VASPs, stablecoin issuers, blockchain-intelligence providers, and traditional financial institutions into structured information-sharing arrangements alongside FIUs and law enforcement authorities (FATF, 2026e).

Balancing Integrity and Inclusion

272. Both FATF and the UN increasingly recognize that financial inclusion is an important component of effective AML/CFT/CPF frameworks. Policies that unintentionally exclude vulnerable populations or small VASPs may contribute to greater reliance on informal channels. Future regulatory frameworks should consider incorporating financial-inclusion indicators into national risk assessments while remaining consistent with broader development objectives, including the Sustainable Development Goals (SDGs). Such an approach can help ensure that financial integrity and development reinforce one another rather than at cross-purposes.

Figure 8.5. Opportunities for Regional Cooperation

Action Area	Integrity	Innovation	Effectiveness
Information sharing & joint enforcement	Egmont-style MOUs; Travel Rule IDs	Early-warning indicators from cross-jurisdiction analytics	Institutionalize secure channels
Capacity building (FIUs, prosecutors, judges)	KYT/BO analytics in STR workflows	Sandbox training for new tools	Regional hubs & peer review
Guidance & knowledge products	Standardized typologies & red flags	DeFi risk-scoping guidance	Annual updates with CFATF/GAFILAT
Public-private partnerships (PPPs)	JMLIT/FINTEL-style models	Communication systems with exchanges & banks	Standing PPP secretariats
Financial inclusion alignment	Proportionate CDD & thresholds	Support on/off-ramps for SMEs	Monitor inclusion metrics in NRAs

Source: Own elaboration.

Conclusion — From Global Mandate to Regional Action

273. The global experience with virtual-asset regulation reveals both meaningful progress and important lessons regarding implementation challenges. Successful experiences demonstrate that coherent policy frameworks, capable institutions, and trusted public–private collaboration can transform technological innovation into a force for greater financial transparency and integrity. Less successful experiences demonstrate that incomplete implementation can generate operational vulnerabilities and weaken regulatory effectiveness. Unintended consequences—including excessive de-risking or unchecked speculation—illustrate the importance of balancing integrity objectives with inclusion, innovation, and proportionality.

274. For Latin America and the Caribbean, the path forward lies in translating international standards and policy commitments into coordinated regional action. FATF standards, the Algeria Guiding Principles, the FATF's 2026 recommended actions on stablecoins, the GAFILAT's 2025 ESR, and the UN resolutions together provide a comprehensive policy framework, while national innovation and regional cooperation will determine its effectiveness. Building interoperable data systems, strengthening the deployment of goAML and related analytical platforms, establishing supervisory colleges for cross-border stablecoin arrangements, and fostering continuous dialogue between supervisors and private-sector stakeholders will be critical steps toward that objective.

275. Ultimately, the region's objective is not to replicate external models but to develop governance frameworks that reflect its own institutional realities: risk-based, inclusive, and technology-enabled. By integrating the lessons of both success and failure, Latin America and the Caribbean can demonstrate that innovation and integrity are not competing objectives but mutually reinforcing foundations of digital trust. If these lessons are translated into sustained cooperation, institutional strengthening, and effective implementation, Latin America and the Caribbean will be well positioned to harness the benefits of digital finance while mitigating its risks and safeguarding financial integrity.

Key Actions for Policymakers and Supervisors — Chapter 8

- **Assess the institutional governance of virtual-asset oversight, not only its formal regulatory coverage**. Review whether mandates, accountability, inter-agency coordination, supervisory capacity, and long-term institutional arrangements are sufficiently clear and sustainable to translate technical compliance into effective implementation. Use the chapter's four dimensions—clarity, cooperation, capacity, and continuity—to identify institutional gaps and assign responsibility for closing them.
- **Conduct proactive, risk-based assessments of domestic DeFi exposure.** Identify the scale and nature of interactions between DeFi arrangements, VASPs, traditional financial institutions, and domestic users; determine whether identifiable natural or legal persons exercise control or sufficient influence over relevant arrangements; and calibrate regulatory and supervisory responses to the jurisdiction's actual ML/TF/PF exposure rather than to technology labels alone.
- **Build a sustained regional implementation and peer-learning mechanism for VA/VASP supervision in Latin America and the Caribbean.** Use recurring regional workshops and peer exchanges—building on GAFILAT, CFATF, UNOCT, and other relevant regional and international initiatives—to convert cross-country experience into practical implementation tools, shared typologies, supervisory guidance, and reusable regional knowledge products rather than relying primarily on one-off training activities.

REFERENCES

References

Bains, P. (2025). *Blockchain Consensus Mechanisms: A Primer for Supervisor (2025 Update).* **International Monetary Fund. Washington, DC.**

Banco Central de la República Argentina. (2023). *Informe de estabilidad financiera.* **Buenos Aires.**

Banco Central del Uruguay. (2026). *El BCU aprueba normativa para proveedores de servicios de activos virtuales.* **Montevideo.**

Banco Central do Brasil. (2023). *Lei nº 14.478/2022 sobre ativos virtuais e o projeto DREX.* **Brasília.**

Banco Central do Brasil. (2025). *Pix at 5 – The innovation that transformed payments in Brazil.* **Brasília.**

Banco Central do Brasil. (2025). *Resolução BCB No. 520, de 10 de novembro de 2025.* **Brasília.**

Banco de México. (2019, as amended). *Circular 4/2019: Disposiciones de carácter general aplicables a las Instituciones de Crédito e Instituciones de Tecnología Financiera en las operaciones que realicen con activos virtuales.* **Mexico City.**

Bank for International Settlements. (2023). *Addressing the risks in crypto: Laying out the options.*

CAF – Banco de Desarrollo de América Latina. (2022). *Inclusión financiera en América Latina y el Caribe: Desafíos y oportunidades digitales.* **Caracas.**

Caribbean Financial Action Task Force. (2023). *Mutual evaluation follow-up reports: The Bahamas, Jamaica, Trinidad and Tobago.* **Port of Spain.**

Caribbean Financial Action Task Force. (2023). *Mutual evaluation trends and typologies in the Caribbean region.* **Port of Spain.**

Chainalysis. (2024a). *Crypto Crime Report 2024: Illicit activity trends and typologies.* **New York, NY.**

Chainalysis. (2024b). *Latin America's Search for Economic Stability: The Rise of Stablecoins Amid Volatility. Excerpt from the 2024 Geography of Cryptocurrency Report.* **New York, NY.**

Chainalysis. (2026). *2026 Crypto Crime Report.* **New York, NY.**

CoinDesk. (2018, February 20). *Finland mandates cold storage, public auctions for seized bitcoins.* https://www.coindesk.com/markets/2018/02/20/finland-mandates-cold-storage-public-auctions-for-seized-bitcoins

Comisión Nacional de Activos Digitales (CNAD). (2026). *Registro Público de Proveedores de Servicios de Activos Digitales and Reglamento de Proveedores de Servicios de Activos Digitales.* **San Salvador.**

Comisión Nacional de Valores (CNV). (2026). *Registro de Proveedores de Servicios de Activos Virtuales (PSAV).* **Buenos Aires.**

Egmont Group. (2025). *Connecting financial intelligence units worldwide.*

EU AML/CFT Global Facility. (2026). *Leveraging Beneficial Ownership Transparency for Virtual Assets.*

European Central Bank. (2023). *Exploring the Digital Euro: Experimentation and prototyping.* **Frankfurt am Main.**

European Commission. (2023). *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).* **Brussels.**

European Commission. (2025). *Next-generation FIU.net: Laying the foundations for an even more effective way to prevent and fight financial crime.* **Brussels.**

Europol. (2023). *Decrypting cryptocurrency investigations: Operational trends and emerging risks.* **Europol Innovation Lab.**

Financial Action Task Force. (2015). *AML/CFT-related data and statistics.* **Paris.**

Financial Action Task Force. (2019/2023). *Guidance for a risk-based approach to virtual assets and virtual asset service providers (updated 2023).* **Paris.**

Financial Action Task Force. (2021). *Report on the state of effectiveness and compliance with the FATF Standards.* **Paris.**

Financial Action Task Force. (2023a). *Targeted update on implementation of the FATF Standards on virtual assets and virtual asset service providers (VASPs).* **Paris.**

Financial Action Task Force. (2023b). *Updated guidance for Recommendation 24 on beneficial ownership and transparency of legal persons.* **Paris.**

Financial Action Task Force. (2025a). *Best Practices in Travel Rule Supervision.* **Paris.**

Financial Action Task Force. (2025b). *Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT/CPF systems.* **Paris.**

Financial Action Task Force. (2025c). *Targeted update on the implementation of the FATF Standards on virtual assets and VASPs.* **Paris.**

Financial Action Task Force. (2026a). *Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs.* **Paris.**

Financial Action Task Force. (2026b). *Targeted Report on Stablecoins and Unhosted Wallets — Peer-to-Peer Transactions.* **Paris.**

Financial Action Task Force. (2026c). *Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers (oVASPs).* **Paris.**

Financial Action Task Force. (2026d). *Targeted Report on Regulatory Challenges from Decentralised Finance.* **Paris.**

Financial Action Task Force. (2026e). *Information Sharing to Combat Illicit Finance: Global Overview of Public and Private Sector Partnerships and Data Protection Arrangements.* **Paris.**

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). (2021). *Reporting large virtual currency transactions to FINTRAC: FINTRAC's compliance guidance.* **Canada.**

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2018). *Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? Review of Financial Studies (forthcoming).* Available at: **https://ssrn.com/abstract=3102645** **https://doi.org/10.2139/ssrn.3102645**

Grupo de Acción Financiera Internacional de Latinoamérica (GAFILAT). (2025). *Evaluación Sectorial de Riesgos de LA/FT de los AV y PSAV de los Países del GAFILAT.* **Buenos Aires.**

International Monetary Fund. (2022). *El Salvador: 2022 Article IV consultation—Staff report.* **Washington, DC.**

International Monetary Fund. (2023). *Crypto-assets and capital flow management in emerging markets.* **Washington, DC.**

International Monetary Fund. (2023). *Virtual assets and anti-money-laundering: Policy responses in emerging markets (Fintech Note 2023/04).* **Washington, DC.**

International Monetary Fund. (2024). *Crypto-assets and cross-border regulatory coordination: Challenges and policy options.* **Washington, DC.**

Inter-American Development Bank. (2024). *Building financial intelligence data labs for the Caribbean and Latin America.* **Washington, DC.**

Inter-American Development Bank. (2024). *Regional approaches to AML/CFT in digital finance: Lessons from Latin America and the Caribbean.* **Washington, DC.**

Monetary Authority of Singapore. (2023). Payment Services Act implementation and supervision report. **Singapore.**

OECD. (2021). *Understanding the Virtual Asset Landscape.* **Paris.**

OECD. (2022). *Crypto-Asset Reporting Framework (CARF) and amendments to the Common Reporting Standard.* **Paris.**

OECD. (2023). *Beneficial Ownership Implementation Toolkit for Latin America.* **Paris.**

OECD. (2023). *Crypto-Asset tax and enforcement report.* **Paris.**

OECD. (2023). *Taxing virtual assets: Global approaches and challenges.* **Paris.**

Reuters. (2024). *Brazil's Pix payments are killing cash. Are credit cards next?* **London.**

RUSI. (2024). *Crypto-asset recovery: Challenges, observed practices, and recommendations.* **London: Royal United Services Institute.**

RUSI. (2024). *Seizing crypto-assets: Legal frameworks and operational challenges.* **London: Royal United Services Institute.**

Securities Commission of The Bahamas. (2024). *Digital Assets and Registered Exchanges Act, 2024 and Guidance Note on Travel Rule Compliance for Digital Asset Businesses.* **Nassau.**

Servicio de Administración Tributaria (SAT). (2026). *Registra tu actividad de activos virtuales / Actividades Vulnerables, Fracción XVI.* **Mexico City.**

Superintendencia de Banca, Seguros y AFP. (2023). *Activos virtuales: legislación comparada y exposición a los riesgos de LA/FT en el Perú.* **Lima, Perú.**

Superintendencia de Banca, Seguros y AFP. (2024). *Resolución SBS No. 02648-2024 and PSAV supervisory materials.* **Lima, Perú.**

Superintendencia Financiera de Colombia. (2026). *Balance del cierre del piloto de operaciones con plataformas de criptoactivos.* **Bogota.**

The White House. (2025). *Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile [Presidential action].* **Washington, DC.**
https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/

TRM Labs. (2021). *A digital migration: How the pandemic has launched Latin America into the cryptoverse.*
https://www.trmlabs.com/resources/blog/a-digital-migration-how-the-pandemic-has-launched-latin-america-into-the-cryptoverse

TRM Labs. (2024). *A digital migration: Crypto adoption and illicit finance in Latin America.* **Washington, DC.**

TRM Labs. (2024). *Illicit Crypto Ecosystem Report: Global and Regional Risk Patterns.* **Washington, DC.**

TRM Labs. (2024). *Must-know crypto investigations of 2023:* **Latin America.**
https://www.trmlabs.com/resources/blog/must-know-crypto-investigations-of-2023-latin-america

TRM Labs. (2024). *The State of Crypto Crime 2024: Trends in Illicit Finance and Blockchain Investigations. TRM Insights.*

TRM Labs. (2024). *From swiping right to exposing a crypto theft ring in Brazil.*
https://www.trmlabs.com/resources/case-studies/from-swiping-right-to-exposing-a-crypto-theft-ring-in-brazil

TRM Labs. (2025). *2025 Crypto Crime Report.*
https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

TRM Labs. (2025). *Crypto Illicit Economy Report 2025.* **Washington, DC.**

TRM Labs. (2025). *Report teaser: Proportion of illicit volume of crypto dropped 51% in 2024.*
https://www.trmlabs.com/resources/blog/report-teaser-proportion-of-illicit-volume-of-crypto-dropped-51-in-2024

TRM Labs. (2025). *Spain's Guardia Civil, in coordination with T3, disrupts criminal enterprise.*
https://www.trmlabs.com/resources/blog/spains-guardia-civil-in-coordination-with-t3-disrupts-criminal-enterprise

TRM Labs. (2025). *Understanding the use of cryptocurrencies by cartels.*
https://www.trmlabs.com/resources/blog/understanding-the-use-of-cryptocurrencies-by-cartels

TRM Labs. (2025). *Shadow Bankers: Chinese underground networks and their connection to North Korean hacks, fentanyl, cartel money laundering, and global organized crime.* **San Francisco, CA.**

UAFE (Unidad de Análisis Financiero y Económico). (2022). *Resolución No. UAFE-DG-2022-0131.* **Quito, Ecuador.**

U.S. Department of Justice. (2022). U.S. Attorney announces historic $3.36 billion cryptocurrency seizure and conviction.
https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction

U.S. Department of the Treasury. (2022). U.S. Sanctions Virtual Currency Mixer Tornado Cash [Press release]. **Washington, DC.**

United Nations Office of Counter-Terrorism. (2024). *Global Programme on Countering the Financing of Terrorism: Annual Progress Report.* **New York, NY.**

United Nations Office of Counter-Terrorism. (2024). *Handbook on Countering the Financing of Terrorism through New Technologies.* **New York, NY.**

United Nations Office of Counter-Terrorism/United Nations Counter-Terrorism Centre & FATF's Eurasian Group. (2024). *Countering the Misuse of Virtual Assets and Virtual Asset Service Providers for Terrorism Financing Purposes: Handbook.* **New York, NY.**

United Nations Office on Drugs and Crime. (2020). *Money-Laundering and Virtual Currencies: An Analysis of Typologies.* **Vienna, Austria.**

United Nations Security Council Counter-Terrorism Committee. (2025). *Algeria Guiding Principles (S/2025/22).* **New York, NY.**

World Bank. (2023). *Migration and Development Brief 38: Remittances 2023.* **Washington, DC.**

World Economic Forum. (2023). Digital Assets and AML: The Future of Compliance. **Geneva.**

World Economic Forum. (2023). *Navigating Cryptocurrency Regulation: An Industry Perspective on Compliance and Supervision.* **Geneva.**

CNBC. (2019, October 1). *UK police raise nearly £300,000 in auction of seized cryptocurrency.* **https://www.cnbc.com/2019/10/01/uk-police-raise-nearly-300000-in-auction-of-seized-cryptocurrency.html**


IDB