pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

# REGULATORY FRAGMENTATION AND ITS CONSEQUENCES FOR COMBATING CRYPTOASSET-RELATED CRIMES: A COMPARATIVE LEGAL ANALYSIS

**Nuriddin Khudoyberdiev**
LL.M., Penn State Law, The Pennsylvania State University, USA; LL.M. and LL.B., Tashkent State University of Law, Uzbekistan.
n.khudoyberdiev.law@gmail.com

**Abstract.** The rapid expansion of cryptoasset markets has exposed a fundamental vulnerability in the global financial governance architecture: deep regulatory fragmentation across jurisdictions. While international bodies have issued guidelines and recommendations, the absence of a unified legal framework has created exploitable gaps that transnational criminal networks increasingly leverage. This study adopts a comparative legal lens to examine how divergent national regulatory approaches to cryptoassets — ranging from permissive to prohibitive — affect the collective capacity of states to detect, investigate, and prosecute cryptoasset-related crimes. Drawing on legislative analysis, institutional reports, and case studies from select jurisdictions, the research argues that regulatory asymmetry — rather than technological anonymity alone — constitutes the primary structural enabler of cryptoasset-related criminal activity. The article concludes with a framework for regulatory convergence that preserves national legal sovereignty while establishing minimum enforceable international standards.

**Key words:** regulatory fragmentation, cryptoassets, comparative law, virtual asset regulation, anti-money laundering, jurisdictional asymmetry, financial crime governance.

## I. Introduction

### The Problem of Regulatory Asymmetry

The global cryptoasset market has evolved from a niche technological experiment into a multi-trillion-dollar financial ecosystem within little more than a decade. This transformation has outpaced the development of commensurate legal infrastructure, producing a patchwork of national regulatory regimes that varies dramatically in scope, rigor, and enforcement capacity. Some states have embraced cryptoassets as legitimate financial instruments and enacted comprehensive regulatory frameworks; others have imposed blanket prohibitions; and a significant number have adopted a posture of regulatory ambiguity, neither sanctioning nor restricting cryptoasset activity in any meaningful way.

This fragmentation has significant consequences for global financial security. Criminal actors are sophisticated in their exploitation of jurisdictional differentials. Where one country imposes stringent Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements on virtual asset service providers, another may impose none. The result is a regulatory arbitrage environment in which illicit funds migrate toward the path of least legal resistance (Zetzsche et al., 2020). According to Chainalysis (2023), illicit transaction volumes in the cryptoasset sector reached approximately 24.2 trillion US dollars in overall market activity, with criminal flows disproportionately concentrated through exchanges operating in low-regulation jurisdictions.

### Scope and Purpose

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

Existing scholarship has devoted considerable attention to the technical dimensions of cryptoasset crime — blockchain anonymization, mixer services, and darknet market ecosystems. Far less attention has been directed toward the structural legal conditions that enable these crimes to persist at scale. This article addresses that gap by examining regulatory fragmentation as a systemic governance failure, analyzing how national legal divergence undermines international law enforcement cooperation, and proposing a convergence framework grounded in comparative legal analysis.

**Research Questions**

This study is organized around three central questions: How do differences in national regulatory approaches to cryptoassets create conditions favorable to transnational criminal activity? What are the measurable enforcement consequences of regulatory asymmetry across jurisdictions? And what models of regulatory convergence are most compatible with effective international cooperation while respecting principles of national legal sovereignty?

## II. Methodology

This research employs a comparative legal methodology, systematically examining the regulatory frameworks governing cryptoassets in six representative jurisdictions: the United States, the European Union, Japan, Singapore, the United Arab Emirates, and El Salvador. These jurisdictions were selected to represent the full spectrum of regulatory approaches — from comprehensive integration to legal prohibition — and to capture variation across levels of economic development, legal tradition, and institutional capacity.

Primary sources include national legislation, regulatory agency guidance documents, parliamentary and congressional records, and judicial decisions pertaining to cryptoasset regulation and enforcement. Secondary sources encompass reports from the Financial Action Task Force (FATF), the International Monetary Fund (IMF), the Bank for International Settlements (BIS), Europol, and UNODC, as well as peer-reviewed scholarship in international law, financial regulation, and criminology.

Quantitative data on cryptoasset crime volumes, enforcement actions, and regulatory compliance rates were drawn from Chainalysis (2023), Europol (2024), and FATF mutual evaluation reports. These figures are used not to establish causal relationships but to identify correlations between regulatory characteristics and observed criminal activity patterns.

The comparative analysis proceeds in three stages: descriptive mapping of each jurisdiction's regulatory framework; evaluative assessment of enforcement outcomes; and synthetic identification of convergence points and divergence risks.

## III. Results

### 3.1 Mapping National Regulatory Approaches

**The United States** has adopted a fragmented but generally stringent domestic framework. The Financial Crimes Enforcement Network (FinCEN) classifies virtual asset service providers as money services businesses subject to AML and KYC obligations under the Bank Secrecy Act. However, regulatory authority is distributed across multiple federal agencies — the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Internal

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

Revenue Service — resulting in jurisdictional overlap and regulatory uncertainty that has complicated enforcement (Brummer & Yadav, 2019).

**The European Union**, through the adoption of the Markets in Crypto-Assets (MiCA) Regulation in 2023, has achieved the most comprehensive regional harmonization to date. MiCA establishes a unified licensing regime for crypto-asset service providers, standardizes disclosure requirements, and extends AML obligations consistent with the EU's Anti-Money Laundering Directives. While this represents a significant step toward regulatory coherence, MiCA's reach is inherently limited to EU member states and does not resolve the asymmetries that characterize the broader international landscape (Zetzsche et al., 2020).

**Japan** was among the first states to recognize cryptocurrencies as legal tender under the Payment Services Act of 2017. Its Financial Services Agency has established a licensing regime for cryptocurrency exchanges with mandatory AML and cybersecurity requirements. Japan's proactive regulatory posture has been credited with improving enforcement outcomes domestically, though its impact on cross-border crime remains limited by the non-adoption of comparable standards elsewhere.

**Singapore** has positioned itself as a regulated cryptoasset hub under the Payment Services Act of 2019, which subjects digital payment token service providers to AML/CFT requirements administered by the Monetary Authority of Singapore. Singapore's approach balances financial innovation with regulatory discipline and has been cited by FATF as a model for developing jurisdictions (FATF, 2021).

**The United Arab Emirates**, through its Virtual Assets Regulatory Authority established in 2022, has developed a comprehensive licensing and supervisory framework. The UAE's regulatory evolution is notable given its historical characterization as a high-risk jurisdiction for money laundering, illustrating that rapid regulatory reform is achievable where political will exists.

**El Salvador** presents a markedly different case. As the first country to adopt Bitcoin as legal tender in 2021, El Salvador has created a regulatory environment in which cryptoasset transactions are normalized without commensurate AML infrastructure. The IMF has repeatedly flagged concerns regarding financial stability and money laundering risks, and the country was subject to heightened FATF monitoring as a consequence (IMF, 2022).

### 3.2 Enforcement Consequences of Regulatory Divergence

The enforcement data reveal a consistent pattern: jurisdictions with weaker regulatory frameworks exhibit higher concentrations of illicit cryptoasset flows. Chainalysis (2023) found that exchanges operating in jurisdictions without mandatory KYC requirements processed a disproportionate share of funds traceable to ransomware payments, darknet market proceeds, and sanctions evasion. Europol (2024) similarly identified regulatory gaps in specific jurisdictions as primary transit points for cryptoasset-based money laundering, with losses attributable to cryptoasset crimes reaching 23.8 billion US dollars in 2023.

Mutual legal assistance mechanisms have proven ill-suited to the pace and technical complexity of cryptoasset investigations. Traditional Mutual Legal Assistance Treaty (MLAT) processes, designed for conventional financial crime, typically require six to twelve months to complete — a timeframe wholly incompatible with the speed at which digital assets can be

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

moved, converted, and obscured (Europol, 2024). Several major investigations have stalled or failed entirely due to evidence degradation during MLAT processing delays.

The dual criminality requirement — which conditions legal cooperation on the predicate offense being criminal in both the requesting and requested jurisdiction — creates additional barriers where cryptoasset-related activities are not uniformly criminalized. In jurisdictions where certain cryptoasset activities remain legally ambiguous or unregulated, mutual assistance requests may be declined on dual criminality grounds, effectively insulating criminal actors from prosecution.

### 3.3 Structural Enablers of Regulatory Arbitrage

Three structural conditions emerge from the comparative analysis as primary enablers of regulatory arbitrage in the cryptoasset sector.

First, the absence of a binding international legal instrument specifically addressing cryptoasset regulation means that states bear no enforceable obligation to maintain minimum regulatory standards. FATF recommendations, while influential, are non-binding and unevenly implemented. As of 2023, FATF reported that fewer than 60% of its members had enacted legislation consistent with its virtual asset standards (FATF, 2023).

Second, significant disparities in technical capacity between developed and developing states limit the practical reach of international regulatory frameworks. Even where legal obligations exist, enforcement requires sophisticated blockchain analytics capabilities, trained investigative personnel, and interoperable data systems that many states lack.

Third, the private infrastructure of the cryptoasset ecosystem — exchanges, wallet providers, mixing services — operates largely outside the direct supervisory reach of law enforcement. Information asymmetries between private sector actors and government agencies create investigative blind spots that criminals exploit systematically.

## IV. Discussion

### Toward a Convergence Framework

The evidence presented in this study supports the conclusion that regulatory fragmentation, rather than technology alone, is the primary structural enabler of large-scale cryptoasset crime. Addressing this problem requires a governance strategy oriented toward regulatory convergence — the progressive harmonization of national legal standards around enforceable minimum requirements.

A convergence framework must navigate the tension between two competing imperatives: the need for uniform international standards sufficient to eliminate regulatory arbitrage opportunities, and the principle of national legal sovereignty that legitimizes and sustains international cooperation. Imposing a single global regulatory model is neither feasible nor desirable; legal systems differ in their institutional architecture, traditions, and developmental contexts. What is both feasible and necessary is agreement on a floor of minimum standards below which no participating jurisdiction may fall.

Such a framework should incorporate several core elements. Mandatory licensing and supervision of all virtual asset service providers operating within or accessible from a

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

jurisdiction would establish a universal baseline for market entry. Standardized AML and KYC obligations, aligned with but extending beyond current FATF recommendations, would reduce the information gaps that facilitate illicit flows. Binding commitments to implement the "Travel Rule" — requiring the transmission of originator and beneficiary information for cryptoasset transfers — would enhance transaction traceability across borders. Expedited mutual legal assistance procedures specific to cryptoasset investigations, with defined response timelines and digital evidence standards, would address the procedural bottlenecks that currently undermine cross-border enforcement. Finally, a permanent international technical assistance mechanism would support developing states in building the institutional and technical capacity necessary for meaningful participation in the framework.

### The Role of Private Sector Actors

An effective convergence framework cannot rely exclusively on state-to-state cooperation. The cryptoasset industry's private infrastructure is both a site of vulnerability and a potential resource for enforcement. Cryptocurrency exchanges, in particular, occupy a strategic position in the transactional ecosystem: they are the primary interface between cryptoasset markets and the conventional financial system, and they possess transaction data of significant investigative value.

Formalizing the obligations and protections of private sector actors within an international legal framework — including clear standards for data retention, suspicious transaction reporting, and cooperation with law enforcement requests — would substantially improve enforcement outcomes. Self-regulatory organizations within the cryptoasset industry have demonstrated willingness to develop compliance standards; international legal frameworks should engage rather than exclude this capacity (Campbell-Verduyn, 2022).

## V. Conclusion

This study has argued that regulatory fragmentation constitutes the foundational structural condition enabling transnational cryptoasset-related crime. The comparative analysis of six jurisdictions demonstrates that divergent legal approaches create exploitable asymmetries, that enforcement outcomes are systematically weaker in low-regulation environments, and that existing international legal mechanisms are structurally insufficient to bridge these gaps.

The path forward lies not in the imposition of regulatory uniformity but in the negotiation of a binding convergence framework — one that establishes enforceable minimum standards, modernizes mutual legal assistance procedures, builds technical capacity in developing states, and integrates private sector actors as partners in enforcement. Such a framework must be adaptive by design, capable of evolving alongside the rapid technological developments that characterize the cryptoasset space.

The stakes extend beyond financial crime. As cryptoassets become increasingly embedded in global financial infrastructure, the governance failures documented in this study carry systemic risks for financial stability and public trust. Addressing regulatory fragmentation is not merely a law enforcement priority — it is a precondition for the legitimate and sustainable development of the digital financial economy.

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

**References**


1. Brummer, C., & Yadav, Y. (2019). Fintech and the innovation trilemma. Georgetown Law Journal, 107(1), 235–307.
2. Campbell-Verduyn, M. (2022). Blockchains, regulatory legitimacy and global financial governance. Review of International Political Economy, 29(3), 814–839.
3. Chainalysis. (2023). The 2023 Crypto Crime Report. Chainalysis.
4. Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2023/2024. European Union Agency for Law Enforcement Cooperation.
5. FATF. (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Financial Action Task Force.
6. FATF. (2023). Targeted Update on Implementation of FATF Standards on Virtual Assets and Virtual Asset Service Providers. Financial Action Task Force.
7. IMF. (2022). El Salvador: 2021 Article IV Consultation. International Monetary Fund.
8. Interpol. (2023). Annual Report 2022. International Criminal Police Organization.
9. UNODC. (2023). Global Report on Financial Crimes and Digital Assets. United Nations Office on Drugs and Crime.
10. Yeoh, P. (2022). Crypto regulations: Harmonizing or disruptive approaches. Journal of Financial Regulation and Compliance, 30(4), 427–444.
11. Zetzsche, D.A., Annunziata, F., Arner, D.W., & Buck-Heeb, P. (2020). The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy. Capital Markets Law Journal, 16(2), 203–225.