International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 5, Issue 6, June - 2026
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Regulation And Supervision of Crypto-Asset Circulation: Mechanisms for Preventing Legal Violations in International Practice

Aytimova Barshinay
Student of the Karakalpak State University Named After Berdakh

Abstract
The rapid growth of crypto-assets has raised serious concerns about financial crimes, including money laundering, fraud, and market manipulation. This article comparatively analyzes the legal frameworks regulating crypto-asset circulation across the EU, the US, the UK, Singapore, and Uzbekistan, as well as international standards set by the FATF.

Keywords: Crypto-assets, regulation, supervision, AML/CFT, FATF, virtual asset service providers, blockchain, DeFi, regulatory technology, international financial law, Uzbekistan.

Introduction

The advent of Bitcoin in 2008 and the subsequent explosion of thousands of crypto-assets have fundamentally disrupted global financial architecture. Unlike conventional financial instruments, crypto-assets operate on decentralised ledgers distributed across thousands of nodes in multiple legal jurisdictions making the application of traditional supervisory tools inherently problematic. By 2023, the total market capitalisation of crypto-assets had exceeded USD 1.7 trillion, and the annual volume of illicit transactions attributable to blockchain-based assets was estimated at approximately USD 24.2 billion, according to Chainalysis data[5]. These figures underscore the urgency of robust, harmonised regulatory frameworks.Legal violations in crypto-asset markets take several forms: money laundering through peer-to-peer exchanges and mixing services, tax evasion through pseudonymous wallets, insider trading and market manipulation on unregulated exchanges, and financing of terrorism via privacy coins and darknet markets. Each of these offence categories challenges existing anti-money-laundering, securities, and tax regimes in distinct ways. Despite the growing consensus on the need for oversight, regulatory responses have varied sharply.

The European Union has enacted comprehensive legislation through the Markets in Crypto-Assets Regulation[9], while the United States relies on a fragmented multi-agency approach[10]. Singapore has adopted a tiered risk-based licensing model, whereas China has moved toward outright prohibition. In the Central Asian context, Uzbekistan presents a particularly instructive

case: since 2018, a series of presidential decrees has progressively constructed one of the most formally structured crypto-asset regulatory regimes in the post-Soviet space, combining mandatory domestic licensing with zero-tax incentives and a presidential-decree-driven supervisory architecture under the National Agency for Perspective Projects (NAPP). These divergent approaches reflect not only differing assessments of systemic risk but also competing economic and geopolitical interests.

Literature Analysis

The analysis of liability for violations in the field of crypto-assets reveals several key areas:1)breaches of AML/CFT requirements; 2) violations of licensing and registration rules; 3) breaches related to investor protection and market manipulation; 4) violations of cybersecurity and operational requirements; and 5) breaches of tax and reporting obligations.In developed countries, each of these areas is subject to established mechanisms of supervision, inspection, and enforcement, encompassing criminal, administrative, and civil liability.

This study is based on a multi-method comparative legal approach and includes three main methods of analysis[3]. First, a doctrinal analysis of regulatory legal acts adopted in the European Union, the USA, Great Britain, Singapore, Japan, Switzerland, and China between 2019 and 2024 was conducted. The recommendations of the Financial Action Task Force and the evaluation reports were also taken into account in this process. Second, a comparative analysis was conducted based on five criteria: the scope of regulated entities, AML/CFT obligations, licensing requirements, investor protection, and cross-border cooperation mechanisms. Third, 42 instances of crypto-asset violations were analyzed based on data from the Financial Crimes Enforcement Network, the Financial Conduct Authority, the European Securities and Markets Authority, and the US Department of Justice. Qualitatively, through thematic analysis, recurring problems and effective identification mechanisms were identified. Limitations include the rapidly evolving legislative landscape particularly in the EU and US which may render certain legislative comparisons partially outdated. Access to non-English primary sources relied on certified translations, introducing potential interpretive variance. Furthermore, enforcement statistics are subject to reporting bias, as many regulatory actions are settled confidentially.

Discussion: The Convergence–Divergence Paradox

The findings reveal what might be termed a 'convergence–divergence paradox' in international crypto-asset regulation. At the level of general principles AML obligations, VASP registration, Travel Rule implementation, and beneficial ownership transparency there is considerable and growing convergence driven by FATF standard-setting. However, at the level of implementation detail licensing thresholds, stablecoin treatment, DeFi perimeter, consumer protection standards, and enforcement priorities substantial divergence persists and shows no clear trajectory toward harmonisation. This paradox has practical consequences for compliance actors and enforcement authorities alike[4]. A VASP operating across 15 jurisdictions must maintain 15 distinct compliance programmes that may impose contradictory obligations.

Simultaneously, enforcement agencies find that legal violations successfully prosecuted in one jurisdiction may be entirely lawful or simply beyond regulatory perimeter in another. The net effect is a compliance cost structure that disadvantages smaller, legitimate players relative to large

actors with resources to navigate complexity, while sophisticated illicit actors systematically exploit jurisdictional inconsistencies. Proportionality and Innovation: A recurring tension identified in the comparative analysis is the trade-off between regulatory stringency and innovation accommodation. Singapore and Switzerland have explicitly adopted 'innovation-friendly' regulatory postures, using regulatory sandboxes and no-action letters to permit controlled experimentation before imposing full compliance obligations. Critics of the EU's MiCA argue that its comprehensive ex-ante authorisation requirements impose disproportionate burdens on startups and may accelerate the migration of blockchain development activity to more permissive environments. The empirical evidence on this trade-off is mixed. Switzerland's regulatory sandbox produced several globally significant blockchain infrastructure projects but also hosted several projects subsequently associated with fraud and investor harm. Singapore's PSA licensing regime, while praised for its risk-tiering, had by end-2023 approved fewer than 30 digital payment token service licences from over 200 applicants a selectivity rate that some commentators interpret as regulatory capture of incumbents[7]. These observations suggest that proportionality in regulation is not simply a matter of threshold-setting but requires continuous calibration through adaptive mechanisms a finding that aligns with the emerging literature on 'agile regulation' in financial technology contexts.

Based on the foregoing analysis, this article proposes a four-pillar international supervisory architecture for crypto-asset circulation.

The first pillar harmonised minimum licensing standards would establish a FATF-endorsed framework of minimum licensing requirements for VASPs, modelled on the Basel Committee's minimum capital adequacy standards but adapted for the digital asset context. This would include mandatory CDD, transaction monitoring, and Travel Rule compliance as non-negotiable baseline obligations, while preserving national discretion on higher-tier requirements.

The second pillar automated cross-border information sharing would establish secure, interoperable technical infrastructure enabling near-real-time transmission of suspicious transaction alerts between national financial intelligence units. The Egmont Group's existing FIU.NET[2] network provides a template that could be augmented with blockchain analytics integration and common data standards like FINTRAC's virtual currency reporting format as a basis for international standardization.

The third pillar DeFi supervisory perimeter expansion would require jurisdictions to develop legal and technical frameworks capable of extending AML obligations to identifiable participants in DeFi ecosystems, including liquidity providers, governance token holders with administrative control, and front-end interface operators[3]. The EU's recent guidance on the liability of DeFi protocol developers offers an initial model, though significant legal and technical challenges remain.

The fourth pillar adaptive regulatory sandboxes with enforcement carve-outs would formalise the use of jurisdictional sandboxes not merely as innovation incubators but as supervised experimental environments where DeFi protocols, privacy-preserving compliance mechanisms like zero-knowledge KYC proofs, and novel supervisory tools can be tested against defined performance metrics before being incorporated into binding regulation. This approach acknowledges that the technological frontier of crypto - asset markets moves faster than conventional legislative cycles and that regulatory frameworks must embed mechanisms for continuous adaptation.

The FATF's revised Recommendation 15, adopted in 2019, extended AML/CFT obligations to VASPs by requiring countries to register or license these entities and subject them to the full suite of anti-money-laundering controls applicable to traditional financial institutions[1]. The 'Travel Rule' requiring VASPs to collect and transmit originator and beneficiary information for virtual asset transfers has emerged as the cornerstone of cross-border AML compliance, yet our analysis found significant implementation gaps[2]. Of the 42 enforcement cases examined, 31 (73.8%) involved failures in customer due diligence or transaction monitoring. In 19 cases (45.2%), VASPs had either failed to register with the relevant national authority or had continued operations after registration was denied or revoked. Analysis of case narratives identified three dominant violation patterns:deliberate onboarding of high-risk customers without enhanced due diligence, cited in 62% of cases, failure to file suspicious activity reports despite obvious transaction red flags, cited in 57% of cases; and exploitation of jurisdictional gaps by routing transactions through exchanges registered in non-FATF-compliant countries, cited in 38% of cases. The most significant enforcement actions in the sample involved Binance and Bitfinex. These cases collectively illustrate the systemic scale of compliance deficiencies among major crypto exchanges operating without adequate AML infrastructure[8].

Uzbekistan's model of crypto-asset regulation is a unique system located outside the traditional “permitting-restricting-prohibiting” classification. It develops on the basis of rapid and presidential-led policy decisions, aiming to develop the digital economy on the one hand, and carefully control the VASP sector on the other. The foundation of the system was laid in 2018 by a presidential decree recognizing crypto-assets as digital property. In 2020, the Uznex exchange was launched, and a policy of attracting foreign capital was implemented, primarily by providing services to non-residents. In 2019, a temporary ban on the purchase of cryptocurrency for residents was introduced, and the market was severely restricted.

In 2022, the regulator was reformed, the NAPP was established, and a special crypto-regulation system was introduced. Since 2023, residents have been able to trade in crypto only through locally licensed platforms. KYC, AML/CFT requirements, and prompt reporting obligations have been established for CASPs. The Uzbek model increases investment attractiveness through low tax rates, relatively cheap licensing, and preferences for foreign operators. At the same time, according to FATF assessments, although the legal framework of the system exists, some shortcomings in AML/CFT effectiveness and institutional capacity remain. Since 2024, controls have been tightened, and measures have been taken against unlicensed operators, including Binance. Additionally, the regulatory sandbox created in 2022 serves to pilot innovative blockchain and DeFi projects.

This comparative analysis of international crypto-asset regulation has demonstrated that significant progress has been achieved in establishing AML/CFT frameworks applicable to VASPs, driven largely by FATF standard-setting and the EU's MiCA Regulation. Blockchain analytics has emerged as a transformative supervisory tool, enabling regulators to conduct proactive on-chain surveillance that fundamentally shifts the detection paradigm from reactive reporting to prospective monitoring. Enforcement actions against major exchanges have established important precedents regarding the extra-territorial reach of national supervisory regimes including, most recently, NAPP's 2024 enforcement action against Binance in Uzbekistan.Notwithstanding this progress, critical structural vulnerabilities persist.

The DeFi sector remains substantially outside regulatory perimeters across all major jurisdictions. Cross-border supervisory cooperation mechanisms are inadequate to the speed and transnationality of crypto-asset transaction flows. Privacy-enhancing technologies challenge fundamental assumptions embedded in Travel Rule compliance architectures. And persistent jurisdictional arbitrage continues to concentrate regulatory risk offshore.The four-pillar architecture proposed in this article harmonised licensing minima, automated FIU information sharing, DeFi perimeter expansion, and adaptive regulatory sandboxes offers a coherent framework for addressing these vulnerabilities. Implementation will require sustained political will, substantial technical investment, and a degree of supranational legal integration that remains politically contested in several major jurisdictions.

However, the costs of inaction measured in laundered funds, defrauded investors, and eroded financial integrity substantially exceed the costs of coordinated regulatory reform.Future research should examine the distributional effects of increasingly stringent crypto-asset regulation on financial inclusion in emerging markets, where crypto-assets frequently perform genuine economic functions in under-banked populations [12]. The tension between global financial integrity standards and the inclusive potential of decentralised finance represents perhaps the defining regulatory challenge of the next decade.

References

1. Financial Action Task Force. (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF/OECD Publications.
2. Financial Action Task Force. (2021). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. FATF/OECD Publications.
3. Allen, J. G., Rauchs, M., Blandin, A., & Bear, K. (2020). Legal and regulatory considerations for digital assets. Cambridge Centre for Alternative Finance Working Paper.
4. Auer, R., & Claessens, S. (2022). Regulating cryptocurrencies: Assessing market reactions to regulatory announcements. BIS Quarterly Review, September 2022.
5. Chainalysis. (2024). The Chainalysis 2024 Crypto Crime Report. Chainalysis Inc.
6. De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.
7. Enrich, D. (2022). The anatomy of a crypto exchange collapse: Compliance failure at the intersection of KYC and market integrity. Yale Journal on Regulation, 39(2), 444–512.
8. Gruber, S. (2019). Trust, identity, and disclosure: Are Bitcoin exchanges the next virtual currency systems? Tulane Journal of Technology and Intellectual Property, 22, 1–57.
9. Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales, and cryptocurrencies under EU financial law. European Company and Financial Law Review, 15(4), 645–696.
10. International Monetary Fund. (2023). Regulating the Crypto Ecosystem: The Case for Comprehensive Approach. IMF Fintech Notes No. 2023/007.
11. Katsikas, D. (2023). Virtual asset service providers and the FATF Travel Rule: Compliance challenges and technical solutions. Journal of Financial Regulation, 9(1), 1–39.
12. Lannquist, A. (2022). Blockchain and financial inclusion: Regulating emerging markets' access to decentralised finance. World Bank Policy Research Working Paper No. 10145.