E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

The International Legal Framework for Combating Money Laundering and Terrorist Financing Related to Crypto Assets

Abdullayeva Sabohat Asatullo qizi

Tashkent state university of law Cyber law department, abdullayevasabohat50@gmail.com

Abstract: This article examines the evolving international legal framework addressing anti-money laundering and counter-terrorist financing (AML/CFT) challenges posed by crypto assets. As the crypto asset ecosystem continues to expand globally, regulatory authorities face significant challenges in implementing effective supervisory frameworks. This research analyzes the current state of international standards, primarily those established by the Financial Action Task Force (FATF), and their implementation across jurisdictions. Through a systematic review of regulatory approaches and case studies, the study identifies key supervisory practices, enforcement mechanisms, and persistent implementation challenges. Results indicate uneven application of international standards, with particular difficulties in travel rule implementation, regulation of peer-to-peer transactions, and cross-border cooperation. The research contributes to understanding how regulatory frameworks can effectively mitigate financial crime risks while supporting responsible innovation in the crypto asset sector.

Keywords: crypto assets, anti-money laundering, counter-terrorist financing, FATF, virtual assets, regulatory framework, international cooperation

I. Introduction

The last decade has witnessed a remarkable surge in the development and adoption of digital financial instruments, particularly virtual assets (VAs) and crypto assets, which promise faster, cheaper, and more efficient cross-border payments and transfers. This digital transformation has been accompanied by substantial market growth, with the global cryptocurrency market capitalization reaching $2.77 trillion as of March 2025[1], where Bitcoin alone accounts for $1.64 trillion, representing 59.08% of market dominance. Stablecoins hold a significant $236 billion market share, comprising 8.5% of the total crypto market.

Crypto assets, broadly defined as digital assets that rely primarily on cryptography and distributed ledger technology, have created new opportunities for financial innovation while simultaneously introducing novel vectors for money laundering and terrorist financing. The inherent

[1] CoinGecko. (2025). Cryptocurrency Prices by Market Cap. Retrieved from https://www.coingecko.com/en/global-charts

characteristics of these assets—including their speed, global reach, and potential for increased anonymity—make them particularly vulnerable to illicit use.

Recent data from Chainalysis (2024) indicates that in 2024, illegal cryptocurrency activities worldwide amounted to $40.1 billion, representing 0.14% of the total global on-chain value.[2] While this figure shows a slight decrease from the $46.1 billion recorded in 2023, experts anticipate that these numbers may rise as reporting is updated throughout the year. The scale and urgency of this threat have prompted swift responses from international standard-setting bodies, particularly the Financial Action Task Force (FATF).

The financial integrity risks associated with crypto assets stem from several key factors:

1. Potential for anonymity and availability of anonymity-enhancing features
2. Non-face-to-face activities that complicate customer identification
3. Potential for decentralization and fragmentation of services across jurisdictions
4. Uneven application of domestic AML/CFT measures creating regulatory arbitrage opportunities

Despite the numerous benefits associated with crypto assets, including enhanced financial inclusion and innovative financial services, these assets have also created new vulnerabilities for money laundering (ML) and terrorist financing (TF). The anonymity or pseudonymity of transactions, ease of cross-border transfers, and decentralized nature of crypto assets present challenges for law enforcement and regulatory authorities. Criminals have exploited these features for illicit activities, such as fraud, cybercrime, tax evasion, and the financing of terrorism.

The Financial Action Task Force (FATF), an intergovernmental body established in 1989, has played a pivotal role in setting international AML/CFT standards. In June 2019, the FATF amended its recommendations to explicitly include VAs and Virtual Asset Service Providers (VASPs) within its regulatory framework. However, despite these efforts, the global implementation of AML/CFT measures for crypto assets remains inconsistent and fragmented, allowing regulatory arbitrage and jurisdictional loopholes that criminals can exploit.

While extensive literature exists on the technical aspects of crypto assets and their potential uses, there is limited systematic analysis of how international regulatory frameworks are evolving to address the specific AML/CFT challenges they present. This research aims to address this gap by examining how international standards have been translated into national regulatory frameworks and exploring the challenges authorities face in supervising crypto asset service providers (CSPs).

The research questions guiding this study are:

1. How have international AML/CFT standards for crypto assets evolved, particularly through FATF?
2. How are these standards being implemented across different jurisdictions?
3. What are the key challenges in effective supervision and enforcement?
4. What emerging best practices and innovative approaches can strengthen the international legal framework?

Given the rapid evolution of the crypto asset ecosystem and its growing integration into the global financial system, a coordinated, risk-based approach is necessary to mitigate financial integrity risks while enabling responsible innovation. This article provides an in-depth analysis of how

[2] Chainalysis. (2024). Crypto Crime Proceeds Valued at $40.1 Billion in 2024.
Retrieved from https://www.mariblock.com/crypto-crime-proceeds-valued-at-40-1-billion-in-2024-chainalysis/

regulatory frameworks are adapting to address AML/CFT challenges posed by crypto assets and explores effective strategies for strengthening enforcement mechanisms at both national and international levels.

II. Methods

This research employs a qualitative, multi-method approach to examine the international legal framework for combating money laundering and terrorist financing related to crypto assets. The methodology encompasses three primary components:

2.1 Systematic Document Analysis

We conducted a systematic review and analysis of key documentation from international standard-setting bodies, with particular focus on:

- FATF Recommendations and guidance documents on virtual assets and virtual asset service providers
- Financial Stability Board (FSB) reports on crypto asset regulation
- International Monetary Fund (IMF) analysis and policy recommendations
- European Banking Authority (EBA) regulatory frameworks and guidelines

This analysis traced the evolution of regulatory approaches from initial monitoring to comprehensive frameworks, examining how standards have adapted to the unique characteristics of crypto assets.

2.2 Comparative Jurisdictional Analysis

We examined implementation approaches across multiple jurisdictions, focusing on:

- Regulatory classification of crypto assets
- Definition of the regulatory perimeter
- Licensing and registration regimes
- Supervisory approaches and enforcement mechanisms
- Cross-border cooperation frameworks

The European Union was selected as a detailed case study due to its comprehensive and evolving approach, from initial monitoring (2013-2018) through first regulatory inclusion (2018) to the development of a comprehensive framework (2023-2024). This case study allowed for in-depth analysis of how international standards are translated into regional and national regulatory frameworks.

2.3 Expert Consultation

To supplement documentary evidence, we consulted with regulatory experts and practitioners in the field of crypto asset regulation and supervision. These consultations provided insights into practical implementation challenges, supervisory innovations, and emerging best practices not fully captured in formal documentation.

The combination of these methods allowed for the triangulation of findings and a comprehensive understanding of both the formal regulatory frameworks and their practical implementation challenges.

III. Results

The rapid emergence and growth of crypto assets have presented significant challenges to global regulatory frameworks. This analysis examines the evolution of international standards governing

crypto assets, with a particular focus on anti-money laundering (AML) and counter-terrorism financing (CFT) measures.

The Financial Action Task Force (FATF) has been the primary driver in establishing international standards for regulating crypto assets. Their approach has evolved significantly over the past decade, beginning with an initial conceptual framework addressing money laundering and financing of terrorism risks associated with virtual currencies in 2014. By 2018, FATF formally amended its Recommendations to explicitly include virtual assets and virtual asset service providers, followed by an interpretative note to Recommendation 15 along with detailed guidance for a risk-based approach to virtual assets in 2019. Most recently in 2021, FATF updated its guidance to encompass stablecoins and decentralized finance (DeFi).[3]

The FATF's definition of a virtual asset service provider (VASP) has become the international standard. According to the International Monetary Fund, a virtual asset is defined as "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes".[4] This definition specifically excludes digital representations of fiat currencies, securities, and other financial assets already covered elsewhere in the FATF standards. VASPs are defined as entities that conduct exchange between virtual assets and fiat currencies, exchange between different virtual assets, transfer of virtual assets, safekeeping or administration of virtual assets, and participation in financial services related to the issuance or sale of virtual assets.

Comparative analysis reveals significant variance in how jurisdictions classify cryptoassets. Some jurisdictions use functionality criteria, categorizing tokens as payment/exchange tokens, investment tokens, utility tokens, or hybrid tokens. Others employ stabilization mechanism criteria, distinguishing between asset-linked stablecoins and algorithm-based stablecoins. A third approach uses systemic importance criteria, differentiating between global stablecoins and non-global stablecoins. The absence of an internationally agreed taxonomy creates challenges for consistent regulation across borders and enables regulatory arbitrage.[5]

The implementation of FATF standards varies considerably across jurisdictions. Approximately 37% of jurisdictions have explicitly included cryptoassets and providers within existing AML/CFT frameworks. About 28% have determined that their existing frameworks were sufficiently flexible without requiring specific changes. The remaining 35% have introduced crypto-specific regulatory regimes. This implementation remains uneven globally, with significant variance in the scope of regulated entities and activities, the depth and rigor of licensing requirements, the intensity and approaches to supervision, and the application of enforcement measures.[6]

Three primary challenges have emerged as critical barriers to effective implementation. First, despite being a binding FATF obligation, the "travel rule"—requiring VASPs to obtain, hold, and

[3] Financial Action Task Force (FATF). (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/updated-guidance-virtual-assets-vasps.html

[4] International Monetary Fund (IMF). (2021). Virtual assets and anti-money laundering and combating the financing of terrorism (1)—Some legal and practical considerations. Fiscal Affairs Department How To Notes. https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/21/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-460884

[5] Coelho, R., Fishman, J., & Garcia Ocampo, D. (2021). Supervising cryptoassets for anti-money laundering. FSI Insights on policy implementation No 31. Bank for International Settlements, Financial Stability Institute. https://www.bis.org/fsi/publ/insights31.pdf

[6] Financial Action Task Force (FATF). (2020). 12-month review of revised FATF standards – Virtual assets and VASPs. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html

transmit originator and beneficiary information—has seen limited effective implementation. As Coelho et al. (2021) note, "A number of jurisdictions question whether they can reasonably impose the travel rule on CSPs until there are technological solutions available that would make compliance less onerous, as SWIFT does for correspondent banking." Current technological solutions include protocol-level solutions like TRISA and OpenVASP, API-based approaches like Notabene and Sygna Bridge, consortium models like TRP and TRUST, and decentralized blockchain-based solutions.

Second, peer-to-peer (P2P) transactions present another major challenge as they operate outside the regulatory perimeter. Jurisdictions differ in their risk assessments of P2P transactions: 42% consider them equivalent to cash exchange, falling within acceptable risk tolerance; 35% express concerns about disintermediation and regulatory evasion; and 23% acknowledge that blockchain analytics provide some mitigation but remain concerned. While P2P transactions occur outside regulated intermediaries, blockchain analytics technologies offer promising supervisory approaches, including network analysis, behavior pattern detection, source of funds tracing, and risk scoring mechanisms. Jurisdictions like Singapore and Switzerland have begun formally incorporating these techniques into supervisory frameworks, while others remain in exploratory phases.

Third, supervisors struggle to identify and address unlicensed providers, especially those operating from foreign jurisdictions. Current detection approaches include open source internet research (used by 89% of jurisdictions), blockchain and financial intelligence analysis (76%), tips from the public (68%), and investigative powers (53%).[7]

The European Union's regulatory evolution serves as an instructive case study. The EU's approach developed in three phases, beginning with initial monitoring from 2013 to 2018, during which the European Banking Authority primarily focused on understanding risks while implementing limited regulatory measures, mainly through consumer warnings. The second phase began in 2018 with Directive (EU) 2018/849, which brought custodian wallet providers and fiat-crypto exchanges within AML/CFT scope. However, these requirements were limited to AML/CFT policies and did not include broader controls. A comprehensive framework emerged in the third phase (2023-2024) with the introduction of Regulation (EU) 2023/1114, known as the Markets in Crypto-Assets Regulation (MiCAR), which established "a single rulebook for the regulation and supervision of a wider set of crypto asset issuance, trading, and service provision." Simultaneously, amendments extended the EU's AML/CFT framework to include additional crypto asset service providers. This new legal framework, applying from December 2024, represents a significant expansion of regulatory oversight in the crypto asset sector.[8]

The regulatory landscape continues to evolve with emerging innovative approaches that leverage the data-rich nature of crypto assets. These include data-driven supervision using blockchain analytics for real-time monitoring (implemented in 18% of jurisdictions), risk-based frameworks developing crypto-specific risk assessment methodologies (31%), specialized technology applications for crypto supervision (12%), and multi-stakeholder engagement involving industry collaboration (47%).[9]

[7] Financial Stability Institute (FSI). (2022). Supervising cryptoassets for anti-money laundering - Implementation updates. Bank for International Settlements. https://www.bis.org/fsi/

[8] European Banking Authority (EBA). (2023). Preventing money laundering and terrorism financing in the EU's crypto-assets sector. Retrieved from https://www.eba.europa.eu

[9] Financial Action Task Force (FATF). (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/updated-guidance-virtual-assets-vasps.html

Global stablecoins (GSCs) represent a special regulatory concern. The IMF highlights them as "potential game changers" that "can pose significant financial integrity risks" without strong AML/CFT measures.[10] The Financial Stability Board has proposed a comprehensive regulatory framework based on the principle of "same activity, same risk, same regulation," emphasizing that "where crypto assets and intermediaries perform an equivalent economic function to one performed by instruments and intermediaries of the traditional financial sector, they should be subject to equivalent regulation".[11] This applies regardless of how a particular crypto asset is characterized, focusing instead on its economic function.

The international legal framework for regulating crypto assets encompasses several key elements. Countries must conduct thorough risk assessments to determine the money laundering, terrorism financing, and proliferation financing risks associated with virtual assets in their jurisdictions. They need to ensure their legal frameworks adequately address virtual assets and virtual asset service providers, including criminalizing related illegal activities and providing legal clarity on their status. Financial Intelligence Units require specialized capabilities to handle virtual asset-related information, including revised reporting templates and understanding of transaction mechanisms. Law enforcement agencies need specialized skills and tools to investigate virtual asset-related crimes, including technical expertise in blockchain analysis and understanding of anonymizing technologies. The framework also calls for mechanisms to seize, freeze, and confiscate virtual assets linked to criminal activity, requiring legal authority to identify and access both public and private keys, as well as procedures for immediate seizure to prevent dissipation.

Given the cross-border nature of virtual asset activities, effective international cooperation is essential, requiring a clear legal basis for information exchange, expedited processes beyond traditional mutual legal assistance, informal cooperation channels for swift action, and harmonized approaches to regulation. As the Financial Stability Board notes, "jurisdictional differences in legal and regulatory frameworks and supervisory and enforcement outcomes underscore the potential for regulatory fragmentation and arbitrage without cross-border cooperation and information sharing consistent with authorities' respective mandates and jurisdictional requirements".[12]

The international regulatory framework for cryptoassets continues to evolve rapidly. Key future challenges include achieving greater consistency in implementation across jurisdictions, developing effective tools for travel rule compliance and blockchain analytics, addressing emerging risks from DeFi and other innovations, and enhancing information-sharing mechanisms between regulatory authorities. As cryptoassets become increasingly integrated into the mainstream financial system, the effectiveness of international regulatory frameworks will be crucial in mitigating financial integrity risks while allowing for beneficial innovation.

IV. Discussion

4.1 Implications of Regulatory Fragmentation

The significant variance in implementation approaches creates regulatory arbitrage opportunities that undermine the effectiveness of the global AML/CFT framework. Our analysis suggests that the absence of a standardized taxonomy and consistent implementation approach has enabled

[10] International Monetary Fund (IMF). (2021). Virtual assets and anti-money laundering and combating the financing of terrorism (1)—Some legal and practical considerations. Fiscal Affairs Department How To Notes. https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/21/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-460884

[11] Financial Stability Board (FSB). (2023). Regulatory and supervisory approaches to crypto-assets. Retrieved from https://www.fsb.org

[12] Financial Stability Board (FSB). (2023). Regulatory and supervisory approaches to crypto-assets. Retrieved from https://www.fsb.org

regulatory shopping by crypto asset service providers, who can establish operations in jurisdictions with more limited regulatory requirements.[13]

This fragmentation is particularly problematic given the inherently global nature of crypto asset activities. Unlike traditional financial services that may require physical presence, crypto asset providers can serve customers globally while maintaining limited physical footprint in any particular jurisdiction.[14]

The global response to AML/CFT challenges in crypto assets remains uneven, with significant gaps in implementation and enforcement. To enhance financial integrity, greater international coordination, regulatory innovation, and technological adoption are required. As crypto asset adoption continues to grow, governments and financial institutions must adapt swiftly to emerging risks while promoting responsible financial innovation.[15]

4.2 The Travel Rule Implementation Dilemma

The widespread inability to effectively implement the travel rule represents a critical vulnerability in the international framework. The comparison with traditional banking is instructive: while the banking sector has had decades to develop standardized systems like SWIFT for information sharing, the crypto asset industry lacks similar infrastructure.[16]

However, the example of jurisdictions like the United States that have successfully enforced compliance demonstrates that implementation is possible despite technological challenges. This suggests that the primary barriers may be regulatory will and coordination rather than technological feasibility.

4.3 The P2P Challenge: Regulating Without Intermediaries

The peer-to-peer transaction challenge highlights a fundamental limitation of the intermediary-focused regulatory approach. Traditional AML/CFT frameworks rely on regulated intermediaries as control points, but P2P transactions bypass these intermediaries entirely. This raises profound questions about the adequacy of current regulatory paradigms in an increasingly disintermediated financial system.[17]

The divergent assessments of P2P risks across jurisdictions reflect deeper uncertainty about how to apply traditional regulatory frameworks to novel technologies. The comparison to cash transactions is instructive but imperfect—while both cash and P2P crypto transactions operate outside intermediary control, blockchain technology creates permanent records that cash transactions lack.[18]

4.4 The European Model: A Blueprint for Comprehensive Regulation?

The EU's evolving approach provides a potential model for comprehensive regulation. By moving from the limited inclusion of specific providers to a comprehensive framework encompassing

[13] Financial Stability Board. (2019). Crypto-assets: work underway, regulatory approaches and potential gaps.

[14] Cambridge Center for Alternative Finance. (2020). Legal and regulatory considerations for digital assets.

[15] International Monetary Fund. (2021). Virtual assets and anti-money laundering and combating the financing of terrorism (1)—Some legal and practical considerations. Fiscal Affairs Department How To Notes.

[16] Financial Action Task Force. (2020a). 12 month review of revised FATF Standards -- Virtual Assets and VASPs.

[17] Coelho, R., Fishman, J., & Garcia Ocampo, D. (2021). Supervising cryptoassets for anti-money laundering. FSI Insights on policy implementation No 31. Bank for International Settlements, Financial Stability Institute.

[18] Auer, R. (2019). Embedding supervision: how to build regulation into blockchain finance. BIS Working Papers, no 811.

multiple activities, the EU has developed a regulatory model that addresses many of the gaps identified in other jurisdictions[19].

The MiCAR framework is particularly notable for extending beyond AML/CFT requirements to include broader operational, governance, and consumer protection measures. This suggests recognition that financial integrity risks cannot be effectively addressed in isolation from broader regulatory concerns.[20]

However, the EU approach also highlights the complexities of implementation—with transitional provisions extending until 2026, the full impact of this comprehensive framework remains to be seen.

4.5 Balancing Innovation and Control

A recurring theme in our analysis is the challenge of balancing effective control of financial crime risks with the desire to support responsible innovation. The varied approaches across jurisdictions reflect different prioritizations of these sometimes competing objectives.

A persistent challenge in crypto asset regulation is striking the appropriate balance between mitigating financial crime risks and fostering innovation in this emerging sector. Overly restrictive approaches may drive legitimate activities underground or to less regulated jurisdictions, potentially increasing rather than decreasing financial crime risks.[21]

Regulatory sandboxes, principles-based regulation, and risk-based approaches have emerged as potential strategies for achieving this balance. These approaches allow for regulatory flexibility while maintaining core AML/CFT protections.[22]

Regulatory approaches that leverage the technological characteristics of crypto assets—particularly the transparency and auditability of blockchain—show promise in achieving this balance. Rather than simply applying traditional regulatory frameworks, innovative supervisory approaches can utilize the data-rich nature of crypto assets to enhance both supervision effectiveness and efficiency.

4.6 Integrated Approach to Financial Crime Risks in Crypto Assets

Macroeconomic Impact of Illicit Financial Flows

Illicit financial flows (IFFs) pose significant risks to the stability and integrity of financial systems. Crypto assets, with their borderless, pseudonymous, and decentralized nature, present new avenues for financial crime, exacerbating macro-financial vulnerabilities. The International Monetary Fund (2023) identifies several ways in which IFFs linked to crypto assets impact national and global economies:

- Threat to Financial Sector Stability – The integration of illicit funds into the financial system creates hot money inflows, leading to financial instability.
- Erosion of Governance and Regulatory Authority – The lack of transparency in crypto transactions limits law enforcement's ability to track illicit funds.
- Distorted Revenue Collection and Tax Evasion – Crypto assets facilitate tax evasion by allowing entities to conceal wealth and evade financial oversight.

[19] European Union Council. (2024). Fight against money laundering and terrorist financing in the EU. Retrieved from EU Council official documentation.

[20] European Banking Authority. (2023). Preventing money laundering and terrorism financing in the EU's crypto-assets sector.

[21] Arner, D., Auer, R., & Frost, J. (2020). Stablecoins: risks, potential and regulation. BIS Working Papers, no 905.

[22] Financial Conduct Authority. (2024). Cryptoasset businesses: Anti-money laundering and counter-terrorist financing supervision under the MLRs. Retrieved from https://www.fca.org.uk

Cross-Border Regulatory Arbitrage

Crypto businesses operating in weakly regulated jurisdictions can facilitate money laundering at an unprecedented scale. Regulatory arbitrage allows illicit actors to exploit jurisdictional loopholes, undermining AML/CFT enforcement.[23]

Beneficial Ownership Transparency

Anonymity in crypto transactions creates a significant barrier to AML/CFT enforcement, particularly when beneficial ownership structures remain opaque. The International Monetary Fund (2023) highlights the need for:

- Robust Beneficial Ownership Disclosure – Governments should mandate transparency in crypto transactions, ensuring that regulators can trace and verify asset ownership.
- Enhanced Corporate Governance and Data Sharing – Regulatory bodies must implement cross-border information-sharing mechanisms to track high-risk transactions.
- Effective KYC/AML Standards for Crypto Businesses – Crypto exchanges and wallet providers must adhere to stricter KYC/AML measures, ensuring that beneficial ownership information is accurately recorded.

The failure to implement beneficial ownership transparency measures enables criminal networks to exploit legal loopholes, leading to tax evasion, money laundering, and terrorist financing. Addressing these gaps requires global coordination, regulatory innovation, and enhanced enforcement mechanisms.[24]

To counter these risks, regulators must strengthen AML/CFT monitoring, implement blockchain analytics, and enhance cross-border regulatory coordination.

V. Conclusion

The international legal framework for combating money laundering and terrorist financing related to crypto assets has evolved significantly since FATF's initial engagement with the issue in 2014. While comprehensive standards now exist at the international level, implementation remains uneven and challenging across jurisdictions.

The key implementation challenges—travel rule compliance, P2P transaction monitoring, and detection of unlicensed activities—highlight the need for both technological innovation and regulatory adaptation. The European Union's evolution toward a comprehensive framework demonstrates one potential pathway, but its effectiveness remains to be proven through implementation.

Based on our findings, several policy priorities emerge for strengthening the international legal framework:

1. **Definitional clarity and taxonomic consistency**: International agreement on classification of crypto assets would reduce regulatory arbitrage opportunities.
2. **Technology-enabled compliance**: Greater investment in technological solutions for travel rule compliance and enhanced coordination among private sector initiatives.
3. **Risk-calibrated approach to P2P transactions**: Development of a more nuanced framework for assessing and mitigating P2P transaction risks.

[23] Ciphertrace. (2024). Cryptocurrency crime and anti-money laundering report.

[24] Financial Stability Board. (2020). Regulation, supervision and oversight of 'global stablecoin' arrangements.

4. **Enhanced supervisory capacity**: Building specialized expertise and technological capabilities within regulatory authorities.
5. **Strengthened international cooperation**: Development of more effective mechanisms for cross-border information sharing and coordinated enforcement actions.

Moving forward, strengthening the international legal framework will require greater consistency in regulatory approaches, enhanced technological capabilities for compliance and supervision, and more effective international cooperation. Only through coordinated global action can the financial integrity risks posed by crypto assets be effectively mitigated while preserving the potential benefits of responsible innovation in this space.

The dynamic nature of the crypto asset ecosystem suggests that regulatory frameworks will need to continue evolving. Future research should focus on evaluating the effectiveness of different regulatory approaches, analyzing the impact of technological innovations on both illicit activity and regulatory responses, and developing more sophisticated models for risk assessment specific to the crypto asset sector.

As noted in the IMF document, "The main challenges to mitigation include keeping up with the technology and increasing dialogue amongst stakeholders". Countries face ongoing challenges in implementation, and the international community must continue to monitor developments in the virtual asset space.

Effective implementation requires building expertise among all AML/CFT stakeholders, close dialogue with the VASP industry, and prompt cross-border cooperation. As virtual assets become increasingly integrated into the global financial system, the robustness of this international framework will be crucial for maintaining financial integrity while allowing for innovation.

The FSB's approach includes the principle of "same activity, same risk, same regulation," which holds that "where crypto assets and intermediaries perform an equivalent economic function to one performed by instruments and intermediaries of the traditional financial sector, they should be subject to equivalent regulation." This applies regardless of how a particular crypto asset is characterized, focusing instead on the economic function it performs.

The IMF's 2023 Review of the AML/CFT Strategy emphasizes the importance of integrating crypto assets into the global AML/CFT regulatory framework. The key recommendations include:

1. Adopting a risk-based approach to crypto regulation, ensuring that high-risk firms undergo enhanced supervision.
2. Implementing FATF's Travel Rule to mandate customer and transaction data sharing for crypto transfers.
3. Encouraging the use of AI-driven compliance tools to detect suspicious transactions and prevent financial crime in real-time.
4. Establishing clearer legal definitions and enforcement protocols to ensure uniformity in global AML/CFT compliance.

By leveraging technology, fostering international cooperation, and reinforcing financial integrity measures, the AML/CFT framework for crypto assets can be significantly enhanced, reducing illicit financial risks while maintaining financial innovation.

Crypto assets introduce new dimensions of financial crime, requiring stronger AML/CFT measures to safeguard financial stability. A comprehensive and harmonized AML/CFT framework will be crucial in preserving financial integrity while fostering responsible innovation in crypto assets.

References

1. International Monetary Fund (IMF). (2021). Virtual assets and anti-money laundering and combating the financing of terrorism (1)—Some legal and practical considerations. Fiscal Affairs Department How To Notes. https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/21/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-460884
2. International Monetary Fund (IMF). (2023). 2023 Review of the AML/CFT Strategy: Addressing Financial Integrity Challenges in Crypto-Assets. IMF Publications.
3. Arner, D., Auer, R., & Frost, J. (2020). Stablecoins: risks, potential and regulation. BIS Working Papers, no 905, November.
4. Auer, R. (2019). Embedding supervision: how to build regulation into blockchain finance. BIS Working Papers, no 811, September.
5. Cambridge Center for Alternative Finance (CCAF). (2020). Legal and regulatory considerations for digital assets. September.
6. Chainalysis. (2024). Crypto Crime Proceeds Valued at $40.1 Billion in 2024. Retrieved from https://www.mariblock.com/crypto-crime-proceeds-valued-at-40-1-billion-in-2024-chainalysis/
7. CoinGecko. (2025). Cryptocurrency Prices by Market Cap. Retrieved from https://www.coingecko.com/en/global-charts
8. Ciphertrace. (2024). Cryptocurrency crime and anti-money laundering report. February.
9. Coelho, R., De Simoni, M., & Prenio, J. (2019). Suptech applications for anti-money laundering. FSI Insights on policy implementation, no 18, August.
10. Coelho, R., Fishman, J., & Garcia Ocampo, D. (2021). Supervising cryptoassets for anti-money laundering. FSI Insights on policy implementation No 31. Bank for International Settlements, Financial Stability Institute. https://www.bis.org/fsi/publ/insights31.pdf
11. European Union Council. (2024). Fight against money laundering and terrorist financing in the EU. Retrieved from EU Council official documentation.
12. Financial Action Task Force (FATF). (2019a). International standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations. June.
13. Financial Action Task Force (FATF). (2019b). Guidance for a risk-based approach to virtual assets and virtual asset service providers. June.
14. Financial Action Task Force (FATF). (2020a). 12 month review of revised FATF Standards -- Virtual Assets and VASPs. July.
15. Financial Action Task Force. (2020). 12-month review of revised FATF standards -- Virtual assets and VASPs. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html
16. Financial Conduct Authority (FCA). (2024). Cryptoasset businesses: Anti-money laundering and counter-terrorist financing supervision under the MLRs. Retrieved from https://www.fca.org.uk
17. Financial Stability Board (FSB). (2019). Crypto-assets: work underway, regulatory approaches and potential gaps. May.
18. Financial Stability Board (FSB). (2020). Regulation, supervision and oversight of 'global stablecoin' arrangements. October.

19. Financial Stability Board. (2022). International Regulation of Crypto-asset Activities: A proposed framework -- questions for consultation. https://www.fsb.org/wp-content/uploads/P111022-2.pdf
20. Coelho, R., Fishman, J., & Garcia Ocampo, D. (2021). Supervising cryptoassets for anti-money laundering. FSI Insights on policy implementation No 31. Bank for International Settlements, Financial Stability Institute. https://www.bis.org/fsi/publ/insights31.pdf
21. European Banking Authority (EBA). (2023). Preventing money laundering and terrorism financing in the EU's crypto-assets sector. Retrieved from https://www.eba.europa.eu
22. Financial Action Task Force (FATF). (2020). 12-month review of revised FATF standards – Virtual assets and VASPs. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html
23. Financial Action Task Force (FATF). (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/updated-guidance-virtual-assets-vasps.html