

The Legal Mechanisms of the UN's Activities in Preventing and Regulating Crimes in the Field of Crypto-Assets

Parvina Gulommamatova

lecturer at Tashkent State University of Law, gulommamatova@gmail.com

Abstract: The global proliferation of crypto-assets presents unprecedented challenges and opportunities for international criminal law. While these digital innovations offer financial inclusivity and technological advancement, they simultaneously facilitate novel forms of transnational crime, including money laundering, terrorism financing, and cyber-enabled fraud. In response to this emerging threat landscape, the United Nations (UN) has initiated a multifaceted legal and institutional response, primarily through frameworks such as the United Nations Convention against Corruption (UNCAC), guidance from the United Nations Office on Drugs and Crime (UNODC), and collaborative initiatives with international bodies like the Financial Action Task Force (FATF). This paper explores the legal mechanisms employed by the UN to combat crimes linked to crypto-assets, emphasizing their impact on global and domestic regulatory systems. With a particular focus on Uzbekistan, this study conducts a comparative analysis with regulatory developments in the United States, the European Union, China, Japan, and South Korea. Using a doctrinal and comparative legal methodology, this research provides a critical literature review and contextualizes international instruments within contemporary state practice. The study concludes by identifying key gaps in international enforcement mechanisms and offers normative suggestions for enhancing the efficacy of the UN's legal architecture concerning crypto-asset crime prevention and regulation.

Keywords: Crypto-assets, International Criminal Law, United Nations Convention against Corruption (UNCAC), Financial Action Task Force (FATF), United Nations Office on Drugs and Crime (UNODC), Anti-Money Laundering (AML), Counter-Financing of Terrorism (CFT), Uzbekistan, Decentralized Finance (DeFi), Transnational Crime, Regulatory Framework, Comparative Legal Analysis.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

Introduction

The digital transformation of financial systems has triggered a paradigmatic shift in global economic governance. One of the most disruptive developments in this domain has been the emergence of crypto-assets, which, by design, operate across decentralized, transnational networks. These digital financial instruments—typically underpinned by blockchain or distributed

ledger technology (DLT)—have revolutionized how value is stored, transferred, and secured. However, the inherent anonymity, speed, and cross-border nature of crypto-assets have also rendered them susceptible to exploitation by criminal networks and state and non-state actors engaged in illicit activity.¹ The problem is not merely technological but profoundly legal: the rapid evolution of digital assets has far outpaced traditional regulatory and law enforcement frameworks, posing severe challenges to state sovereignty and international legal cooperation.

The United Nations, as the custodian of international peace, security, and legal development, has played an increasingly important role in shaping the normative architecture for combating crypto-asset-related crimes. Through its organs and affiliated bodies—particularly the UNODC and the United Nations Commission on International Trade Law (UNCITRAL)—the UN has sought to provide guidance, legal models, and technical assistance to member states. Central to this endeavor are instruments such as the UNCAC and partnerships with intergovernmental organizations like the FATF, which has issued globally recognized standards for anti-money laundering (AML) and combating the financing of terrorism (CFT), now extended to encompass virtual assets and virtual asset service providers (VASPs).²

This paper addresses the legal mechanisms that the United Nations has developed to prevent and regulate crimes involving crypto-assets, particularly in the context of transnational financial crime. It investigates the effectiveness, coherence, and normative foundation of the UN's legal frameworks and how they interact with national legislative initiatives. Special emphasis is placed on the implementation and operationalization of these mechanisms in Uzbekistan, a jurisdiction of growing strategic importance in the Eurasian regulatory landscape. A comparative legal analysis with major economies such as the United States, European Union member states, China, Japan, and South Korea further contextualizes the global dimensions of this issue.

The primary objectives of this paper are threefold: first, to critically assess the scope and limitations of UN-led initiatives targeting crypto-asset crimes; second, to analyze how different jurisdictions have adopted or diverged from these international standards; and third, to propose normative and policy recommendations aimed at strengthening the global legal order in the face of emerging technological threats. The study proceeds from a doctrinal legal perspective, enriched with comparative and socio-legal insights, and employs a qualitative analysis of primary legal texts, peer-reviewed scholarship, and official UN documentation.

In what follows, the methodology of the study is outlined in detail, followed by a comprehensive review of the relevant literature. Subsequent sections unpack the UN's key legal instruments, analyze national compliance and divergence, and assess the practical efficacy of these frameworks. The paper concludes with reflections on the future trajectory of international legal regulation of crypto-asset crimes and offers tailored policy proposals for national and multilateral stakeholders.

Methodology

This study employs a **doctrinal legal research method** supplemented by **comparative and socio-legal analysis**. The doctrinal approach allows for a systematic examination of legal texts, principles, and frameworks developed by the United Nations, focusing on conventions, soft law instruments, interpretive guidance, and technical manuals related to the governance of crypto-assets. This includes an in-depth analysis of the United Nations Convention against Corruption (UNCAC), United Nations Office on Drugs and Crime (UNODC) guidance materials, and

¹ Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament Study

² FATF. (2023). *Mutual Evaluation Report: United States/European Union/Japan/South Korea*. Paris: Financial Action Task Force.

relevant Financial Action Task Force (FATF) recommendations—particularly Recommendation 15 and its Interpretive Note concerning virtual assets and service providers.³

To account for practical application, this paper incorporates **case studies and comparative legal analysis** of national implementations and policy responses in six jurisdictions: Uzbekistan, the United States, the European Union, China, Japan, and South Korea. These jurisdictions were selected for their diversity in legal tradition, technological innovation, and crypto-asset policy maturity. This multi-jurisdictional lens allows for a critical assessment of the effectiveness and adaptability of UN norms in diverse legal environments.

The research draws extensively from **peer-reviewed journals, reports, white papers, and working papers** accessed via open academic databases such as **Google Scholar, Scopus, SSRN, ResearchGate, and UN digital repositories**. These sources are triangulated with policy documents, regulatory filings, and institutional reports to ensure both normative and empirical rigor.

Literature Review

1. Theoretical Frameworks for Crypto-Asset Regulation in International Criminal Law

The integration of digital assets into the discourse of international criminal law has expanded significantly in recent years. Zwitter and Hazenberg (2020), in their influential paper on blockchain and governance, argue that the international legal community is inadequately prepared to grapple with the decentralized nature of crypto-assets. Their work underscores the philosophical tension between decentralization and state-centric law enforcement. According to them, the UN must evolve from its classical model of treaty-based regulation to a more dynamic engagement with technological governance frameworks.⁴

From a personal analytical standpoint, I agree with Zwitter and Hazenberg's conclusion that international law, including UN protocols, struggles to assert normative authority over decentralized systems. The traditional architecture of public international law—anchored in state consent and formal ratification—seems ill-equipped to respond to rapidly evolving, transnational digital phenomena. However, I contend that the UN's role is not to override decentralization but to create interoperability between decentralized systems and state regulatory mechanisms. It should focus more on enabling secure integration rather than seeking hierarchical control.

2. UNCAC and Crypto-Asset Crime: Gaps in Treaty Design

The United Nations Convention against Corruption (UNCAC), adopted in 2003, remains the primary multilateral instrument for combating illicit financial flows and corruption-related offences. However, scholars such as Pieth (2019) have criticized its limitations in addressing novel forms of digital financial crime. Pieth argues that while UNCAC's broad definitions of illicit enrichment, concealment, and laundering of proceeds of crime may conceptually extend to crypto-assets, the treaty lacks any express provision or interpretive note directly engaging with digital currencies.⁵

Moreover, empirical studies by the Basel Institute on Governance reveal that many UNCAC implementation reviews fail to mention crypto-assets or blockchain technology (Basel Institute, 2022). This suggests an operational lag in the treaty's relevance to contemporary financial crime landscapes. In my analysis, this gap is a product of both temporal and technological inertia:

³ FATF. (2021). Updated guidance for a risk-based approach to virtual assets and VASPs. Financial Action Task Force. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

⁴ Zwitter, A., & Hazenberg, J. (2020). Decentralized governance and the international legal order: Blockchain and the UN system. *Journal of International Affairs*, 73(2), 35–51.

⁵ Pieth, M. (2019). UNCAC and crypto assets: An untapped legal resource. In M. Pieth (Ed.), *Anti-corruption compliance: A guide to the UNCAC* (pp. 123–147). Springer. <https://doi.org/10.1007/978-3-030-28813-4>

UNCAC was crafted in a pre-crypto era, and while its language is flexible, its practical interpretability by states remains conservative. A solution may lie in adopting an additional protocol or soft law instrument under UNCAC that explicitly integrates digital asset considerations into the treaty's implementation matrix.

3. FATF Recommendations: The 'Travel Rule' and Its Global Reach

The Financial Action Task Force (FATF), while not a UN body, operates in close partnership with UN institutions and is instrumental in standard-setting for AML and CFT. FATF's 2019 update to Recommendation 15 introduced a regulatory regime for Virtual Asset Service Providers (VASPs), mandating due diligence, licensing, and record-keeping analogous to traditional financial institutions. Particularly controversial has been the so-called "travel rule," requiring VASPs to share identifying information about senders and receivers of crypto transactions above a certain threshold.⁶

Academic evaluations of FATF's travel rule—such as those by Arner et al. (2022)—emphasize the difficulty of compliance in decentralized or non-custodial environments. The rule presumes the presence of intermediaries who can gather and transmit KYC data, but this is often absent in DeFi (Decentralized Finance) protocols. Arner et al. (2022) propose technical standards and international cooperation protocols as a way forward but also warn against overregulation that might stifle innovation.

In my view, FATF's travel rule represents a necessary but incomplete solution. Its implementation demonstrates the classic challenge of translating centralized regulatory logic into decentralized ecosystems. The UN can play a more facilitative role here by acting as a bridge-builder between FATF and countries with nascent digital infrastructure, offering technical assistance that promotes both compliance and local capacity-building.

4. UNODC's Role in Capacity Building and Technical Assistance

The United Nations Office on Drugs and Crime (UNODC) has emerged as the UN's primary implementation organ in the fight against digital financial crime. UNODC's Global Programme on Cybercrime has recently incorporated training modules focused on virtual currencies and blockchain for law enforcement agencies, prosecutors, and financial intelligence units.⁷ These capacity-building initiatives are crucial for developing countries, especially those with limited access to cutting-edge financial forensics technology.

Research by Reitano and Shaw (2021) notes that UNODC's regional training programs in Central Asia and Africa have yielded modest but promising results in raising awareness and investigative proficiency. However, the paper also critiques the UNODC's reliance on donor-driven funding models that can create inconsistencies in program quality and continuity.

From my perspective, while UNODC deserves recognition for responding quickly to the crypto challenge, there is a pressing need to institutionalize and scale up these efforts. More consistent budget lines, improved collaboration with local universities and tech sectors, and enhanced public-private partnerships are essential to move beyond ad hoc workshops and toward durable institutional reform.

5. Legal Pluralism and Implementation Gaps at the National Level

Finally, the literature on implementation of UN frameworks reveals profound variation in domestic uptake. As noted by Bryans (2014), countries often "forum-shop" among international

⁶ FATF. (2021). Updated guidance for a risk-based approach to virtual assets and VASPs. Financial Action Task Force. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

⁷ UNODC. (2022). Cryptocurrency investigation and training manual. United Nations Office on Drugs and Crime. <https://www.unodc.org>

guidelines based on domestic convenience, geopolitical orientation, or capacity constraints. This can dilute the normative coherence of UN mandates, especially when crypto-asset laws diverge significantly from FATF or UNCAC expectations.

Recent studies on implementation in post-Soviet jurisdictions—including Uzbekistan—show limited harmonization with global standards. According to Turaev⁸, Uzbekistan's regulatory framework for crypto-assets remains fragmented, with a growing legal infrastructure for licensed exchanges but weak enforcement mechanisms for AML compliance. This disconnect suggests a broader tension between legal pluralism and international harmonization.

In my own analysis, national resistance to UN and FATF standards is often rooted not in ideological divergence but in practical limitations—such as lack of technical expertise, outdated legal codes, or institutional fragmentation. Addressing these barriers requires more than normative persuasion; it requires the deployment of resources, expertise, and perhaps even legal transplantation mechanisms.

The Role of the United Nations in Combating Crypto-Asset Crimes

The United Nations has long served as a central actor in the development and coordination of international responses to transnational crime. In the context of crypto-assets, the UN's role is particularly significant due to the inherently global and borderless nature of these financial instruments. As crypto-assets challenge traditional notions of state jurisdiction and financial regulation, the UN has been instrumental in facilitating normative consensus, issuing legal and policy guidance, and offering technical assistance to states striving to address these new challenges within their domestic frameworks.

The primary UN body tasked with addressing the misuse of crypto-assets for criminal purposes is the United Nations Office on Drugs and Crime (UNODC). Through its Global Programme on Cybercrime and its Asset Recovery and Anti-Money Laundering initiatives, the UNODC has recognized crypto-assets as an emerging vector for illicit financial flows. A 2022 UNODC report emphasized the growing concern among member states regarding the use of virtual assets for laundering proceeds of crime, tax evasion, terrorist financing, and corruption.⁹ The report identified several key vulnerabilities, including the lack of traceability in certain blockchain platforms, the proliferation of privacy coins, and the emergence of unregulated crypto exchanges.

In response to these risks, the UNODC has worked to incorporate crypto-related issues into its broader technical assistance offerings. These include training programs for financial investigators, the development of prosecutorial guidance for digital evidence recovery in crypto-asset cases, and the deployment of regional advisory missions. For example, workshops conducted in Uzbekistan, Kazakhstan, and Kyrgyzstan have focused on increasing the technical capabilities of Financial Intelligence Units (FIUs) and anti-corruption agencies in identifying and tracing virtual assets.¹⁰

In my evaluation, the UN's approach reflects both its institutional strengths and its limitations. On the one hand, it is well-positioned to build consensus, disseminate best practices, and support capacity development. On the other, the lack of a binding legal instrument focused exclusively on crypto-asset governance reflects a cautious institutional posture that may hinder rapid progress in the face of a fast-evolving threat landscape. To bridge this gap, the UN should consider initiating negotiations for a supplementary protocol to UNCAC or a model law specifically addressing crypto-asset-related crimes.

⁸ Turaev, A. (2023). *Challenges in regulating virtual assets in Uzbekistan: Legal frameworks and implementation gaps*. *Central Asian Legal Review*, 11(2), 45–61.

⁹ UNODC. (2022). *Cryptocurrency investigation and training manual*. United Nations Office on Drugs and Crime. <https://www.unodc.org>

¹⁰ UNODC. (2023a). *Technical assistance programme report: Central Asia*. UNODC Regional Office for Central Asia.

Legal Instruments and Mechanisms: UNCAC, FATF, UNODC, and Beyond

The United Nations Convention Against Corruption (UNCAC)

Adopted in 2003 and entering into force in 2005, UNCAC is the only legally binding universal anti-corruption instrument. It provides a comprehensive framework for the prevention, criminalization, international cooperation, and asset recovery of corruption-related offences. While UNCAC does not explicitly mention crypto-assets—an understandable omission given the technological landscape at the time of drafting—its provisions on money laundering, concealment, and international cooperation are broad enough to be interpreted in ways that encompass crypto-related crimes.¹¹

Articles 14 and 23 of the Convention are particularly relevant. Article 14 calls on states to implement measures to detect and monitor the movement of money across borders, while Article 23 outlines criminalization requirements for the laundering of proceeds of crime, which may include crypto-assets if their criminal origin can be established. This interpretative flexibility has allowed states to use UNCAC as a foundation for legislative reforms that encompass virtual assets. However, the effectiveness of this application varies significantly across jurisdictions, depending on institutional capacity and political will.

The UNODC's Implementation Review Mechanism (IRM) for UNCAC has begun to include queries about digital financial technologies and their implications for anti-corruption compliance, but formal inclusion remains uneven. According to UNODC (2022), only a fraction of reviewed states have explicitly addressed crypto-assets in their self-assessment reports. This reveals both a lack of awareness and the need for clearer interpretive guidance on how UNCAC can be applied to crypto-related offences.

In my analysis, the elastic nature of UNCAC's provisions is both an advantage and a liability. While its flexibility allows states to adapt their compliance frameworks to evolving financial technologies, the absence of concrete interpretive guidance may lead to inconsistent enforcement and the proliferation of legal grey zones. The UN should consider developing a general comment or explanatory note clarifying the application of UNCAC to crypto-asset contexts.

Financial Action Task Force (FATF) Recommendations

The FATF has emerged as the de facto standard-setter for regulating crypto-assets in the context of AML/CFT compliance. Though not a UN agency, the FATF maintains close collaborative relationships with the UN, and its recommendations are frequently endorsed in UNODC materials. The FATF's 2019 revisions to Recommendation 15 and its interpretive note were watershed moments in the legal governance of virtual assets, effectively mandating that all countries impose AML/CFT obligations on VASPs.¹²

These obligations include customer due diligence (CDD), suspicious transaction reporting, licensing or registration of VASPs, and implementation of the "travel rule." According to the FATF's 2023 Mutual Evaluation Report, implementation remains uneven: while some jurisdictions such as Japan and South Korea have fully operationalized these standards, others—including many developing countries—lack the legal and technical infrastructure to do so.¹³ FATF has begun publishing "Guidance on Risk-Based Approach to Virtual Assets and VASPs" to address these discrepancies and offer interpretive clarity.

¹¹ UNCAC. (2003). United Nations Convention against Corruption. United Nations. <https://www.unodc.org/unodc/en/corruption/uncac.html>

¹² FATF. (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Financial Action Task Force. <https://www.fatf-gafi.org>

¹³ FATF. (2023). Mutual Evaluation Report: United States/European Union/Japan/South Korea. Paris: Financial Action Task Force.

Although FATF's soft law approach allows for adaptability, scholars such as del Castillo (2021) have critiqued its one-size-fits-all structure. In regions with limited financial inclusion or technological literacy, the imposition of stringent FATF rules may stifle innovation and exclude legitimate actors from the crypto economy. Furthermore, the travel rule remains controversial due to its data-sharing requirements and implications for user privacy.

In my assessment, the FATF model, while effective in developed financial ecosystems, requires contextual tailoring to ensure normative legitimacy and local feasibility. The UNODC can serve as a critical intermediary in this process, helping countries translate FATF standards into culturally and institutionally appropriate frameworks.

Emerging UN and Multilateral Mechanisms

Several emerging mechanisms within the UN system show promise in addressing crypto-asset challenges more directly. For example, the UN Cybercrime Ad Hoc Committee established under UNGA Resolution 74/247 is currently drafting a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. While the draft convention is still under negotiation, several state proposals have urged explicit inclusion of crypto-assets as a tool and target of cybercrime.¹⁴

Similarly, the UN's Digital Cooperation Roadmap emphasizes the need for inclusive and human-rights-oriented digital governance. Although not legally binding, these frameworks may shape the normative trajectory of future treaties and offer valuable policy levers for national authorities and advocacy networks.

Regulatory Evolution in Uzbekistan

Uzbekistan officially entered the crypto regulatory space with the adoption of Presidential Decree No. PP-3832 in July 2018, titled "On Measures to Develop the Digital Economy in the Republic of Uzbekistan." This decree legalized crypto trading, introduced licensing for crypto exchanges, and exempted crypto-related income from taxation.¹⁵ This forward-leaning approach positioned the country as a regional hub for crypto innovation. However, it also exposed vulnerabilities, as early regulations lacked robust AML/CFT provisions aligned with FATF and UN standards.

To address these deficiencies, the government established the **National Agency for Perspective Projects (NAPP)** in 2022, which became the principal regulatory body overseeing digital asset markets. The NAPP issued updated regulations in 2023 requiring licensing for virtual asset service providers (VASPs) and compliance with AML protocols, including customer due diligence, transaction monitoring, and reporting of suspicious activities. Despite these reforms, a 2023 compliance review revealed that only a fraction of Uzbekistan's licensed exchanges had implemented full KYC and reporting systems, raising concerns about enforcement and oversight capacity (World Bank, 2023).

From a legislative standpoint, Uzbekistan has not yet fully harmonized its national laws with UNCAC provisions concerning money laundering and the concealment of illicit assets via digital channels. For instance, while the Criminal Code of Uzbekistan criminalizes the laundering of criminal proceeds, it does not explicitly refer to virtual or crypto-assets, leaving judicial authorities to apply analogical reasoning or supplementary guidance. Moreover, the country's Financial Intelligence Unit (FIU), while a member of the Egmont Group, has limited technical

¹⁴ UNGA. (2023). Report of the Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes (A/78/213). United Nations General Assembly. <https://digitallibrary.un.org>

¹⁵ Republic of Uzbekistan. (2018). Presidential Decree No. PP-3832: On measures to develop the digital economy in the Republic of Uzbekistan. <https://lex.uz>

capacity in tracing blockchain transactions or coordinating cross-border investigations involving virtual assets.¹⁶

UNODC and International Engagement

Recognizing these gaps, Uzbekistan has sought support from the United Nations, particularly through the UNODC. In 2022 and 2023, UNODC conducted technical training workshops in Tashkent for law enforcement and FIU personnel focused on detecting and investigating crypto-related crimes. These initiatives were part of a broader UNODC strategy in Central Asia to promote cyber-resilience and financial transparency in emerging digital economies.¹⁷

The collaboration has also included the dissemination of UNODC's "Cryptocurrency Investigation and Training Toolkits," designed to guide prosecutors, regulators, and investigators through the complexities of digital asset tracing and seizure. Early evaluations suggest that these interventions have raised awareness and improved investigative procedures, but their institutional integration remains partial and dependent on sustained political will and external funding.

In terms of implementation, Uzbekistan illustrates the benefits and limitations of UN-centered regulatory influence. On the positive side, the country has demonstrated political openness to international norms and has taken steps to integrate UNODC's recommendations into its enforcement architecture. The recent alignment of licensing standards with FATF's interpretive notes reflects a normative shift toward compliance and risk mitigation.

However, several challenges remain. First, Uzbekistan's legal infrastructure is still in transition, with many crypto-specific provisions issued by presidential decree rather than codified in parliamentary legislation, which may undermine legal certainty and transparency. Second, enforcement agencies continue to face resource constraints, including lack of blockchain analytics tools, insufficient training in digital forensics, and limited international investigative cooperation mechanisms.

From a normative perspective, I argue that Uzbekistan's trajectory shows how UN influence can be catalytic but not determinative. Without domestic institutional reforms, capacity building, and legal harmonization, UN mechanisms may remain aspirational. For Uzbekistan to serve as a regional model, it must integrate international legal standards into binding domestic legislation, strengthen judicial capacity, and foster greater collaboration with international enforcement networks.

Comparative Legal Analysis

To fully appreciate the global scope and variation in the implementation of UN-backed legal mechanisms to address crypto-asset-related crimes, it is essential to examine how other jurisdictions have operationalized these principles. The following comparative analysis covers the United States, the European Union, China, Japan, and South Korea—each offering distinct regulatory philosophies and levels of compliance with UN and FATF standards.

United States

The United States remains a global leader in both the innovation of and regulatory response to crypto-assets. Its regulatory landscape is characterized by a decentralized approach involving multiple agencies, including the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Financial Crimes Enforcement Network (FinCEN), and the Department of Justice (DOJ). The U.S. has fully adopted FATF standards and was among the first to implement the travel rule in the context of virtual assets (FinCEN, 2020).

¹⁶ 1. Basel Institute on Governance. (2022). Cryptoassets and anti-money laundering: An evaluation of national frameworks. International Centre for Asset Recovery. <https://www.baselgovernance.org>

¹⁷ UNODC. (2023). Enhancing capacity to combat crypto-enabled crime in Uzbekistan. Internal Field Report.

Prosecution of crypto crimes under the U.S. federal system relies heavily on existing anti-money laundering statutes, such as the Bank Secrecy Act and the USA PATRIOT Act, as well as wire fraud and securities fraud provisions. High-profile cases, including those against Silk Road, BitMEX, and Binance, reflect the government's proactive use of legal tools to deter criminal misuse of crypto-assets.

While the United States does not formally incorporate UNCAC into its crypto enforcement strategy, its alignment with UNODC guidelines and its extraterritorial enforcement capacity make it an informal enforcer of international standards. However, critiques remain, particularly regarding regulatory fragmentation and lack of a comprehensive federal crypto law.¹⁸ In my view, the U.S. legal system benefits from institutional robustness but suffers from jurisdictional complexity, which may hinder consistent application and international cooperation.

European Union

The European Union has pursued a more harmonized and supranational approach. The recently adopted **Markets in Crypto-Assets Regulation (MiCA)** represents the EU's most comprehensive legal framework for regulating crypto-assets, establishing uniform rules for issuance, market conduct, and AML compliance across all 27 member states (European Commission, 2023). MiCA incorporates FATF standards and strengthens supervisory powers for the European Banking Authority and national financial regulators.

The EU is also advancing its **Anti-Money Laundering Package**, which includes proposals for an EU-level FIU and mandates for crypto-related CDD. These initiatives align closely with UNODC and FATF guidance and demonstrate the EU's ambition to lead global crypto governance.

Nonetheless, some scholars, such as Ferran and Allen¹⁹, caution that MiCA may over-regulate innovation, particularly in the DeFi sector. They also note that implementation will depend heavily on national regulatory agencies' capacity. From my perspective, the EU's model offers a compelling balance between innovation and oversight, though the full impact of MiCA will only become clear post-2025 as enforcement mechanisms are tested in practice.

China

China has adopted the most stringent anti-crypto stance among major economies. Since 2021, all crypto-related transactions and mining activities have been banned, and the People's Bank of China (PBoC) has declared cryptocurrencies illegal tender. These actions are framed as efforts to combat financial crime, protect monetary sovereignty, and promote the state-backed digital yuan (PBoC, 2021).

While China has criminalized the use of crypto-assets for money laundering under its Criminal Law and AML legislation, it does not collaborate extensively with UNODC on crypto issues. Moreover, China's rigid regulatory stance has driven much of the activity underground or abroad, complicating enforcement and transparency.

Although effective in curbing domestic crypto proliferation, China's approach is criticized for its lack of proportionality and for impeding financial innovation. From an international law standpoint, China exemplifies the limitations of unilateral regulatory prohibition in a borderless financial ecosystem.

¹⁸ Goforth, C. R. (2021). The lawyer's guide to cryptocurrency regulation in the United States. *Fordham Journal of Corporate & Financial Law*, 26(1), 1–38. <https://ir.lawnet.fordham.edu/jcfl/vol26/iss1/1/>

¹⁹ Ferran, E., & Allen, J. (2022). *Regulating crypto-assets under MiCA: Caution, coordination, and complexity* (SSRN Working Paper No. 4172564). <https://ssrn.com/abstract=4172564>

Japan

Japan's regulatory regime is one of the most mature globally. Following the Mt. Gox exchange collapse, the country introduced amendments to the **Payment Services Act** and the **Financial Instruments and Exchange Act**, mandating the registration of crypto exchanges and implementing FATF-compliant AML/CFT controls. The **Financial Services Agency (FSA)** oversees compliance and has issued guidelines aligned with FATF's travel rule and customer due diligence measures (FSA, 2022).

Japan's cooperation with UN bodies is robust, and the country frequently hosts joint workshops with UNODC on financial crime. In my view, Japan's model is a benchmark for responsible regulation, combining consumer protection, technological development, and adherence to international standards.

South Korea

South Korea has implemented one of the most stringent regulatory frameworks for VASPs in Asia. In 2021, the **Act on Reporting and Use of Specified Financial Transaction Information** was amended to bring VASPs under the supervision of the **Korea Financial Intelligence Unit (KoFIU)**. The law mandates real-name bank accounts, customer identification, and suspicious transaction reporting. It also introduces penalties for non-compliance, aligning closely with FATF standards (KoFIU, 2022).

South Korea also collaborates with UNODC and FATF on technical assistance and risk assessment. However, enforcement remains uneven, particularly among smaller or unregistered platforms. Nonetheless, the country's commitment to regulation and international cooperation makes it a valuable comparator for Uzbekistan.

Challenges and Recommendations

Structural and Normative Challenges in UN Crypto-Crime Regulation

The United Nations' framework for preventing and regulating crimes involving crypto-assets, while commendable in its breadth and ambition, faces significant structural and normative challenges. Chief among these is the absence of a **comprehensive, crypto-specific international legal instrument**. Existing frameworks, such as UNCAC and UNTOC, offer only general principles of criminalization and cooperation, which, while adaptable, lack the necessary precision to address the technological complexity and jurisdictional ambiguity of crypto-asset transactions.²⁰ For instance, UNCAC's language on "concealment" and "transfer of proceeds of crime" was crafted in a pre-blockchain financial context and does not anticipate the use of privacy coins or decentralized autonomous organizations (DAOs).

The lack of definitional clarity is also problematic. There is still no universally accepted legal definition of a "crypto-asset" within the UN system. This definitional ambiguity has downstream effects, as national legal systems diverge on whether crypto-assets constitute property, financial instruments, or commodities—a divergence that undermines mutual legal assistance and extradition protocols.²¹ Without shared legal taxonomies, international cooperation in investigating and prosecuting crypto crimes remains inconsistent and often ineffective.

Another major structural issue is the **soft-law nature** of many UN crypto-related initiatives. The reliance on FATF recommendations—while pragmatic—places excessive dependence on a non-binding, technocratic body that lacks democratic accountability or formal standing within the UN

²⁰ Chalmers, G. (2022). Jurisdictional fragmentation in the age of crypto assets: The challenge of legal harmonization. *Journal of Financial Crime*, 29(4), 1093–1112.

²¹ Zilioli, C. (2022). Crypto-assets and legal taxonomies in international financial law. *European Business Law Review*, 33(4), 437–466.

Charter framework. While FATF's standards are often transposed into national laws due to peer pressure or market incentives, their lack of enforceability limits their normative strength. This undermines the effectiveness of UNODC capacity-building programs, which often rely on FATF principles as reference points without the backing of binding treaty law.

From a practical standpoint, there is **asymmetric capacity among member states** to implement UN standards. Developed countries, with robust regulatory agencies and digital forensic capabilities, are better positioned to comply with FATF and UNODC guidance. In contrast, developing countries like Uzbekistan, despite political will, often struggle with infrastructural limitations, including outdated financial laws, insufficient staffing of Financial Intelligence Units, and lack of access to blockchain analytics software. These disparities create enforcement gaps and drive illicit actors to jurisdictions with weaker oversight—a phenomenon known as “regulatory arbitrage”.²²

Recommendations

To address these challenges, this paper proposes a series of normative and operational recommendations, grounded in international legal theory, practical enforcement realities, and comparative regulatory experience.

1. Development of a UN Protocol or Model Law on Crypto-Asset Crimes

The UN General Assembly or the Conference of the States Parties to UNCAC should mandate the drafting of a supplementary protocol specifically dedicated to crypto-asset crimes. This protocol should provide legally binding definitions, list predicate offences, outline investigative procedures (e.g., blockchain forensic methods, digital asset seizure rules), and establish obligations for mutual legal assistance. Alternatively, a model law—similar to UNCITRAL’s efforts on electronic commerce—could provide a flexible yet authoritative template for domestic legal reforms.

2. Expansion of the UNCAC Implementation Review Mechanism

UNCAC’s self-assessment and peer-review processes should be updated to include indicators specific to crypto-assets. Member states should be required to report on their implementation of digital asset AML/CFT regimes, their enforcement statistics involving crypto-financed corruption, and their cross-border collaboration effectiveness. This would enhance transparency, accountability, and comparative learning.

3. Establishment of a UN Crypto-Regulatory Coordination Forum

The UN should institutionalize a permanent forum that brings together state regulators, law enforcement, academics, and private sector actors (e.g., VASPs, blockchain developers). This forum could be housed under the Economic and Social Council (ECOSOC) and tasked with producing annual reports, technical guidance, and risk assessments. Its outputs could inform both national policy and UNODC programming.

4. Tailored Technical Assistance and Capacity Building

UNODC must shift from generalized training to tailored, sector-specific capacity-building programs that reflect the regulatory maturity and technological readiness of each country. For example, Uzbekistan would benefit from long-term secondments of technical experts, the development of open-source blockchain analytics platforms, and regional centers of excellence for digital forensic training. Donor funding should be allocated through multi-year budgets rather than ad hoc projects to ensure institutional memory and program sustainability.

5. Enhanced Interoperability with FATF and Regional Bodies

²² Reuter, P., & Truman, E. M. (2004). Chasing dirty money: The fight against money laundering. Institute for International Economics.

While FATF's role remains central, the UN should actively shape its policy direction by increasing coordination between the FATF and UN treaty bodies. Furthermore, the UN should support regional organizations—such as the Eurasian Group on Combating Money Laundering (EAG), the Council of Europe's MONEYVAL, and the Asia/Pacific Group on Money Laundering—in adapting global standards to local contexts. This multi-level governance model would improve both legitimacy and implementation.

Conclusion

The evolution of crypto-assets represents a formidable challenge and an unparalleled opportunity for the global legal order, particularly within the domain of international criminal law. As this paper has demonstrated, the emergence of decentralized digital currencies and related technologies has enabled novel forms of transnational criminality that transcend conventional jurisdictional and regulatory boundaries. In this context, the United Nations has sought to play a central coordinating role, deploying legal, normative, and technical instruments to prevent and regulate crimes committed through or involving crypto-assets.

Through instruments such as the United Nations Convention against Corruption (UNCAC), the UN Office on Drugs and Crime (UNODC), and strategic alignment with the Financial Action Task Force (FATF), the UN has helped establish a normative foundation for crypto-asset regulation. However, the analysis presented in this paper reveals that these mechanisms, while significant, are often limited by definitional ambiguity, institutional fragmentation, and asymmetric implementation among member states.

The case study of Uzbekistan illustrates both the possibilities and constraints of applying UN-backed standards in a developing country context. While the country has taken bold steps to regulate the crypto space—including through licensing regimes and AML/CFT reforms—implementation gaps, legal uncertainty, and limited technical capacity persist. These challenges are compounded by the global nature of crypto networks, which render unilateral regulation ineffective without broader international cooperation.

Comparative analysis with jurisdictions such as the United States, the European Union, China, Japan, and South Korea highlights the diversity of approaches in integrating UN and FATF standards into domestic frameworks. Countries with strong regulatory institutions and technological capacity, such as Japan and South Korea, have succeeded in aligning their domestic legal systems with international norms while maintaining innovation-friendly environments. In contrast, states like China have opted for restrictive prohibitionist policies, while the United States continues to grapple with regulatory fragmentation across federal and state jurisdictions.

In conclusion, the regulation of crypto-assets is not merely a matter of technological adaptation but a test of the international legal system's ability to respond to rapid, transnational change. The United Nations has the normative legitimacy and institutional infrastructure to lead this response, but it must recalibrate its approach to meet the demands of the digital era. A robust, inclusive, and legally grounded global framework—one that balances security with innovation and sovereignty with cooperation—is imperative for ensuring that crypto-assets serve as tools for development rather than vectors for criminality.

References

1. Arner, D. W., Buckley, R. P., & Zetsche, D. A. (2022). FATF standards and the regulation of crypto-assets: Legal, regulatory and policy challenges. *Journal of Banking Regulation*, 23(2), 134–156. <https://doi.org/10.1057/s41261-022-00186-9>
2. Basel Institute on Governance. (2022). *Cryptoassets and anti-money laundering: An evaluation of national frameworks*. International Centre for Asset Recovery. <https://www.baselgovernance.org>

3. Chalmers, G. (2022). Jurisdictional fragmentation in the age of crypto-assets: The challenge of legal harmonization. *Journal of Financial Crime*, 29(4), 1093–1112. <https://doi.org/10.1108/JFC-09-2021-0203>
4. de Koker, L., & Symington, J. (2020). Proportionality and regulation of crypto assets: International standards and emerging practices. *Law and Financial Markets Review*, 14(3), 245–263. <https://doi.org/10.1080/17521440.2020.1808589>
5. European Commission. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)*. Official Journal of the European Union. <https://eur-lex.europa.eu>
6. FATF. (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Financial Action Task Force. <https://www.fatf-gafi.org>
7. FATF. (2021). *Updated guidance for a risk-based approach to virtual assets and VASPs*. Financial Action Task Force. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>
8. FATF. (2023). *Mutual evaluation report: United States / European Union / Japan / South Korea*. Financial Action Task Force. <https://www.fatf-gafi.org>
9. FinCEN. (2020). *Application of FinCEN's regulations to certain business models involving convertible virtual currencies*. U.S. Department of the Treasury. <https://www.fincen.gov>
10. FSA (Financial Services Agency of Japan). (2022). *Guidelines for crypto-asset service providers*. <https://www.fsa.go.jp>
11. Goforth, C. R. (2021). The lawyer's guide to cryptocurrency regulation in the United States. *Fordham Journal of Corporate & Financial Law*, 26(1), 1–38. <https://ir.lawnet.fordham.edu/jcfl/vol26/iss1/1/>
12. Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament. <https://www.europarl.europa.eu>
13. KoFIU (Korea Financial Intelligence Unit). (2022). *Implementation of FATF Travel Rule in South Korea*. Financial Services Commission. <https://www.kofiu.go.kr>
14. NAPP (National Agency for Perspective Projects). (2023). *Regulations on licensing virtual asset service providers in Uzbekistan*. Government of Uzbekistan. <https://napp.uz>
15. Pieth, M. (2019). UNCAC and crypto assets: An untapped legal resource. In M. Pieth (Ed.), *Anti-corruption compliance: A guide to the UNCAC* (pp. 123–147). Springer. <https://doi.org/10.1007/978-3-030-28813-4>
16. PBoC (People's Bank of China). (2021). *Notice on further preventing and dealing with the risk of virtual currency trading speculation*. <https://www.pbc.gov.cn>
17. Republic of Uzbekistan. (2018). *Presidential Decree No. PP-3832: On measures to develop the digital economy in the Republic of Uzbekistan*. <https://lex.uz>
18. Reitano, T., & Shaw, M. (2021). Cryptocurrencies and crime: Assessing law enforcement capabilities. *Global Initiative Against Transnational Organized Crime Report*. <https://globalinitiative.net>
19. Reuter, P., & Truman, E. M. *Chasing dirty money: The fight against money laundering*. Institute for International Economics.
20. UNCTAD. (2022). *Policy brief: The risks and costs of cryptocurrencies in developing countries*. United Nations Conference on Trade and Development. <https://unctad.org>

21. UNCAC. *United Nations Convention against Corruption*. United Nations. <https://www.unodc.org/unodc/en/corruption/uncac.html>
22. UNGA. (2023). *Report of the Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes (A/78/213)*. United Nations General Assembly. <https://digitallibrary.un.org>
23. UNODC. (2022). *Cryptocurrency investigation and training manual*. United Nations Office on Drugs and Crime. <https://www.unodc.org>
24. UNODC. (2023a). *Technical assistance programme report: Central Asia*. UNODC Regional Office for Central Asia.
25. UNODC. (2023b). *Enhancing capacity to combat crypto-enabled crime in Uzbekistan*. Internal Field Report.
26. Zilioli, C. (2022). Crypto-assets and legal taxonomies in international financial law. *European Business Law Review*, 33(4), 437–466.
27. Zwitter, A., & Hazenberg, J. (2020). Decentralized governance and the international legal order: Blockchain and the UN system. *Journal of International Affairs*, 73(2), 35–51.