EUI SCHOOL OF TRANSNATIONAL GOVERNANCE

STG Policy Papers

POLICY BRIEF

COMBATING FINANCIAL CRIMES: HOW ARE CRYPTO-ASSET PROVIDERS NAVIGATING REGULATORY CHALLENGES?

Author:

Huda Ismail

Florence School of Transnational Governance

ISSUE 2025/04
FEBRUARY 2025

SCHOOL OF TRANSNATIONAL GOVERNANCE

EXECUTIVE SUMMARY

While cryptocurrencies are seen by some as a "get-rich-quick" tool, they are increasingly stigmatised as a medium for illicit transactions. Recent statistics reveal a significant rise in cryptocurrency platform hacks, with stolen funds surging 21% from the previous year to reach $2.2 billion in 2024. Crimes such as fraud, scams, organized crime, and money laundering are frequently linked to cryptocurrency trading platforms. These platforms, legally recognised as Crypto Asset Service Providers (CASPs), have become a focal point for intense regulatory scrutiny worldwide. As a result, many CASPs face substantial challenges in keeping up with rapidly evolving regulatory frameworks as well as operational and technological advancements. This policy brief examines the regulatory challenges CASPs face in combating financial crimes while fostering innovation. It emphasizes the critical need for collaboration between regulators and CASPs. By tackling these issues, the brief offers recommendations to establish a robust regulatory framework that mitigates risks of financial crime, builds trust, and supports innovation within the digital currency ecosystem.

Author:

Huda Ismail | Policy Leader Fellow (2024-2025), Florence School of Transnational Governance, EUI

1. INTRODUCTION

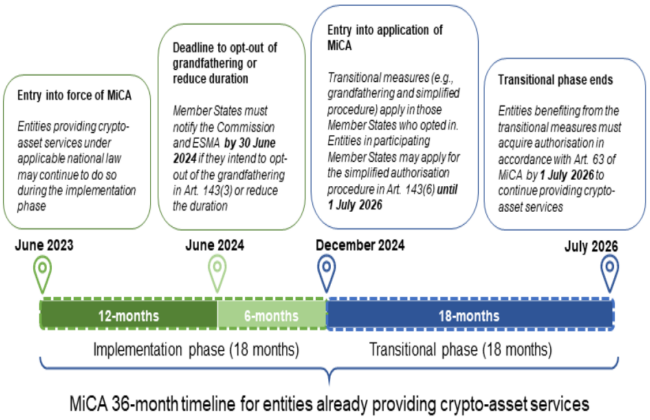
"Criminals aren't giving up on misusing cryptocurrencies anytime soon," remarked Jean-Philippe Lecouffe, Europol's Deputy Executive Director, in October 2023, during an international conference on trends and strategies to combat crimes involving digital currencies. To date, cryptocurrencies have attracted millions of users worldwide with their accessibility, decentralised nature, and opportunities for financial investment. Despite the appeal of these characteristics, cryptocurrencies are also considered one of the greatest challenges to regulators and policymakers due to the criminal risks they present.

Recent cases have highlighted the use of cryptocurrencies in high-profile financial crimes and exploitation by malicious actors. Notable examples include the Ponzi scheme involving the cryptocurrency VITAE, which defrauded over 223,000 victims across 177 countries, resulting in the seizure of €1.5 million in cryptocurrencies. Another case involved a Franco-Israeli criminal group that defrauded victims of €38 million.

A common factor in these crimes was the use of Crypto- Asset Service Providers (CASPs), which are increasingly recognised as mediums for facilitating crimes such as fraud, drug trafficking, cybercrimes, and money laundering. These platforms have inadvertently become tools for illicit activities, a trend attributable to their semi-anonymous nature and global reach. To globally counter these risks, over 200 countries and jurisdictions have adopted the Financial Action Task Force (FATF) international standards. These standards serve as guidelines to combat money laundering and terrorist financing. Among these guidelines, the FATF introduced the 'Travel Rule', which requires Crypto-Asset Service Providers (CASPs) to collect and share information about the originators and beneficiaries of cryptocurrency transfers. These guidelines aim to enhance transparency, improve traceability, and mitigate the illegal use of cryptocurrencies. Building on global efforts to combat financial crimes, the European Union introduced Markets in Crypto-Assets Regulation (MiCAR), which is a comprehensive legislative framework to regulate the crypto-asset market. It aims to provide legal clarity, ensure consumer protection, and address the risks associated with financial crimes like money laundering and financial support for terrorism. While the FATF sets global standards for regulating the trading platforms, MiCAR tailors these rules for the EU, creating a localised framework for crypto regulation. MiCAR places a sharp focus on the role of (CASPs), recognizing them as key entities providing services such as custody, trading platforms, exchanges, and wallet services.

30 December 2024 marked the launch of the next transnational phase of MiCAR, set to span 18 months (Figure 1). This phase introduces detailed guidelines for CASPs, including authorisation applications, record-keeping requirements, and standardised templates for crypto-asset white papers.

Figure 1. Market in crypto-asset (MiCA) timeline



Before delving into the challenges faced by cryptocurrency trading platforms, regulators must first understand the unique nature and vulnerabilities of crypto platforms and the gateways criminals exploit within the system. Therefore, the following section will outline the main types of transactions on crypto platforms, particularly those operated by CASPs, and highlight the red flags that regulators and policymakers should consider when establishing a robust regulatory framework.

2. OVERVIEW OF TRANSACTIONS ON CRYPTO PLATFORMS

The ultimate goal for criminals who use crypto platforms is to cash out the crypto with low traceability and a high degree of anonymity. Usually, there are four types of transactions conducted on crypto platforms. First, criminals can exchange one cryptocurrency for another (crypto-to-crypto) on these platforms, which are favoured thanks to their ability to bypass traditional financial systems and obfuscate the origin of funds (thereby making them harder to trace). By exchanging one digital asset for another, criminals can break the links to illicit sources without using fiat currencies. Second, converting cryptocurrencies into traditional currencies (crypto-to-fiat) also poses risks for exploitation by criminal actors, as crypto platforms provide a direct path to cash out illicit funds, particularly in poorly regulated markets. The third type of transaction, which involves purchasing cryptocurrencies using fiat money (fiat-to-crypto), is less desirable to criminals because the source of funds in traditional financial systems is easier to identify. Lastly, using digital assets to acquire physical or digital goods (crypto-to-goods) can be exploited for money laundering or buying illicit products, although it typically involves more external entities and therefore involves a higher risk of detection.

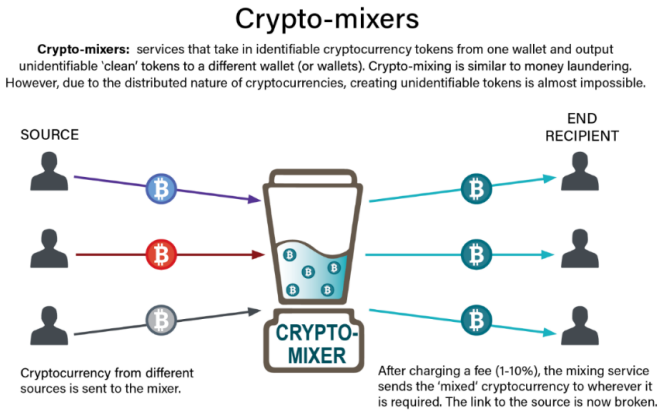
2.1 Alternative red flags in crypto transactions

While exchange platforms serve as the primary mechanism for cryptocurrency transactions, criminals often exploit other complex transaction methods, creating additional challenges for regulators in terms of traceability and regulatory gaps. These red flags are classified into the following categories.

- Direct trading channels represented by peer-to-peer (P2P) trading: These channels facilitate the direct exchange of cryptocurrencies between individuals without an intermediary, thus reducing traceability and hindering regulatory oversight. These characteristics make such channels an attractive option for criminals to transfer funds while evading detection. Over-the-counter (OTC) trading, used for larger transactions, occurs outside public exchanges. Criminals exploit OTC desks or independent brokers to execute high-value transactions under the guise of legitimacy.
- Cash-out channels, including Bitcoin ATMs (BATMs): These machines enable users to quickly exchange cryptocurrencies for cash or vice versa. Their rapid conversion process and limited Know Your Customer (KYC) measures, which are crucial for verifying and identifying individuals involved in transactions, make them appealing for illicit cash-outs. Another widely used platform, cryptocurrency gambling, facilitates deposits and withdrawals in cryptocurrencies, allowing criminals to obscure the origin of funds and integrate illicitly obtained money into the financial system.
- Concealment channels: Frequently preferred by criminals and exemplified by the mixers and tumblers service (Figure 2), these tools break the traceable chain of transactions by routing funds through multiple intermediary wallets, thereby obscuring their origins. Nested services, though they operate within legitimate exchanges, blend illicit transactions with legitimate ones, exploiting the exchanges' liquidity and broad access to trading pairs. Non-fungible tokens (NFTs), which are unique digital assets on a blockchain, can be misused for laundering funds by artificially inflating prices (wash trading) or disguising illicit proceeds. As indicated, over $8 million have been laundered through NFTs.

The sophistication of the channels mentioned above highlight the growing complexity of criminal activity in the cryptocurrency space, illustrating the urgent need for stronger regulations to ensure compliance. However, several challenges remain in the process. The following section discusses the key obstacles CASPs face in adhering to regulatory frameworks, including technological and operational barriers that hinder effective compliance.

Figure 2. Crypto-mixers: tools for hiding crypto transactions



Source: unodc.org

3. TOWARDS EFFECTIVE COMPLIANCE: BARRIERS HINDERING CASPS

3.1 Technological and operational barriers

Technological barriers: One of the major challenges facing CASPs is the significant investment required to develop and maintain advanced technologies for compliance. These technologies are essential for monitoring suspicious activities, detecting sanctions violations, and preventing illicit transactions. A notable example involves Kraken, a prominent CASP that onboarded 1,500 individuals with Iranian addresses, violating sanctions imposed by the U.S. Treasury's Office of Foreign Assets Control (OFAC). This case highlights the lack of adequate technological tools to monitor and prevent sanctioned clients during the onboarding process.

Operational barriers: In addition to technological challenges, compliance demands substantial investment in human resources, including hiring skilled experts to manage compliance tasks, which often entails significant operational costs.

It is crucial to note that smaller CASPs, particularly startups in the early stages of development, may struggle to address both technological and operational challenges. Limited resources can hinder their ability to meet compliance demands, potentially impacting their capacity to operate legally and securely.

3.2 Regulatory ambiguity: the European case

Regulatory frameworks for cryptocurrencies are still evolving, leaving CASPs to navigate a landscape of uncertainty. Different jurisdictions are adopting varying regulatory approaches, leading to operational confusion, especially for CASPs operating across borders. Below are key challenges that exemplify the regulatory ambiguity faced by CASPs in the EU.

- Compliance ambiguity: The regulatory framework in the EU (MiCA) requires that E-Money Tokens (EMTs) only be offered by authorised credit or electronic money institutions, which must comply with specific regulations and publish a white paper. However, some issuers do not fit these categories, complicating classification and regulatory compliance for CASPs working with them.
- Stablecoin ambiguity: The regulation of stablecoins—a type of cryptocurrency that offers a more stable alternative to traditional digital currencies—has become increasingly ambiguous. Nowadays, stablecoins – including Tether, USD Coin, and Ethena USDe, all in high demand -- have a market capitalisation approaching $210 billion. A key issue is the uncertainty surrounding their classification under MiCAR, which does not specify whether these currencies should be classified as Asset-Referenced Tokens (ARTs) or E-Money Tokens (EMTs). This ambiguity complicates the regulatory treatment of stablecoins, creating challenges for CASPs in navigating compliance requirements effectively.
- Data privacy and security ambiguity: Compliance requires CASPs to collect and store sensitive customer information for extended periods. However, balancing this requirement with data privacy laws, such as the General Data Protection Regulation (GDPR), presents significant challenges. Ensuring secure storage and transmission of personal data while also meeting anti-money laundering (AML) requirements adds further complexity.

3.3 Compliance with anti-money laundering (AML) standards

CASPs face significant challenges in aligning with AML standards, primarily due to the lack of standardised KYC protocols across jurisdictions. The global nature of CASPs adds complexity, as the existence of crypto bans in some countries makes it difficult to establish reliable systems for monitoring transactions and ensuring compliance. Furthermore, noncompliance can result in severe consequences, including significant fines, reputational damage, and even legal action. For instance, the Binance exchange was fined $4.3 billion for not preventing illicit crypto activity on the platform. The pressure of potential penalties often leads CASPs to adopt costly and extensive compliance measures, straining resources and operational efficiency.

3.4 International cooperation shortfalls

One study shows that only 30% of countries effectively cooperate on addressing cybercrime and money laundering in the cryptocurrency space. This lack of coordination undermines efforts to build capacity and share critical insights, despite CASPs offering valuable resources to support enforcement. The borderless nature of cryptocurrencies further complicates matters, particularly in asset seizure and confiscation. Many law enforcement agencies lack the expertise required to navigate the technical complexities of digital asset recovery, while inconsistent regulatory frameworks hinder effective cross-border enforcement. These gaps emphasize the urgent need for robust international partnerships to address the challenges posed by cryptocurrency-related financial crimes.

4. POLICY RECOMMENDATIONS

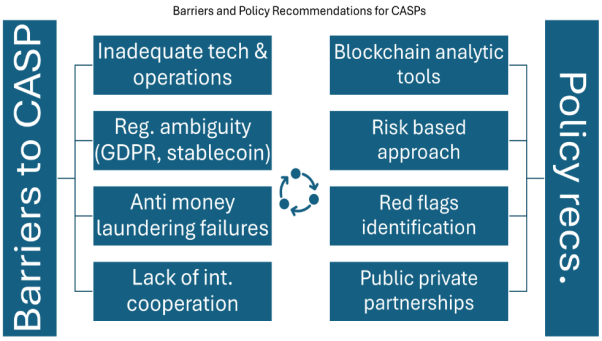
Policymakers must craft clear, actionable regulations and actively involve CASPs in decision-making to ensure a robust, crime-resistant crypto landscape. By fostering collaboration and aligning efforts, regulators can build trust and create practical solutions.

- Prioritising a risk-based regime: Rather than attempting a 'one size fits all' approach, countries must tailor their regulatory approaches to align with their specific legal and economic frameworks. Policymakers should start by assessing the financial risk profiles of crypto service providers in their jurisdiction, identifying vulnerabilities unique to their markets while aligning with international standards like those of the Financial Action Task Force (FATF). A tiered regulatory approach is essential to balance innovation and oversight. Smaller CASPs, which typically lack the resources to implement stringent compliance measures, can operate under proportionate requirements that encourage innovation and market participation. Meanwhile, larger CASPs, with greater market influence and risk exposure should adhere to comprehensive regulations to ensure market stability and robust compliance. This stratified method reduces unnecessary burdens on smaller firms while maintaining systemic integrity.
- Streamline compliance by identifying red flags: Identifying red flags is crucial for detecting suspicious activities within cryptocurrency transactions. To tackle this effectively, competent authorities, supervisors, and crypto service providers must work together to identify and categorize common warning signs. These red flags typically fall into several categories: a) geographic risks, whereby criminals may exploit countries with weak or non-existent regulations; b) irregular transaction patterns, including structured transactions designed to avoid detection or those that appear unusual; c) unusual transaction size, where the amount and frequency of the transaction lack a logical business explanation; d) suspicious profiles of senders or recipients, particularly when these profiles are associated with high-risk jurisdictions or have limited transaction history; and e) suspicious sources of funds or wealth, which may be difficult to verify or linked to illicit activities. By recognizing these indicators, stakeholders can improve monitoring and detection efforts, contributing to the overall integrity of the cryptocurrency ecosystem.
- Enhancing public-private partnerships: These partnerships are key to effectively

combating financial crime risks in the cryptocurrency sector. By collaborating, the public and private sectors can co-create innovative solutions that benefit both parties and strengthen the overall regulatory framework. Involving CASPs in shaping these frameworks fosters a sense of ownership and ensures that regulatory requirements are effectively implemented. Additionally, creating "regulatory sandboxes," where CASPs, law enforcement, and regulatory bodies can exchange insights, challenges, and best practices, will enhance the detection and reporting of illicit activities. Better cooperation between law enforcement agencies, competent authorities, and CASPs is also essential for successful confiscation and seizure of assets, which will ultimately lead to more effective financial investigations and improved asset management.

- Investing in technology: There should be incentives to encourage both CASPs and supervising authorities to invest in adopting blockchain analytic tools, such as Chainalysis and TRM Labs, which are vital for combating financial crime in the digital currency space. These tools provide comprehensive insights into transaction monitoring and help to ensure compliance with sanctions lists. By leveraging these tools, authorities and CASPs can enhance their ability to trace illicit funds, detect suspicious activity, and ensure greater transparency within the crypto ecosystem. This proactive approach is essential for improving overall regulatory effectiveness and mitigating risks associated with digital currencies.

Figure 3. Barriers and policy recommendations for CASPs



Source: Huda Ismail

5. CONCLUSIONS

The rapid evolution of the cryptocurrency ecosystem has introduced new complexities, making it increasingly vulnerable to misuse by criminals. The challenges faced by CASPs in achieving compliance with regulatory frameworks — such as technological barriers, operational limitations, and evolving criminal methodologies — highlight the urgent need for a coordinated and adaptive regulatory approach. Without robust oversight, these gaps will continue to be exploited, posing significant risks to financial integrity and global security.

To address these issues effectively, collaboration and cooperation with CASPs is essential, as they serve as the primary gatekeepers in the cryptocurrency world. By engaging closely with CASPs, regulators can stay abreast of industry advancements, design practical solutions, and establish policies that balance innovation with effective safeguards. This policy brief provides some recommendations for regulators, policymakers, and other members of crucial partnerships for crypto regulation. The goal is to ensure the development of a resilient regulatory framework that not only mitigates the risk of financial crime but also supports the growth and legitimacy of the digital asset ecosystem.

The School of Transnational Governance (STG) delivers teaching and high-level training in the methods, knowledge, skills and practice of governance beyond the State. Based within the European University Institute (EUI) in Florence, the School brings the worlds of academia and policy-making together in an effort to navigate a context, both inside and outside Europe, where policy-making increasingly transcends national borders.

The School offers Executive Training Seminars for experienced professionals and a Policy Leaders Fellowship for early- and mid-career innovators. The School also hosts expert Policy Dialogues and distinguished lectures from transnational leaders (to include the STG's Leaders Beyond the State series which recorded the experiences of former European Institution presidents, and the Giorgio La Pira Lecture series which focuses on building bridges between Africa and Europe). In September 2020, the School launched its Master-of-Arts in Transnational Governance (MTnG), which will educate and train a new breed of policy leader able to navigate the unprecedented issues our world will face during the next decade and beyond.

The STG Policy Papers Collection aims to further the EUI School of Transnational Governance's goal in creating a bridge between academia and policy and provide actionable knowledge for policy-making. The collection includes Policy Points (providing information at-a-glance), Policy Briefs (concise summaries of issues and recommended policy options), and Policy Analyses (in-depth analysis of particular issues). The contributions provide topical and policy-oriented perspectives on a diverse range of issues relevant to transnational governance. They are authored by STG staff and guest authors invited to contribute on particular topics.

Florence School of Transnational Governance
European University Institute
Via Camillo Cavour, 65a, 50129 Firenze (FI), Italy
Tel. +39 055 4685 545
Email: stg.publications@eui.eu

www.eui.eu/stg

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

doi:10.2870/2928792
ISBN:978-92-9466-647-5
ISSN:2600-271X
QM-01-25-015-EN-N