Prospects and Models of Combating Cryptocurrency Crimes

The India-EU Dialogue as a Perspective?



Article

Varun VM

ABSTRACT

This article discusses the growing concerns regarding the convergence of virtual currencies and mainstream finance, which is leading to an increase in illicit activities such as money laundering and terrorism financing. The challenges that law enforcement faces in addressing these crimes are exacerbated by limited technological expertise and a sense of impunity among perpetrators. The article highlights successful asset recovery cases involving crypto assets in the United States and the extension of anti-money laundering laws to virtual assets in the United Kingdom and India. While advanced jurisdictions are making progress in addressing these challenges, the article emphasizes the need for policy recommendations and best practices, particularly for jurisdictions in Africa, which is experiencing rapid growth in the crypto market. It also delves into potential avenues for collaboration between the European Union (EU) and India in addressing capacity deficiencies in developing or least developed countries. The cybersecurity practices and frameworks employed by both European and Indian entities may serve as instructive models for developing and least developed countries to combat terrorism financing with virtual assets.

AUTHOR

Varun VM

Research Officer Rashtriya Raksha University

CITATION SUGGESTION

V. VM, "Prospects and Models of Combating Cryptocurrency Crimes", 2023, Vol. 18(4), eucrim, pp365–370. DOI: https://doi.org/10.30709/eucrim-2023-032

Published in 2023, Vol. 18(4) eucrim pp 365 – 370 ISSN: 1862-6947 https://eucrim.eu





I. Introduction

The rapid convergence of virtual currencies and assets with the mainstream financial system has resulted in a blurred distinction between physical and virtual assets/currencies. This merging has led to a significant increase in occurrences of money laundering, transnational organized crime, and terrorism financing facilitated by the use of illicit cryptocurrencies, thereby raising concerns about the effectiveness of regulatory measures governing the "virtual currency/asset" domain. Moreover, the limited expertise in conducting technology-based law enforcement and the growing sense of impunity further compound the challenges faced by criminal justice administration.

According to a report from the blockchain analysis company Chainanalysis, cited by the Basel Institute on Governance, illicit cryptocurrency addresses received a total of \$14 million in 2021.1 This figure represents a significant increase of almost 80 percent compared to the previous year. In India, as of 31 January 2023, the Directorate of Enforcement, investigating several cases related to cryptocurrency fraud, has seized/attached proceeds of crime amounting to INR 9,360 million (approximately 112.91 million USD).² Recognising that the flow of illicit money through transfer of funds and crypto assets can damage the integrity, stability, and reputation of the financial sector, the European Union recently adopted a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets.³ The Regulation acknowledges that the traceability of transfers of funds and virtual assets can be a particularly important and valuable tool in the prevention, detection, and investigation of money laundering and terrorism financing as well as in the implementation of restrictive measures in compliance with Union regulations implementing such measures. A joint report by Europol and the Basel Institute on Governance stated that existing asset recovery laws, both conviction and non-conviction based, have enabled some jurisdictions to confiscate large amounts of illicit crypto assets. In India, the application of the 2002 Prevention of Money Laundering Act was recently extended to virtual assets/currencies and fiat currencies transactions.5

Although advanced jurisdictions are making progress in addressing this type of crime and related legal challenges, policymakers in Africa, one of the fastest growing crypto markets in the world, have expressed concern over cryptocurrencies being used to transfer funds illegally out of the region. This article attempts to create a compilation of best practices, including policies, legislative and administrative measures, and institutional recommendations derived from or implemented by advanced jurisdictions. These findings offer potential guidance for jurisdictions that lack effective anti-money laundering and/or counter-terrorism financing regulation (AML/CTF).

II. Challenges in Regulating the Virtual Asset Sector

According to the Financial Action Task Force (FATF), a varied approach is taken among countries to regulate the virtual asset sector. While some countries have implemented regulatory measures in recent years, others have chosen to prohibit virtual assets entirely. However, the majority of countries have not yet commenced with regulation of this sector. This global regulatory gap has created significant loopholes that can be exploited by criminals and terrorists. Of the 98 jurisdictions that responded to FATF's survey in March 2022, only 29 jurisdictions have enacted relevant laws, and only a small subset of these jurisdictions has introduced enforcement actions. This disparity in regulatory efforts further emphasizes the urgent need for a comprehensive and coordinated international approach to address the risks associated with virtual assets, including their potential use in illicit activities such as terrorism financing.

Cryptocurrencies have emerged as a novel method for criminals to finance a wide range of illicit activities, including terrorist fundraising beyond national boundaries. Evidence indicates that certain terrorist organizations are utilizing cryptocurrencies as a means to raise funds. Although the available public data regarding terrorist use of cryptocurrencies is limited, it is evident that these networks have engaged in fundraising activities through online platforms that rely on crowdsourcing and/or anonymous donations, aiming to circumvent the regulatory measures implemented within the international banking system. In August 2020, the US Department of Justice made a significant announcement regarding the largest-ever confiscation of cryptocurrency associated with terrorism. This action came in the wake of the dismantling of terrorism financing campaigns linked to the al-Qassam Brigades (the military wing of Hamas), al-Qaeda, and ISIS.¹⁰

Terrorist organizations employ cryptocurrencies to create venture capital and obtain higher funding. 11 The European Union's efforts to combat money laundering and terrorism financing within its regional financial system are praiseworthy, with the 5th Anti-Money Laundering Directive being a notable example of such regulations. Difficulties persist, however, due to the potential for jurisdictional arbitrage and the existence of grey areas when determining applicable law, particularly in cross-border contexts.¹² For instance, the integration of crypto assets into general property law varies across jurisdictions, with some successfully incorporating them, while others face complexities due to the requirement of physical existence for property qualification. Even when crypto assets fall within established categories, applying traditional rules to these assets can still be challenging due to their digital nature and the use of Distributed Ledger Technology (DLT), especially in cross-border contexts. A distributed ledger is "a database that is consensually shared and synchronized across networks, spread across multiple sites, institutions or geographies, allowing transactions to have [multiple private or] public 'witnesses. The underlying technology requires the consensus of many data storage points ("nodes"), spread of different jurisdictions. 13 The presence of DLTs with nodes across borders may have technical advantages, however, from a regulatory perspective, it further complicates identification of the applicable jurisdiction's law for crypto asset transactions. This lack of clarity in determining the appropriate legal framework adds to the difficulties in addressing the transnational nature of crypto asset transactions and contributes to the complexities of international cooperation in combating terrorism financing effectively. 14

III. Compilation of Certain Best Practices

In confronting the multifaceted challenges engendered by crypto assets, a discerning identification and prioritization of best practices emerge as imperative. The following presents some best practices that may contribute to building a more secure and trustworthy crypto ecosystem, mitigating the risks associated with crypto crimes.

1. Need for state-driven protective measures

The FATF recommendations require countries to identify, assess, and understand the money laundering and terrorism financing risks emerging from virtual asset activities and the activities or operations of Virtual Asset Service Providers (VASPs). States should adopt a risk-centric methodology to guarantee that countermeasures targeting the prevention or reduction of money laundering and terrorism financing align appropriately with the identified risks. It is imperative for countries to mandate VASPs to undertake the identification, evaluation, and implementation of efficacious measures in order to alleviate the risks associated with money laundering and terrorism financing. For example, a research briefing by the UK House of Commons Library assessing the development of a new regulatory regime for the crypto sector in the UK addressed these risk factors. The report highlights that cryptocurrencies pose major risks to consumers, as they lack

adequate safeguards for investment protection. Cryptocurrency exchanges are susceptible to hacking incidents, thereby jeopardizing the financial assets of users. Moreover, individuals who misplace their cryptographic keys face total forfeiture of their funds. Additionally, the realm of cryptocurrency engenders a diverse array of fraudulent schemes.

Coming to the best practice is the UK Government's commendable initiative, the Consultation on the future regulatory framework for crypto assets, undertaken from February 1, 2023, to April 30, 2023.¹⁷ It elicited responses that underscored a prominent challenge in enforcement. Respondents emphasized the regulatory difficulty in taking enforcement actions against offshore market participants, expressing concerns over practicality and prohibitive costs. However, what is noteworthy the best practice embedded in the Consultation, involving diverse stakeholders such as legal and consulting firms, FinTechs, crypto native firms, academia, and industry associations. This collaborative effort aimed to identify and address challenges associated with enforcement in the crypto asset domain, reflecting a proactive approach to regulatory refinement.

2. Involvement of private entities

The implementation of technology-driven inquiries and the development of the operational capabilities of law enforcement agencies play a vital role in combating contemporary forms of criminal activity. The utilization of blockchain technology serves as the foundational framework for virtual assets or currencies. It is essential that law enforcement agencies possess the necessary proficiency in harnessing blockchain technology in order to effectively identify individuals responsible for criminal acts, trace illicit gains, gather relevant evidence, and seize unlawfully obtained proceeds.

Recognising the importance of technology in the prevention of new age crimes, Interpol, in 2017, launched a project to prevent the criminal use of blockchain technology. The project involved developing efficient and effective forensic tools enabling the reasonable use of different types of data from various sources, including virtual currency ledgers. Similarly, in 2017, the United Nations Office on Drugs and Crime (UNODC) launched training on tackling cryptocurrency-enabled organized crime. A distinctive characteristic of the training programme is its notable collaboration with industry leaders, such as *Chainanalysis*, aimed at providing assistance to law enforcement agencies in the identification and tracking of illicit financial transactions. Binance, one of the largest crypto trading platforms, launched the Global Law Enforcement Training Program to help law enforcement detect financial crimes and cybercrimes and assist in the prosecution of bad players who exploit digital assets.

In short, specialised blockchain companies possess the ability to contribute significant insights regarding money laundering typologies related to cryptocurrencies through analysis of the extensive datasets they possess. The sharing of these findings with law enforcement agencies can serve as a catalyst for initiating investigations and formulating more focused crime prevention strategies.²¹ Furthermore, such information sharing reinforces the fact that fostering a robust cryptocurrency market is a requirement necessitating collaboration between the public and private sectors.

3. Capacity building

The process of asset confiscation and recovery holds significant importance in the realm of law enforcement, ultimately contributing to the enhancement of public trust in the justice system. However, in the context of virtual currency or assets, the challenge is caused by their "virtual", "intangible", "volatile" and, in some cases, "transnational" nature. Hence, the traditional court process and methods of confiscation and recovery may have limited application. The situation is worsened by cryptocurrency tumblers facilitating

money laundering. Recognizing this limitation, the US Department of Justice formed a Virtual Asset Exploitation Unit within the Federal Bureau of Investigation (FBI), which is dedicated to blockchain analysis and virtual asset seizure. The Australian Federal Police also formed a cryptocurrency unit to prevent funnel money and money laundering.²² Thus, the enhancement of capacity within law enforcement authorities stands as an indispensable aspect in the combat against cryptocurrency crimes.

4. Enhancing transparency – the "Travel Rule"

It is of paramount importance that criminals be prevented from exploiting legal loopholes in the national frameworks for anti-money laundering and countering the financing of terrorism by utilizing judicial arbitrage as a means to evade liability. The effective adoption and implementation of the FATF guidelines, particularly the "Travel Rule", introduced in 2019, for VASPs, serve as a crucial protective measure. ²³ The "Travel Rule" is a regulatory provision that imposes an obligation on originating VASPs to acquire and transmit specific information to the beneficiary VASP during the transfer of virtual assets, comparable to the requirements placed upon traditional financial institutions in wire transfers. This information typically includes personal identifiers (such as names, addresses, and account numbers) or unique identifiers such as national identity number or passport number. ²⁴ The overarching objective of the Travel Rule is to bolster transparency, traceability, and accountability of virtual asset transactions, thereby increasing the threshold for illicit activities, such as money laundering and terrorism financing, to transpire without detection.

5. Improvement of mutual legal assistance

In India, challenges revolved around the issue of regulatory arbitrage and the transformation of security challenges from "hawala to crypto currency".²⁵ One potential way to address this matter could involve enhancing the mutual legal assistance treaty framework (MLAT).²⁶ The efficacy of MLAT in facilitating the confiscation of illicit proceeds and discouraging the cross-border location or transfer of crypto assets is exemplified by a recent case in which the United States Department of Justice seized virtual currency valued at approximately \$24 million on behalf of the Brazilian government under the bilateral Treaty between the United States of America and the Federative Republic of Brazil on Mutual Legal Assistance in Criminal Matters.²⁷ Law enforcement agencies may seek assistance through other formal channels, such as the United Nations Convention on Transnational Organized Crime and the Council of Europe Convention on Cybercrime. In the event that no treaty mechanism exists, assistance can be sought through letters rogatory, foreign domestic law mechanisms, and/or comity and reciprocity.²⁸ Therefore, strengthening the international legal framework is crucial for promoting extensive information sharing, early coordination, and deconfliction efforts to ensure the accountability of offenders.

6. Awareness raising

Lastly, it is of utmost importance to raise awareness among the general public and deepen people's understanding of virtual currencies and assets, the legal framework embraced by their respective jurisdictions, the governing regulations, and the inherent risks associated. Knowledge should be shared about potential scams, types of fraud, and other forms of illicit activities. Such an increase level of consciousness is vital for the overall mitigation of digital crimes.

IV. India-EU Collaboration: The Vanguard of Security

At the 12th India-European Union Counter Terrorism Dialogue on 19 November 2020, India and the European Union strongly condemned terrorism in all its forms and manifestations including the use of terrorist proxies

for cross-border terrorism. The participants of the Dialogue emphasised the need for strengthening international cooperation to combat terrorism in a comprehensive and sustained manner. They reaffirmed how crucial it is that perpetrators of violence and terrorism be brought to justice.²⁹

Building upon the strong condemnation of terrorism at the 12th India-European Union Counter Terrorism Dialogue, all stakeholders should consider intensifying their collaborative efforts to counter crypto crimes, focusing specifically on terrorism financing through virtual assets. Recognizing the evolving nature of financial crimes associated with emerging technologies, the upcoming iteration of the India-European Union Counter Terrorism Dialogue presents an opportune moment for India and the European Union to share and implement best practices in countering illicit financial activities facilitated by cryptocurrencies. By leveraging their joint commitment to combatting terrorism and by emphasizing the importance of international cooperation, the stakeholders can establish frameworks and protocols that address the challenges posed by crypto crimes. This collaboration could involve information sharing, capacity building, and the development of legal frameworks enabling the effective investigation and prosecution of individuals involved in terrorism financing through virtual assets. By incorporating these priorities into their ongoing dialogue, India and the European Union can contribute significantly to the global efforts aimed at preventing and combating illicit financial activities associated with terrorism.

V. Conclusion

This article highlighted the main factors necessary for effectively preventing and combating crimes related to virtual currencies and assets. Effective international cooperation emerges as a key element, emphasizing the importance of information sharing, targeted technical assistance, and the establishment of uniform standards and best practices across jurisdictions. By fostering collaboration among countries, the global community can enhance its collective ability to address the challenges posed by these emerging forms of crime. In addition, the establishment of an effective asset confiscation and recovery system both at national level and international level holds significant value, regardless of the geographical location of the illicit proceeds. Such a system acts as a deterrent, impeding the proliferation of organized crime and safeguarding the integrity of the financial market.

Additionally, capacity building for law enforcement officials assumes a vital role, necessitating the creation of specialized units equipped with the requisite skills and knowledge to investigate virtual currency-related crimes. Concurrently, raising public awareness about the risks associated with virtual currencies and assets is crucial, as it empowers individuals to make informed decisions and contributes to the overall prevention of such crimes. By incorporating these key components into their policies, policymakers and stakeholders can formulate comprehensive strategies to mitigate the threats posed by virtual currency-based crimes, ensuring the integrity, stability, and security of the global financial landscape. Indeed, the dialogue forum between India and the European Union offers a valuable platform for fostering the exchange of ideas and engaging in active capacity building activities, particularly in the realm of countering crypto crimes and addressing terrorism financing through virtual assets.

^{1.} Basel Institute of Governance, Crypto asset recovery-scope, laws, and cooperation, February 2022, https://baselgovernance.org/blog/crypto-asset-recovery-qa-part-1-scope-laws-and-cooperation>. All hyperlinks in this article were last accessed on 5 March 2024. ↔

^{2.} Press Information Bureau, Crypto assets are borderless, require international collaboration to prevent regulatory arbitrage, Release ID: 1896722, <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1896722>.↔

^{3.} Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ L 150, 9.6.2023, 1.↔

^{4.} Europol and Basel Institute on Governance, Seizing the opportunity: 5 recommendations for crypto assets-related crime, 2022, https://baselgovernance.org/sites/default/files/2022-12/2022_Recommendations_Joint_Working_Group_on_Criminal_Finances_and_Cryptocurrencies.pdf, p. 3 et seq. ↔

- Ministry of Finance-Government of India, Notification published on 07 March 2023 Gazette ID CG-DL-E-07032023-244184, ..
- 6. H.Fuje, S. Quayyum and T. Molosiwa, "Africa's Growing Crypto Market Needs Better Regulations", IMF Blog 22.11.2022 .↔">https://www.imf.org/en/Blogs/Articles/2022/11/22/africas-growing-crypto-market-needs-better-regulations>.↔
- 7. Financial Action Task Force, Virtual Assets: What, When, How? FATF booklet, https://www.fatf-gafi.org/content/dam/fatf-gafi/brochures/FATF-Booklet VA.pdf>.↔
- 8. Financial Action Task Force, Targeted update on Implementation of FATF's Standards on VA and VASP's, June 2022, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html>.↔
- 9. UN Security Council CTED, Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions, December 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.
- 10. US Department of Justice, Report of the Attorney General's cyber digital task force, October 2020, , €">https://www.justice.gov/archives/ag/page/file/1326061/download>, €
- 11. RAND Corporation, National security implications of virtual currency, 2015, https://www.smallake.kr/wp-content/uploads/2016/02/RAND_R-R1231.pdf.↔
- 12. V. Covolo, "The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive", (2020) 28 (3) European Journal of Crime, Criminal Law and Criminal Justice, 217-251. (also available at https://doi.org/10.1163/15718174-bja10003). ↔
- 13. D.A. Zetzsche, L. Anker-Sørensen, M.L. Passador and A. Wehrli, *DLT-based enhancement of cross-border payment efficiency-a legal and regulatory perspective*, BIS Working Papers No 1015, Bank for International Settlements, May 2022, available at https://www.bis.org/publ/work1015.pdf>.↔
- 14. International Monetary Fund, *Elements of Effective Policies for Crypto Assets*, IMF Policy Paper 23 February 2023, available at .↔
- 15. FATF, Updated guidance for a risk-based approach to virtual assets and virtual assets service providers, 2021, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>. ↔
- 16. House of Commons Library, Cryptocurrencies, Research Briefing, 22 February 2023, https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf. ↔
- 17. HM Treasury- United Kingdom, Future financial services regulatory regime for cryptoassets Response to the consultation and call for evidence, October 2023, https://assets.publishing.services.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf. ↔
- 18. Interpol, *Project to prevent criminal use of blockchain technology launched by international consortium*, 24.5.2017, .↔
- 19. United Nations Office on Drugs and Crime, UNODC launches training to tackle cryptocurrency enabled Organized Crime, 8.5.2017, .↔
- 20. Binance, "Amid growing demand, Binance boosts its global law enforcement training program", Binance Blog 27.9.2022, https://www.bin-ance.com/en/blog/markets/amid-growing-demand-binance-boosts-its-global-law-enforcement-training-program-4745079635127044663.↔
- 21. Europol and Basel Institute on Governance, op. cit. (n. 4).←
- 22. A. de Kretser, "Australian Federal Police forms cryptocurrency unit to hit criminals", Financial Review 5.9.2022, .↔
- 23. U.S. Department of Justice, The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067: How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets, June 2022, https://www.justice.gov/ag/page/file/1510931/download.↔
- 24. FATF, Updated guidance for a risk-based approach, op. cit. (n. 15)↔
- 25. Press Information Bureau of India, "Crypto Assets are borderless, require international collaboration to prevent regulatory arbitrage Under PMLA, Rs. 936 crore related to crypto currency is attached/seized/freezed by ED as on 31.01.2023", https://pib.gov.in/PressReleseDetailm.aspx?
 PRID=1896722> . See also: Press Information Bureau of India, "Full text of Union Home Minister Shri Amit Shah's address at the inaugural session of G20 Conference on Crime and Security in the age of NFTs, Artificial Intelligence and Metaverse in Gurugram, Haryana", 13.7.2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1939176.↔
- 26. S. Parsheera and P. Jha, Cross-Border Data Access for Law Enforcement: What are India's Strategic Options?, Carnegie India, Working Paper November 2020, https://carnegieendowment.org/files/ParsheeraJha_DataAccess.pdf. ↔
- 27. U.S. Department of Justice, "US seizes virtual currencies valued at USD 24 million assisting Brazil in major internet fraud investigation", 4.11.2020, .↔
- 28. S. Parsheera and P. Jha, op. cit. (n. 26), at page 10.←
- 29. Ministry of External Affairs, India, "Joint press release of the 12th India-European Union counter-terrorism dialogue", 19.11.2020, .↔">https://www.mea.gov.in/press-releases.htm?dtl/33217/Joint_Press_Release_of_the_12th_IndiaEuropean_>.↔

COPYRIGHT/DISCLAIMER

© 2024 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.

Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.

Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.

All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

