CRYPTOCURRENCY AND FINANCIAL TERRORISM: AN EMERGING PARADOX IN INDIA

Chandhini T, Christ (Deemed to be University), Bengaluru, India

ABSTRACT

The rapid growth of cryptocurrencies presents a significant challenge in global financial security architecture. In India, particularly the new era of financial innovation and cryptocurrency offers a sophisticated mean of money laundering and financial terrorism. Individuals and Companies uses cryptocurrencies as a medium of exchange. This paper argues that India's current legal system particularly the Prevention of Money Laundering Act, 2002 is inadequate to talk about the unique, decentralized and pseudonymous nature of cryptocurrency. The Cryptocurrency features make the law enforcement authorities difficult in tracing the transaction. When the new digital payment in cryptocurrency developed namely Bitcoin, the terrorist is the first one who take advantage of digitalization to increase profitability. In cryptocurrency the confidentiality is extremely fragile, decentralized and pseudo-anonymous characteristics makes it easier to do crime. This paper analyzed that a cryptocurrency is a prominent tool for money laundering and terrorist financing because of its anonymous features over owner's money. This paper evaluates the legal hurdles in prosecuting cross-border crypto transaction linked to terrorist financing. Finally, by suggesting that India must recognize the need for strong regulation to fight cryptocurrency facilitated financial terrorism.

Keywords: Cryptocurrency, Virtual Digital Asset (VDA), Combating the Financing Terrorism (CFT), Digital Transformation.

Introduction:

Transition in financial technology to digital economy, creates a positive improvement such as unification of the global payment system, high speed transactions etc., on the other way this digitalization paves way for committing crime. Specifically, digitalization has led to the transition of traditional kind of crime to digitalized crime.[1] Modernizing the crime in online space have the characteristics like speed, anonymity, uncertainty in jurisdiction and limitlessness make it easier to commit crime[2]. In recent years, the most of the digital transactions are done by cryptography, which is peer-to-peer transaction, that have no centralized or mediator for the transaction. This crypto transaction has been used easily to do money laundering and financial terrorism transaction because of its pseudonymous and cross-border transaction.[3] In India, the PMLA gradually adopted Virtual Digital Asset (VDA) service providers[4], that have the features of decentralized and jurisdictional challenges which amplify to traditional risk of money laundering and financial terrorism. This research critically evaluate how recent amendment of PMLA is effective in cryptocurrency transaction.

Cryptocurrencies are the forms of virtual currency that are enabled by blockchain technology, are utilized as peer-to-peer alternatives for legal tender, and may be exchanged for and against legal tender.[5] Usually cryptocurrencies will encrypt the coding data to make it unreadable to anyone who lacks a password. The modern cryptocurrencies are known as decentralized system by distributing data that are based on blockchain technologies. The Bitcoin is the first modern cryptocurrency that succeeded in attacking much interest or establishing themselves in financial markets[6]. The rapid growth of cryptocurrency, challenges the global financial security infrastructure. In India, particularly because of financial technological disruptions, cryptocurrency simultaneously offers challenges like financial terrorism and money

[1] C. Rivera, Digital Transformation in Global Finance: How Technology is Shaping the Financial Landscape, 29 Acad. Acct. & Fin. Stud. J. (Special Issue 1) 1, 1-3 (2025).
[2] Anita Singh, Pradeep Kulshrestha & Ritu Gautam, *Cyber Crime, Regulations and Security – Contemporary Issues and Challenges* (The Law Brigade Publishers, Libertatem Media Pvt. Ltd. 2022), https://www.researchgate.net/publication/365172688_CYBER_CRIME_REGULATION_AND_SECURITY_CONTEMPORARY_ISSUES_AND_CHALLENGES.
[3] Chiara Jezerca*, The Rise of Cryptocurrencies: A Tool for Money Laundering or an EU Regulatory Failure?* (Apr. 7, 2025) SSRN 5331403, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5331403.
[4] https://fiuindia.gov.in/pdfs/downloads/VDASP04072023.pdf.
[5] Rumer Ramsey, *An Examination of the Challenges Posed by Cryptocurrencies to AML/CTF Regulation,* 12 *Amst. L.F.* 20, 20-25 (2020), https://amsterdamlawforum.org/articles/10.37974/ALF.368.
[6] Christian Leuprecht, Caitlyn Jenkins & Rhianna Hamilton, *Virtual Money Laundering: Policy Implications of the Proliferation in the Illicit Use of Cryptocurrency,* 30 *J. Fin. Crime* 1036, 1036-1054 (2023), https://www.emerald.com/insight/1359-0790.htm.

laundering. The cryptocurrencies have the characteristics of decentralization, pseudonymity and cross-border transaction makes resistant to the centralized transfers that traditionally underpin financial regulation. In India, even though there are multiple agencies to regulate Virtual Assets, like Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Enforcement Directorate (ED), Financial Intelligence Unit (FIU-IND) and Income Tax Department, but there is no single regulatory authority to exclusively authorize the challenges created by cryptocurrency.[7]

Money laundering is the illegal process of converting the illegal source of money into legitimate money, so that the money can be used freely in the legitimate business operation and does not have to be hide from authorities.[8]Money Laundering is the process that criminal uses to transfer the illegal money into legal money through three stages called placement, layering and integration. Money laundering is considered as a crime in many jurisdictions with various definitions. In India, the money laundering is known as Hawala transactions. The Prevention of Money Laundering Act (PMLA), 2003[9] is the act to prevent money laundering in India and to confiscate and seize the property derived from money laundering. A high-profile money laundering patterns have been used in recent years like by virtual currencies, online gaming, online marketplace, blockchain technology, decentralized finance (DeFi) and financial grooming scams are being used to launder illicit money. Because of the limited expertise in conducting technology-based enforcement and the rising sense of impunity are the challenges faced by criminal justice administrator.[10]

Terrorist Financing aim to help terrorist by providing funds for terrorist activities or organization by soliciting, collecting or providing funds to them.[11] Terrorist groups require financial resources to maintain their operation and to execute the terrorist attack, through various methods employed by these groups to secure funding for their activities. The various legitimate sources like profit from business or charitable organizations or illicit method like trafficking in weapons, humans as well as kidnapping etc., Also money laundering and financial terrorism are the common sources where criminal uses by taking advantage from the

[7] https://finlaw.in/blog/cryptocurrency-law-in-india-current-legal-status-and-regulatory-landscape-2025.
[8] https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/money-laundering/
[9] The Prevention of Money Laundering Act, 2002
https://www.indiacode.nic.in/bitstream/123456789/2036/5/A2003-15.pdf.
[10] https://finlaw.in/blog/cryptocurrency-law-in-india-current-legal-status-and-regulatory-landscape-2025.
[11] https://notabene.id/crypto-travel-rule-101/counter-terrorism-financing-crypto#:~:text=Summary%3A,(AML)%20rules%20via%20cryptocurrency.

weakness of financial systems, that permit excessive anonymity and opacity in financial transactions.[12]

Research Methodology:

The study involves the methodology of primarily doctrinal and analytical, focusing on the legal evaluation and analysis within the Indian regulatory framework. The paper follows a doctrinal research methodology by critically examining the Indian Laws like Prevention of Money Laundering Act (PMLA) and their adaptations to emerge digital financial risks like cryptocurrencies. It also reviews the understanding of how recent amendment treat Virtual Digital Assets (VDA) and analyzes the challenges faced by enforcement authorities such as Enforcement Directorate (ED). The research follows qualitative approach by legal and policy analysis with the help of secondary data like Prevention of Money Laundering Act, 2023 amendment and comparative insights with European Union AML directives by highlighting regulatory gaps and technological challenges[13]. Also, the study analysis challenges faced by authorities in practical and real-world and gave insights like implementing KYC and international MLAT usage etc., The research highlighted the comparative study of cryptocurrency with banking transactions, to understand better how banking transactions are regulated monitored easily and know the identity of the customer.

Research Question:

1. How do the characteristics of cryptocurrencies undermine the principles of traditional anti-money laundering (AML) and counter financial terrorism (CFT) framework established under the PMLA?

2. How the recent amendment of PMLA is effective on VDA Service Providers and what are the challenges faced by ED enforcement?

3. What are the legal hurdles in prosecuting cross-border crypto transactions linked to terror financing?

[12] Eziho Promise Ogele, *Terrorist Financing in the Digital Age: An Analysis of Crypto- currencies and Online Crowd Funding,* 6 *J. Terrorism Stud*. 4, 4-25 (2025), https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1121&context=jts.
[13] Chiara Jezerca, *The Rise of Cryptocurrencies: A Tool for Money Laundering or an EU Regulatory Failure? SSRN Elec. J.* 5331403 (2025), https://dx.doi.org/10.2139/ssrn.5331403.

AML/CFT Technological Disruption:

The recent development in digital economy, on the one side it is positively upper handed such as the high speed of transactions, unification of the global payment system etc., on the other side it is the reason for the development of traditional types of crimes that have been known for a long time[14]. The Anti-Money Laundering and Counter Financial Terrorism (AML/CFT) law plays as an integral and viable to the global financial system as well as the economy of the member nations.[15] Crypto money laundering happens by exploiting digital assets such as Bitcoin and privacy coins to get illicit proceeds. The rapid growth in technology and the adoption of digital payment system, virtual currencies, and online platforms have opened opportunities for criminals to launder money. The technological development challenges the government, financial institution and law enforcement agencies. However, digital revolution has presented unique challenges, especially in financial crime. Also, the revolutionized financial transactions like online banking, e-commerce platforms and mobile payment apps have increased the volume and complexity of digital financial transactions, this digitalization in financial transactions also create a new opportunity for money laundering. In the Bitcoin Extortion case in 2018,[16] highlighted the ability of legal system in handling complex crimes involving digital assets and digital transactions and the consequences for those who got financial gain from extortion and court sentenced life imprisonment and imposed significant fines and ordered seizure of assets.

The technological innovation in digital economy challenges the financial norms such as Anti-Money Laundering and Counter Financial Terrorism. The money launders and financial terrorist are getting advantages from new technological methods. The comparative study of banking transaction and cryptocurrency, in Banking, transactions are centralized, traceable, identity of the customer linked with banks and will be monitored for compliance but in cryptocurrency method, it decentralized, pseudonymous, cross-borders transaction, details of the customers will be encrypted and peer-to-peer transaction. Thus, the cryptocurrency transactions, involves sending and receiving digital assets between wallets on public or private blockchains without intermediaries or encrypted identification parties' details make it easier to

[14] Viktoriia Dyntu & Oleksandr Dykyj*, Cryptocurrency as an Instrument of Terrorist Financing,* 7 Baltic J. Econ. Stud. 67 (2021), https://doi.org/10.30525/2256-0742/2021-7-5-67-72.
[15] International Monetary Fund: *New strategic direction in the Fund's AML/CFT Engagement*, https://www.imf.org/en/Topics/Financial-Integrity/amlcft#overview.
[16] Bitcoin Extortion case, 2018

commit crime.[17]Thus, the prevailing legal framework of AML/CFT provides framework for traditional financial transactions like 'Know Your Customer'(KYC), Customer Due Diligence (CDD) and customer's money transaction monitoring obligations etc.,[18] The basic reason for Know your customer is to understands the normal transaction pattern of the customer so that everything will be updated and reported by the authority. Like criminals, authorities also learning to develop their skills in new technologies by learning Artificial Intelligence (AI), machine learning, to improve transaction monitoring system called 'RegTech'.[19]

Challenges Posed by Cryptocurrencies and AML/CFT Regulations:

Cryptography is the kind of technique where information will be encrypted into an unreadable format that can only be decrypted when customers apply the secret key. The secret key will be randomly generated as a set of numbers or characters that is used to encrypt or decrypt information.[20] Cryptocurrencies is the type of Virtual Currency, which are typically supported by blockchain technology. Comparing to banking transactions, cryptocurrency have no intermediary that will report everything, the transaction will be anonymous, peer-to-peer transaction that only the parties know the information with the help of private and public key.[21] The money laundering is the method of 'layering' the illegal money into 'clean' money before giving it back to the owner,[22] and the terrorist financing means generating and transferring the money to terrorist group to do the terrorist attack. Criminals collect cryptocurrencies either from purchasing them on exchanges or Peer-to-peer platforms, after receiving money from darknet markets or crypto-enabled scams criminals will try to convert that money through money laundering with three stages are placement, layering and integration.[23] Once money laundering process started in placement is the first stage, here parties will find the place to launder the money usually like business, shell companies, NGOs, bank accounts, Real estate,

[17] N. Gowda & C. Chakravorty, *Comparative study on cryptocurrency transaction and banking transaction.* Global Transitions Proceedings, 530 (2021), https://doi.org/10.1016/j.gltp.2021.08.064.
[18] Agrima Dwivedi, Cryptocurrency in India: KYC and AML Regulations [2026 Guide], Signzy (Jan. 16, 2026), https://www.signzy.com/blogs/cryptocurrency-in-india-kyc-and-aml-regulations-2025-guide.
[19] https://moringa-tech.com/the_role_of_regtech_in_strengthening_indias_financial_infrastructure.php.
[20] https://www.c-sharpcorner.com/article/cryptography-in-net/.
[21] Robby Houben & Alexander Syners, *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*, Policy Dept. for Economic, Sci. & Quality of Life Policies, European Parliament (20218), https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf.
[22] https://www.unit21.ai/blog/3-stages-of-money-laundering-placement-layering-integration.
[23] Emily Fletcher, Charles Larkin and Shaen Corbet, *Countering Money Laundering and Terrorist Financing: A case for Bitcoin Regulation.* 56 Res. In Int'l Bus. & Fin. 101387 (2021), https://doi.org/10.1016/j.ribaf.2021.101387.

professional services and there are many that criminals are finding to invest the money to hide it from government authorities. Next stage is layering criminals will use bookkeeping and other practices to make transaction legitimate and last stage will be Integration, where criminals will withdraw the clean money and deposit in financial institution so that they can use it later without any fear from government.[24]

Firstly, the cryptocurrencies are used for money laundering and financial terrorism, which is because of decentralized and peer-to-peer transfer nature of transactions. Usually, cryptocurrencies use blockchain, where there will be no intermediaries. But in traditional financial transactions like fiat currency, where the intermediaries are required to guarantee the security of customer's accounts and transactions. As per AML/CTF regulations, for traditional transactions the intermediary will be focused mainly. For example, in the EU's perspective, the fourth AML Directives[25] when parties entering in any business or having bank account, the authorities to identify, verify and monitor transactions and to report suspicious transactions. To verify and identify the identity of the clients 'Know Your Customer' or KYC required. Hence, cryptocurrency is totally contrast with fiat currency where no central party in cryptocurrency transactions on which to place the regulatory burden. This will conceal their identity, because coins are sent and received by 'public address' which is a combination of character not linked publicly to each owner.[26] The pseudonymous and anonymous characteristic will be depend on the type of cryptocurrency. For example, Bitcoin is pseudo-anonymous in nature, since the customers address will be displayed on the public Bitcoin blockchain.[27] In pseudo anonymity method it allows individual to engage in an online transaction without exposing their sensitive details, the identity will be linked to an alias. Example Bitcoin wallet addresses. This pseudonymous nature and P2P transactions frustrate the authorities to identify the transaction details this clashes with AML/CTF framework and particularly frustrate 'KYC' requirement. There is no chance to identify if they don't know who the parties are.[28] In order to successfully combat money laundering and terrorist financing via cryptocurrencies, it is necessary to move

[24] Ibid.,
[25] https://finance.ec.europa.eu/document/download/899697f5-b2f4-4127-bf8b-b5514b01ab3a_en?filename=amld4-level-2-measures-full_en.pdf.
[26] Lucas Auffenberg, *Crypto Currencies as a New Challenge to Anti-Money Laundering Regulation and the Know- Your- Customer- Principle* (2019), https://fsblockchain.medium.com/crypto-currencies-as-a-new-challenge-to-anti-money-laundering-regulation-and-the-e6429461c13e.
[27] Ibid., p.3.
[28] Ibid., quoting Deloitte principal Fred Curry.

beyond a regulatory paradigm that is focused on intermediaries.[29]

The cross-border transaction in cryptocurrency which will be based on online transfers and there will be no limitation in national jurisdiction,[30] this challenges the general system of regulation and enforcement by nation states. Mostly it is difficult for regulators to assert national jurisdictional over specific cryptocurrency systems or players. As per EU Members, the member states must come under AMLD5, can simply choose to locate themselves in jurisdiction with lax AML/CTF controls.[31] The anonymous, P2P, and intangible digital nature of cryptocurrencies, which are not tied to any particular location and can be almost instantaneously transacted, means they are particularly hard for regulator to reach.[32] In order to regulate money laundering and terrorist financing the rules must be adopted to international or global level. The Financial Action Task Force (FATF) plays the important role to regulate them in globally, who sets global standard for AML. Even though the EUs' AMLD5 approach is there but it is generally slow and incremental and a varied global patchwork or regulation remains. To suggest that possibility of adopting 'non-state' or 'a national' laws detached from state jurisdictions.[33] Overall, cryptocurrency is challengeable to AML/CFT regulation, that doesn't solvable with current regulatory paradigm. By using privacy, it grants cryptocurrency the full anonymity and no intermediary which undermine the AML/CFT regulation. The borderless cryptocurrency transactions make it necessary for borderless regulatory solution, which seems out of reach within a system based on state sovereignty.

PMLA's 2023 Amendment on Cryptocurrency Regulation:

In the year of 2023, Prevention of Money Laundering Act, 2002, got amended by adding Virtual Digital Asset (VDA) or Crypto Asset comes under the regulatory ambit, further the potential risk, including economic, financial, operational, legal and security concerns will be handled by Reserve Bank of India (RBI) and identifying the operational and enforcement challenges by Enforcement Directorate (ED).[34] Further, this study evaluates the assess whether

[29] Ibid.,
[30] Bank for International Settlements – "Digital Currencies" (CPMI Report): Bank for Int'l Settlements, Comm. On Payments & Market Infrastructures, Digital Currencies 12 (2015), https://www.bis.org/cpmi/publ/d137.pdf.
[31] European Parliament, 2018, Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion. P.54.
[32] Financial Action Task Force, *Guidance for a Risk Based Approach: Virtual Currencies 32* (June 2015), https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html?utm_source=chatgpt.com.
[33] https://www.nottingham.ac.uk/research/groups/commercial-law-centre/blog/what-is-a-national-law.aspx.
[34] https://www.virtualassets.com/news/what-is-the-difference-between-a-virtual-asset-and-a-digital-asset/.

the inclusion of cryptocurrency exchanges, wallet providers and reporting entities under the Prevention of Money Laundering Act has genuinely bridged the regulatory gap between the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) frameworks. This study aims to explore how the recent amendment of PMLA is adapting the decentralized, borderless and pseudonymous nature of cryptocurrency transactions as like centralized financial transactions, and whether ED is sufficiently equipped to enforce compliance in such dynamic environment.

The amendment mandated that all the entities dealing with exchange, transfer, safekeeping and administration of VDAs or providing related financial services, will regulate under PMLA.[35] Which means VDAs service provider must conduct Know Your Customer (KYC) checks, and to maintain transaction records and report suspicious activity to the Financial Intelligence Unit (FIU-IND).[36] The amendment has expanded the ED's jurisdiction to cover crypto assets also making it harder for the illicit actor to exploit exchanges as "black holes" for laundering money. By adding Virtual Digital Asset in the PMLA, makes the VDA service providers to report entities if they found any suspicious transaction, that law ensures they must verify the identities of their customers.[37] In theory, this strengthens the capacity to detect, trace and disrupt laundering schemes involving cryptocurrencies. For example, if criminal group attempts to convert illicit money into Bitcoin through India exchange method, then the platform to perform due diligence and notify authorities. These duties specifically have unregulated space and aligned India more closely with global AML norms.

However, in practical this structural and operational challenges are effectively limited. Comparatively, the bank account is centralized and the data will be updated to government automatically but in the cryptocurrencies, they are not like bank accounts, cryptocurrencies are decentralized, pseudonymous and cross-border nature, the crypto wallets do not have names or address attached;[38] so, the enforcement agencies rely on blockchain forensics, which requires technical expertise and costly tools. The Enforcement Agencies, automatically struggles to investigate due to lack of specialized manpower and training. Secondly, the crypto transactions are vague that occur on foreign exchanges or through decentralized finance (DeFi) protocols,

[35] Rohan Bagai, Aprajita Rana & Navdeep Baidwan, *Virtual Currency Regulation Review* (2025), AZB Partners, Advocates & Solicitors, https://www.azbpartners.com/bank/virtual-currency-regulation-review-2025/.
[36] https://blogs.law.ox.ac.uk/oblb/blog-post/2023/07/digital-assets-indian-anti-money-laundering-regime.
[37] Ibid.,
[38] Vajiram & Ravi, Cryptocurrency, Functioning, Advantages and Disadvantages, Concern (2025), https://vajiramandravi.com/upsc-exam/cryptocurrency/.

which are not bound by India law. In India, it is easy to open an account with an offshore platform, bypassing PMLA obligation altogether. Thirdly, even within India, the compliance levels among VDA Service Providers vary widely. Some people have updated to KYC mechanism, but smaller platforms may lack the resources or incentives to fully implement reporting systems, creates uneven enforcement. Fourth, the amendment lacks to specify privacy coins, mixers, decentralized exchanges and peer-to-peer transfers, which continue to facilitate laundering activities outside the scope of traditional regulation.[39]

Under the PMLA, in the viewpoint of Enforcement Directorate, the ED have extensive investigative authority in the form of attachment, seizure and arrest, which presupposes one of the centralized intermediaries over which the ED can put pressure or even compel to disclose information[40]. There will be no single transactions made in the crypto space, the hundreds of transactions across the borders will be made every second. Gathering evidence in the international exchange will be tedious and cumbersome as it requires the use of the Mutual Legal Assistance Treaties (MLATs). Besides, the definition of Virtual Digital Asset has been left wanting under the PMLA itself and this creates legal uncertainty in courts, which may undermine prosecutions.

The technological transparency, cross-border enforcement restriction, imbalanced a multi-pronged reform strategy to reinforce the amendment so as to become more effective. To begin with the PMLA must clearly identify VDAs and implement its requirements to the new technology such as DeFi protocols, privacy-enhancing cryptocurrencies and NFT markets. Second, India needs to take initiative to resolve the jurisdictional issues through the active involvement of the international co-operation via joining FATF to spearhead initiatives and entering new faster digital-principal-data-exchange agreements and exchanges with the international regulators. Third, the VDAs Service Providers compliance schemes has to reinforce Uniform KYC standards, periodical audits and mandatory registration with the FIU.

In conclusion, the amendment to the PMLA it is a standard move towards identifying the VDA Service Providers within the compliance regime, as much as operational and enforcement issues pose a challenge to the ED, both in terms of technological overburden as well as jurisdiction. In addition, there should be as elaborate and progressive regulatory framework to

[39] Ibid.,
[40] Directorate of Enforcement, September, 2021, https://enforcementdirectorate.gov.in/what-we-do.

make sure that India is able to promote innovation int the digital economy and at the same time to protect against money laundering and financial terrorism.

Cross-Border Crypto Jurisdictional Challenges:

A special legal and jurisdictional challenge to explore and pursue by the authorities as per traditional Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regimes were never intended to address.[41] Cryptocurrency transfers are not limited by geographical borders and a central authority as the centralized banks do, but rather exist on decentralized, peer-to-peer networks where the asset transfer is not regulated by law and no bilateral treaties are involved. This renders it especially challenging to determine the physical or legal jurisdiction in which a transaction is done by the law enforcement agencies.[42] For example, a terrorist group in South Asia can be funded by a donor in Europe, captured through privacy-enhancing coins such as Monero due to the privacy mix hosted on servers in Eastern Europe and later withdraw it in one of the exchanges in the Middle East, all with the help of Bitcoin. In this case, one particular country does not have all the jurisdiction in the chain of transactions.

The majority of the nations such as India have numerous legal challenges such as absence of harmonized regulation over the cryptocurrencies. Although recently Virtual Digital Asset (VDA) Service Providers have been brought within the ambit of the Prevention of Money Laundering (PMLA) law in India, the law does not provide extra-territorial force unless it is backed by international treaties. The official of Enforcement Directorate (ED) may investigate domestic dealings but not oblige a foreign exchange in Singapore or Seychelles to exchange customer information or free wallets until there is a worldwide cooperation framework there. This is further complicated by anonymity and pseudonymity of cryptocurrency. When it is possible to track a suspicious flow with blockchain analysis tools, foreign exchanges or custodians are needed to match a wallet address with a real word identity, and not all of them have the same or more rigorous AML requirement. Moreover, the collection of evidence in the digital course also poses significant evidentiary issues: the Indian courts are yet to decide on the admissibility of evidence based on blockchain, not to mention the issues which may arise when the evidence is collected in other jurisdictions with different data-protection regulations.

[41] Jordan Nelson, Linda Peter & Alice Martin, *Cross-border Cryptocurrency Transactions and their role in Money Laundering: Challenges and Regulatory Responses* (Aug. 2025), https://www.researchgate.net/publication/394520272.
[42] Ibid.,

Technologically, cryptocurrencies challenge the underlying basis of the conventional AML/CFT models, which presupposes the presence of financial intermediaries, which are centralized to implement compliance and report suspicious activity. In decentralized system there are no such intermediaries and regulators are faced with the challenges of fitting an entity centric concept to a protocol centric reality. The fact that there is not a globally adopted definition of cryptocurrencies also makes the issue worse.[43] Other countries treat them as assets, commodities or even securities or even currencies. An example is India which does acknowledge Virtual Digital Assets as taxable and compliant with PMLA but has nit provided a legal characterization. This ambiguity of definition results in a grey situation in international law: can seizure or repatriation of assets be implemented when India sees crypto as property by PMLA, but it is not in another jurisdiction?[44]

Even the PMLA itself presents significant gaps in the application to cryptocurrencies, firstly, although VDA Service Providers are identified as reporting entities, only the physically present or those which are operating in India are subject to this requirement. Platforms that serve to the Indian users are not subject to enforcement. Secondly, the PMLA lacks specifications on dealing with crypto evidence, including blockchain transaction records, private keys or decentralized exchange transactions. This lack of evidentiary clarity creates an opportunity to fight prosecutions by defense lawyers, thirdly the ED possesses sweeping authority in the PMLA, the authority assumes collaboration with centralized institutions like banks: in crypto, collaboration depends on foreign jurisdictions, most of which have a limited interest in doing so. Lastly, the dependence of India on traditional MLATs and diplomatic requests means that a procedural gap does exist, since once request are processed, money is often laundered away.[45]

These gaps can only be removed with the help of legislative changes, technology, investment as well as international collaboration. First, India needs to come up with a holistic cryptocurrency legislation that defines cryptocurrencies legalistically and explicitly covers them in the property category of the PMLA. This would seal the loopholes in the process of seizing assets and allows crypto-assets to be attached and forfeited in the same way as fiat

[43] Samuel Chibueze Udenta, *Anti-Money Laundering and Countering the Financing of Terrorism using Blockchain Technology in the United States: Challenges and Ways Forward* (May 27, 2024), SSRN Paper No. 4870208, https://dx.doi.org/10.2139/ssrn.4870208.
[44] Ibid.,
[45] Ibid.,

assets.[46] Second, the government ought to create a specialized process of digital evidence in crypto cases such as identification of blockchain transaction records and standardized procedures of recording wallet data. The judicial and investigative system should be trained to deal with the technical issues of crypto forensics to ensure that evidence is not lost in court.[47]

Finally, the enforcement activities should be accompanied by prevention strategies, by intensifying the KYC standards of Indian VDA Service Providers, imposing the monitoring of transactions, and imposing punishments on non-observing will minimize domestic risks. Meanwhile, social sensitization efforts should inform users of the dangers of fallings prey in the terror money laundering activities like being used as money mules. Shell companies would also be checked by transparency in corporate ownership and connection of the VDA platforms with useful ownership registries. Combined, these actions would not only enable Indian authorities to investigate and prosecute cross-border crypto crimes more efficiently, but also make India an active driver of the global regulation of the rules of digital finance. To conclude, the cryptocurrency paradox of being an innovation and a danger means India must do more than patchwork amendments since the innovative and threatening aspects of crypto-facilitated terror demand both a paradigm shift in Indian law, technical and diplomatic policies that will see the financial system resistant to the new menace of crypto-facilitated terror being final.

Finally, enforcement efforts must be complemented with preventive measures. Strengthening KYC norms for Indian VDA Service Providers, mandating transaction monitoring, and enforcing penalties for non-compliance will reduce domestic risks. At the same time, public awareness campaigns should educate users about risks of becoming unwitting participants in terror financing schemes, such as being recruited as "money mules".[48] Transparency in corporate ownership and linking VDA platforms to beneficial ownership registries would also curb misuse by shell companies. Taken together, these measures would not only empower Indian authorities to investigate and prosecute cross-border crypto crimes more effectively but also position India as a proactive global player in shaping the rules of digital finance.[49] In

[46]https://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA%20In%20The%20Media/News%20Articles/Crypto-assets-brought-under-PMLA_-First-step-towards-legitimizing-Crypto-Industry---Times-of-India.pdf.
[47] Kushalveer Singh Bachchas, *Digital Forensics in the Age of Cryptocurrency: Investigating Blockchain and Crypto Crimes* (2024), LevelBlue, https://levelblue.com/blogs/security-essentials/digital-forensics-in-the-age-of-cryptocurrency-investigating-blockchain-and-crypto-crimes.
[48] Guna Sekar S. & Preetham Kumar B., *The Impact of Cryptocurrencies on Anti-Money Laundering and Counter-Terrorist Financing* (2023), https://www.jetir.org/papers/JETIR2308496.pdf.
[49] Caribbean Fin. Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Aruba-Mutual Evaluation Report* (2022), https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-mer/CFATF-Mutual-Evaluation-Report-Aruba-2022.pdf.coredownload.inline.pdf.

conclusion, the paradox of cryptocurrencies as both an innovation and a threat requires India to go beyond patchwork amendments as both an innovation and a threat requires India to go beyond patchwork amendments and embrace a paradigm shift in legal, technical and diplomatic approaches ensuring that its financial system is resilient against the emerging threat of crypto-facilitated terror final.

Analysis:

The emergence of cryptocurrency has permanently changed the financial sector of the world and India, bringing about new opportunities and enormous threats, especially in the area of money laundering and terrorist financing.[50] The paper highlights that the fundamental principles of cryptocurrencies, decentralization, pseudonymity, and borderless transactions are the direct adversaries of the principles of the traditional anti-money laundering and counter terrorist financing (AML/CFT) policies such as the Prevention of Money Laundering Act, (PMLA).

With the transition to online finance, the traditional crimes have been transformed into advanced cybercrimes. The anonymity, real-time, lack of jurisdiction and ability to cross borders of cryptocurrencies makes it extremely easy to use such technologies to process illegal activities by criminals as well as terrorist groups.[51] In contrast to banks, which is a centralized and easily controlled structure, crypto transactions are peer-to-peer and takes place in the absence of any third party, which makes such traditional compliance measures as KYC and CDD hard to implement.[52]

India does not have a central regulator although different agencies exist to control some elements of the virtual assets such as RBI, SEBI, ED, and FIU-IND, as well as the IT Department. The fact that Virtual Digital Asset (VDA) service providers now fall under the amended PMLA, still exist loopholes. Technological opaqueness, a lack of forensic proficiency and the lack of concise legal definitions or standard operating procedures with which is to work

[50] Urvashi Malik & Rishabh Miglani, (2025), *Cryptocurrency and Money Laundering: Risks and Regulatory Challenges* 2025), https://www.ijfmr.com/papers/2025/2/40898.pdf.
[51] Kanishka Raju, *Cryptocurrency and Requirement of Specific Indian Legal Regulatory Framework for Cryptocurrency* (2025), https://www.researchgate.net/publication/392524793_Cryptocurrency_and_Requirement_of_Specific_Indian_Legal_Regulatory_Framework_for_Cryptocurrency.
[52] Ibid., p. 14

with cryptographic evidence all hinder the enforcement agencies.

Cryptocurrencies make the flow of funds across borders relatively effortless, which enables the criminal and terror networks to make complex, nontraceable webs of value transfer across borders. These enforcement issues are compounded by the lack of harmonized international laws and definitions of crypto-assets, and authorities are left to use slow diplomatic processes and few legal avenues to address when assets are moved to jurisdictions that do not comply.[53]

Suggestions and Conclusion:

The regulatory effectiveness of cryptocurrency related AML/CFT threats, the robust and multiagency legislative framework would have to include and explicitly address all crypto assets, such as DeFi technologies, privacy coins and NFT markets, etc. The uniform KYC and CDD should become obligatory to all virtual digital asset service providers and backed by a strong audit and severe punishment in case of non-compliance. At the same time, advanced AI oriented blockchain analytical tools and training of investigators require considerable investment to allow tracing the use of digital evidence in real-time. The international collaboration must be expanded by data sharing arrangements and aligning evidentiary principles to enable the authorities to control the offshore transactions and cross border processes. The preventive disclosure of beneficial ownership and pervasive public awareness of the dangers of crypto-based financial crime will further enhance the enforcement process and the preventive perspective, which allow India to stabilize its financial system without a drag on technological development and innovation. India should understand that combating financial terrorism through cryptocurrency is not only a regulatory battle, but a battle of existence; that must be fought with legislative, technological and international forces. Such a comprehensive solution is the only way of ensuring that the financial system and society of India is resistant to the new challenge of crypto-driven crime so that innovation should be supported and the basic national and international interest is preserved.

[53] Caribbean Financial Action Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Mutual Evaluation Report* 2022, https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-mer/CFATF-Mutual-Evaluation-Report-Aruba-2022.pdf.coredownload.inline.pdf.

References:

1. C. Rivera, Digital Transformation in Global Finance: How Technology is Shaping the Financial Landscape, 29 Acad. Acct. & Fin. Stud. J. (Special Issue 1) 1, 1-3 (2025).

2. Anita Singh, Pradeep Kulshrestha & Ritu Gautam, *Cyber Crime, Regulations and Security – Contemporary Issues and Challenges* (The Law Brigade Publishers, Libertatem Media Pvt. Ltd. 2022), https://www.researchgate.net/publication/365172688_CYBER_CRIME_REGULATION_AND_SECURITY_CONTEMPORARY_ISSUES_AND_CHALLENGES.

3. Chiara Jezerca, The Rise of Cryptocurrencies: A Tool for Money Laundering or an EU Regulatory Failure? (Apr. 7, 2025) SSRN 5331403, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5331403.

4. Rumer Ramsey, *An Examination of the Challenges Posed by Cryptocurrencies to AML/CTF Regulation,* 12 *Amst. L.F.* 20, 20-25 (2020), https://amsterdamlawforum.org/articles/10.37974/ALF.368

5. Christian Leuprecht, Caitlyn Jenkins & Rhianna Hamilton, Virtual Money Laundering: Policy Implications of the Proliferation in the Illicit Use of Cryptocurrency, 30 J. Fin. Crime 1036, 1036-1054 (2023), https://www.emerald.com/insight/1359-0790.htm.

6. Eziho Promise Ogele, Terrorist Financing in the Digital Age: An Analysis of Crypto-currencies and Online Crowd Funding, 6 J. Terrorism Stud. 4, 4-25 (2025),

   https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1121&context=jts.

7. Viktoriia Dyntu & Oleksandr Dykyj, Cryptocurrency as an Instrument of Terrorist Financing, 7 Baltic J. Econ. Stud. 67 (2021), https://doi.org/10.30525/2256-0742/2021-7-5-67-72.

8. International Monetary Fund: New strategic direction in the Fund's AML/CFT Engagement, https://www.imf.org/en/Topics/Financial-Integrity/amlcft#overview.

9. N. Gowda & C. Chakravorty, Comparative study on cryptocurrency transaction and banking transaction. Global Transitions Proceedings, 530 (2021), https://doi.org/10.1016/j.gltp.2021.08.064.v

10. Agrima Dwivedi, Cryptocurrency in India: KYC and AML Regulations [2026 Guide], Signzy (Jan. 16, 2026), https://www.signzy.com/blogs/cryptocurrency-in-india-kyc-and-aml-regulations-2025-guide.

11. Robby Houben & Alexander Syners, Cryptocurrencies and Blockchain: Legal Context

and Implications for Financial Crime, Money Laundering and Tax Evasion, Policy Dept. for Economic, Sci. & Quality of Life Policies, European Parliament (20218), https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf.

12. Emily Fletcher, Charles Larkin and Shaen Corbet, Countering Money Laundering and Terrorist Financing: A case for Bitcoin Regulation. 56 Res. In Int'l Bus. & Fin. 101387 (2021), https://doi.org/10.1016/j.ribaf.2021.101387.

13. Lucas Auffenberg, Crypto Currencies as a New Challenge to Anti-Money Laundering Regulation and the Know- Your- Customer- Principle (2019), https://fsblockchain.medium.com/crypto-currencies-as-a-new-challenge-to-anti-money-laundering-regulation-and-the-e6429461c13e.

14. Bank for International Settlements – "Digital Currencies" (CPMI Report): Bank for Int'l Settlements, Comm. On Payments & Market Infrastructures, Digital Currencies 12 (2015), https://www.bis.org/cpmi/publ/d137.pdf

15. Financial Action Task Force, Guidance for a Risk Based Approach: Virtual Currencies 32 (June 2015), https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html?utm_source=chatgpt.com

16. Rohan Bagai, Aprajita Rana & Navdeep Baidwan, Virtual Currency Regulation Review (2025), AZB Partners, Advocates & Solicitors, https://www.azbpartners.com/bank/virtual-currency-regulation-review-2025/.

17. Vajiram & Ravi, Cryptocurrency, Functioning, Advantages and Disadvantages, Concern (2025), https://vajiramandravi.com/upsc-exam/cryptocurrency/.

18. Samuel Chibueze Udenta, Anti-Money Laundering and Countering the Financing of Terrorism using Blockchain Technology in the United States: Challenges and Ways Forward (May 27, 2024), SSRN Paper No. 4870208, https://dx.doi.org/10.2139/ssrn.4870208.

19. Kushalveer Singh Bachchas, Digital Forensics in the Age of Cryptocurrency: Investigating Blockchain and Crypto Crimes (2024), LevelBlue, https://levelblue.com/blogs/security-essentials/digital-forensics-in-the-age-of-cryptocurrency-investigating-blockchain-and-crypto-crimes.

20. Guna Sekar S. & Preetham Kumar B., The Impact of Cryptocurrencies on Anti-Money Laundering and Counter-Terrorist Financing (2023), https://www.jetir.org/papers/JETIR2308496.pdf.

21. Caribbean Fin. Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Aruba-Mutual Evaluation Report* (2022), https://www.fatf-

gafi.org/content/dam/fatf-gafi/fsrb-mer/CFATF-Mutual-Evaluation-Report-Aruba-2022.pdf.coredownload.inline.pdf

22. Urvashi Malik & Rishabh Miglani, (2025), Cryptocurrency and Money Laundering: Risks and Regulatory Challenges 2025), https://www.ijfmr.com/papers/2025/2/40898.pdf.

23. Kanishka Raju, *Cryptocurrency and Requirement of Specific Indian Legal Regulatory Framework for Cryptocurrency* (2025), https://www.researchgate.net/publication/392524793_Cryptocurrency_and_Requirement_of_Specific_Indian_Legal_Regulatory_Framework_for_Cryptocurrency.