A CURRENCY WITHOUT BORDERS, A CRIME WITHOUT FACE: RETHINKING LAW AND POLICY FOR CRYPTO GOVERNANCE

Isha Agarwal, Symbiosis Law School, Noida

ABSTRACT

Emerging cryptocurrencies have disrupted financial ecosystems worldwide and have provided decentralised systems to replace traditional banking systems. The extensive use of cryptocurrencies in India has increased through high rates of digitalisation and accelerated fintech activity during the COVID-19 pandemic. Nonetheless, these assets' decentralised and anonymous nature has also fostered an explosion in cybercrimes such as money laundering, Ponzi schemes, dark-net purchases, and cross-border frauds such as pig butchering and crypto drainers. This research critically analyses the technological, legal and regulatory intricacies of cryptocurrency crimes in India, noting weaknesses in the system and the obstacles to enforcement. It then examines the national and international legal response, the responsibility of exchanges and intermediaries, and proposes effective regulatory reforms. India is balancing innovation with enforcement, making a flexible, harmonised legal framework aligned with global best practices essential for curbing misuse and ensuring safe crypto adoption.

Keywords: Cryptocurrency, Cybercrime, Money Laundering, Legal Regulation, Blockchain Technology

INTRODUCTION

The rapid expansion of internet access has transformed India's digital landscape, reshaping social behaviour and financial transactions.[1] With the number of internet users in India expected to cross 900 million by 2025,[2] and over 107 million individuals reportedly holding cryptocurrency assets, the country is witnessing a significant shift in how people manage and invest their money.[3] The onset of the COVID-19 pandemic accelerated this trend. As banks and ATMs temporarily shut down, cryptocurrencies emerged as an alternative financial tool, gaining widespread traction.[4] Cryptocurrency as an economic asset has seen phenomenal growth in the 21st century and has changed how individuals, businesses and a few governments interact with finances, garnering immense public attention[5]. The advent of cryptocurrency in late 2008 has changed the banking and financial world and opened the gateway for new methods of money laundering, crimes of a severe nature[6].

While cryptocurrency had already seen phenomenal global growth since its inception in 2008, the pandemic created conditions for its mass adoption in India. Legal ambiguity, technological accessibility, and socio-economic stress contributed to this surge. One of the primary technological advantages of cryptocurrency is its borderless nature, which enables peer-to-peer transfers without intermediaries or government oversight. This decentralised system offered instant financial solutions at a time when traditional infrastructure was inaccessible. The Hon'ble Supreme Court in 2020 in the case of ***Internet and Mobile Association of India vs. The Reserve Bank of India***[7] struck down the RBI circular that prohibited banks and RBI-regulated entities from dealing with virtual currency exchanges. The Court held the circular to

[1]J. P. Singh and J. Saxena, "Navigating Cybercrime in India: Legal Complexities, Enforcement Dynamics, and Emerging Challenges in a Digitally Connected Society" (2025) 3 *LawFoyer International Journal of Doctrinal Legal Research* 650.
[2]S. Sen, "India to Cross 900M Internet Users by 2025 Led by Rural Areas" *YourStory* (25 January 2025), available at https://yourstory.com/2025/01/india-to-cross-900m-internet-users-by-2025-led-by-rural-areas (last accessed on 8 July 2025).
[3]India Crypto Research, "Crypto Adoption & Blockchain Outlook in India" *India Crypto Research* (28 April 2025), available at https://indiacryptoresearch.co.in/learn/blogs/crypto-adoption-blockchain-outlook-in-india (last accessed on 10 July 2025).
[4]Virendra Pratap Singh Rathod, "Negotiating Transborder Money Laundering in the Wake of Cryptocurrency: Legal Challenges and Regulatory Responses in a Post-Pandemic Economy" (21 October 2024), SSRN, available at https://ssrn.com/abstract=5026074.
[5]Samuel Aidoo, "Cryptocurrency and Financial Crime: Emerging Risks and Regulatory Responses" (May 2025), available at https://www.researchgate.net/publication/391630261 (last accessed on 8 July 2025).
[6]Manuel Santos Mailland, *Navigating Criminal Liability of Crypto Exchange Platforms: The Role of Blockchain Analytics in Ensuring Compliance* (Master's thesis, Università degli Studi Roma Tre – Dipartimento di Giurisprudenza, 2023–2024) (supervised by Prof. Doménico Notaro).
[7]*Internet and Mobile Association of India v. Reserve Bank of India,* (2020) 10 SCC 274.

be disproportionate and violative of fundamental rights, noting that cryptocurrency trading was not unlawful. This ruling restored public confidence in virtual currencies and was seen as a legitimisation of crypto activity in India. The pandemic boosted the digital ecosystem with a significant shift towards fintech and online payments, and it coincided with global Bitcoin and Ethereum rallies, creating a strong need in young India to invest and own these cryptocurrencies. Moreover, initiatives like Digital India and UPI led to the expansion of the internet and adoption of smartphones, which equipped investors with the tools and confidence to enter the crypto space. At the same time, Indian exchanges such as WazirX, CoinDCX, and ZebPay facilitated easy onboarding. WazirX alone reported a tenfold rise in users, surpassing 10 million by late 2021[8].

However, with the rise in technology and the rapid adoption of cryptocurrency, India has also seen a surge in vulnerabilities. The very features, such as anonymity, decentralisation, and ease in cross-border transfer, that made cryptocurrency lucrative have also made it a massive site for exploitation. Through the use of this asset, financial evasion and offences like money laundering and financing terrorist organisations have become easier.[9] The decentralised nature of cryptocurrency has allowed users to transfer it across countries without any intervention from intermediaries like banks or government platforms, which has contributed to a large extent to the use of such digital assets for money laundering and terrorism financing. It is estimated that illicit cryptocurrency-based money laundering exceeded $1 billion in the first half of 2020 alone, with transactions associated with the Darknet comprising approximately 40% of this amount.[10] Decentralised Finance (DeFi) platforms, which enable users to lend, borrow, and trade digital assets without relying on traditional financial intermediaries, witnessed a surge in total value locked, rising from $700 million in January 2020 to over $100 billion by December 2021. Due to their limited regulatory oversight and enhanced privacy features, these platforms increasingly become channels for laundering illicit gains[11]. Ever since the pandemic, India too has seen a sharp increase in illegal transactions of cryptocurrency, a significant part of it coming from sale proceeds of drug trafficking, human trafficking and evasion of taxes. These funds are

[8]Jack Crawley, "Indian Crypto Exchange WazirX Says User Base Has Grown Tenfold in 2021" *CoinDesk* (12 November 2021), available at https://www.coindesk.com/business/2021/11/12/indian-crypto-exchange-wazirx-says-userbase-has-grown-over-10-times-in-2021/ (last accessed on 7 July 2025).

[9] David Carlisle, *The Crypto Launderers: Crime and Cryptocurrencies* (Wiley 2023) 45.

[10]Elliptic, *Financial Crime Typologies in Cryptoassets* (December 2020) 28, available at https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf (last accessed on 8 July 2025).

[11]Daniel Dupuis and Kimberly Gleason, '*Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic*' (2021) 28 *Journal of Financial Crime* 60, 63.

then moved out of India through decentralised exchanges, thus allowing criminals to evade liability and mask the origins of these transactions[12]. Without immediate laws or regulatory frameworks to oversee its use, the resulting legal vacuum created an ideal environment for money launderers to operate. Consequently, India witnessed a 100% surge in cryptocurrency-related money laundering cases between 2020 and 2021[13]. Despite the rapid expansion of the cryptocurrency ecosystem in India, the country continues to lack a comprehensive legal framework to effectively regulate digital assets and address offences arising from their misuse. This regulatory vacuum has enabled illicit actors to exploit systemic and technological loopholes, resulting in a marked escalation in cryptocurrency-related criminal activities.

THE ARCHITECTURE OF CRYPTOCURRENCY: A GATEWAY FOR CRIME

Blockchain and Mining

Cryptocurrency entered the sphere of finance as a digital medium of exchange, with the use of cryptography for securing transactions, verification of fund transfers, and control over the creation of new units. The term "cryptocurrency" came from the combination of encryption protocols supporting transactional data security and conveying secure communication between electronic wallets where the cryptos are stored and the blockchain network. Bitcoin, created in 2009, was the first and most popular type of cryptocurrency. Bitcoin was successful; therefore, many digital currencies followed suit. Cryptocurrency can be purchased from brokers and exchanges. It can also be created through a computational process that involves solving complex math problems (mining), and high-speed computer systems process extremely complex math puzzles to authenticate transactions and create new coins. Cryptocurrency ownership is not ownership of a physical good; rather, it is a right of control over a unique private key to exchange the unique units of the digital good on the blockchain without intermediaries such as banks or other institutional third parties. Even after more than ten years, cryptocurrencies and the broader uses of blockchain technology continue to develop in the world's financial system. The underlying technology has the potential to transform not just currency transactions but also the trading and management of a broad universe of financial

[12]Financial Action Task Force, *Mutual Evaluation Report on India* (September 2024) https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mutualevaluationofindia.html last accessed 10 July 2025.
[13] Ibid.

instruments such as stocks, bonds, and other digital assets shortly[14].

Decentralisation and Pseudonymity

Unlike fiat currencies, central banks or governmental authorities do not regulate cryptocurrencies. Instead, they operate on a decentralised, peer-to-peer network powered by blockchain technology. This decentralisation poses a significant challenge for authorities, as it limits their ability to monitor or control transactions effectively, creating a haven for criminal activities. While every transaction is recorded on the blockchain, the individuals' identities are not disclosed. Instead, wallet addresses consisting of random alphanumeric codes represent the transacting parties. This built-in layer of privacy, known as **pseudonymity**, enables individuals to engage in illicit activities without revealing their true identities. Accessing and transferring cryptocurrency requires an internet connection, allowing users to send large sums of money instantly, without any involvement from banks or financial institutions. Its borderless nature further enables transfers across jurisdictions with minimal regulatory oversight, making it an attractive tool for misuse. The low barrier to entry, coupled with its user-friendly features, allows even those with limited technical knowledge to easily buy, sell, and trade these digital assets. The absence of consistent global regulations has made it easier for bad actors to shift illicit funds across borders by exploiting weaker legal systems. This fragmented enforcement framework allows criminals to hide behind the system's anonymity and evade detection by law enforcement agencies[15].

Stablecoins, Privacy Coins and Evolution of Illicit Preferences

In 2024, $40.9 billion went to the illegal cryptocurrency addresses; estimates indicate that amount could rise to $51 billion as more attributions are made. Even while this only accounts for 0.14% of all on-chain transactions, the absolute scale shows how frequently cryptocurrency is used for illegal purposes. Notably, the kind of cryptocurrency utilised for illegal transactions has changed significantly. Stablecoins, which currently make up about 63% of all unlawful transaction activity, have surpassed Bitcoin (BTC), which was once the most popular asset due to its availability and early acceptance. This has been made possible due to the growing popularity of stablecoins in bigger cryptocurrency platforms, stability in price, and ease of use,

[14]Kaspersky, *"What is Cryptocurrency and How Does It Work?"* (n.d.) https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency (last accessed 9 July 2025).
[15]Samuel Aidoo, *"Cryptocurrency and Financial Crime: Emerging Risks and Regulatory Responses"* (May 2025) https://www.researchgate.net/publication/391630261 (last accessed 10 July 2025).

particularly in countries with limited access to the US dollar. Although privacy coins such as Monero are usually overlooked due to enhanced anonymity features, Bitcoin is still widely used in malware and darknet market activity. This illustrates how enforcement and regulatory efforts globally are becoming increasingly challenging with the increasing complexity and professionalisation of illicit crypto activity via anonymising platforms and laundering services[16]. As blockchain technology evolves, so do criminals' methods to exploit its loopholes. This ongoing cat-and-mouse dynamic highlights the urgent need for global adaptive legal and regulatory strategies.

TYPOLOGY OF CRYPTOCURRENCY CRIMES

Hyip and Ponzi schemes

Various recognised cryptocurrency fraud methods exist, including Ponzi schemes and high-yield investment programs (HYIPs). HYIP was found to have contributed 50.2% of the total crypto fraud done in 2024, which amounted to 12.4 billion dollars.[17] Ponzi schemes are a type of white collar crime where the schemers scam by providing lucrative investment returns to attract investors. They often have a vast base of local networks to spread influence and enlist local people in this scheme. It always begins with good and timely returns on the initial investment and ends with schemers defaulting in repayments later on and scurrying away with the money.[18] Ponzi schemes lure people in by promising quick, unusually high returns, often presenting themselves as exclusive investment opportunities or "high-yield investment programmes" (HYIPs). These scams thrive on trust, exploiting personal networks, social media, and even word of mouth to attract new victims.[19] In 2024, over 1.2 million people were defrauded an average of $12,400 by bitcoin Ponzi and pyramid schemes[20]. These scams have

[16]Chainalysis, "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized" (15 January 2025), available at https://www.chainalysis.com/blog/2025-crypto-crime-report/ (last accessed on 10 July 2025).

[17]Chainalysis Team, "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication" *Chainalysis* (13 February 2025), available at https://www.chainalysis.com/blog/2025-crypto-crime-report-pig-butchering-ai-fraud/ (last accessed on 10 July 2025).

[18]Shubhasree Bhadra and Kamakhya Narain Singh, "Ponzi Scheme Like Investment Schemes in India – Causes, Impact and Solution" (2024) 27(2) *Journal of Money Laundering Control* 348.

[19]Tyler Moore, Jonathan Han and Richard Clayton, "The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs" (2012) vol 7397 *Proceedings of the International Conference on Financial Cryptography and Data Security* (Springer, Berlin) 41–56.

[20]Barry Elad, "Cryptocurrency Fraud Trends Statistics 2025: Analyzing Trends and Prevention Measures" *CoinLaw* (19 June 2025), available at https://coinlaw.com/cryptocurrency-fraud-trends-statistics-2025/ (last accessed on 11 July 2025).

become increasingly sophisticated, with scammers using artificial intelligence to develop believable identities and social media platforms to reach a wider audience.[21] In 2025, a cryptocurrency Ponzi scheme of ₹350 crore was discovered by the Indian Central Bureau of Investigation (CBI). The scammers used social media to advertise the plan, ran multiple modules in multiple jurisdictions, and hid their source by turning illicit profits into cryptocurrency. The CBI's probe exposed the widespread use of bank accounts and digital wallets, underscoring regulators' difficulties in tracking down and retrieving money.[22] These frauds represent just one facet of the multi-dimensional topology of cryptocurrency crimes. While they prey on financial trust, others exploit technological gaps, forming an interconnected web that challenges existing regulatory and enforcement frameworks.

Darknet market

The structure of cryptocurrency crimes includes deeply ingrained networks of illegal commerce driven by darknet markets and cryptocurrency anonymity, going well beyond Ponzi and HYIP scams. The widespread use of dark websites and crypto-assets in drugs and human trafficking is one of the most urgent issues. According to the UNODC's 2020 World Drug Report, cryptocurrency is a significant financial component of darknet marketplaces like Hydra, Dream Market, AlphaBay, and Empire Market, where more than 62% of listings are related to the sale of illegal drugs. Other services include the trafficking of weapons, the exploitation of children, and the smuggling of people[23]. While cryptocurrencies, particularly Bitcoin, Monero, and Litecoin, enable anonymous, international transactions that circumvent traditional financial monitoring, the darknet supplies the operational environment. Digital spaces are quickly turning into black markets for illegal trade, as demonstrated by Europol's 2025 cybercrime bust of the Cracked and Nulled forums, which had over 10 million users and made €1 million in earnings. Nearly 60% of the 30,000 active dark web domains as of 2025 are associated with illegal activity, with drug trafficking and financial fraud accounting for 34% of these

[21]Dylan Butts, "Crypto Scams Likely Hit a New Record in 2024, Driven by 'Pig Butchering' and AI, Says Chainalysis" *CNBC* (13 February 2025), available at https://www.cnbc.com/2025/02/13/crypto-scams-hit-new-record-in-2024-driven-by-pig-butchering-and-ai.html (last accessed on 11 July 2025).
[22]"CBI Busts Rs 350 Crore Countrywide Crypto Ponzi Scam" *The Economic Times* (24 January 2025), available at https://economictimes.indiatimes.com/news/india/cbi-busts-rs-350-crore-countrywide-crypto-ponzi-scam/articleshow/106023302.cms (last accessed on 11 July 2025).
[23]United Nations Office on Drugs and Crime, *World Drug Report 2020: Cross-Cutting Issues – Evolving Trends and New Challenges* (United Nations publication, Sales No. E.20.XI.6, 2020), available at https://www.unodc.org/unodc/en/data-and-analysis/wdr2020.html (last accessed on 14 July 2025).

connections.[24] These platforms imitate real e-commerce websites with ratings, escrow systems, and product listings, but they use cryptocurrency to obfuscate financial records. In 2024, the darknet drug industry alone brought in over $1.7 billion in cryptocurrency transactions, with synthetic substances exhibiting a greater reliance on online sales than either heroin or cannabis[25]. The Narcotics Control Bureau in India recorded 92 drug crimes employing darknet and cryptocurrency between 2020 and April 2024, with 1,025 more instances involving courier-based trafficking.[26] Government officials claim that 15 of the 27 online sex marketplaces in the US currently accept cryptocurrencies, and that ATMs that do so are increasingly being used to launder the proceeds of human trafficking.[27] Despite blockchain analytics tools offering some insight, the technological superiority of darknet suppliers and the lack of extensive regulatory enforcement continue to give these criminal networks a competitive edge. Thus, cryptocurrencies provide trafficking groups with the anonymity and infrastructure they require to thrive in the criminal underworld of the internet.

Pig butchering

Pig butchering scams, an insidious blend of bitcoin fraud, romance fraud, and psychological manipulation, are quickly rising to the top of the list of the most destructive cybercrimes in the world.[28] These scams, which have their roots in China and are known as sha zhu pan, figuratively "fatten up" the victim by preparing them over weeks or months before financially "slaughtering" them by convincing them to invest in phoney cryptocurrency platforms and seizing all of their assets.[29] Frauds involving pig butchering made up 33.2% of the $12.4 billion global cryptocurrency fraud in 2024, increasing by almost 40% a year and affecting millions

[24]Camilla Silvi Marchini, "The Digital Drug Revolution: How Online Markets Are Reshaping Global Illicit Trade" *Global Initiative Against Transnational Organized Crime* (27 May 2025), available at https://globalinitiative.net/analysis/digital-drug-revolution/ (last accessed on 14 July 2025).
[25]Ibid.
[26]Ministry of Home Affairs, *Drug Trafficking in the Country* (Press Information Bureau, 24 July 2024), available at https://pib.gov.in/PressReleasePage.aspx?PRID=2036398 (last accessed on 14 July 2025).
[27]US Government Accountability Office, *Virtual Currencies: Federal Agencies Need to Better Coordinate on Regulations and Guidance for Human and Drug Trafficking Risks* (GAO, 24 February 2022), available at https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement (last accessed on 14 July 2025).
[28]Trend Micro, "Unmasking Pig-Butchering Scams and Protecting Your Financial Future - Noticias de seguridad - Trend Micro ES" (3 November 2023), available at https://www.trendmicro.com (archived 3 November 2023, last accessed on 14 July 2025).
[29]United States Department of Justice, "District of Massachusetts | United States Files Forfeiture Action to Recover Cryptocurrency Traceable to Pig Butchering Romance Scam" (13 March 2024), available at https://www.justice.gov(archived 28 April 2024, last accessed on 14 July 2025).

of victims, with an average loss of $12,400.[30] These scams frequently start with an unintentional or unwelcome text message on social media, dating apps, WhatsApp, or Telegram. After making initial contact, scammers use fictional backstories, stolen images, and even deepfakes, particularly those that use generative AI to establish emotional relationships.[31] Victims are exposed to fraudulent cryptocurrency platforms that imitate reputable exchanges like Coinbase or Robinhood, complete with phoney dashboards and even fictitious "withdrawals" to establish legitimacy. When the victim eventually tries to get their money back, the platforms either shut them out or want more money under the guise of taxes or fees[32]. As per the Telangana Cyber Security Bureau, pig butchering scams are among India's most prevalent and financially damaging cyber threats, making about 56% of all financial losses associated with cybercrime.[33] In scam centres like these in Myanmar, Cambodia, Laos, and the Philippines, hundreds of thousands of people are forced to commit cybercrime under threats of violence, according to the UN Office of the High Commissioner for Human Rights.[34] Pig butchering scams are now a transnational crypto-financial threat, especially in vulnerable and emotionally manipulated demographics. Nations like India must increase public awareness, enforce stricter Know Your Customer (KYC) regulations on exchanges, and fortify victim response systems.

Crypto Drainers

The crypto drainers are one of the rapidly changing types of cryptocrime that can be particularly risky to the Web3 sector. Such malware programs in the form of phishing attacks are aimed at stealing money in silence out of the victims' wallets, who have accidentally agreed to the seemingly reasonable, ephemeral fake transactions. Unlike conventional phishing, these applications use a blockchain-powered, decentralised trust framework to circumvent custodial controls. They usually use fake web3 apps, DeFi, and NFT project websites to trick users into connecting their wallets. As soon as it is approved, the drainers will send digital assets to

[30]Chainalysis, "Crypto Scam Revenue 2024: Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication" *Chainalysis* (13 February 2025), available at https://www.chainalysis.com (last accessed on 14 July 2025).
[31]National Cybersecurity Alliance, "What Is Pig Butchering and How to Spot the Scam" (27 September 2024), available at https://staysafeonline.org (last accessed on 14 July 2025).
[32]Trend Micro, "Unmasking Pig-Butchering Scams and Protecting Your Financial Future" *Noticias de Seguridad* (3 November 2023), available at https://www.trendmicro.com (last accessed on 14 July 2025).
[33]Telangana State Cyber Security Bureau, "Pig Butchering Scams: Rising Threat in India's Cybercrime Landscape" (2025) [unofficial source], last accessed on 14 July 2025.
[34]Reuters, "'Hundreds of Thousands' Trafficked into SE Asia Scam Centres – UN" (29 August 2023), available at https://www.reuters.com (archived 11 December 2023, last accessed on 14 July 2025).

criminals' wallets forever and immediately. The reach and the outcome of these operations have become hazardous.[35] In the two months since the start of 2024, crypto drainers have already stolen more than 104 million; in 2023, they already stole about 300 million, and the number of victims exceeds 320,000 users. The now-famous Inferno Drainer, a Pyramid botnet given the name in November 2022, used a scam-as-a-service (SaaS) model during the period between November 2022 and 2023 to create over 16,000 phishing domains, impersonating more than 100 legitimate cryptocurrency trading companies, and stealing assets worth an alleged amount of $80 million. Criminals are actively cleaning up the money with DeFi bridges and mixing services instead of centralised exchanges to control more untraceable behaviour.[36] The initial example of a Bitcoin-based crypto drainer, purporting to be Magic Eden, emerged in 2024 and drained more than 500,000 dollars in 1,000 transactions, which implies the greater dispersion between blockchain protocols. However, most of the drainers are Ethereum-based, regardless. There is a need for a broader, more collaborative approach to cybersecurity, as the custodians of decentralised finance (DeFi) have yet to fall under any form of conventional regulation.[37]

Crypto Pumping and Siphoning

Pump, dump, and crypto siphoning are two of the most common forms of market manipulation and theft within the cryptocurrency ecosystem. The concept of pump and dump involves malicious actions when insiders accumulate tokens with low liquidity and generate the value of these tokens by synchronizing their enthusiasm on such social media platforms as Telegram and Twitter. Such insiders will sell out as soon as the token value reaches its peak and this will reduce the value of the token and leave the rest of the investors bearing immense losses.[38] In 2024 alone, pump-and-dump schemes drained investors out of over $560 million and signs of the practice were detected in one out of every 27 newly issued tokens. On the other hand, crypto siphoning is an illegal process of extracting digital assets out of wallets of users; in general, this process can be performed by means of malicious scripts, phishing attacks, or smart contract

[35]Chainalysis, "Understanding Crypto Drainers" *Chainalysis* (16 May 2024), available at https://www.chainalysis.com/blog/crypto-drainers/ (last accessed on 14 July 2025).
[36]Group-IB, "Crypto Wallet Drainers: New and Fast-Growing Threat" *Group-IB* (2024), available at https://www.group-ib.com/blog/crypto-wallet-drainers/ (last accessed on 14 July 2025).
[37]Tangem Team, "What Are Crypto Drainers?" *Tangem* (20 August 2024), available at https://tangem.com/blog/what-are-crypto-drainers/ (last accessed on 14 July 2025).
[38]Kaspersky, "What is Cryptocurrency and How Does it Work?" *Kaspersky* (8 December 2018), available at https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency (last accessed on 14 July 2025).

exploits.[39] It is curious to mention that another meaning of the siphoning is widespread DeFi exploit: rug pulls and flash loan attacks, as the process by which the developer of a project or a hacker drains a liquidity pool and steals the money invested by the investors. According to data in 2024, decentralized platforms lost more than $2.9 billion due to these siphoning cases.[40]

Money Laundering and Terrorism Funding

As a part of the greater financial global framework, cryptocurrencies are a two-faceted tool: at once they are an enabling mechanism to achieve financial inclusion and innovation by decentralized peer transactions, and simultaneously an enabler of money laundering of illicit business and terrorist funding. The main attractiveness of virtual assets to malignant actors is related to pseudo-anonymity, decentralized structure, and inherently global nature.[41] Therefore, this dual-character forms one of the major security concerns within India that the Ministry of Home Affairs has identified the use of cryptocurrency as a crime involving drugs trafficking and terrorism and in doing so created a Special Task Force on Darknet and Cryptocurrency to track questionable transfers. According to the Financial Intelligence Unit (FIU) in the timeframe of April 2022 to November 2022, over 3,300 crypto accounts were reported to be involved in crimes like child pornography, narcotics and unrest, out of which 70 per cent of them were blocked and the rest have been put under Enforcement Directorate (ED) and Central Bureau of Investigation (CBI).[42] An action taken in one of the regions of Uttar Pradesh in 2024 exposed a washing cathedral operated using Telegram and channeling money through Tron/USDT wallets as well as bank accounts of the property of the mules, avoiding Know-Your-Customer (KYC) regulation by delivering Atomic swaps.[43]

Indian investigators have already identified transactions and offshore Tron/USDT wallets linked to networks associated with insurgent groups in Jammu & Kashmir and elsewhere in disturbances, at the counter-terrorism level thus motivating efforts aimed at enhancing its

[39]Bitget, "How to Spell Siphon in the Context of Blockchain Finance" *Bitget* (2 May 2025), available at https://www.bitget.com/wiki/how-to-spell-siphon (last accessed on 14 July 2025).
[40]Kaspersky, "Crypto wallet drainer: what it is and how to defend against it" *Kaspersky* (n.d.), available at https://www.kaspersky.com/blog/what-is-a-crypto-wallet-drainer/50490/ (last accessed on 14 July 2025).
[41]Shauli Shah et al, "Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation" (2023) SSRN, available at https://ssrn.com/abstract=4674925 (last accessed on 14 July 2025).
[42]**Ministry of Home Affairs, Annual Report 2023–24,** available at https://www.mha.gov.in (Last visited on July 14, 2025).
[43]*Telegram-Based Crypto Laundering Ring Busted in UP, ED Seizes ₹75 Lakh in USDT,* THE TIMES OF INDIA (2024), available at https://timesofindia.indiatimes.com/india/telegram-usdt-crypto-laundering-ed-uttar-pradesh/articleshow/105098118.cms (Last visited on July 14, 2025).

cryptocurrency-related anti-money laundering and combating of terrorism financing (AML/CFT) system. However, regardless of these policies measures, a sum of over 120 crore in illegal cryptocurrency assets have been seized by authorities in India in 2024 alone, drawing criticism to both the country and the methods of such seizures by the Financial Action Task Force (FATF) over a lack of development in the enactment of cryptocurrency-related crimes.[44] Bitcoin has created irreversibility and peer-to-peer orientation, which reduces the window of detection that can be gained by law-enforcement agencies. Despite the Financial Action Task Force having established compulsory governance policies concerning Virtual Asset Service Providers (VASPs), India remains at the forefront in terms of adoption and enactment, exposing the country to local and cross-border abuse of cryptocurrencies.[45]Without real-time analysis of blockchain, cross-agency coordination and long-term cross-border cooperation, India could experience an even greater perpetuation of illegal crypto-financing enablers that drive the organized crime business and extremist violence.[46]

LEGAL LIABILITY

Justice Surya Kant during the proceedings of ***Shailesh Babulal Bhatt v. State of Gujarat & Another***[47] observed "*If you can tax it at 30%, also please regulate it as you have recognised it by taxing it.*" This highlights the need for a comprehensive regulatory framework to address the needs of growing cryptocurrency related frauds and scams in India since it has already been acknowledged as these assets are already being taxed at 30%. In the absence of explicit laws, the question of liability whether civil or criminal becomes more complex. A case-by-case investigation is required to ascertain who is responsible for unlawful or negligent behavior because of the complex network of participants in the cryptocurrency ecosystem, which includes wallet providers, exchanges, developers, promoters, financial middlemen, influencers, and even users. Legal frameworks need to evolve to clearly define the duties and obligations of all stakeholders in this decentralized ecosystem, in addition to safeguarding consumers.

[44]*Crypto-Terror Link Traced to Kashmir Using USDT: FIU Signals to NIA,* THE ECONOMIC TIMES (2024), available at https://economictimes.indiatimes.com/news/india/fiu-crypto-terror-link/articleshow/105559004.cms (Last visited on July 14, 2025).
[45]Shlomit Wagman, Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing, 14 HARVARD NATIONAL SECURITY JOURNAL 87 (2022), available at https://harvardnsj.org (Last visited on July 14, 2025).
[46]Emily Fletcher, Charles Larkin & Shaen Corbet, Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation, SSRN WORKING PAPER (2023), available at https://ssrn.com/abstract=4674925 (Last visited on July 14, 2025).
[47]*Shailesh Babulal Bhatt v. State of Gujarat & Another*, AIR ONLINE 2021 GUJ 70.

Liability of cryptocurrency exchange platforms

Cryptocurrency exchange venues are the key participants in the virtual assets market, which connects buyers and sellers of digital assets and enables trading. That being the case, the legal requirements that are placed on them most especially within the contexts of anti-money laundering (AML) and counter-financing of terrorism (CFT) are considerable.[48] In India, the Prevention of Money Laundering Act, 2002 (PMLA) has been extended to the virtual digital asset (VDA) service providers due to which these exchanges have become accountable reporting entities. Now they have to carry out a sound customer due diligence, exercise KYC and e-KYC, preserve transaction records, not less than five years, report suspicious transactions to the Financial Intelligence Unit-India (FIU-IND), and receive periodic audits on AML. The effect of being non-compliant is serious. Exchanges and the management of such exchanges can also suffer financial fines and be criminally liable should it be established to accommodate illicit money flows willfully or through negligence.[49] As an unprecedented case in February 2025, the Enforcement Directorate (ED) identified 1,646 crore of cryptocurrency seized in a PMLA case in which a fraud is done through an investment scam. It was found out that there was a complicated chain of payments between several wallets and it was suspected that the exchange was facilitating such transfers without sufficient control. The Indian law on liability of crypto exchanges is in a youthful state but courts and those enforcing the law are progressively taking the position that platforms can no longer be passive intermediaries.[50] In the case of ***Internet and Mobile Association of India v Reserve Bank of India***[51], although the Supreme Court quashed the circular issued by the RBI that barred banks against transacting with firms engaged in the crypto business, it also recognised that the government needed to exercise control over the same in order to prevent such a virtual currency being misused. Most recently, and in a similar light, in ***Directorate of Enforcement v Zanmai Labs Pvt Ltd (WazirX)***[52] ED has dug into the exchange due to its activities in money laundering, into the

[48]Hazem Mulhim, *Opinion: Why Crypto Businesses Need Anti-Money Laundering Regulations,* WORLD ECONOMIC FORUM, September 21, 2022, available at https://www.weforum.org/agenda/2022/09/opinion-why-crypto-businesses-need-anti-money-laundering-regulations/ (Last visited on July 14, 2025).

[49]Reddy Pawan Kumar & Athif Ahmed, *Blockchain & Cryptocurrency Laws and Regulations 2025 – India,* GLOBAL LEGAL INSIGHTS, October 25, 2024, available at https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/india (Last visited on July 14, 2025).

[50]PTI, *ED Seizes "Biggest" Crypto Fund Worth Rs 1,646 Crore in PMLA Case,* DECCAN HERALD, February 15, 2025, available at https://www.deccanherald.com/india/ed-seizes-biggest-crypto-fund-worth-rs-1646-crore-in-pmla-case-2925474 (Last visited on July 14, 2025).

[51]*Internet and Mobile Association of India v Reserve Bank of India,* (2020) 10 SCC 274.

[52] Directorate of Enforcement v Zanmai Labs Pvt Ltd (WazirX), Enforcement Directorate Press Release, 5 August 2022.

poor regulation of its wallet transfers.

International Courts have taken this extra step of determining the boundaries of exchange-liability. The UK High Court, in ***Jones v Persons Unknown***[53], made the determination that an exchange holding wallets that contain stolen assets could be considered a constructive trustee, with a duty of fiduciary obligation to repay the stolen funds. In ***D Aloia v Persons Unknown & Others***[54], it was acknowledged that there was a duty on exchanges to help in the freezing and tracing of stolen cryptoassets, especially where the exchange had infrastructure which had enabled the fraud. Thus, both on a national level and in international jurisprudence, legal guidelines are becoming staunchly on one side of the court. Cryptocurrency exchanges are not just intermediary platforms, but are obligated to ensure that they do not contribute to their abuse. They may therefore be prosecuted based on complicity in and inability to impede illegal activity either by culpable negligence or criminal neglect.

Legal Liability of Innocent Mules

The increase in terms of financial crime involving cryptocurrency in India has put both light on as well as increased the use of so-called money mules, people whose bank account or crypto wallet is used to launder proceeds of crime.[55] The involvement of these mule accounts in laundering money through various means including phishing and online frauds which subsequently gets transformed into cryptocurrencies and shifted to offshore accounts via unregulated cryptocurrency exchanges like Binance was revealed by the Central Bureau of Investigation (CBI) in February 2024 and found to be operating within a huge network of cybercrimes and included more than 8.5 lakh mule bank accounts. The accounts were regularly fabricated with forged KYC documentation, or leased, not only emphasising user complicity but also revealing system-wide failures on the part of financial institutions.[56] Legally, the liability of such innocent mules is hinged on mens rea, i.e., guilty mind. The Orissa High Court, in considering bail in a crypto Ponzi scheme, stated in ***Sandeep Kumar Choudhury v State of***

[53]*Jones v Persons Unknown*, [2022] EWHC 2543 (Comm).
[54]*D Aloia v Persons Unknown & Others*, [2022] EWHC 1723 (Ch).
[55]Federal Bureau of Investigation, *Money Mules,* FBI (updated 2025), available at https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/money-mules (Last visited on July 14, 2025).
[56]Central Bureau of Investigation, *CBI Launches Nation-Wide Searches at 42 Locations in Connection with Mule Bank Accounts Being Used in Cyber Frauds; Around 8.5 Lakh Mule Accounts in More than 700 Branches of Various Banks Across India; 9 Accused Persons Arrested; Drive Against Organized Cyber Crime/ Digital Arrest Under Operation Chakra-V,* June 26, 2025, available at https://cbi.gov.in/press-releases/26-06-2025-operation-chakra-v-mule-accounts(Last visited on July 14, 2025).

Odisha[57], that transactional interaction or holding of digital currency is not the basis to be considered guilty. The prosecution should prove that it has either knowledge or was a part of the fraud. In like manner, the Supreme Court of India in ***Internet and Mobile Association of India v Reserve Bank of India***[58], affirmed that even though transactions involving cryptocurrencies are not a criminal offense by itself, they attract the general penal provisions of law such as the Prevention of Money Laundering Act, 2002 (PMLA) and the Bharatiya Nyaya Sanhita, 2023.

Nevertheless, regulators and investigative agencies are applying a more vigorous approach despite this legal subtlety. In February 2025, the Enforcement Directorate (ED) had seized 1,646 crore in digital assets associated with a cryptocurrency fraud case. After examining the transactions, it was discovered that the complex layering involved several wallets, some of which were run by so-called mules, and that despite numerous red flags, the exchange did not raise any suspicions on the transactions relevant to the case under investigation.[59] Also boosting investigative prowess, during a consultative session in March 2025, the Union Home Minister revealed the addition of tools powered with Artificial Intelligence (AI), affording them early identification of mule accounts. These tools, in coordination with the Reserve Bank of India (RBI) and private banks, have already detected more than 19 lakh mule accounts and blocked anything suspicious to the tune of more than 2,038 crore rupees, many of these being amounts layered using cryptocurrencies. This is not simply an interesting technological advancement but an expression of an effort at the policy level to curb the systemic exploitation of digital financial platforms.[60] The Indian legal system is gradually shifting to a model in which ignorance does not provide absolute defence anymore. Intentionally closing eyes, grave negligence, or multiple failures to exercise due diligence, especially in risky areas, such as cryptocurrency, can be an adequate basis to charge the criminal liability of both innocent mules and intermediaries. The inclusion of AI-based monitoring systems and the growth of an

[57] *Sandeep Kumar Choudhury v State of Odisha*, MANU/OR/1065/2024.
[58] *Internet and Mobile Association of India v Reserve Bank of India*, (2020) 10 SCC 1.
[59] *ED Seizes "Biggest" Crypto Fund Worth Rs 1,646 Crore in PMLA Case,* DECCAN HERALD (India), February 15, 2025, available at https://www.deccanherald.com/india/ed-seizes-biggest-crypto-fund-worth-rs-1646-crore-in-pmla-case-3407700 (Last visited on July 14, 2025).
[60] Press Trust of India, *Govt Mulling AI Use to Identify Mule Accounts to Check Cybercrime: Home Minister Amit Shah,* THE ECONOMIC TIMES, February 11, 2025, available at https://economictimes.indiatimes.com/industry/banking/finance/banking/govt-mulling-ai-use-to-identify-mule-accounts-to-check-cybercrime-says-union-home-minister-amit-shah/articleshow/118140161.cms (Last visited on July 14, 2025).

enforcement machine have prompted all digital asset ecosystem players to consider greater responsibilities.

Legal Liability of other stakeholders

Courts approach to crypto schemers

In ***Vijay Kumar Juneja v State of Himachal Pradesh***[61], the High Court of Himachal Pradesh rejected the bail application of the petitioner, who had masterminded a massive cryptocurrency fraud. The court has concluded that the accused actively handled proceeds of the fraud and invested them in properties, which showed a conspiracy that was deep-rooted. Considering the gravity of the economic offence, and in reference to the possible reason of tampering with evidence, interim protection was removed. However, in ***Sandeep Kumar Choudhury v State of Odisha***[62], there was an allegation of the operation of a Ponzi scheme through Yes Token. It was struck down as bail was granted by the Orissa High Court, arguing that cryptocurrency trading was not necessarily illegal in India by citing ***Internet and Mobile Association of India v RBI***[63]. The petitioner was then granted bail with conditions, including a 5 lakh bond.

Technical Actors, Custodians and Developers

Smart contract developers who design systems or decentralised protocols might be held liable in case they have knowingly promoted faulty or fraudulent systems. Although not directly judged by Indian courts, developers are now liable under the broadened definition of the term Virtual Digital Asset Service Providers (VASPs) in the PMLA, 2002. Dishonest practices, such as a so-called rug pull, may be subject to criminal charges[64]. The Hong Kong High Court in ***Re Gatecoin Ltd***[65] observed that crypto asset balances on exchanges may be held on trust and emphasised the liability of custodians. Providers of custodial wallets in India are now required to comply with PMLA. They have to do KYC, record keeping and reporting suspected activity. The non-custodial wallet providers are usually incurring lower liability unless their programs

[61] *Vijay Kumar Juneja vs. State of Himachal Pradesh*, MANU/HP/2532/2024.
[62] *Sandeep Kumar Choudhury vs. State of Odisha*, MANU/OR/1065/2024.
[63] *Internet and Mobile Association of India v RBI*, (2020) 10 SCC 1.
[64] Gaurav Pandey, *Regulation of Virtual Digital Assets in India: Additional Obligations on Service Providers under PMLA,* TAXGURU, May 31, 2023, available at https://taxguru.in/corporate-law/regulation-virtual-digital-assets-india-pmla.html (Last visited on July 14, 2025).
[65] *Re Gatecoin Ltd*, [2023] HKCFI 914.

can be demonstrated to err in an intentionally, negligently, or maliciously designed way.[66]

INDIA AND GLOBAL APPROACHES TO CRYPTOCURRENCY REGULATION

The regulatory system regarding cryptocurrencies is quite heterogeneous in the world. Nations have adopted different positions with regards to national priorities of consumer protection, financial innovation, economic stability, and prevention of illicit finance. The measures undertaken vary, including complete bans, an innovation bus, and finding a compromise through the integration of cryptocurrencies into the existing financial regulatory systems in a number of jurisdictions. [67]

India's Regulatory Trajectory

The regulatory trend in India has gone through a shift towards ambiguity to be more formal over the past couple of years. First, RBI issued a de facto cryptocurrency prohibition in 2018, instructing banks not to support transactions linked to crypto. Nevertheless, this action was overturned by the Supreme Court in ***Internet and Mobile Association of India v Reserve Bank of India[68]***, which supported the constitutional right to trade.[69] The verdict proved critical to reinstating the Indian cryptocurrency industry and the start of a more sophisticated policy consideration. Thereafter, a formal structure of taxation was proposed by the Indian government in the Union Budget 2022 23. All cryptocurrency income is subject to a fixed 30% rate of taxation, and a 1% Tax Deducted at Source (TDS) is applicable on the majority of transactions. Cryptocurrencies above 50,000 rupees are subject to taxation under gifts. Nevertheless, cryptocurrencies have yet to be treated as legal tender and cannot be used to pay for goods or services. These advancements indicate that India accepts cryptocurrencies as a source of tax but not necessarily as an outright monetary instrument[70]. In March 2023, a paradigm-changing regulatory change came with the Ministry of Finance introducing Virtual

[66]Vibhore Batwara, Purushotham Kittane, Alipak Banerjee & Vaibhav Parikh, *Making Crypto Industry Compliant in India: A Welcome Move under the Anti-Money Laundering Laws,* NISHITH DESAI ASSOCIATES, March 13, 2023, available at https://www.nishithdesai.com/SectionCategory/33/Research-and-Articles/12/60/NDAHotline/9522/1.html (Last visited on July 14, 2025).
[67]Divya P. & Shobha B.G., *A Study on Legal Regulation of Cryptocurrency Between India and G-20 Countries: A Comparative Analysis,* 14(79) INDIAN JOURNAL OF NATURAL SCIENCES 58331, 58332–58334 (2023), available at https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/32129181/350a4273-07a6-4f08-a536-11cfec35ab60/2-CRYPTO.pdf (Last visited on July 15, 2025).
[68]*Internet and Mobile Association of India v Reserve Bank of India*, [2020] 10 SCC 1.
[69]Raghav Sood, *Cryptocurrency – What It Is and Its Legal Status in India and Globally?* 2(2) INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 1 (2021), available at https://heinonline.org/HOL/Page?handle=hein.journals/injlolw2&id=5017 (Last visited on July 14, 2025).
[70]Finance Act, 2022, §115BBH; Income-tax Act, 1961, §§56(2)(x), 194S.

Digital Assets (VDAs) to the Prevention of Money Laundering Act, 2002 (PMLA). The step requires Virtual Digital Asset Service Providers (VASPs), including crypto exchanges and wallet providers, to comply with rigorous Anti-Money Laundering (AML) and counter terrorism financing (CFT) requirements. These are the Know Your Customer (KYC) verification, record-keeping and reporting suspicious activities to the Financial Intelligence Unit - India (FIU-IND). VASPs are also to be registered in the FIU-IND and considered at par with financial institutions regarding compliance requirements.[71] This notwithstanding, India has not managed to establish a proper crypto-specific law. The government is still actively discussing the possibility to prohibit the use of privately-issued cryptocurrencies although it is already working on the pilot of a Central Bank Digital Currency (CBDC) aka the Digital Rupee. Such a conservative approach is prompted by regulatory doubts arising due to volatility of the market, capital flight, and misuse of digital currencies to conduct illegal activities.[72] In the meanwhile, regulators including the Securities and Exchange Board of India (SEBI) and RBI push towards a multistakeholder model to regulate the crypto industry.[73]

Global Strategies: Diverging Paths and a Push for Convergence

Regulatory approaches in many countries around the globe fall in one of these four categories: *prohibitive, permissive with regulation, innovation-centric, and harmonized frameworks*.[74] China is at the extreme end of the inhibition. It initiated a prohibition on all types of cryptocurrency trade and cryptocurrency mining from 2021, exercising financial stability and capital control risks. Conversely, Argentina, Brazil, and Canada have cryptocurrency operations that operate under the current financial and AML regulations.[75] As an example, Canada defines exchanges as money services business and requires them to be registered with Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and Australia

[71]Saikrishna & Associates, *Department of Revenue Brings Virtual Digital Assets Within the Ambit of the Prevention of Money Laundering Act, 2002,* March 8, 2023, available at https://www.saikrishnaassociates.com/department-of-revenue-brings-virtual-digital-assets-within-the-ambit-of-the-prevention-of-money-laundering-act-2002/ (Last visited on July 15, 2025).
[72]KYC Hub, *Cryptocurrency Regulations in India: A Guide for 2025,* July 14, 2025, available at https://www.kychub.com/blog/cryptocurrency-regulations-in-india/ (Last visited on July 15, 2025).
[73]Reserve Bank of India, *Concept Note on Central Bank Digital Currency,* October 2022, available at https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218 (Last visited on July 15, 2025).
[74]Analytics Insight, *Crypto Regulations: Global Policies to Watch in 2025,* February 13, 2025, available at https://www.analyticsinsight.net/cryptocurrency-analytics-insight/crypto-regulations-global-policies-to-watch-in-2025(Last visited on July 15, 2025).
[75]OSL, *How Global Crypto Regulations Are Evolving in 2025,* March 10, 2025, available at https://www.osl.com/hk-en/academy/article/how-global-crypto-regulations-are-evolving-in-2025 (Last visited on July 15, 2025).

requires crypto businesses to be registered with AUSTRAC, which is Australia's financial intelligence agency.[76] The countries such as the United Arab Emirates (UAE), Japan, and Switzerland have implemented innovation-based models. The VARA Virtual Assets Regulatory Authority of the UAE allows regulated crypto trading and services. Japan officially accepts Bitcoin as a legal property under its Payment Services Act and approves crypto exchange licenses, with user protection and AML requirements. Switzerland, which is commonly referred to as a Crypto Valley, has legal clarity over many digital assets, and has an active blockchain ecosystem.[77]

Among the most striking regulatory frameworks is the European Union Markets in Crypto-Assets (MiCA). MiCA subscribes to a regulated system that unifies the issuers and service providers of crypto-assets in all countries of the EU. It classifies crypto assets, prescribes transparency and disclosure regulation and consumer protection requirements. MiCA further proposes the so-called passporting, wherein companies licensed in any one EU nation could begin operating inside the bloc, an innovation that could spur cross-border crypto activity across the EU under the same applicable standards.[78] Standardization is proceeding at the international level where organizations such as Financial Action Task Force (FATF) and Organisation for Economic Co-operation and Development (OECD) are promoting standardization. FATF guidelines make countries control Virtual Asset Service Providers (VASPs) according to the traditional financial institutions. The so-called FATF Travel Rule requires that information concerning originator and beneficiary be disclosed in transactions above a certain limit, with a substantial impact on how crypto companies manage international transfer activities.[79] India together with other G20 countries is geared to adhere to these international standards. In its suggestion of the G20 Roadmap on crypto-regulation, the focus has been on global coordination, uniform regulatory frameworks, and more effective information-sharing platforms. The commitments associated with India, especially in the area of fighting financial crimes, have come into place through its extension of the PMLA to cover VDAs. Summing up, the present system in India is an example of a controlled permissibility system that is not quite liberal but neither prohibitive. Although a wholesome legislative framework has yet to come through, the recent tax measures and AML compliance standards

[76]KYC Hub (n 72).
[77]Analytics Insight (n 74).
[78]Ibid.
[79]PwC, *Global Crypto Regulation Report 2025,* 2025, available at https://legal.pwc.de/content/services/global-crypto-regulation-report/pwc-global-crypto-regulation-report-2025.pdf (Last visited on July 15, 2025).

are nearing the regulatory vogue globally.[80] In the meantime, MiCA developed by the EU turned out to be an example of a harmonized approach to crypto regulation. There is a consolidation behind the scenes, which bears out across jurisdictions: We should promote innovation on a risk-reduced basis as a stable, transparent, and trustworthy digital asset ecosystem.[81]

RECOMMENDATIONS

1. ***Pass New Comprehensive Regulation:*** India should have specific, comprehensive legislation covering cryptocurrencies. This ought to categorise VDAs unambiguously (e.g., utility, security, payment tokens), introduce a strong framework of licensing all VDA Service Providers (VASPs) beyond existing registration with the FIU-IND, and should have specific ramifications of platform negligence and security breaches. It would provide clarity, lower arbitrage, and comply with global benchmarks, such as the EU ‘s Markets in Crypto-Assets (MiCA) Regulation.

2. ***Increase the Cross-Border Crypto Scams Police Department of I4C:*** The Indian Cyber Crime Coordination Centre (I4C) needs to be given much greater powers, along with resources, to tackle the nature of crypto scams that is inherently global. This involves giving I4C express permission to directly communicate with foreign law enforcement that is beyond the power provided by MLAT, and crypto intelligence companies and a massive investment into expert training regarding blockchain forensic tools and on-chain analysis capabilities.

3. ***Introduce a National Crypto Awareness Programme:*** Educated society is the best fight against crypto scams. Government, educational institutions, and industry players need to tool an awareness program to educate citizens on crypto volatility, typical scam tactics (e.g., phishing, rug pulls, Ponzi schemes), and best practices in secure digital environments. More importantly, it should encourage open means of reporting cybercrime including through the National Cyber Crime Reporting Portal.

CONCLUSION

Cryptocurrency is an emerging area with voluminous legal complications. In India, there have

[80] KYC Hub (n 72).
[81] Analytics Insight (n 74).

been developments in the regulatory landscape, which are still relatively emerging; however, defined responsibilities are present to different stakeholders. As the centre-stage facilitators, the cryptocurrency exchanges bear a prime responsibility of strong Anti-Money Laundering (AML) and Know Your Customer (KYC) enforcement under the Prevention of Money Laundering Act, 2002.[82] The unregulated state of virtual currencies has raised very serious concerns for the Indian judiciary. This fear was strongly expressed by the Supreme Court, which said on Monday (5 March 2025), that accessing Bitcoins in India is similar to operating a sophisticated Hawala business. There is a radical contrast here regarding the extreme danger of anonymity and the transnational tendency of crypto manipulations, which could reproduce the features of informal money transfer networks, leaving them vulnerable to criminal operation.[83] In order to establish a safe and transparent crypto-environment, India will have to focus more on the sphere of complex regulation. These include the clear categorisation of digital assets, the strong licensing regime of all Virtual Digital Asset Service Providers (VASPs) and liability certainty, which comes into effect when platforms are found to be negligent. It is essential to increase the competence of agencies to conduct cross-border crypto-criminal-scam investigations, such as the Indian Cyber Crime Coordination Centre (I4C), granting it expanded powers and avenues of international cooperation. Lastly, the country needs a national crypto education initiative to orient people on the dangers and best practices, so they can safely explore this digital wild west.

[82]LexisNexis Risk Solutions, *Stopping Money Mules for Financial Security in India,* 2025, available at https://risk.lexisnexis.com/insights-resources/article/stopping-money-mules-for-financial-security-in-india (Last visited on July 14, 2025).

[83]*Trading in Bitcoin in India is a Refined Way of Doing Hawala Business: Supreme Court,* THE HINDU (New Delhi), 6 May 2025, available at https://www.thehindu.com/news/national/trading-in-bitcoin-in-india-is-refined-way-of-doing-hawala-business-supreme-court/article68132724.ece (Last visited on 14 July 2025).