

Regulation of Cryptocurrency by Indian Law and Agencies

Aryan Khandeparkar

Student at NMIMS, Mumbai

Abstract

This research paper explores the evolving landscape of cryptocurrency regulation in India, analysing the roles and limitations of existing regulatory frameworks under the Securities and Exchange Board of India (SEBI), the Reserve Bank of India (RBI), and the Prevention of Money Laundering Act (PMLA). As digital assets gain prominence, the Indian legal ecosystem struggles to keep pace due to a lack of comprehensive legislation, institutional clarity, and definitional coherence. The study begins by examining the classification dilemma surrounding crypto-assets under Indian securities law, particularly whether certain tokens could fall within the ambit of "securities" under Section 2(h) of the Securities Contracts (Regulation) Act, 1956. By comparing characteristics of cryptocurrencies to conventional financial instruments and referencing international legal benchmarks such as the Howey Test, the paper argues that many tokens exhibit sufficient investment features to warrant regulatory scrutiny by SEBI.

In parallel, the RBI's approach, rooted in concerns over monetary stability, has largely treated cryptocurrencies as a threat to sovereign currency systems. Although the 2018 RBI circular attempted to isolate the financial system from crypto-related activities, the Supreme Court overturned the ban in 2020, underscoring the need for proportional regulation rather than prohibition. Meanwhile, the Indian government has taken significant steps under the PMLA by designating crypto intermediaries as "reporting entities," thereby mandating KYC, transaction monitoring, and suspicious activity reporting to the Financial Intelligence Unit-India (FIU-IND). While these moves align with global anti-money laundering standards, the application of PMLA to a fast-evolving digital sector presents both legal and practical challenges.

A key argument advanced in this paper is the need for a dedicated regulatory authority—tentatively called the Digital Asset Regulatory Authority of India (DARA)—to oversee the crypto ecosystem holistically. The study highlights how SEBI and the Enforcement Directorate (ED) are already overburdened with their existing mandates, leading to delays, inefficiencies, and enforcement gaps. A specialised regulator could centralise policymaking, enforcement, and innovation facilitation, thereby addressing jurisdictional ambiguity and improving investor protection without stifling technological growth. This research concludes that the future of digital assets in India demands a balanced, innovation-friendly regulatory framework.

For this, a pragmatic regulatory approach—combining institutional reform, international cooperation, and respect for crypto's foundational features such as decentralisation and pseudonymity

Research Objectives:

1. To examine the legal status and regulatory uncertainty surrounding cryptocurrencies in India, particularly in light of the absence of a comprehensive legislative framework

2. To critically analyse the extent to which cryptocurrencies may be classified as ‘securities’ under Indian law and the resulting jurisdictional scope of SEBI.
3. To assess the impact and constitutionality of applying the Prevention of Money Laundering Act (PMLA) to Virtual Digital Assets (VDAs) and crypto intermediaries.
4. To propose viable legal and regulatory reforms for effective, balanced, and innovation-friendly regulation of cryptocurrencies in India.

Research methodology

In this research paper, a secondary research methodology has been employed to analyse the regulatory landscape of cryptocurrencies in India. The study is rooted in the examination of existing legal frameworks, regulatory pronouncements, judicial decisions, and policy documents, with an emphasis on interpreting and evaluating the roles of SEBI, RBI, and the PMLA in governing virtual digital assets.

The data sources include a wide range of academic research papers, law firm publications, government notifications, court judgments, and news articles from credible financial and legal journalism platforms. Particular focus has been given to policy reports issued by Indian regulatory authorities, legislative drafts such as the Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019, RBI circulars, SEBI statements, and recent updates to the PMLA framework as notified by the Ministry of Finance.

Could Cryptocurrencies be classified as a security ?

- Crypto assets are purely digital assets that use public ledgers over the internet to prove ownership.
- They use cryptography, peer-to-peer networks and a distributed ledger technology (DLT) such as blockchain to create, verify and secure transactions.
- It encompasses cryptocurrencies, non-currency tokens such as utility tokens and non-fungible tokens among others.
- Crypto assets generally operate independently of a central bank, central authority or government.
- Functions- They may be used as a medium of exchange, a way to store value or for other business purposes.

The current Indian securities law framework lacks the clarity and specificity required to regulate cryptocurrencies effectively, and SEBI’s jurisdiction over digital tokens remains uncertain in the absence of legislative classification—necessitating legal reform or judicial interpretation to bridge the regulatory gap.

Under the **Securities Contracts (Regulation) Act, 1956 (SCRA)**, the term "security" is defined in Section 2(h). It provides a broad and inclusive definition to cover various types of instruments that may be traded in financial markets.

Section 2: Definitions- In this Act, unless the context otherwise requires,

(h) “securities” include—

(i) shares, scrips, stocks, bonds, debentures, debenture stock or other marketable securities of a like nature in or of any incorporated company or other body corporate;

(ia) derivative;

(ib) units or any other instrument issued by any collective investment scheme to the investors in such schemes;

- (ic) security receipt as defined in the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002;
- (id) units or any other such instrument issued to the investors under any mutual fund scheme;
- (ie) any certificate or instrument (by whatever name called), issued to an investor by any issuer being a special purpose distinct entity which possesses any debt or receivable...;
- (ii) Government securities;
- (iia) such other instruments as may be declared by the Central Government to be securities; and
- (iii) rights or interest in securities.

This leads to understand that the key Characteristics of “Securities” in India are:

1. **Marketability:** Must be capable of being bought and sold in the market.
2. **Representation of Value:** Often represent a financial stake in a company or fund.
3. **Expectation of Profit:** Especially relevant when evaluating tokens or investment contracts.
4. **Collective Investment Aspect:** Instruments where returns depend on the efforts of others (e.g., ICOs resembling mutual funds or investment schemes).
5. **Inclusion of Derivatives:** Even contracts based on the future value of underlying assets.

From this we could easily draw up a conclusion that crypto coins would come under the definition of **Derivative contracts:** Under Clause (i) of SCRA, which are financial agreements whose value is derived from the performance of an underlying asset, such as stocks, bonds, commodities, or indices. They are used for various purposes, including hedging, speculation, and speculation. Common types of derivatives include futures, options, forwards, and swaps.

Marketable securities: Under Clause (ia) of SCRA, which are financial assets that can be easily converted into cash, like stocks, bonds, or Treasury bills, within a year of investment. They are considered current assets because they are expected to be converted to cash within a year, ie are considered a are highly liquid assets, meaning they can be bought or sold quickly without significant loss of value.

A notable aspect of this definition is the inclusion of the term “marketable securities of a like nature,” which implies that an instrument, even if not explicitly listed in the definition, may qualify as a security if it shares characteristics such as transferability, tradability, and the ability to be bought and sold in a market. Crypto-assets, by their very design, may or may not align with this definition. Their classification depends heavily on their characteristics and intended use. Broadly speaking,

Crypto-assets can be divided into three categories:

Utility tokens – which provide access to a product or service,

Payment tokens – primarily used as a medium of exchange, and Security or

Investment tokens – which often promise returns based on the efforts of a third party.

Cryptocurrencies share traits with conventional assets like stocks and derivatives particularly in their role as speculative investment instruments and their market-driven price swings.

Crypto tokens are exchanged on exchanges, just like stocks, and their values fluctuate in response to macroeconomic developments, supply and demand, and market sentiment. It has now been noted that investors often retain cryptocurrencies for capital appreciation rather than just for transactions, viewing them as assets with profit potential, which is a requirement of the Securities Contracts (Regulation) Act of 1956.

Furthermore, just like shares are traded on stock exchanges, a lot of cryptocurrencies are regularly bought and sold on trading platforms. These platforms support price discovery, market liquidity, and peer-to-peer transactions—all essential components of a healthy securities market. Crypto tokens that are issued through processes like token generation events or initial coin offerings (ICOs) frequently represent a stake in a project or protocol, and investors anticipate profits contingent on the project's success or failure. Clause (ib) of Section 2(h) of the SCRA, which covers instruments issued by collective investment schemes whose value is dependent on managerial or entrepreneurial initiatives, is closely aligned with this. Treating crypto tokens as securities would not only be consistent with their economic reality but also offer much-needed investor protection through SEBI's regulatory framework. Crypto investors are similarly vulnerable to market manipulation, insider trading, and fraud, just as shareholders in listed companies are.

Security tokens are the ones that most closely resemble conventional securities among them. For instance, a crypto-asset starts to resemble the components of a conventional investment contract if it is presented to investors with the assurance of returns resulting from the issuer's or a third party's managerial efforts. In the Indian context, this is where concepts from foreign jurisprudence—specifically, the U.S. Howey Test—may hold water. The U.S. Supreme Court's ruling in SEC v. W.J. Howey Co. (1946) served as The precedent for the Howey Test which outlines four key elements for an instrument to be considered a security:

- a) An investment of money,
- b) In a common enterprise,
- c) With an expectation of profits,
- d) Primarily from the efforts of others.

By answering questions posed in the Indian Parliament in 2022, SEBI made its stance known to the public. It made it clear that it had not authorised any exchange-traded instruments or investment products pertaining to cryptocurrencies¹. SEBI underlined that complete policy clarity from the federal government would be necessary for any action or effort pertaining to crypto-assets. This cautious approach showed that SEBI was not eager to unilaterally acquire jurisdiction over a new and poorly defined asset class, and it also highlighted the regulatory gap that existed in the Indian crypto industry. The Reserve Bank of India (RBI), the Ministry of Finance, and other authorities needed to take a coordinated inter-agency approach, which was the general governmental mood at the time and was reflected in SEBI's response.

The absence of a legal definition for crypto-assets, combined with concerns over their speculative nature, volatility, and potential use in illicit activities, made unilateral regulation a risky proposition

A consistent theme in SEBI's public communications has been its concern for investor protection. SEBI has repeatedly flagged the possibility of retail investors being misled or defrauded in the unregulated crypto space. High-profile crypto crashes, misleading advertisements, and influencer-driven hype in India have strengthened SEBI's resolve to approach the issue conservatively. Crypto -assets, unlike traditional securities, are often marketed directly to consumers through social media without adherence to disclosure norms or risk warnings.

In traditional capital markets, SEBI enforces stringent listing, prospectus, and disclosure requirements to ensure that investors make informed decisions. The lack of analogous requirements in the crypto ecosystem raises concerns of asymmetric information, pump-and-dump schemes, and price manipulation

¹ <https://taxguru.in/sebi/cryptocurrencies-securities-post-gift-city-regulations-sebis-viewpoint.html>

factors that could undermine the integrity of Indian capital markets. Furthermore, many crypto projects operate on opaque mechanisms, with anonymous founders, limited governance, and no investor recourse mechanisms. SEBI's wariness also stems from the decentralised and cross-border nature of blockchain-based assets, which limits regulatory oversight and complicates enforcement actions².

The approach towards cryptocurrencies in India has come a long way since the global growth of it worldwide earlier in 2019 there was the incident of the Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019, which was a draft bill proposed by an inter-ministerial committee (IMC) led by former Finance Secretary Subhash Chandra Garg.

RBI's possible role and crypto's classification as a currency

An important point levied here by coin holders is that cryptocurrencies as the name suggests are "currencies" that are used to transact through digital wallets

The RBI has not yet softened up fully to the mass usage of crypto, last October, the then-RBI Governor Shaktikanta Das warned that cryptocurrencies pose significant risks to financial and monetary stability, potentially undermining central banks' control over the money supply.

Das said cryptocurrencies could destabilise the banking system and hinder inflation control during crises, calling for international cooperation to address these cross-border risks. Das also questioned the legitimacy of privately issued cryptocurrencies, arguing that currency issuance is a sovereign function, and warned against allowing a parallel private currency system that could destabilise the financial system³.

The Reserve Bank of India (RBI) issued a circular in April 2018 that forbade all regulated organisations, including banks, payment service providers, and non-banking financial companies (NBFCs), from dealing in or offering services to people or companies that trade or settle virtual currencies. This action crippled the activities of cryptocurrency exchanges and traders by preventing them from accessing the official banking infrastructure, even if it did not completely forbid the usage or possession of cryptocurrencies. The RBI used significant worries about market volatility, money laundering, consumer protection, and dangers to financial stability as justification for this decision.

Cryptocurrencies are not a currency because every modern currency needs to be issued by the central bank or Government.

The Supreme Court lifted the ban imposed by the Reserve Bank of India (RBI) on virtual currency trading, including cryptocurrencies. on the "ground of proportionality".

*"When the consistent stand of RBI is that they have not banned virtual currencies and when the government of India is unable to take a call despite several committees coming up with several proposals, including two draft bills, both of which advocated exactly opposite positions, it is not possible for us to hold that the impugned measure is proportionate,"*⁴

Four considerations were noted by the Court when it invalidated the circular:

² <https://economictimes.indiatimes.com/markets/cryptocurrency/sebi-considers-regulatory-role-in-crypto-trading-diverging-from-rbis-approach-heres-what-experts-think/articleshow/110201982.cms?from=mdr>

³ <https://www.cnbtv18.com/market/cryptocurrency/rbi-governor-sanjay-malhotra-india-cryptocurrency-stance-discussion-paper-19555335.htm>

⁴ <https://hsalegal.com/article/legalising-trade-in-cryptocurrency/#:~:text=The%20Supreme%20Court%20lifted%20the,the%20%E2%80%9Cground%20of%20proportionality%E2%80%9D.&text=The%20RBI's%20core%20defence%20included,monetary%20system%20and%20overall%20stability.>

- In the last five years or more, the RBI has not discovered any instances in which the operations of virtual currency exchanges have negatively affected the operations of the organisations under its regulation.
- Up until and including in their response dated September 4, 2019, the RBI has consistently maintained that it has not outlawed virtual currencies in the nation.
- Even the November 2, 2017-formed Inter-Ministerial Committee, which at first suggested a particular legal framework that included the introduction of a new law called the Crypto-token Regulation Bill 2018, believed that a ban might be an extreme measure and that regulatory measures could accomplish the same goals.
- The court also referred to cryptocurrencies as a “by-product” of blockchain technology and said the government could separate the two.

Regulating Cryptocurrency Under the Prevention of Money Laundering Act (PMLA)

As cryptocurrencies became more popular in India, worries about their possible abuse for illegal activities including tax evasion, money laundering, and financing terrorism grew. In response, the Indian government expanded the Prevention of Money Laundering Act, 2002 (PMLA) to include a wide variety of cryptocurrency-related activities in a historic regulatory action. Virtual Digital Asset (VDA) service providers, such as cryptocurrency exchanges, wallet custodians, and intermediaries, were designated as "reporting entities" under the PMLA as of March 2023.

Under the supervision of the Financial Intelligence Unit-India (FIU-IND), this signified a dramatic change from an uncontrolled arena to one that is now subject to mandatory KYC standards, transaction monitoring, and suspicious activity reporting duties. The scope, proportionality, and efficacy of applying a traditional anti-money laundering framework to a rapidly changing digital asset ecosystem are important legal and policy issues that are brought up by this step, even though it brings India into compliance with international AML standards like those established by the Financial Action Task Force (FATF).

Section 3 of the PLM act defines Money laundering-

Offence of money-laundering.—Whoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the 1 [proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming] it as untainted property shall be guilty of offence of money-laundering. 2 [Explanation.—For the removal of doubts, it is hereby clarified that,—

- (i) a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely:—
 - (a) concealment; or
 - (b) possession; or
 - (c) acquisition; or use; or
 - (d) projecting as untainted property; or
 - (e) claiming as untainted property, in any manner whatsoever;

(ii) the process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.]⁵

India's main legislative framework for preventing money laundering and related financial crimes is the Prevention of Money Laundering Act (PMLA), 2002. The Act aims to stop the creation and concealment of illicit wealth and was passed in response to India's international commitments under agreements like the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and the Financial Action Task Force's (FATF) recommendations. Fundamentally, the PMLA makes it illegal to transform or transfer "proceeds of crime"—that is, assets or value obtained through illegal activity—into supposedly lawful assets. It gives designated authorities, such as the Enforcement Directorate (ED), the authority to look into, prosecute, and seize assets related to money laundering.

On March 7, 2023, the Ministry of Finance, Government of India, issued a notification titled "Notification No. S.O. 1072(E), dated 7th March, 2023" under the Prevention of Money Laundering Act (PMLA), 2002, officially extending the scope of anti-money laundering regulations to include specific cryptocurrency-related activities.⁶

The Central Government hereby notified that the following activities when carried out for or on behalf of another natural or legal person in the course of business as an activity for the purposes of said sub-clause, namely:-

- (i) exchange between virtual digital assets and fiat currencies;
- (ii) exchange between one or more forms of virtual digital assets;
- (iii) transfer of virtual digital assets;
- (iv) safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets; and
- (v) participation in and provision of financial services related to an issuer's offer and sale of a virtual digital asset.

One of the foundational AML requirements is robust **KYC** and **CDD** norms. Crypto exchanges service providers must:

- **Verify customer identity** before allowing transactions, just like banks.
- Collect **officially valid documents (OVDs)** like Aadhaar, PAN, and passports.
- Conduct **enhanced due diligence (EDD)** for the high-risk customers and transactions.

The PMLA is the investigative counterpart of the lady of justice with the sword and balance who is blinded. But it has a flaw of its own. "Proceeds of crime, including its concealment, possession, acquisition, or use and projecting or claiming it as untainted property," is what Section 3 PMLA says. This is precisely where mapping the crypto world would be challenging. One must examine the element of "consideration" for a transaction in order to comprehend cryptocurrencies. In the crypto realm, it is an underlying code, while in the actual world, it is fiat or money. The PMLA has successfully breached the barriers that guard the cryptocurrency world, despite the fact that it is challenging to understand who the owner is and that the transaction is untraceable.

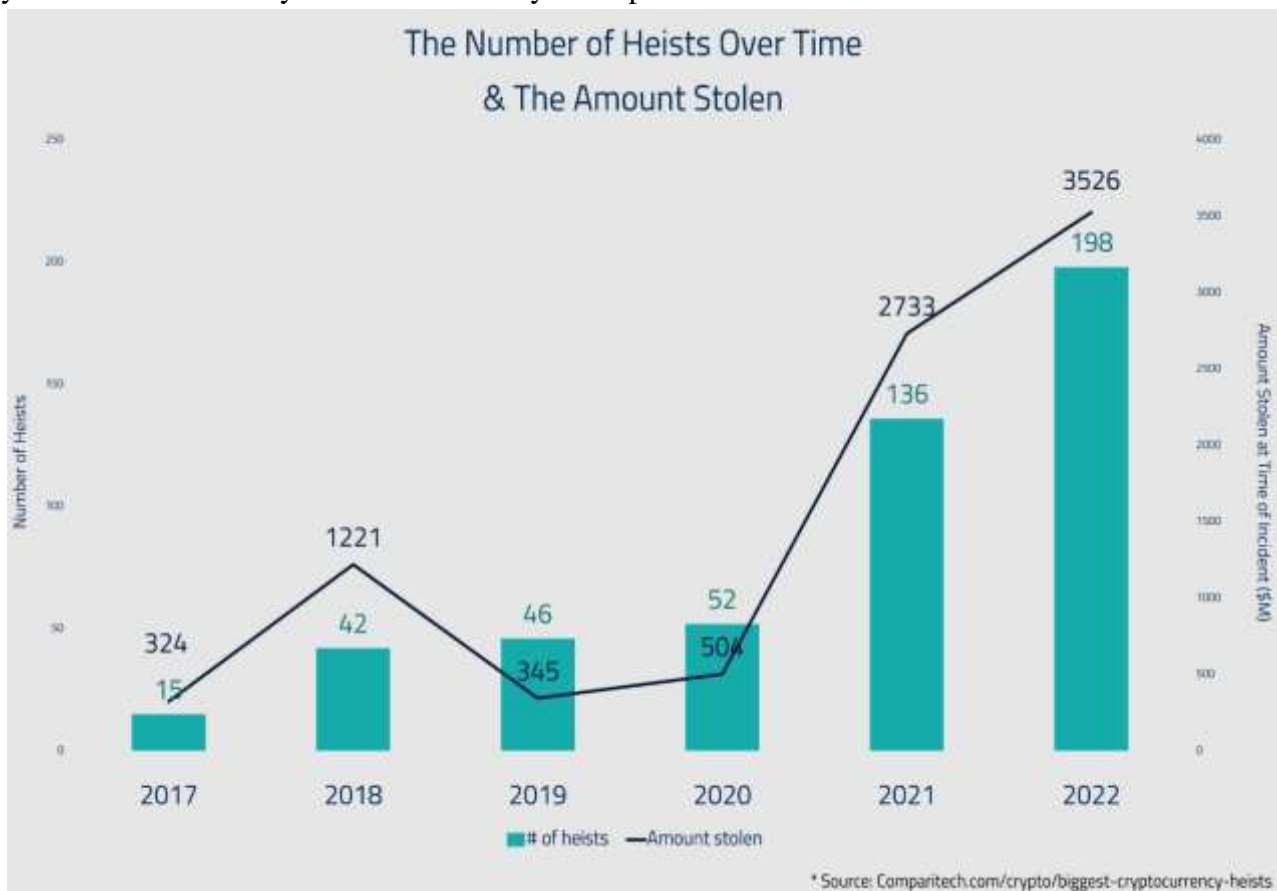
⁵

<https://enforcementdirectorates.gov.in/sites/default/files/Act%26rules/THE%20PREVENTION%20OF%20MONEY%20LAUNDERING%20ACT%2C%202002.pdf>

⁶ <https://egazette.gov.in/WriteReadData/2023/244184.pdf>

The PMLA intervenes and renders the conversion of fiat to cryptocurrency a contaminated transaction and, consequently, a tainted property as a crypto world cannot exist in a vacuum and must use actual fiat or currency as a means of exchange. The deterrent effect of the cryptocurrency's surgical attack might not materialise, though. The Reserve Bank of India has long maintained that cryptocurrency threatens a country's sovereignty and stability. This was demonstrated by the lawsuits filed against significant cryptocurrency trading firms based in India and their claims that "crypto" is the same as "a Ponzi scheme." A cryptocurrency platform must submit a Suspicious Transaction Report (STR) to the Financial Intelligence Unit-India (FIU-IND) if it notices suspicious activity, such as abnormally large or frequent transactions, the usage of privacy-focused cryptocurrencies, or connections to high-risk nations. Serious penalties may result from non-reporting.⁷

There must be an internal system in place for cryptocurrency exchanges and other VDA-related companies to keep track of all transactions, including cash transfers over INR 10 lakhs (~USD 12,000). In addition, they have to keep track of all cash transactions that are closely related to one another and have a total value of less than INR 10 lakhs each, even if the monthly total exceeds that amount. These documents, which should be kept for five years, should contain information about the type, amount, and date of transactions.⁸ In case of non-compliance with the PMLA Rules, the newly designated reporting entities i.e., crypto exchanges and other VDA service providers can be subjected to monetary penalties which will not be less than INR 10,000 but may extend to INR 1,00,000 for each failure. The monetary penalty is in addition to any other action that may be taken under any other provisions of the PMLA⁷.



⁷ <https://blogs.law.ox.ac.uk/oblb/blog-post/2023/07/digital-assets-indian-anti-money-laundering-regime>

⁸ <https://www.lexology.com/library/detail.aspx?g=0e6e9a42-fb65-4a69-9b09-38c405a3bda0>

The same strictures that apply to any other transaction using fiat currencies will now apply to any activity involving crypto transfers that are suspected of being related to money laundering. Exchanges have a responsibility to uphold identification, transparency, and regulatory compliance. Additionally, banks, other financial institutions, cryptocurrency exchanges, and intermediaries will be required to check the identity of their customers and counterparties, maintain records, and submit notifications regarding any suspicious behaviour as reporting entities under the PMLA. The Enforcement Directorate now has the authority to look into any alleged financial misconduct involving bitcoin holdings thanks to these measures.

This also aligns India's crypto policy with the FATF guidelines, which recommend treating Virtual Asset Service Providers (VASPs) similarly to other financial institutions. It provides the Enforcement Directorate (ED) and FIU-IND a legal basis to demand information, freeze assets, or initiate investigations into suspicious crypto-related transactions.

In 2024 an estimated \$41 billion worth of illicit volume, but that could rise another \$10 billion given historical trends and as more illicit addresses are identified.⁹

In 2024, terrorist organisations continued to rely on traditional financial systems — cash, banks, money service businesses, and hawalas — to move funds. But evidence of the growing use of cryptocurrency by terrorist groups is clear. Of particular concern is cryptocurrency's growing role for ISIS 'affiliate in Afghanistan, Islamic State Khurasan Province (ISKP), one of the most significant transnational terrorist threats today.

In March 2024, ISKP carried out a deadly attack in Moscow that was partially financed with cryptocurrency.

In June 2024, a German individual, who sent USD 1,700 of cryptocurrency to ISKP, was arrested after applying to work as a security guard at a major European soccer tournament — the type of event ISKP has repeatedly urged its supporters to target.

In the same month, Turkish authorities announced that they had arrested ISIS financiers operating within the country and seized cryptocurrency wallets. In December 2024, a UK-based individual was sentenced to prison for sending more than GBP 16,000 worth of cryptocurrency to ISKP.¹⁰

These events serve as a warning sign for Indian authorities that strict regulation is necessary for crypto exchanges especially foreign transfers, it could be a wide spread route to fund terror activities by our neighbouring countries, all due to the inherent anonymity of crypto wallets.

ChipMixer Takedown (\$3 Billion Laundered): An example of laundering was the ChipMixer takedown. In March 2023, an international law enforcement operation dismantled ChipMixer, a cryptocurrency mixing service based in Vietnam which brought down the Vietnamese cryptocurrency mixing business ChipMixer. Over \$3 billion in illegal funds, including the profits of ransomware attacks, darknet market transactions, and other criminal operations, were allegedly laundered through the site. Authorities confiscated over \$46 million in cryptocurrencies along with the service's infrastructure.¹¹

\$263 Million Cryptocurrency Theft and Laundering Scheme USA May 2025: In a RICO conspiracy involving the theft and laundering of more than \$263 million in bitcoin, 12 people were accused by the

⁹ https://cointelegraph.com/news/illicit-crypto-volumes-51-billion-2024-share-falls-chainalysis?utm_source=chatgpt.com

¹⁰ https://www.trmlabs.com/resources/blog/category-deep-dive-use-of-crypto-in-terrorist-financing-expanded-in-2024?utm_source=chatgpt.com

¹¹ <https://eucrim.eu/news/chipmixer-taken-down/>

US Department of Justice. The defendants are accused of stealing digital assets through fraudulent methods, including as SIM-swapping attacks and house invasions. Luxury purchases, such as \$4 million spent at nightclubs and \$9 million on exotic cars, were used to launder the proceeds.¹²

Cryptocurrencies offer a unique combination of features—decentralisation, pseudonymity, global accessibility, and ease of transfer—which make them attractive tools for money laundering. In a typical laundering process, illicit funds (such as those obtained from drug trafficking, cybercrime, or corruption) are first converted into cryptocurrency through various on-ramps like exchanges or peer-to-peer platforms. Since many of these transactions can occur without stringent Know Your Customer (KYC) norms—especially on unregulated exchanges or over-the-counter (OTC) desks—criminals can enter the crypto ecosystem with relative anonymity.

The launderer may employ strategies like mixing or tumbling services, which combine cryptocurrencies from several sources to conceal their origin, once the illegal monies are in cryptocurrency form. Another popular technique is chain-hopping, which makes traceability even more difficult by quickly transferring money between several platforms and cryptocurrencies (such as Bitcoin, Monero, and Ethereum), frequently across several jurisdictions. Criminals occasionally buy NFTs and virtual assets as a way to store and exchange value, or they use decentralised finance (DeFi) protocols to weave a web of intricate transactions.

Converting the cleaned funds back into fiat money or using them to purchase legal goods and services is the last stage of laundering, referred to as integration. This is accomplished by using cryptocurrency ATMs, exchanges with loose compliance guidelines, or even by paying with cryptocurrency for upscale goods, real estate, and services. By this point, the funds' source is mostly concealed, making enforcement very challenging. This entire procedure takes advantage of legal gaps and the absence of consistent international norms for crypto governance, highlighting the urgent need for stricter regulation, international cooperation, and strong enforcement of the Prevention of Money Laundering Act (PMLA) in India and elsewhere.

By bringing crypto activities under PMLA, the Indian government has taken a strong stance on ensuring that the sector does not become a safe haven for financial crime. However, while this legal step strengthens oversight, it also places a heavy compliance burden on crypto businesses, especially smaller startups. It raises concerns about how enforcement will be handled in the absence of a comprehensive cryptocurrency law. Nonetheless, this framework provides regulators a much-needed tool to track suspicious financial flows in the crypto space, sending a clear message that digital assets are not beyond the reach of financial regulation in India.

Path Forward

The premise going forward with crypto in India is that it is here to stay and grow, if we look at it like this i.e. realistically then we need more comprehensive regulation of crypto.

Governments through out the world including United States which is the largest known state holder of bitcoin in the world, estimated to hold about 200,000 BTC, as of March 2025.¹³

India needs a unique regulatory strategy that doesn't hinder innovation or jeopardise financial stability, given the bitcoin ecosystem's quick growth and dynamic nature. The Reserve Bank of India (RBI), the

¹² https://www.justice.gov/usao-dc/pr/additional-12-defendants-charged-rico-conspiracy-over-263-million-cryptocurrency-thefts?utm_source=chatgpt.com

¹³ <https://www.aljazeera.com/news/2025/3/4/trump-announces-us-crypto-reserve-what-it-is-and-why-it-matters>

Securities and Exchange Board of India (SEBI), and the Financial Intelligence Unit (FIU) under the PMLA are examples of existing regulatory agencies that currently carry out fragmented monitoring according to their respective areas. However, the distinctions between securities, currencies, commodities, and digital assets are blurred by the very nature of cryptocurrencies. Regulatory overlaps, investor confusion, and a murky compliance environment for Virtual Asset Service Providers (VASPs) are the results of this. The industry now lacks coherence and clarity, which can be supplied by a distinct, specialised organisation. SEBI is already overburdened with regulating stock exchange related securities and companies, which have led to delays in addressing cases. Reports suggest that SEBI has only 1,067 employees to manage its extensive responsibilities. This shortfall in staff and myriad of cases has resulted in prolonged response times, with cases related to registered entities taking approximately 6+ months to resolve. Complaints against unregistered entities also experience similar delays¹⁴, and issues requiring suo motu action are often left unaddressed due to resource constraints.

Additionally, the burden of ED has skyrocketed in recent years. The ED performed 3,010 raids between 2014 and 2022, which is roughly 27 times more than the 112 searches that were undertaken between 2004 and 2014. The requirement to handle ongoing investigations and the intricacy of new cases under the Prevention of Money Laundering Act (PMLA) are the reasons for this increase.¹⁵

The overextension of SEBI and the ED underscores the necessity for a dedicated regulatory body to oversee the cryptocurrency sector in India. A specialised authority could alleviate the burden on existing agencies, ensure more efficient regulation, and foster a more conducive environment for innovation in the digital asset space.

The authority might have quasi-legislative, executive, and adjudicatory functions, much like SEBI or the Telecom Regulatory Authority of India (TRAI). Its establishment would also aid in the centralisation of data, intelligence, and policy initiatives, guaranteeing that digital assets are not just monitored but also governed in a manner that encourages ethical innovation and global competitiveness. Additionally, the organisation may concentrate on cross-border investigations of crypto crimes, cooperate with international authorities, and make sure India complies with global norms such as those established by the Financial Action Task Force (FATF).

By lowering uncertainty, minimising financial crimes, and creating an environment where India may responsibly lead in Web3 and blockchain-based innovation, DARA would eventually benefit all stakeholders, including government organisations, corporations, investors, and the general public. Unquestionably, digital assets have a big future, and India cannot afford to lag behind because of disjointed governance. A specialised crypto regulator would offer the capacity, clarity, and consistency required to successfully oversee this revolutionary area.

Additionally Crypto markets are global and borderless. India must actively collaborate with other countries and follow FATF's "Travel Rule" and Virtual Asset Service Provider (VASP) guidance. This includes setting data-sharing protocols, conducting joint investigations, and ensuring interoperability of compliance standards to track cross-border laundering and terror financing.

Keeping all this in mind, one of the key characteristics of cryptocurrency are the-

¹⁴ https://aseemjuneja.in/sebi-under-fire-toxic-work-culture-or-unrealistic-employee-demands/?utm_source=chatgpt.com

¹⁵ https://timesofindia.indiatimes.com/india/ed-raids-jumped-27-times-during-2014-2022-compared-to-2004-14-govt/articleshow/93144184.cms?utm_source=chatgpt.com

- Lack of extensive procedures and paperwork, unlike bank transfers
- Autonomy
- Anonymity

The government should keep in mind these factors which are a significant part of the basis and attraction of cryptocurrencies. Cryptocurrency's no doubt in some circles seeks to challenge the existing fiat reserve bank system however this is a mammoth task and near impossible.

The government at this stage, with the explosion of the value of Bitcoin post 2024, is at the point of balancing coin holders interests and regulations, crypto must adhere to the norms of legality in India.

Bibliography

1. <https://hsalegal.com/article/legalising-trade-in-cryptocurrency/#:~:text=The%20Supreme%20Court%20lifted%20the,the%20%E2%80%9Cground%20of%20proportionality%E2%80%9D.&text=The%20RBI's%20core%20defence%20included,monetary%20system%20and%20overall%20stability.>
2. <https://www.thehindu.com/news/national/supreme-court-sets-aside-rbi-ban-on-cryptocurrency-transactions/article61967124.ece>
3. <https://www.ibanet.org/article/2e4fb646-4ffd-4660-a5be-5e41e79c5576>
4. https://www.nishithdesai.com/Content/document/pdf/Articles/181207_A_The-Virtual-Currency-Regulation-Review-India.pdf
5. <https://www.lexology.com/library/detail.aspx?g=d8b27c01-6215-4dba-abe9f1b0fba86073#:~:text=Key%20highlights%20and%20issues%20of,to%2010%20years%2C%20or%20both.>
6. https://www.justice.gov/usao-dc/pr/additional-12-defendants-charged-rico-conspiracy-over-263-million-cryptocurrency-thefts?utm_source=chatgpt.com
7. <https://www.gk8.io/blog/cryptocurrency-crime-statistics-a-visual-guide/>
8. https://cointelegraph.com/news/illicit-crypto-volumes-51-billion-2024-share-falls-chainalysis?utm_source=chatgpt.com
9. <https://blogs.law.ox.ac.uk/oblb/blog-post/2023/07/digital-assets-indian-anti-money-laundering-regime>
10. <https://www.sconline.com/blog/post/2023/03/15/pmla-crypto-currency-when-prevention-is-better-than-cure/>
11. <https://egazette.gov.in/WriteReadData/2023/244184.pdf>
12. <https://www.aljazeera.com/news/2025/3/4/trump-announces-us-crypto-reserve-what-it-is-and-why-it-matters>
13. https://aseemjuneja.in/sebi-under-fire-toxic-work-culture-or-unrealistic-employee-demands/?utm_source=chatgpt.com
14. https://timesofindia.indiatimes.com/india/ed-raids-jumped-27-times-during-2014-2022-compared-to-2004-14-govt/articleshow/93144184.cms?utm_source=chatgpt.com
15. <https://www.ijfmr.com/papers/2025/2/40898.pdf>
16. <https://ijrpr.com/uploads/V5ISSUE12/IJRPR36609.pdf>

17. <https://anvpublication.org/Journals/HTMLPaper.aspx?Journal=International%20Journal%20of%20Reviews%20and%20Research%20in%20Social%20Sciences;PID=2019-7-2-13>
18. <https://www.researchgate.net/publication/352191701> The Regulation Problem of Cryptocurrencies The Regulation Problem of Cryptocurrencies
19. <https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti>