INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

Emerging Economic Crimes in the Digital Age: The Legal Challenge of Cryptocurrency

K. Sai sivani, P. Kesavarthini
students,
SASTRA deemed university Thanjavur
129117016@sastra.ac.in , 129117019@sastra.ac.in

Abstract

The term currency had evolved in many forms that it is beyond human possibility. the term currency was not evolved as a concept and there were only existence of the barter exchange and in later times the usage of currency was introduced in coins and then in currency notes currently the currency had evolved in current stage where transactions are made through debit/credit card and now a new type of transaction is evolving that is digital wallet and bitcoins. Bitcoins is a decentralized digital currency that uses blockchain technology to enable peer-to-peer transactions without the need for a central authority like a bank or government.[1] Both the bitcoin and blockchain is digital currency and ledger it leads to easy transaction, anonymity, global transactions and decentralized control. The crypto currency is a new evolving kind of money it doesn't have a clear statutory law. In India the government had made attempts to govern the transaction of crypto currency but it didn't done its intended duty due to a single framed law. The lack of laws in many countries like India the bitcoin is made a gateway for illegal transaction and through the illegal transaction black money are transferred, black market runs through the means of crypto currency. This paper says what is crypto currency and block chain technology and its functioning, its problem and government attempt to govern the area and the need to create a separate law to govern crypto transactions

Key words: *cryptocurrency, block chain, PMLA, income tax Act, finance Act, digital currencies*

I. INTRODUCTION:

The rapid advancement of technology and globalisation has significantly transformed traditional financial systems and methods of economic transaction. In modern society, digital modes of payment have become an essential component of international commerce and financial accessibility. Situations involving cross-border travel and international transactions increasingly demonstrate the convenience and efficiency of the digital financial system, where electronic transfers and digital wallets often replace traditional physical currency. The evolution of currency has progressed from barter systems and metallic coins to paper currency and, in recent years, to digital and virtual forms of financial assets.

One of the most significant developments in the digital financial sector is the emergence of cryptocurrency, a decentralised digital asset operating through blockchain technology. Unlike traditional currencies regulated by central banks, cryptocurrencies function through peer-to-peer networks without centralised control or governmental supervision. Bitcoin, the first and most widely recognized cryptocurrency, introduced a system of borderless financial transactions that enables users to transfer digital assets with greater speed and reduced dependence on financial intermediaries. Cryptocurrencies are generally stored in digital wallets and recorded through blockchain technology, which functions as a decentralized and immutable digital ledger. Blockchain technology ensures transparency and security through encrypted records of transactions, making alteration of data extremely difficult.[2]

However, the same technological features that make cryptocurrency innovative and efficient have also created serious legal and regulatory concerns. The pseudonymous, decentralized, and transnational nature of cryptocurrency transactions makes it difficult for authorities to trace the identity of users and monitor the movement of illegal funds. Consequently, cryptocurrencies have increasingly become vulnerable to misuse in economic crimes such as money laundering, cyber fraud, terror financing, tax evasion, ransomware attacks, and illegal darknet transactions. Criminal organizations often exploit cryptocurrency systems to transfer illicit funds across borders while avoiding traditional financial oversight mechanisms.

Cryptocurrency can therefore be regarded as a double-edged sword. On one hand, it promotes financial innovation, borderless transactions, and digital economic growth; on the other hand, its misuse for illegal financial activities exposes serious weaknesses in existing economic crime laws. The fragmented regulatory approach adopted in India has created uncertainty in the prevention, investigation, and prosecution of cryptocurrency-related offences. In this context, this paper seeks to critically examine the nature

[2] JainMar, A. (n.d.). Crypto Under PMLA. What does it mean for you? - Flitpay. Flitpay.com. https://www.flitpay.com/blog/crypto-under-pmla-what-does-it-mean-for-you

of cryptocurrency, its vulnerability to economic crimes, and the adequacy of the Indian legal framework in addressing such challenges.

The primary research problems addressed in this paper are:

1. Existing Indian economic crime laws are inadequate to address offences involving cryptocurrency transactions.
2. India's fragmented approach toward cryptocurrency regulation creates uncertainty in preventing and prosecuting economic offences.

II. NATURE OF CRYPTO CURRENCY:

The idea of crypto currency existed before it was created. During 1980's computer scientists attempted to develop electronic payment systems that could function independently of traditional banking institution. Modern crypto currency began with the creation of bitcoin in 2008 by a anonymous individual named Satoshi Nakamoto. In 2009 the blockchain-based cryptocurrency systems were created.
From 2009 to 2017 the growth of crypto currency were rapid it also created risk of many illegal transaction due to its nature[3].

A) The major characteristic of cryptocurrency is its decentralized nature. Unlike traditional currencies regulated by central bank and financial institution cryptocurrencies operate through blockchain technology. The transaction are verifies by network participant than a central authority. Although this promotes efficiency and financial autonomy it creates significant regulatory challenges. The absence of central authority enables offenders to transfer funds without any scrutiny by banking systems[4]. As a result cryptocurrencies are frequently associated with economic crimes such as money laundering, financial fraud , tax evasion.

B) The next nature is that its Pseudonymity and Anonymity. The cryptocurrency are conducted through digital Vallet addresses than identity although blockchain record transaction publicly finding the actual individual behind the Vallet is extremely difficult. The pseudonymous nature of crypto currency enhances privacy and financial freedom for users however it also creates opportunities for criminal misuse. Criminals often use cryptocurrencies in darknet market places, ransomware attacks, tax evasion schemes. This anonymity significantly limits the effectiveness of enforcement of agencies in detecting economic offences.

C) Cryptocurrency operates though blockchain technology, which records all transaction in a immutable digital ledger. Each transaction is permanently stored in block connected chronologically making changes in it is highly difficult. Blockchain technology provides transparency because transaction histories are publicly accessible and verifiable. Despite this transparency blockchain system can still be exploited for economic crimes. Criminals often use privacy-enhancing technology to hide transaction trails.

D) Cryptocurrency markets are highly volatile due to speculative trading, technological investment and regulatory uncertainty. Prices of cryptocurrencies such as bitcoin fluctuate within short periods. Unlike traditional currency cryptocurrency is not backed by government. This speculative nature attract investors seeking high returns but also risk of market manipulation and financial instability. Economic criminals may exploit public interest and lack of investor awareness by conducting ponzi schemes and investment frauds using cryptocurrency. The absence of a comprehensive regulatory provision increases the chances of financial crimes

While these characteristics distinguish from traditional financial system and these characteristics promote innovation and digital inclusion they also create significant vulnerabilities to economic crimes such as money laundering, and taxation fraud. The existing legal and regulatory framework face substantial challenges in effectively monitoring and controlling cryptocurrency- related criminal activity.

III. LEGAL FRAMWORK GOVERNING CRYPTOCURRENY IN INIDA:

If you try to find a single law in India that governs cryptocurrency, you won't find one because it doesn't exist. What exists instead is a collection of older laws, each written for a different purpose, that have been gradually stretched and adapted to cover a technology nobody anticipated when those laws were drafted. Tax statutes, anti-money laundering provisions, cybercrime rules these form the scaffolding of India's crypto regulation, even though none of them were ever designed with digital assets in mind.

India has not declared cryptocurrency legal tender, and the government's overall attitude has shifted back and forth over the years. At one point, regulators seemed ready to shut the whole thing down. More recently, the approach has become less confrontational leaning toward compliance requirements and taxation rather than prohibition. But "less hostile" is not the same as "clearly regulated." Crypto in India today occupies a strange middle ground: tolerated, taxed, and watched, but never truly defined.

The PMLA and Anti-Money Laundering Obligations

[3] Sharma, D., Pant, D., & Kumar, A. (2023). Cryptocurrency: An Overview of its History, Technology and Future Prospects. International Journal of Advanced Research in Science, Communication and Technology, 427-430.
[4] Collins, J. A. (2025). Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti-Money Laundering Regulations. U. Miami Bus. L. Rev., 34, 71.

The law that has had the most direct impact on the crypto sector in recent years is the Prevention of Money Laundering Act, 2002. The reason is not hard to understand. Cryptocurrency's decentralized design means that money can cross borders without touching a bank. Transactions are recorded on a public ledger, but the people behind the wallet addresses are not. That combination visible transactions, invisible people created serious problems for enforcement agencies trying to track illicit money flows.[5]

The government's response came in 2023, through notifications that brought crypto exchanges, wallet providers, and Virtual Digital Asset service providers formally within the PMLA's scope as "reporting entities." This meant they were now subject to the same kinds of obligations that banks have long operated under verifying customer identities, maintaining records, monitoring transactions, and reporting suspicious activity to the Financial Intelligence Unit–India (FIU-IND).

The Enforcement Directorate gained sharper tools as a result. With a broader definition of "proceeds of crime" now covering virtual digital assets, the agency could investigate crypto-linked money laundering and move to seize or attach digital assets suspected of having criminal origins. This mattered practically, as a number of investigations into darknet platforms, fraudulent exchanges, and transnational scams had already shown how routinely crypto was being used to launder money.[6]

But the PMLA has obvious limits here. It was conceived for a world of banks and financial intermediaries, where money moves through identifiable institutions. DeFi platforms, privacy coins, peer-to-peer transfers, and mixing services follow none of that logic. They are specifically designed to route around centralised checkpoints, and the PMLA's enforcement framework was not built to follow them there. Offshore exchanges outside Indian jurisdiction add another layer of difficulty. And unlike countries such as Singapore or the United States, India still has no dedicated licensing system for crypto businesses, which means there is no formal gate at which compliance can be required before a business is permitted to operate.

The IT Act's Supporting Role

The Information Technology Act, 2000, was written to address the challenges of an internet-connected economy electronic records, digital contracts, and cybercrime. It was not written with cryptocurrency in mind, but it becomes relevant to crypto in a fairly obvious way: since everything about crypto happens digitally, the law that governs digital activity inevitably touches it.

Where the IT Act matters most in practice is in cybercrime situations when a wallet is hacked, when a user is phished, when exchange systems are breached, or when personal data is stolen from a crypto platform. The provisions covering computer-related offences and unauthorised access are regularly used in such cases[7]. The Act also creates an expectation that exchanges operating in India will maintain basic cybersecurity standards and data protection practices.

What the IT Act cannot do, however, is regulate cryptocurrency itself. Its engagement with crypto is essentially incidental it reaches crypto only because crypto happens to live in the same digital space the Act governs. It cannot classify digital assets, assign regulatory jurisdiction, or set rules for the crypto industry. That kind of comprehensive regulation requires purpose-built legislation, which India still lacks.

The RBI's Long-Running Scepticism

Of all the institutions involved in India's crypto debate, the Reserve Bank of India has been the most consistently and vocally opposed. The RBI has raised concerns about monetary stability, consumer risk, and the potential for cryptocurrencies to facilitate money laundering, terror financing, and speculative market excess. Its worry, broadly stated, is that decentralized private currencies threaten the state's control over the monetary system and that the risks this creates outweigh the benefits.

That concern became policy in April 2018, when the RBI directed banks and other regulated financial institutions to refuse services to anyone dealing in cryptocurrency. Technically, this did not make owning or trading crypto illegal. Practically, it strangled the industry. Without banking access, exchanges could not process payments, and most of them ground to a halt.

The industry took the matter to court, and in 2020, the Supreme Court overturned the RBI's circular. The Court's reasoning was that the central bank had not shown actual evidence of harm to the banking system from crypto activity, and that any restriction on trade and business must satisfy constitutional standards of reasonableness under Article 19(1)(g). The ruling reopened the market and set off a wave of renewed interest and investment in crypto across India.

The RBI, however, has not changed its underlying view. It continues to push for stricter controls or even prohibition of private cryptocurrencies, and at the same time actively promotes the Digital Rupee India's official Central Bank Digital Currency. In the RBI's framing, CBDCs and private crypto are fundamentally different things: the Digital Rupee offers the efficiency of digital transactions without surrendering state control over monetary policy, while private cryptocurrencies do the opposite.

Taxation: Acknowledgment Without Recognition

The Finance Act, 2022 brought the most explicit government acknowledgment yet that crypto exists and matters economically even if that acknowledgment stops well short of legal recognition. Virtual Digital Assets were formally defined under Section 2(47A) of the Income Tax Act, 1961. Under Section 115BBH, profits from crypto transfers attract a flat 30% tax rate. Section 194S introduced a 1% TDS on transactions above specified thresholds.[8]

In practical terms, what the government was saying was this: we may not be prepared to call crypto a legitimate currency, but we are very prepared to tax the money people make from it. It was a pragmatic move one that brought revenue without requiring a policy position on the fundamental question of what crypto actually is.

The Bottom Line

[5] JainMar, A. (n.d.). Crypto Under PMLA. What does it mean for you? - Flitpay. Flitpay.com. https://www.flitpay.com/blog/crypto-under-pmla-what-does-it-mean-for-you

[6] Verma, A., & Tiwari, L. K. (May 2025). Cryptocurrency and Its Regulation in India. Advances in Mathematical Modelling, Applied Analysis and Computation.

[7] Srujana, D. (2024). BLOCK CHAIN AND CRYPTOCURRENCY LAWS AND REGULATIONS 2024–AN ANALYSIS. International Journal of Information Technology (IJIT), 5(01), 51-62.

[8] Pradhan, R. Cryptocurrency Taxation in India: A Comparative Analysis with the US, the UK, and Singapore.

Where does all of this leave India? With a regulatory framework that is, in a word, incomplete. The combination of PMLA obligations, tax provisions, IT Act coverage, and the Supreme Court's intervention has created something, but it has not created a coherent system. There are real gaps in how crypto assets are classified, how crypto businesses are licensed, how investors are protected, and how cross-border crypto crime is investigated and prosecuted. India's approach to cryptocurrency is still a work in progress, and a rather cautious one at that, reflecting a government that recognises the technology is not going away, but has not yet decided how to fully come to terms with it.

IV. ANALYSISING LEGAL JUDGEMNT REGARDING CRYPTOCURRENCY:

In the case of **Internet and Mobile Association of India v. Reserve Bank of India** brought into sharp focus a tension that runs through much of India's crypto policy debate the conflict between a regulator's instinct to restrict what it does not fully understand, and the constitutional right of citizens to carry on legitimate economic activity.

The story begins in April 2018, when the RBI issued a circular directing all banks and regulated financial entities to stop offering services to cryptocurrency exchanges and individuals trading in virtual currencies. The circular stopped short of declaring crypto illegal, but its practical effect was nearly identical cut off from the banking system, exchanges could not process deposits or withdrawals, and the industry effectively came to a standstill. The RBI's stated justification was that cryptocurrencies posed unacceptable risks to the financial system: money laundering, terror financing, tax evasion, fraud, and the difficulty of tracing anonymous digital transactions.

The Internet and Mobile Association of India, along with several crypto exchanges, challenged the circular before the Supreme Court. Their core argument was straightforward by making it impossible to run a cryptocurrency business in India, the RBI had infringed upon the constitutional right to trade and carry on business guaranteed under Article 19(1)(g) of the Constitution.

What makes the judgment analytically rich is that the Court did not simply dismiss the RBI's concerns. It acknowledged them. The bench recognised that cryptocurrency had grown into a significant economic activity, with a large and expanding user base, substantial transaction volumes, and rising market capitalisation. It equally acknowledged that the same features that make cryptocurrency attractive, decentralisation, pseudonymity, and the ability to transfer value across borders instantly also make it vulnerable to serious misuse. Money laundering, illegal fund transfers, and terror financing were specifically noted as risks that enforcement agencies were struggling to address.

The Court engaged meaningfully with the technical realities of crypto. It observed that identifying the real individuals behind wallet addresses is genuinely difficult, and that tools like mixers, tumblers, and privacy coins create additional layers of obscurity that further complicate investigations. These observations are directly relevant to the anti-money laundering challenges discussed in the context of the PMLA they reflect a judicial understanding that the pseudonymous nature of blockchain is not merely a theoretical concern but a live enforcement problem.

The judgment also grappled with the definitional ambiguity surrounding cryptocurrency. The Court noted that crypto does not fit comfortably within any established legal category it is not quite currency, not quite a commodity, and not quite a conventional financial instrument. This ambiguity, the Court recognized, creates genuine difficulties for regulators trying to apply existing law to a technology that was not anticipated when those laws were written. In this respect, the judgment offered an unusually candid acknowledgment of the gaps in India's regulatory framework.

Interestingly, the Court also looked outward. It surveyed the approaches taken by the United States, the European Union, Japan, and China, using that comparative lens to illustrate that no country had yet found a definitive answer to the regulatory challenge that cryptocurrency poses. This comparative dimension gave the judgment a broader intellectual context and implicitly suggested that India's regulatory response needed to be thoughtful rather than reactive.

The legal principle on which the case ultimately turned was proportionality. The Court accepted that the RBI has the authority to regulate the financial system and take steps to prevent economic crime. What it questioned was whether the specific restriction the RBI had chosen a blanket ban on banking services was proportionate to the risk it was trying to address. The answer was no. The RBI had not demonstrated, with adequate empirical evidence, that cryptocurrency exchanges had actually caused measurable harm to the banking system. Equally importantly, the central bank had not meaningfully explored less drastic alternatives regulatory oversight, KYC requirements, AML safeguards, transaction monitoring before reaching for a complete restriction.

There was another dimension to the Court's reasoning that is worth noting. It took cognizance of the Inter-Ministerial Committee's earlier warning that a complete ban might produce the opposite of the intended effect driving crypto activity underground, fueling peer-to-peer black markets, and making transactions harder to monitor rather than easier. In other words, excessive restriction could deepen the very problem it sought to solve.

On those grounds, the Supreme Court struck down the RBI circular. But it is important to be clear about what the judgment did and did not do. It did not declare cryptocurrency legal tender. It did not provide blanket legal sanction for all crypto activities. What it did was establish that regulation of cryptocurrency must be proportionate, evidence-based, and respectful of constitutional rights and that merely invoking the possibility of risk, without demonstrating actual harm or considering less restrictive options, is not enough to justify shutting an industry out of the formal financial system.[9]

The ruling revived the Indian crypto market and remains a foundational reference point in the ongoing debate about how the country should regulate digital assets. More broadly, it serves as a reminder that effective cryptocurrency governance requires not just regulatory authority, but regulatory judgment the kind that weighs real risks against real rights, and resists the temptation to treat restriction as a substitute for regulation.

V. KEY LEGAL CHALEENGES:

[9] Internet And Mobile Association of India vs Reserve Bank Of India, AIR 2021 SUPREME COURT 2720

Technology moves faster than law. That is true in most domains, but it is especially true of cryptocurrency, which has managed to outpace regulatory systems in almost every country in the world. For India, the challenge is particularly sharp because the existing legal infrastructure was designed for a different era one where money moved through banks, identities were tied to accounts, and borders meant something to financial transactions.

The Problem of Tracing Who Did What

The most basic enforcement challenge with cryptocurrency is a simple one: you cannot easily tell who is behind a transaction. Blockchain records addresses, not names. The ledger is open and public, but figuring out which real world person controls which wallet usually requires information that the blockchain itself does not hold. And when someone actively wants to hide by routing funds through multiple wallets, using privacy enhancing tools, or bouncing transactions across decentralized exchanges the trail can become nearly impossible to follow.

Because crypto transactions are also irreversible by design, theft and fraud are especially damaging. Once funds have moved, getting them back is rarely possible through legal or technical means.[10]

India's investigative agencies currently depend largely on exchanges for KYC records and transaction data. That helps, but only so far and only with regulated, compliant exchanges. The deeper problem is that India has not developed the same kind of blockchain forensic infrastructure that agencies in the United States have. The FBI, SEC, and other American agencies now routinely use sophisticated analytics platforms to trace crypto flows. The EU, through MiCA, has pushed for stronger transparency obligations on service providers to make monitoring more effective from the start. India has made progress through PMLA amendments, but genuine investigative capacity in this area remains limited.

When Crimes Cross Borders

Cryptocurrency is, by its nature, global. A fraud scheme might be run from one country, target victims in another, and route funds through exchanges registered in a third all in a matter of minutes. Traditional law enforcement, built around national jurisdiction and physical evidence, struggles to keep up.

Offshore exchanges are a particular problem. If a platform operates outside Indian jurisdiction, Indian authorities cannot compel it to share records, freeze assets, or cooperate with investigations. Cybercriminals and money launderers have become adept at exploiting these gaps, moving funds across jurisdictions faster than any coordination mechanism can follow.[11]

The EU has gone some way toward solving this within its own borders through MiCA, which creates consistent rules across all member states, removing the regulatory arbitrage that criminals might otherwise exploit. The United States has shown willingness to pursue aggressive cross-border enforcement, particularly where American investors or financial systems are involved. India lacks an equivalent framework there is no dedicated international coordination mechanism for crypto crime, and existing mutual legal assistance arrangements were not designed for the speed and scale of blockchain-based offences.

What Is Crypto, Legally Speaking?

This might sound like an abstract question, but it has very concrete consequences. Whether cryptocurrency is classified as currency, property, a commodity, or a security determines who regulates it, how it is taxed, what legal protections apply to people who hold it, and what happens to those who misuse it. In India, that question remains unanswered in any formal statutory sense.

Different Indian regulators approach crypto differently. The RBI treats it primarily as a monetary risk. SEBI looks at certain tokens through the lens of securities law. The income tax department treats it as a taxable asset. Each of these approaches is internally coherent, but they do not add up to a clear, unified legal framework and that uncertainty falls hardest on ordinary investors and legitimate businesses that need to know what rules apply to them.[12]

The United States has not fully resolved the classification question either, but it has at least achieved some agency-level clarity: the SEC covers tokens that function like securities, while the CFTC handles those treated as commodities. The EU has gone further, with MiCA establishing defined categories of crypto assets and specifying which rules apply to each. India has not yet taken that step.

Enforcement Gaps and the Consumer Left Behind

India's crypto oversight is spread across multiple agencies the RBI, the Enforcement Directorate, FIU-IND, SEBI, and income tax authorities all have a hand in different aspects of the market. None of them has full authority over the sector. The result is a fragmented system where jurisdictions overlap, accountability is diffuse, and enforcement is inconsistent.

For ordinary users, this creates a real problem. Victims of crypto scams, exchange hacks, or fraudulent investment schemes often discover that the legal system offers them very little. Transactions cannot be reversed. Platforms may be offshore. Agencies may lack jurisdiction or technical capacity. Even when a crime is clear, prosecution is hard.

The United States and EU have both moved to strengthen consumer protections within their crypto frameworks clearer disclosure requirements, licensing obligations, and mechanisms for redress. India has tightened AML compliance but has not yet put equivalent consumer protection rules in place.

The Bigger Picture

Comparing India to more developed regulatory environments reveals a consistent theme: India's approach to crypto is reactive rather than proactive, and fragmented rather than coherent. Steps have been taken taxation, AML compliance, the Supreme Court judgment but they do not constitute a system. Building one will require more than adding new provisions to existing laws. It will require making deliberate, legislative choices about what crypto is, who governs it, and what obligations come with operating in that market.

---

[10] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE symposium on security and privacy (pp. 104-121). IEEE.

[11] Savona, P. (2022). Prospects for reforming the money and financial system. Open Economies Review, 33(1), 187-195

[12] Drakopoulos, D., Natalucci, F., & Papageorgiou, E. (2021). Crypto boom poses new challenges to financial stability. International Monetary Fund. Obtenido de https://blogs. imf. org/2021/10/01/crypto-boom-poses-new-challenges-to-financial-stability.

VI. CRITICAL EVALUATION AND NEED FOR LEGAL REFORM:

The honest assessment of India's cryptocurrency regulatory framework is that it was never really designed it accumulated. Laws passed for unrelated purposes were pressed into service to deal with a new technology, and what emerged is a patchwork that covers some ground, leaves other ground exposed, and creates confusion about almost everything in between.

Where the System Falls Short

The most fundamental gap is definitional. India has no statutory answer to the question of what cryptocurrency actually is. Without that foundation, everything else is built on uncertain ground tax treatment, regulatory jurisdiction, investor rights, and criminal liability all remain contestable in ways that create real-world uncertainty for people trying to operate legitimately within the system. And where the law is ambiguous, those with bad intentions often find ways to exploit the gaps.

Blockchain's pseudonymous architecture makes things harder still. Conventional anti-money laundering law was built on the assumption that money flows through identifiable institutions banks, brokers, money transfer services that can be required to report, verify, and monitor. Cryptocurrency allows all of that to be bypassed. Funds can move through a chain of wallets, across international borders, in seconds. By the time a complaint is filed, the money may be gone.

Extending PMLA obligations to Virtual Asset Service Providers was the right move, but it has not solved the problem. Compliance is uneven across the industry smaller and decentralized platforms often sit beyond regulatory reach entirely. Meanwhile, the agencies responsible for enforcement frequently lack the technical expertise, forensic tools, and international connections needed to effectively investigate complex crypto crime.

Why Getting the Balance Right Matters

There is a temptation, when looking at these problems, to conclude that stronger regulation is always better. But that is not quite right either. If India imposes restrictions that are too severe, it risks pushing crypto activity underground, driving legitimate businesses to friendlier regulatory environments, and losing the economic benefits that blockchain technology could otherwise generate. Outright bans are also notoriously hard to enforce when the technology is global and decentralized by design.

The genuine risks of under-regulation are just as real, though fraud, market manipulation, money laundering, terror financing, and investor losses from exchange collapses or scams. India has already seen significant harm in each of these categories. The task is not to choose between regulation and no regulation, but to design regulation that is effective without being so burdensome that it defeats its own purpose.

What a Better Framework Would Look Like

Other countries offer useful reference points. The United States distributes crypto oversight across multiple specialist agencies the SEC, CFTC, and FinCEN each responsible for the dimensions of crypto that fall within their existing expertise. The EU has taken a more unified approach through MiCA, creating a single regulatory framework that covers licensing, transparency, AML compliance, and consumer protection for all crypto service providers across member states. Both models have their flaws, but both represent deliberate, structured regulatory choices rather than improvisation.

India needs to make similar choices The starting point should be dedicated legislation a purpose-built statute that establishes the legal status of crypto assets, defines which authority is responsible for which aspects of the market, and creates binding obligations for exchanges, wallet providers, DeFi platforms, and others. That law should cover KYC and AML requirements, investor protection, taxation, and the particular challenges posed by newer instruments like stablecoins and NFTs.

Beyond the legislation itself, India needs uniformly enforced KYC and AML standards across the entire crypto industry not just the largest, most compliant exchanges. Mandatory identity verification, transaction monitoring, and suspicious activity reporting, backed by real penalties for non-compliance, would significantly reduce the enforcement gaps that currently exist.

International cooperation also needs to be treated as a priority rather than an afterthought. Crypto crime is inherently cross-border, and India's capacity to deal with it is partly a function of its relationships with foreign agencies and bodies like FATF and Interpol. That means investing in bilateral and multilateral enforcement coordination, and building the domestic forensic capacity needed to contribute meaningfully to joint investigations.

And through all of this, policymakers need to keep in mind that the goal is not to prevent cryptocurrency from existing in India it is to ensure that it operates in a way that is transparent, fair, and safe for those who participate in it. Blockchain and crypto technology carry genuine economic potential. A regulatory framework that treats the entire sector as a threat, rather than as something to be thoughtfully governed, would be a mistake. The aim should be clarity, accountability, and the kind of legal certainty that allows innovation to flourish without becoming a cover for harm.[13]

VII. CONCLUSION:

Cryptocurrency did not come with an instruction manual for regulators. It grew quietly in the background, and by the time governments around the world sat up and paid attention, it had already become too large and too deeply embedded to simply wish away. India found itself in this position too and as this research has tried to show, its response has been more reactive than ready.

Looking at what India has built so far, the honest description is a patchwork. The PMLA, the IT Act, the Income Tax Act, RBI guidelines, and a landmark Supreme Court judgment have each contributed something but they were never designed to work together as a coherent whole. The IAMAI v. RBI ruling was genuinely important; it stopped an overreaching restriction and reminded regulators that constitutional rights apply to digital businesses too. But one court decision, however well-reasoned, cannot do the work that Parliament has so far avoided doing.

The problems this research has identified are not minor technical issues. India still has no legal definition of what cryptocurrency actually is. Regulatory responsibility is scattered across agencies that were never meant to share it. Ordinary investors who lose

[13] Fakrulloh, Z. A. (2024). Reform of law enforcement to strengthen the legal system in eradicating money laundering through cryptocurrency investments. Journal of Social Research, 4(1), 1-15.

money to scams or exchange failures find that the law has very little to offer them. And as DeFi, stablecoins, and privacy coins continue to grow, the gap between what the law covers and what actually exists in the market keeps widening.

The comparison with the United States and the European Union is sobering. Neither system is perfect, but both reflect something India has struggled to demonstrate the willingness to sit down and make clear legislative decisions about crypto rather than managing it through improvisation. MiCA, in particular, shows what it looks like when a jurisdiction actually commits to governing this space properly.

India needs to make that commitment too. A dedicated cryptocurrency law one that defines assets clearly, assigns regulatory authority cleanly, protects consumers meaningfully, and enables real cross-border cooperation is not a luxury at this point. It is overdue. And it needs to be built with enough flexibility to grow alongside the technology, because this field will not wait for the law to catch up.

Where Research Should Go Next

This study has tried to give an honest account of where India stands today what exists, what is missing, and what the consequences of that gap are. But several questions remain open, and they deserve serious attention from researchers willing to take this work further.

The most pressing is empirical. The 2023 PMLA amendments gave enforcement agencies new tools, but nobody has yet properly examined whether those tools are being used. How many investigations have followed? How many prosecutions? Are crypto businesses actually complying, or just going through the motions? These are questions that matter enormously and that existing scholarship has not answered.

DeFi is another frontier that Indian legal scholarship has largely ignored. Because decentralized platforms have no central operator, the entire logic of "reporting entity" compliance breaks down. How the law should reach these platforms or whether it can at all under the current framework is an urgent and genuinely difficult question.

A wider comparative study would also be valuable. This research focused on the US and EU, but Singapore, Japan, and the UAE have each developed their own distinct approaches to crypto regulation, and given India's regional ties, their experiences may offer more directly transferable lessons.

The privacy dimension of KYC compliance also deserves closer study. Crypto exchanges collect significant amounts of personal financial data, and with India's data protection law still finding its feet, the question of how that data is governed sits uncomfortably between two regulatory frameworks that have not yet been properly reconciled.

And finally, the arrival of the Digital Rupee raises questions that will become unavoidable about how a state-backed digital currency and private cryptocurrencies can coexist, and whether the regulatory playing field between them is fair or distorted.

The work this research has started is far from finished. If anything, the most interesting and consequential questions are still ahead and the researchers who take them on will find the terrain both challenging and genuinely important.