INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 3 [June, 2026] | Page 210 – 221

CRYPTOCURRENCY-ENABLED FINANCIAL FRAUDS IN INDIA: CHALLENGES FOR INVESTIGATION AND PROSECUTION UNDER EXISTING CYBER LAWS

- Deepanshi Choudhary[1]

ABSTRACT

Over the last few decades, the financial systems in India have shifted from a cash-based economy to a digitised economy as cryptocurrencies have gained popularity ever more rapidly. This 'digital revolution' has provided different avenues of criminality for scammers to deceive unwary customers. In the present article, the author critically analyses the different types of cryptocurrency-enabled financial crimes in India, problems that authorities and regulators face in investigations and prosecutions under existing laws, and possible lacunas under the existing law that impact the prosecution. It discusses whether the IT (2000), the BN (2023), and the PMLA (2002) are applicable to these offences and certain key lacunas for evidence, jurisdiction, and recovery of assets. The article discusses how regulations have evolved from the Reserve Bank of India's (RBI) 2018 ban on banking services being the first step, the Supreme Court's decision in ***Internet and Mobile Association of India v Reserve Bank of India***, and the introduction of PMLA obligations on Virtual Digital Asset Service Providers, for example. Because of the intricacies of blockchain, the current legal structure for prosecuting blockchain-related fraud is not only insufficient but also very disjointed. Among other things, the paper argues that a separate Cryptocurrency and Virtual Digital Asset Regulation Act should be brought in, a Specialised Cryptocurrency Investigation Team should be established, and there should be better compliance with FATF standards including the Travel Rule. A regulatory setup which enables digital innovation and, at the same time, holds users accountable will lead to constitutional validity and also economically safeguard the increasing number of retail investors.

[1] LL.M., Cybersecurity & Digital Laws, UPES Dehradun

Keywords: *Cryptocurrency frauds, Cybercrime, Blockchain technology, Indian cyber laws, Digital evidence, Financial fraud.*

ABOUT THE AUTHOR

Deepanshi Choudhary is currently pursuing her LL.M. in Cybersecurity and Digital Laws from the School of Law, University of Petroleum and Energy Studies (UPES), Dehradun. She holds a BBA LL.B. (Hons.) with a specialisation in Criminal Laws. Her academic interests lie at the intersection of technology law, cybercrime, and digital governance, with a particular focus on the regulatory challenges posed by emerging financial technologies in the Indian legal landscape.

I. INTRODUCTION

Bitcoin is the world's first digital currency without a Central Bank or a Government. It is also the first application of the concept of decentralised ledgers, which was first described by Satoshi Nakamoto in 2008. A blockchain is a distributed ledger that is immutable and cryptographically secure. It allows users to exchange value directly without the need for an intermediary. This development has led to a fundamental change in the functioning of the traditional financial system. In India, the cryptocurrency industry has experienced a considerable surge in popularity owing to the extensive use of smartphones, the rising inclination towards digital payment methods, as well as the keen interest of millennials and novice investors who are in search of high ROI.[2]

The very features that give crypto its charm, such as decentralization pseudonymity irreversibility of transactions, and global reach, are also the main factors that have led to the rise of cryptocurrencies as a vehicle for financial crime. Only in India, there are increasing reports of various types of crypto frauds, which include Ponzi schemes with promises of very high returns, phishing techniques aimed at cryptocurrency wallet credentials, Bitcoin payment for ransomware, and fake exchange platforms that run away with investor funds worth millions. Most of the time, these frauds are committed against first-time or inexperienced investors who do not have enough understanding of blockchain technology and the risks involved.

[2] Reserve Bank of India, 'Annual Report 2022-23: Digital Payments' (RBI 2023) <https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx>.

Challenges related to the investigation and prosecution of these offenses are major. The existing legal system in India, which is mainly designed for a non-blockchain setting, falls short when it comes to addressing such criminal activities effectively. This paper looks at the present status of crypto-related crimes in India. It works out if the current laws are sufficient in preventing possible frauds. It also highlights the loopholes in the investigation and prosecution by the authorities. Finally, it presents detailed proposals for changes.

II. ANATOMY OF CRYPTOCURRENCY FRAUD IN INDIA

Cryptocurrency frauds in India take several distinct but often overlapping forms, each exploiting a different dimension of blockchain's structural design.

A. INVESTMENT AND PONZI SCHEMES

Using referral-based Ponzi schemes, fraudsters trick victims with ridiculous promises of getting guaranteed returns, they pay the earlier investors by taking money from the later ones. A big fraud example is that of Amit Bhardwaj's Gain Bitcoin, which led to losses of more than 2,000 crores, and Morris Coin, which was a multi-state fraud. Since crypto transactions cannot be reversed, victims have no way to recover the money that was transferred. Schemes like these will always leave you empty handed financially, most in particular those investors who lack experience in investing in digital assets.

B. PHISHING ATTACKS AND WALLET THEFT

Cybercriminals acquire private keys, seed phrases, and login credentials via fake websites, impersonation schemes, and social engineering.[3] As soon as an intruder gets hold of a private key, they can have absolute and permanent access to the victim's crypto wallet. Unlike traditional bank cards, cryptocurrency wallets don't have chargeback or fraud departments, so losses will be permanent. Tracing a thief will be a very tough, if not impossible, task without blockchain analysis tools as pseudonymous wallet addresses don't reveal any information about the wallet owner.

C. RANSOMWARE ATTACKS

Cybercriminals use encryption methods to block people's devices and then ask for a ransom - usually in digital currency - to give them back the access. The feature of digital asset transactions which is

[3] CERT-In, 'Annual Report 2022' (Ministry of Electronics and Information Technology 2022) <https://www.cert-in.org.in>.

anonymous and without borders makes it really hard for the police to find the bad guys and get the stolen money back. In India, there has been a rise in number of ransomware attacks targeting private companies and government agencies including healthcare industry and critical infrastructure.

D. FAKE CRYPTOCURRENCY EXCHANGES

Fake platforms simulate real trading exchanges using slick interfaces, fake trading records, and altered price charts. Such scammers get investors' money, display fake returns to lure more deposits, and perform an 'exit scam' by running away with the whole deposited amount. Since these platforms usually function in overseas jurisdictions with anonymous registration information, it is very hard to find their operators.

E. DARK-WEB TRANSACTIONS

Digital currencies are the dominant form in the payment for trafficking in drugs, malware distribution, stolen identities, and forgeries at the highest level of criminal organization. Recently, there has been an increase in Enforcement Directorate probes linking cryptocurrency wallets to drug trafficking and the illicit hawala banking system in India.

F. COMPARATIVE OVERVIEW OF FRAUD TYPES

Fraud Type	**Mechanism**	**Key Challenge for Law Enforcement**
Ponzi / Investment Schemes	Referral-based returns funded by later investors; promises of unrealistic gains	Transaction irreversibility; cross-border operators
Phishing / Wallet Theft	Fake websites, social engineering to extract private keys	Pseudonymous wallets; no identity linkage
Ransomware	Encrypts victim devices; demands crypto payment for decryption	Anonymity of recipients; servers in foreign jurisdictions
Fake Exchanges	Simulated trading interfaces; exit scam upon sufficient deposits	Foreign registration; absence of Indian licensing regime

Fraud Type	Mechanism	Key Challenge for Law Enforcement
Dark Web Transactions	Crypto payments for illegal goods and services	Privacy coins; mixing services break transaction trail

The psychological aspect of scams with cryptocurrencies should not be left out. The very thing that makes blockchain technology obscure and complicated also lead to an information imbalance so that the fraudsters, who have better knowledge, can take advantage of the victims, who are not that knowledgeable. Because of Truth is a blockchain can be used both in a legitimate way and be a source of a dishonest exploitation, the fraudsters get to wear a mask of believability that even the victims who have more education and are financially sophisticated, are hardly able to find out.

III. THE EXISTING LEGAL FRAMEWORK: APPLICABILITY AND LIMITATIONS

At present, India's reaction to crypto currency fraud is dependent on a combination of laws that were initially not written with blockchain technology in mind.

A. THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act outlines the primary cyber law framework. Relevant provisions include Section 43 (Unauthorised access to a computer), Section 66 (Dishonestly receiving any data), Section 66C (Identity Theft), and Section 66D (Cheating by impersonation using computer resources).[4] These rules may be relevant in cases of phishing, wallet theft, or counterfeit exchanges but the Information Technology Act was drafted with a centralised internet in mind and does not account for decentralised blockchain networks, smart contracts, or cryptographic wallet structures. There is ongoing legal uncertainty regarding whether the definition of 'computer resource' under Section 2(k) of the IT Act extends to a node connected to a decentralised blockchain operating simultaneously across thousands of jurisdictions. Creative judicial interpretation may be required, though such interpretations may not withstand prosecutorial scrutiny.

[4] Information Technology Act 2000, s 43 (Unauthorised access); s 66 (Data theft); s 66C (Identity Theft); s 66D (Cheating by impersonation).

B. THE BHARATIYA NYAYA SANHITA (BNS), 2023

The BNS includes provisions addressing Section 318 (Cheating), Section 316 (Criminal Breach of Trust), Section 336 (Forgery), Section 61 (Criminal Conspiracy), and Section 111 (Organised Crime), all of which could apply to Ponzi schemes and fake investment platforms.[5] The BNS is a major change to the criminal laws of the country as it completely overhauls the Indian Penal Code of 1860. Yet, similar to the IT Act, the BNS has not introduced any direct clauses for cryptocurrencies. As the blockchain has a distinct nature, using only regular fraud clauses may not work, mainly since issues like different jurisdiction, ownership, and cause remain very blurry and it is still a huge problem to decide the place of a court for a case. This is even more difficult when a victim perpetrator exchange and server are all in different countries.

C. THE PREVENTION OF MONEY LAUNDERING ACT (PMLA), 2002

Among the major laws related to the regulation of cryptocurrencies, one is the PMLA 2002. In fact, the Ministry of Finance's 2023 notification, which widened the scope of the act by including virtual digital asset service providers (VDASPs) as 'reporting entities' who need to carry out KYC, has been the main focus area. Cryptocurrency exchanges, wallet providers, and brokers are, that means, required to keep an eye on customers and report suspicious transactions to FIU-IND. This is a major step forward; yet, the actual influence is rather limited because of the huge number of decentralized platforms and peer-to-peer (P2P) trades that are not done through registered exchanges and so, are beyond the PMLA's reporting authority. Decentralized Finance (DeFi) protocols that allow transactions through self-executing smart contracts without any human intermediary lead to a major regulatory loophole in the PMLA's entity-based reporting system.

IV. INVESTIGATIVE AND EVIDENTIARY CHALLENGES

Even if there are applicable legal provisions, prosecuting cryptocurrency fraud cases successfully is an exceedingly technical task that India's law enforcement agencies are very poorly equipped for at the moment. There are four challenges in particular that are very significant.

[5] Bharatiya Nyaya Sanhita 2023, s 318 (Cheating); s 316 (Criminal Breach of Trust); s 336 (Forgery); s 61 (Criminal Conspiracy); s 111 (Organised Crime).

A. TRANSACTION TRACING

Publicly accessible are blockchain ledgers; Even so, it is highly difficult to identify the individuals behind wallet addresses. To disguise the source of funds, criminals utilize mixing services that combine and redistribute cryptocurrency, or they carry out cross-chain transfers which disrupt the transaction trail. Monero and other privacy coins use ring signatures and stealth addresses, making the transactions almost untraceable. Conducting blockchain analysis is a complex task that demands specialised skill sets and expensive licensing arrangements, which most cyber cells in India do not have. Besides the Central Bureau of Investigation, the Enforcement Directorate is also creating in-house blockchain forensics capabilities. Though, they cannot yet handle many crypto fraud cases at the state level technically.

B. JURISDICTIONAL COMPLEXITY

Cryptocurrency fraudsters are making more use of platform exchanges registered in a foreign country, servers distributed over different countries, and also involve victims and criminal groups operating in different legal systems. India through its reliance on Mutual Legal Assistance Treaties (MLATs) and bilateral cooperative agreements generally experience delays, inconsistency and at times it is even impossible to execute the obtained requests Mostly when dealing with the jurisdictions like Seychelles, Malta, and the British Virgin Islands which have very minimal disclosure obligations. Getting subscriber information or transaction records from these exchanges through the MLATs can probably take months or years - during which time the money is moved over and over again.

C. EVIDENTIARY ADMISSIBILITY

The Supreme Court in ***Anvar PV v PK Basheer***[6] and ***Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal***[7] established that a secondary electronic record can only be admitted into evidence if accompanied by a valid and duly executed Section 65B Certificate under the Indian Evidence Act.[8] The issue is that because blockchain operates on a decentralised and distributed basis, a single 'responsible person in charge of the computer system' who can issue the necessary Section 65B Certificate for a particular blockchain transaction record does not exist. In fact, the courts have

[6] ***Anvar PV v PK Basheer*** [2014] 10 SCC 473 <https://indiankanoon.org/doc/138898625/>.

[7] ***Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*** [2020] 7 SCC 1 <https://indiankanoon.org/doc/53422855/>.

[8] Indian Evidence Act 1872, s 65B (Admissibility of electronic records).

not clarified yet the question of who can be authorised to issue such a certificate, this way creating a major evidential problem for cases of cryptocurrency fraud.

D. ASSET RECOVERY

Cryptocurrency transactions are programmed to be final with no one able to change them. Sending money through various wallets - and even more so if the money is changed into privacy coins or sent abroad - makes the recovery of lost money a real challenge. At present, there is no law in India that gives power to the authorities to properly seize freeze evaluate, or return the stolen digital assets. Enforcement Directorate tried to make provisional attachments under the PMLA, but the legal foundation is still disputed and there has not been any appellate court ruling on this issue. Lack of a legal procedure for holding, valuing, and disposing of seized cryptocurrency - added to the extremely fluctuating crypto market values - results in both legal and practical difficulties which the present asset recovery systems were not even meant to handle.

V. THE REGULATORY LANDSCAPE: PROGRESS AND GAPS

The Supreme Court invalidated the Reserve Bank of India's 2018 prohibition on banking services to cryptocurrency businesses in ***Internet and Mobile Association of India v Reserve Bank of India***[9], ruling such prohibition constitutionally impermissible. Rather than banning virtual currencies outright, the government instituted a taxation scheme imposing a flat 30% tax on capital gains from virtual digital asset transfers and a 1% TDS on transfers under Section 194S of the Income Tax Act.[10] While these measures were intended to establish a de facto regulatory framework, they do not address the entire problem of cryptocurrency-enabled fraud.

On a global scale the Financial Action Task Force (FATF) has produced very detailed guidelines for Virtual Asset Service Providers, one of which is the Travel Rule stipulated in FATF Recommendation 16 that takes exchanges to share the sender and recipient information for transactions above a certain threshold.[11] India's regulatory structure at the domestic level still lags behind on these international

[9] ***Internet and Mobile Association of India v Reserve Bank of India*** [2020] SCC Online SC 275 <https://indiankanoon.org/doc/1333412/>.

[10] Income Tax Act 1961, s 115BBH (tax on VDA gains) and s 194S (TDS on VDA transfers), as inserted by Finance Act 2022.

[11] FATF, 'Recommendation 16: Wire Transfers (Travel Rule)' in FATF Recommendations (FATF 2012, updated 2022) <https://www.fatf-gafi.org/en/topics/fatf-recommendations.html>.

standards. For instance, the lack of a licensing system for cryptocurrency exchanges in India - as in Japan, Singapore, and the European Union - has left Indian users without a trustworthy means to distinguish between compliant and non-compliant exchanges.

The Reserve Bank of India and SEBI have shown their interest in cryptocurrency regulation, thereby causing a jurisdictional conflict that is still unresolved. The lack of a clear regulatory setup has become a part of the fraud environment platforms run without definite compliance requirements, and individuals who get cheated have no official way of getting a remedy. Besides that, the heavy taxation has driven some of the retail trading volume to unregulated foreign exchanges where Indian investors neither have PMLA protection nor legal recourse.

A. REGULATORY TIMELINE

Year	Development
2018	RBI circular prohibiting banking services to crypto businesses
2020	Supreme Court strikes down RBI ban in IAMAI v RBI [2020] SCC Online SC 275
2022	Finance Act: 30% tax on VDA capital gains; 1% TDS under s 194S of Income Tax Act
2023	Ministry of Finance Notification: VDASPs brought under PMLA as reporting entities
Ongoing	SEBI and RBI indicate interest in crypto oversight; jurisdictional mandate unresolved

VI. RECOMMENDATIONS

To fill the gaps in India's cryptocurrency fraud governance, a collaborative effort has to be legislated, institutionalized, and even internationalized.

A. LEGISLATIVE REFORM

India needs an exclusive Cryptocurrency and Virtual Digital Assets Regulation Act that (i) gives definition of digital assets, digital wallets, digital asset exchanges, and smart contracts in a language that is legally unambiguous; (ii) sets up a compulsory licensing system for all types of digital currency

exchanges and wallet providers, with the licensing requirements including fit-and-proper criteria similar to those under the Payment Systems Act 2007; (iii) works out legal provisions for confiscation freezing valuation, and repatriation of stolen crypto assets resulting from crimes; and (iv) determines through what evidence standards blockchain-based records are to be considered, thereby resolving the Section 65B certification issue for decentralised distributed ledger data. The current modus operandi of using IT Act and BNS against blockchain crimes is both legally shaky and practically unfeasible.

B. INSTITUTIONAL CAPACITY BUILDING

Within the state and central cybercrime departments, specialised cryptocurrency investigation units must be established. These units should comprise blockchain analysts, cyber-forensic investigators, and prosecutors who specialize in digital asset law. This will also necessitate the building of blockchain analytics facilities akin to that of the US Department of Justice's National Cryptocurrency Enforcement Team (NCET)[12] and European Cybercrime Centre (EC3) of Europol is indispensable. Education plans for judges and magistrates on how blockchain proofs be evidence will also lead to a massive rise in the effectiveness of cases.

C. INTERNATIONAL COOPERATION

India's MLAT structures should be enhanced specifically for cryptocurrency cases, including fast-tracking procedures for requests involving digital asset exchanges. Domestic VASP regulations should be fully aligned with FATF standards, including full implementation of the Travel Rule.[13] India may wish to explore the possibility of bilateral data-sharing agreements with the countries that house the leading crypto exchanges. By being part of the FATF meetings and hosting the G20 summit, India had excellent opportunities to shape the global regulatory structure for digital assets. It is high time these efforts were reflected in actual regulatory changes at home.

[12] US Department of Justice, 'National Cryptocurrency Enforcement Team (NCET)' <https://www.justice.gov/criminal/criminal-ccips>.

D. SUMMARY OF RECOMMENDATIONS

Area	Recommendation	Global Precedent
Legislation	Dedicated Cryptocurrency & VDA Regulation Act with licensing, evidence, and asset recovery provisions	EU MiCA Regulation; Singapore MAS Framework
Institutions	Specialised Crypto Investigation Units at state and central level with blockchain forensic capability	US DOJ NCET; Europol EC3
Evidence	Statutory clarification of s 65B certification requirements for decentralised blockchain records	UK Police, Crime, Sentencing and Courts Act (proposed reform)
International	Full FATF alignment including Travel Rule; enhanced MLATs for crypto cases	FATF Recommendation 16; G20 Digital Asset Framework

VII. CONCLUSION

The technology behind cryptocurrencies isn't intrinsically good or bad it's a potent financial infrastructure and how the law deals with it will decide if it serves honest purposes or becomes a refuge for deceits. At present, India's cyber laws are merely a patchwork and a makeshift response to crimes facilitated by crypto-assets. The Information Technology Act, the Bharatiya Nyaya Sanhita, and the PMLA collectively provide the means for prosecution, but they were not designed for decentralized blockchain systems and leave large loopholes in transaction tracking, evidence admissibility, jurisdictional reach, and asset recovery.

The rise in India's desire to adopt cryptocurrencies has also in parallel led to an increase in scams related to this area. This calls for an appropriate legislative measure with a major reliance on technology. In fact, a specific statute, skilled investigatory authorities and robust international collaboration should not be merely aspirations but the key pillars of effective governance. It is the fraudulent investor in a typical retail setting who through the system must be reached, tracked and

compensated. A major issue is whether the Indian legal system can be transformed quickly enough to protect people who live in a financial environment which is far from the examples that the law has laid down till now. A legal setup which promotes a digital revolution First and at the same time ensures real accountability is not only necessary looking at the constitution but also beneficial from the economic perspective.