ARTICLE

FROM DECEPTION TO DISAPPEARANCE: THE CRIMINAL ECOSYSTEM OF CRYPTOCURRENCY INVESTMENT FRAUD, MONEY LAUNDERING AND ASSET RECOVERY

Ankan Rudra[*] & Sneha Kundu[**]

Abstract

The rapid growth of cryptocurrency has introduced new opportunities within the digital financial ecosystem while simultaneously creating major problems such as investment fraud, money laundering and concealment of criminal proceeds. This paper examines the criminal ecosystem of cryptocurrency fraud, focusing on methods through which fraudulent proceeds are transferred, concealed and potentially converted into legitimate financial assets. This paper further analyses India's legal and regulatory response, particularly the application of existing laws and subsequent inclusion of specified virtual digital asset activities with the amendment of Prevention of Money Laundering Act, 2002, in 2023. It also examines the challenges faced by investigative authorities in tracing transactions, securing digital assets and ensuring asset recovery and compensation to victims. The study evaluated existing loopholes in the legal framework and proposed recommendations on how a dedicated comprehensive framework is needed to address the evolving nature of cryptocurrency related financial crime and ensure effective protection of investors.

Keywords – Cryptocurrency investment, fraud, Money laundering, Asset recovery, Prevention of Money Laundering Act (PMLA), Blockchain technology.

I. INTRODUCTION

In the modern world, there has been a rapid development in the Blockchain technology and the growing use of cryptocurrencies which have transformed the way financial transactions are conducted across digital platforms. Transfer and storage of digital assets virtually has created new opportunities for investment, financial innovation and international transactions without necessarily relying on traditional financial intermediaries. With opportunities, these developments have also made a wide space for fraudulent investment schemes, cyber enabled financial crime and movement of illicit proceeds across digital and geographical boundaries. The central point of concern is not just

[*] 5th Year, BBA LLB (H.) Student, Amity University, Kolkata.
[**] 5th Year, BBA LLB (H.) Student, Amity University, Kolkata.

cryptocurrency but the manner in which its technological features and cross border nature of digital transactions may be exploited by offenders for criminal purposes.

Cryptocurrency investment fraud commonly involves deceptive schemes used by the scammers which helps them to trick victims into sending cryptocurrencies under false promises of high returns or investment opportunities, then vanish with the funds. These scams mostly use fake websites, platforms, impersonation or manipulative techniques to lure and defraud victims. These frauds include various methods such as Ponzi schemes, romance scams, phishing scams and many more types of scams which induce victims to transfer money or digital assets as they are persuaded by promises of usually high returns and misleading claims regarding investment performance or legitimacy of an online platform. In certain schemes, at the initial level some investors are paid using funds collected from subsequent participants to create a rapport or false impression of profitability until the arrangements become unsustainable. Then once such substantial funds are collected, the scammers tend to discontinue operations or restrict withdrawals, leaving the victims with little to no room for recovery.

The problems extend beyond the initial act of deception. The money or digital assets generated through these fraudulent schemes are generally transferred between crypto currency wallets, exchanged for other digital assets across numerous geographical locations, mixing or tumbling of services, technological features increasing anonymity or converted into conventional currency. This is generally done with intention to conceal the origin or ownership.[1] However, mere usage of multiple wallets or cross border transfers does not itself indicate or establish money laundering or criminal liability but in order to establish the criminal intent, it is required evidence that proves the connection of transactions. Although blockchain records may provide traceable records of transactions by identifying individuals who have control to particular wallet addresses presenting substantial investigative challenges.

In the Indian context, these concerns intersect with the legal frameworks that govern cheating, cybercrime, money laundering and preservation of digital evidence. The Prevention of Money Laundering Act of 2002 (PMLA) provides a statutory framework for addressing money laundering and dealing with property connected to criminal proceeds. In March 2023, an important regulatory development took place where the scope of the PMLA framework was widened through an amendment by the Ministry of Finance to include specified activities involving virtual digital assets. Key additions involved reporting records on the DARPAN portal and maintaining such records for

[1] FATF, "*Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*" (September, 2020)

5 years after business relationship between client and reporting agency has ended and collection of details of registered offices addresses and principal place of business of their clients. This increased compliance obligations of relevant non profit organisations (NPO's) with strict reporting and recordkeeping of records, strengthening the regulatory basis for financial intelligence and investigation.[2] Nevertheless, the mere existence of statutory powers does not automatically help in timely identification of offenders, proper preservation of assets or compensation and justice to affected investors.

II. THE CRIMINAL ECOSYSTEM: FROM DECEPTION TO DISAPPEARANCE

a. NATURE AND FORMS OF CRYPTOCURRENCY INVESTMENT FRAUD

The rapid evolving nature of the cryptocurrency market has created a hyper sensitive environment that is increasingly vulnerable to financial exploitation and investment related fraud. Cryptocurrency transactions are majorly conducted through digital platforms and blockchain networks, where pseudonymous participation, cross border transfers and irreversible nature of transactions makes it complex and poses a challenge on regulatory supervision and the recovery of illicitly obtained funds. The fraudulent measures used by perpetrators to obtain digital assets unlawfully involve several forms, including Ponzi Schemes, fraudulent investment platforms, pump and dump schemes and fake Initial Coin Offerings (ICOs). In Ponzi schemes, certain returns are initially promised to the investors in order to gain investor confidence and trust by pooling funds from subsequent participants to create artificial profitability appearance and after some time, restricts the withdrawals and vanishes with the money. Pump and Dump schemes involve inflating the market value of a cryptocurrency artificially through ways like misleading promotional campaigns and coordinated online activity, following which the perpetrators sell their holdings at inflated prices, leaving other investors with grief of losses. ICOs involve such types of offerings that lure individuals to invest in fictitious projects through exaggerated and misleading claims regarding future prospects of profitability. Apart from direct investment deception, scammers also use methods of impersonation, phishing attacks and malicious softwares to obtain private keys, confidential credentials and other sensitive information giving unauthorised access to investor's digital assets. Fraudsters generally tend to exploit and manipulate individuals by posing themselves as cryptocurrency exchange

[2] Ministry of Finance amended PMLA: Tightens NPO reporting norms, Beneficial Ownership Rules, India, *available at:* https://affairscloud.com/ministry-of-finance-amended-pmla-tightens-npo-reporting-norms-beneficial-ownership-rules/ (last visited on October 30, 2026)

representatives, financial advisors or influential industrial figures. With the help of psychological tactics such as urgency, fear and promises of exclusive investment opportunities facilitates the individuals in disclosure of sensitive information. This interconnected nature of methods shows that cryptocurrency investment fraud is not only limited to conventional financial deception but also market manipulation, fraudulent massive fundraising, impersonation and technological exploitation thus collectively evolving or working as a criminal ecosystem in which digital assets are illicitly acquired and transferred across multiple wallets and further concealed through complex networks and routes to hide their identities, making it close to impossible to track them.[3]

b. CROSS BORDER TRANSACTIONS AND JURISDICTIONAL CHALLENGES

The cross border nature of cryptocurrency poses significant challenges in the investigations and prosecution of cryptocurrency investment frauds. Unlike conventional financial transactions which may be often traced through identifiable banking institutions operating within established jurisdiction, cryptocurrency transactions can involve participants, platforms and service providers that can be located across several countries. This geographical separation makes it really difficult for investigative authorities to determine the location of offenders, identify the appropriate jurisdiction for investigation and exercise effective control over the movement of fraudulent proceeds.

A major difficulty arises from the different regulatory frameworks that govern virtual digital assets across countries. Some differences include some countries introducing registration and reporting requirements for virtual asset service providers, whereas some countries limit regulatory supervision or lack adequate enforcement mechanisms. Fraudsters tend to exploit these differences by operating through offshore platforms or service providers that are not effectively supervised in countries where the victim resides, thus taking advantage of the loophole present. The absence of a clear physical presence complicates the process of determining the appropriate jurisdiction which is needed to obtain information and initiate enforcement action.[4]

Another obstacle is the collection of digital evidence. Investigative authorities require access to customer identification records, transaction statements and any relevant information which are maintained by foreign cryptocurrency service providers, for which they may require cooperation from appropriate authorities in the jurisdiction where the service provider operates. Mutual Legal

[3] Sufiyan Asad and Faisal Zaheer, *Digital Asset Scams and Cryptocurrency Fraud: Investigating the tactics of convicted fraudsters* (ResearchGate, March 2025)

[4] FATF, "*Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers*" (March, 2026)

Assistance Treaties (MLATs) and other international cooperation mechanisms help in facilitating the exchange of evidence and assistance in criminal investigations. Formal procedures involve more time and administrative procedures, delaying the investigations in which the digital assets can be transferred across borders in a short span of time. The problem becomes serious when authorities attempt to freeze or recover assets outside their territorial jurisdiction. Sometimes investigative authorities become successful in identifying the movement of fraudulent cryptocurrency, securing those assets requires coordination with foreign law enforcement agencies, financial intelligence units and relevant service providers. Differences in domestic laws relating to freezing, seizure and confiscation of properties further complicates the efforts. Consequently, the identification of fraudulent proceeds in one country does not automatically vests the authorities with the powers that are needed to recover those assets in another jurisdiction.[5]

These challenges demonstrate that these frauds cannot be effectively addressed through isolated domestic enforcement measures. Timely information sharing, proper identification of transaction addresses, coordination among law enforcement agencies and consistent regulatory standards are essential to address the international movement of illicit proceeds. The Financial Action Task Force (FATF) has consistently emphasized the importance of international cooperation and effective supervision of digital asset service providers, keeping in mind the loopholes associated with the offshore operations. Ultimately, the effectiveness of investigations depends heavily upon the capacity of various jurisdictions to cooperate in identifying offenders, securing evidence and recovering criminal assets.

c. CHALLENGES IN INVESTIGATION, PROSECUTION AND ASSET RECOVERY

One of the most significant challenges that is associated with cryptocurrency investment fraud is firstly the identification of suspicious transactions and secondly turning that identification into successful criminal investigation followed by prosecution. Even though blockchain technology maintains transaction records, it does not necessarily mean that the records will establish the identity of individuals that are responsible for the malicious transactions. Wallet addresses generally operate through pseudonymous identifiers which makes it difficult to directly associate a particular transaction with an identifiable person. Thus it requires additional evidence including electronic communications, device information, financial records and customer identification records to establish any connection between the transactions and the individuals involved.

[5] FATF, "*Countering Ransomware Financing*" (March 2023)

The process of establishing criminal liability poses further difficulties. The investigative authorities need to demonstrate all the relevant transactions that are connected with the alleged fraud and must satisfy the essential elements constituting the crime. Mere demonstration of moving of cryptocurrency across multiple wallets or accounts is not enough. Establishment of the dishonest intention, identifying beneficiaries of the proceeds and demonstration of connection between accused and transactions requires extensive investigation. Collection, preservation and admissibility of electronic evidence is specifically very important as incomplete records or difficulties may affect the authenticity of digital material.[6]

Another complicated process is the recovery of assets, even in situations where fraudulent proceeds have been successfully traced. In circumstances where the cryptocurrencies are transferred to other wallets or converted to other digital assets, identifying the location or movement of assets does not automatically ensure whether they can be frozen or secured. However, this process may require timely intervention, cooperation from relevant service providers, where assets are located and assistance from foreign authorities. Delays in this process reduces the possibility of preserving assets for further confiscation or restitution.[7]

The distinction between confiscation of criminal proceeds and compensation of affected investors is a very important aspect during the investigation as the attachment or confiscation of property under applicable legal provisions does not necessarily mean that the victims will be compensated immediately. Authorities need to first establish the legal connection between the property and alleged office, complete relevant proceedings and procedures for distribution or restoration of assets. Where the cryptocurrencies are transferred into multiple wallets, transferred or in any other means which cannot be readily recovered, victims generally face substantial difficulties in obtaining compensation even after an investigation has been commenced. Therefore, cryptocurrency investment fraud presents challenges at several interconnected stages beginning from identification of suspicious accounts to eventually recovery of assets. The measurement of enforcement cannot be solely measured by the ability to trace cryptocurrency transactions but it must also be assessed by the capacity of relevant authorities, cooperation and combination of numerous mechanisms and authorities and provide meaningful remedies to affected investors.

[6] FATF, *"Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing"* (September 2020)
[7] FATF, *"Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Providers"* (October 2021)

III. INDIA'S REGULATORY LANDSCAPE EVOLUTION GOVERNING CRYPTO SECTOR

a. INDIA'S LEGAL POSITION AND ENFORCEMENT APPROACH PRIOR TO AMENDMENT

The regulatory landscape that revolves around the cryptocurrency sector has experienced a rapid growth in recent times. With the inclusion of cryptocurrencies in the Anti-Money Laundering Act in March 2023, a major step was taken by the government towards their commitment to addressing potential risks promoting the responsible use of digital assets. It included crypto exchanges, NFT marketplaces and custody service wallet providers legal accountability for monitoring and reporting of any suspicious financial activities.[8] Prior to March 2023, India did not have a specific anti money laundering compliance framework governing cryptocurrency exchanges and other virtual digital asset service providers. Prior to March 2023, India did not have a specific anti-money laundering compliance framework governing cryptocurrency exchanges and other virtual digital asset service providers but this does not mean that cryptocurrency related frauds existed outside the reach of the Indian criminal system. There were existing provisions relating to cheating, criminal breach of trust, criminal conspiracy and offences involving computer systems which could be invoked by investors who faced inducement to transfer money or cryptocurrency through false or exaggerated promises. Consequently, Investigations depended largely upon the conventional criminal law framework even in situations where the alleged fraud involved sophisticated digital platforms and cryptocurrency transactions.

The regulatory position remained uncertain due to RBI's approach towards virtual currencies as in April 2018, the Reserve Bank of India directed regulated entities not to provide banking services that were dealing in virtual currencies. This was done due to rising concerns regarding consumer protection, market integrity and the potential for money laundering associated with the virtual currencies. It led to the famous case of *Internet and Mobile Association of India v. Reserve Bank of India (2020)*, where this action by RBI was challenged on the grounds of unjustness. The Supreme Court of India however upheld RBI's decision on grounds of consumer need for regulatory measures in the rapidly growing landscape of virtual currencies and it was needed to ensure financial stability and consumer protection.[9]

[8] Edul Patel, "How India Regulatory Landscape Is Evolving The Crypto Sector Across The Globe In 2023" *Abp LIVE*, July, 27, 2023

[9] Supreme Court upholds RBI's Circular on Virtual Currencies - Regulatory measures for Financial Stability. The RBI's prohibition on virtual currencies was deemed necessary for consumer protection and financial stability, India, *available at*: https://lawtext.in/judgement.php?bid=7089 (last visited on 1st November, 2026)

Following this judgement of the Supreme court of India, RBI clarified in May 2021 that banks could not rely on the invalidated circular in order to restrict cryptocurrency related transactions, while remaining obligated to comply with applicable KYC, AML and other regulatory requirements. The absence of specific reporting and monitoring systems for Virtual Digital Assets (VDAs) service providers genuinely created huge difficulties in systematic identification of suspicious transactions and tracing of proceeds. This regulatory gap led to the inclusion of specified VDA activities within the Prevention of Money Laundering Act framework in March 2023.

b. EVOLUTION OF INDIA'S CRYPTOCURRENCY REGULATORY FRAMEWORK SINCE 2023

7 March 2023 marked a significant date in India's approach towards cryptocurrency legislation, as the Ministry of Finance brought specified activities involving digital assets (VDAs) within the scope of the Prevention of Money Laundering Act, 2002 (PMLA) to enhance clarity and stringency of money laundering prevention efforts.. This amendment covered practical measures for identification and monitoring of suspicious activities by relevant service providers or reporting authorities which includes conduction of risk assessment to determine associated, Enhanced Due Diligence (EDD), screening against suspicion list, ongoing monitoring and training of reporting entities for them to understand suspicious activities and proper monitoring procedures.[10]

Following this notification, VDA service providers carrying out specified activities are required to register with the Financial Intelligence Unit - India, known as FIU-IND. They work under the department of Revenue as the national agency who is responsible for receiving, processing, analysing and disseminating information on suspicious financial information. They are obligated to comply with applicable obligations relating to customer verification, maintenance of records and reporting of suspicious transactions. This enabled financial intelligence authorities to obtain relevant information and strengthen monitoring of transactions that may be connected with money laundering or other criminal activities. However, an important point to be noted here is that, not every individual cryptocurrency holder or personal transactions are subjected to these reporting requirements, thus its application totally depends upon the nature of the activity, whether it is found to suspicious in nature or not and whether it is carried out in the course of business for on behalf of any other person.

[10] Prevention of Money Laundering (Maintenance of Records) Amendment Rules, India, *available at*: https://www.indiafilings.com/learn/prevention-of-money-laundering-maintenance-of-records-amendment-rules-2023 (last visited on 2nd November,2026)

The present legal framework reflects a broader enforcement approach. The FIU-IND is primarily responsible for receiving, analyzing and disseminating information on suspicious financial transactions. This intelligence is further investigated by the Enforcement Directorate (ED), which is an investigative and prosecuting agency. Both FIU-IND and ED work together to combat money laundering and related financial crimes in India. The requirements implemented to international service providers operating in the Indian market was further illustrated by FIU-IND's 2025 order concerning Coinbase, which addressed its reporting entity obligations under the PMLA. In September 2026, FIU-IND issued notifications to 15 virtual digital asset providers for failing to comply with the provisions of PMLA, 2002. The initiation of this action by the Director of FIU-IND under Section 13 of PMLA demonstrates efforts to address entities operating without adherence to India's anti-money laundering regulations.[11]

Despite these developments, India is yet to have a comprehensive standalone regulatory framework dedicated to every aspect of cryptocurrency activity. The present approach relies primarily on anti-money laundering requirements and existing criminal laws. Bringing specified VDA activities within the PMLA has strengthened supervision and financial monitoring but it does not by itself resolve the major concerns relating to investor protection, cross border enforcement and the recovery of assets lost through cryptocurrency investment fraud.

c. CASE SCENARIOS AND PRACTICAL ENFORCEMENT

The practical application of India's legal framework can be well understood with real life case scenarios involving investigations of cryptocurrency investment fraud. One well known and prominent example is the GainBitcoin case. It is considered to be India's biggest cryptocurrency investment fraud involving Ponzi Scheme. In this case, Bitcoin's early popularity was used to induce or lure individuals to invest in Bitcoin mining with promise of exaggerated or monthly fixed returns. The investigation revealed alleged use of multiple cryptocurrency wallets to conceal and transfer the proceeds and the participants used to receive incentives upon recruitment of others. Early payouts gained confidence and attracted investors across the country to reinvest. In December 2023, CBI as per direction by Supreme court conducted searches across several locations and arrested Darwin's Labs co-founder whom they found to be an aid behind this criminal proceed. The GainBitcoin case illustrated how cryptocurrency, referral marketing and guaranteed return promises can be used in an

[11] India sends notice to 15 illegal digital asset providers, India, *available at*: https://www.cnbctv18.com/india/financial-intelligence-unit-india-sends-notices-to-15-vda-sps-for-non-compliance-under-pmla-19987449.htm (last visited on 3rd November, 2026)

alleged Ponzi scheme.[12] It also demonstrated the difficulties involved in tracing cryptocurrency transactions, identifying the ones behind these criminal proceeds and asset recovery distributed across different jurisdictions.

Another example is the cryptocurrency investment and mining application fraud which is documented in India's Mutual Evaluation Report by the Financial Action Task Force (FATF) in 2024. Here, FIU-IND analysed information from state police authorities and identified the entities that were allegedly operating fraudulent investment applications. The intelligence provided was shared with law enforcement agencies which enabled CBI to register an FIR and conduct searches upon it. The Enforcement Directorate (ED) further filed a prosecution complaint against 299 individuals and entities, while approximately 86.5 Rs. Crores which were held in banks were frozen. This case demonstrated the importance of financial intelligence and coordination between FIU-IND, the CBI and ED in identification of suspicious entities and prevention of further movement of suspected proceeds.[13]

These investigations demonstrate that India has developed stronger mechanisms for identifying suspicious transactions, coordinating investigations and freezing digital assets that are connected with cryptocurrency related offences. Apart from these, the effectiveness of these measures also depends upon the actual recovery too. Identifying and freezing assets does not automatically result in confiscation or return of money back to the affected investors. Some huge obstacles and interruptions are also faced in this process including delays in investigation, difficulty in establishing ownership of digital assets, cross border cooperation and movement of assets through multiple wallets. Thus, although the existing framework has strengthened the enforcement response, effective asset recovery and timely compensation of investors still remains a significant challenge.

IV. REGULATORY GAPS AND RECOMMENDATIONS

a. EXISTING REGULATORY GAPS IN INDIA'S CRYPTOCURRENCY FRAMEWORK

Despite the major developments in the regulation in 2023, India's existing framework continues to face several limitations and challenges while addressing cryptocurrency investment fraud effectively. One of the primary concerns is the absence of a comprehensive regulatory framework dedicated solely to cryptocurrency activities. While specified virtual digital asset service providers

[12] How the GainBitcoin Scam Became India's Biggest Cryptocurrency Ponzi Scheme, India, *available at*: https://cryptonewsindia.com/cryptocurrency/how-the-gainbitcoin-scam-became-indias-biggest-cryptocurrency-ponzi-scheme/ (last visited on 4th November, 2026)

[13] FATF, "*India's measure to combat money laundering and terrorist financing*" (September 2024)

are brought within the PMLA framework, broader aspects such as exchange operations, consumer protection and grievance redressal remain inadequately addressed. The existing framework focuses mainly on monitoring financial transactions and identification of who is behind the criminal proceeds, rather than providing comprehensive protection to cryptocurrency investors.

The investigation and identification of individuals who are involved behind these cryptocurrency proceeds poses another hurdle. Even though blockchain technology helps in providing a record of transactions, identifying individuals behind control of particular wallet addresses is considerably a tougher job, especially when multiple wallets, non custodial services and foreign exchanges are involved. The limited availability of specialised technological advancement or expertise and blockchain investigation capabilities and complexities further complicates the process of tracing or movement of fraudulent proceeds.

Another challenge is the cross-border nature of transactions. Cryptocurrency platforms and intermediaries mostly operate from jurisdictions of countries that have weak tracing and enforcement systems or they transfer the fraudulently acquired cryptocurrencies to different wallets that are in jurisdictions having weak tracing capabilities or lack technological advancement that is needed to do such. Thus it makes it difficult for domestic authorities to obtain customer information, transaction records and other relevant evidence. Differences in regulatory standards and delays in international cooperation further obstructs investigations and prevention of assets located abroad.

Finally, a major limitation lies in the gap between identifying and freezing suspected proceeds and ensuring asset recovery of the investors affected. However, the freezing of assets does not necessarily result in confiscation or distribution in the way of compensation. Therefore, despite improvements in financial monitoring and enforcement, the framework which is existing presently, continues to face significant challenges in ensuring effective investigation, cross border cooperation and victim oriented asset recovery.

b. RECOMMENDATIONS FOR STRENGTHENING INDIA'S REGULATORY FRAMEWORK

First and foremost, to address the existing limitations, India should move towards a more comprehensive regulatory framework governing virtual digital assets. A dedicated legal framework should clearly classify different categories of cryptocurrency assets, prescribe requirements for licensing for exchanges, establish investor protection mechanisms, strengthen cybersecurity obligations, and define roles of IND-FIU, SEBI, RBI and other relevant authorities. Such legislation

would help in establishing a clearer standard for greater legal certainty while promoting responsible innovation and protecting the interests of investors and the financial system as a whole.[14]

There is a major need of dedicated regulatory authority for virtual digital assets in India or the designation of a specialised statutory regulatory authority with clearly defined supervisory powers. Presently, the regulatory responsibilities are distributed among different authorities with no single body who is exercising comprehensive oversight over the cryptocurrency sector, which creates a major gap. A dedicated regulator could supervise providers, establish licensing, set operational standards, monitor compliance, address grievances and coordinate with FIU and enforcement agencies. Such authority would help create a central mechanism for reporting suspicious activities and responding to fraudulent investment schemes.

There is also a need to strengthen the technological capabilities of investigating agencies. Specialised units equipped with blockchain analytics and digital forensic tools are needed to be developed to trace cryptocurrency transactions, identify suspicious wallet addresses and establish connections between digital assets and individuals involved in the crypto investment frauds. Regular training and coordination between the FIU-IND, ED, CBI and cybercrime authorities will help improve the effectiveness of investigations.

To address the cross border nature of cryptocurrency transactions, India should strengthen international cooperation through faster information sharing arrangements between financial intelligence units and law enforcement agencies. Better cooperation with foreign regulators and cryptocurrency exchanges facilitates access to transaction records, identification of suspicious accounts and preservation of assets located outside the jurisdiction of India. These measures will help reduce the possibility of offenders exploiting differences between nation regulatory systems.

Greater emphasis should be put on asset recovery and victim compensation. There must be a structured mechanism developed for the preservation, management and eventual distribution of recovered assets to legitimate and aggrieved victims, subject to applicable judicial procedure and competing claims which should not be heavily delayed. Timely freezing of suspicious assets, improvement in tracking systems and transparency while recovering assets would help in mitigating the risks associated with funds during transfer before legal action can be completed.

[14] Cryptocurrency Laws in India: Legal Status, Regulations and the Future of Digital Assets, India, *available at*: https://lawfullegal.in/cryptocurrency-laws-in-india-legal-status-regulations-and-the-future-of-digital-assets/ (last visited on 4th November, 2026)

Preventive measures should be formed as an essential and integral part of India's regulatory response. Government authorities and financial regulators should strengthen public awareness initiatives regarding fraudulent investment applications, unrealistic returns and impersonation schemes. Clearer investor advisories, accessible reporting mechanisms and cooperation with digital platforms could help individuals identify suspicious activities before suffering financial losses.

V. CONCLUSION

The growing use and appealing popularity of cryptocurrencies has created new opportunities within the financial sector while simultaneously introducing challenges relating to investment fraud, money laundering and recovery of assets. The decentralised and cross border nature of cryptocurrency has further made it complex and increasingly difficult for investigative authorities to identify offenders, trace fraudulent proceeds and secure assets before they are transferred or concealed to hide identities of the offenders. In India, the inclusion of specified virtual digital activities within the PMLA in 2023 marked an important and needed development helping in strengthening financial monitoring and regulatory oversight. However, as examined in this paper, the existing framework has kept on facing limitations and challenges concerning a dedicated comprehensive regulation, technological investigation, international cooperation and effective and fast recovery of victim's funds. The existence of legal provisions and enforcement powers alone cannot guarantee effective outcomes unless they are supported by timely implementation and institutional cooperation and coordination. In order to address these challenges, there is a need for a more comprehensive standalone legal approach including establishment of a dedicated regulatory authority for virtual digital assets, stronger investigative capabilities, improved international cooperation and effective mechanisms for asset recovery and investor protection. A great emphasis should also be placed on preventive measures and public awareness to reduce the vulnerability of individuals to fraudulent investigative schemes. Ultimately, the effectiveness of India's response to cryptocurrency investment fraud will depend upon the ability to adapt its legal and regulatory institutions to this evolving nature of digital financial crime. The objective should not merely be to investigate offences after financial loss but to also prevent fraudulent activities, preserve criminal proceeds and ensure that affected investors have a meaningful opportunity to obtain justice and recover their losses.