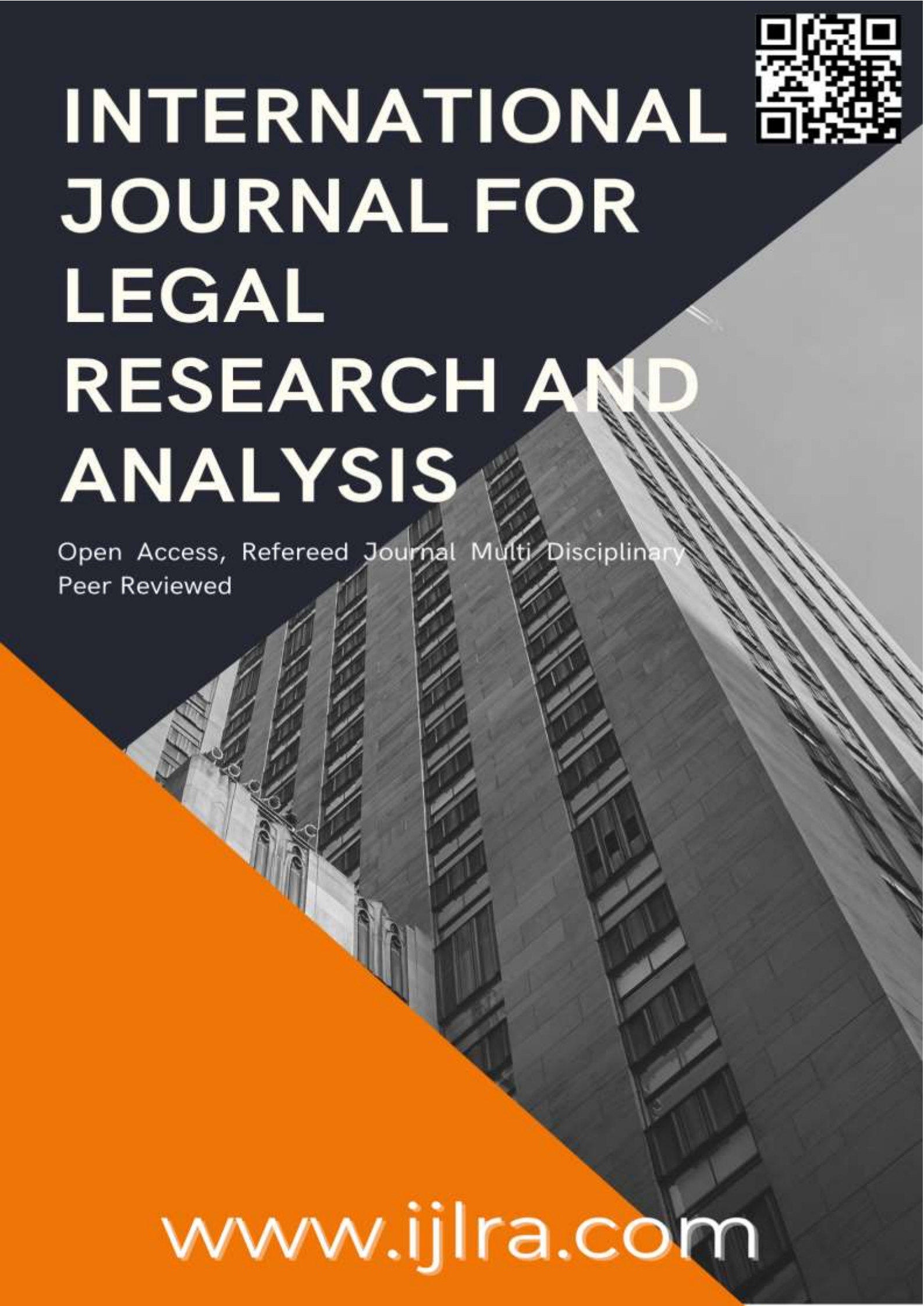
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CRYPTOCURRENCY BASED CRIMES: REGULATIONS, INVESTIGATION, PROSECUTION OF BLOCKCHAIN OFFENCES

AUTHORED BY - PRIYANSHU KANYAL

TABLE OF CONTENTS

ISSN: 2582-6433

TABLE OF CONTENTS

ISSN: 2582-6433

ABSTRACT

Cryptocurrency-related offenses in India have become a pressing issue in the modern digital financial era due to the growing use of Virtual Digital Assets and blockchain technology. Cryptocurrency-related crimes may be classified as including fraud, money laundering, ransomware, phishing, and Ponzi schemes that take advantage of the decentralization and anonymity of cryptocurrencies. Although the blockchain technology provides transparency and efficiency, the problem lies in the lack of any centralized authority, which makes the process of regulation and law enforcement rather challenging for the Indian government.

The regulatory framework in place regarding the use of cryptocurrency in India is quite new and is based mainly on existing laws. Thus, the lack of any legislative instrument dedicated to cryptocurrency poses an issue when trying to regulate and enforce relevant laws. Nevertheless, some recent changes in regulations can be observed, as there is an initiative to regulate Virtual Digital Asset Service Providers and impose tax on cryptocurrency.

Cryptocurrency crime investigations are based on advanced cyber forensic methods, blockchain analysis, and collaboration among various agencies. The agencies monitor digital wallets, analyze the flow of transactions, and obtain KYC details from crypto exchanges to locate criminals. However, despite the advent of technology, difficulties such as international transactions, anonymity, employment of mixers, and lack of standardized investigation techniques have hampered successful enforcement.

Cases of blockchain crimes are registered under several legal jurisdictions, such as under the PMLA, Information Technology Act, and other criminal laws regarding fraud and conspiracy. Courts in India have begun to recognize cryptocurrencies as “assets” or “property,” thus enabling their incorporation into criminal cases. Nonetheless, legal hurdles like jurisdictional barriers, difficulty in proving evidence, and valuation of virtual currencies remain.

ISSN: 2582-6433

CHAPTER 1

INTRODUCTION

Cryptocurrency is one of the most disruptive innovations of the 21st century because it changes the principles of value creation and transmission through decentralized peer-to-peer networks. Despite its revolutionary role, the absence of any regulating authority poses serious risks of misusing the cryptocurrency system. In India, the popularity of using cryptocurrency as a means of transaction has been growing rapidly in recent years. However, there are also concerns related to the increase in cybercrimes committed using cryptocurrencies.

The Indian experience with cryptocurrency shows that Bitcoin, Ethereum, and many other altcoins have become extremely popular in the country. The decentralized nature and anonymity offered by blockchain networks make cryptocurrencies vulnerable to misuse for criminal purposes, including fraud, ransomware attacks, money laundering, and illegal transactions. Therefore, cryptocurrency has become an issue of discussion from both regulatory and enforcement perspectives due to its innovative features and possible use for crime commission.[1] Crimes related to cryptocurrency in India are not only restricted to financial crimes, but rather they range across a vast array of cybercrimes, such as ponzi schemes that guarantee high rates of return, phishing scams directed against online digital wallets, hacking of online cryptocurrency trading platforms, using cryptocurrency for terror financing, and conducting illegal dealings through the dark net. In this respect, blockchain technology has posed additional challenges due to its borderless nature and because offenders conduct themselves across different borders, making it difficult to identify and prosecute them.

Regarding laws on cryptocurrency in India, no specific legislation has been enacted that provides for a dedicated legal framework pertaining specifically to cryptocurrency. Rather, there have been gradual developments in the legal framework that deal with cybercrimes committed through the use of cryptocurrency. For instance, laws such as the Information Technology Act of 2000, the Prevention of Money Laundering Act, 2002, and some sections of the Indian Penal Code have been relied on to curb cybercrimes using cryptocurrency.

The taxing of virtual digital assets forms an important part of regulatory measures taken by the Indian government. The Finance Act has put into place a taxation system applicable to cryptocurrency and has brought these under the scope of income taxation and taxed the transfer

[1]Vanathi Krishna, Role of Intellectual Property in Blockchain Indian J Integrated Rsch L. 8 (2022)

ISSN: 2582-6433

of such digital assets. Although the introduction of such a law is not legalization but rather just recognition of the fact that they exist in the financial world, they lack proper regulations in the form of a comprehensive act.[2]

Examining crimes associated with blockchain technology is not an easy task for law enforcement agencies in India. Contrary to conventional financial systems where transaction details can be linked to individual accounts, blockchain technology maintains a record of transactions in public ledgers, but the identities of the users involved cannot be determined. In addition, cybercrime departments and financial intelligence units must use blockchain analysis software and forensic methods to track illegal transactions.[3]

Investigating authorities of India like ED, CBI, and cybercrime units of the states are responsible for investigating cryptocurrency crimes. They work alongside international law enforcement agencies and private blockchain technology companies that help in tracing financial transactions. However, inadequate investigation procedures, coupled with the technical knowledge of cryptocurrency, is a significant problem faced by India in combating cryptocurrency crimes.

Proving cryptocurrency crimes in India has its fair share of difficulties. The courts are often called upon to apply provisions of existing legislation to new technologies, which were perhaps unknown to legislators at the time of their enactment. Difficulties related to admissibility of evidence, identification of owners of cryptocurrency and jurisdiction issues arise. Moreover, due to the absence of a proper definition of cryptocurrency in law, proving offenses committed by offenders becomes an uphill task.

The judiciary in India has slowly started recognizing the value of digital evidence and the importance of using blockchain technology while investigating criminal cases. The use of electronic records as evidence has been accepted by courts through the provisions of the IT Act if it meets all the requirements of being acceptable as evidence. However, the development of a proper jurisprudence related to cryptocurrencies has not yet evolved.

One of the key difficulties in dealing with crimes involving cryptocurrencies is the issue of seizing and recovering stolen property. While in the case of regular financial crimes, the stolen money can easily be frozen since it is in bank accounts, cryptocurrencies can be moved easily

[2]Narayanan, S., "Cryptocurrency Regulation and Legal Challenges in India", (2022) 64(3) Journal of the Indian Law Institute 345.

[3]Gupta, R. & Sharma, A., "Blockchain Technology and Criminal Liability: Emerging Issues in Cyber Law", (2021) 63(2) Journal of the Indian Law Institute 198.

ISSN: 2582-6433

between wallets and even exchanged for other cryptocurrencies, thus making it extremely difficult for law enforcement agencies to recover such assets.

However, India is progressively adopting an organized approach to cryptocurrency regulation. There have been discussions regarding a model that will strike a balance between encouraging innovation and protecting consumers as well as the country's finances. International collaboration, advances in blockchain analysis technology, and improved legislation will be instrumental in determining how cryptocurrency regulation will look like in the future in India. A holistic approach incorporating regulation, enforcement, and judiciary measures will help in tackling the threat of blockchain-based offenses in a constructive manner.

PROBLEM STATEMENT

The fast pace adoption of cryptocurrencies and blockchain in India has resulted in the emergence of a parallel financial system based on digital currency. Although this development has resulted in the emergence of several avenues for investments as well as financial inclusiveness, it has also been responsible for a surge in criminal activities associated with the use of cryptocurrencies like fraud, money laundering, ransomware, and other illicit cross-border monetary transactions. However, due to the decentralized and pseudonymized nature of blockchain technology, it is extremely challenging for law enforcement authorities to track down offenders as well as their fraudulent dealings using current legislation.

Even after using the existing statutes like the Information Technology Act, 2000 and the Prevention of Money Laundering Act, 2002, India does not have a well-established and specific legislation for the offences committed through cryptocurrencies. The investigative agencies find it difficult to trace the transactions on the blockchain, whereas the court faces problems in making sense out of digital evidence. Moreover, there is ambiguity in dealing with jurisdiction issues relating to the cross-border nature of the offences and lack of globally recognized uniform standards for such offences.

ISSN: 2582-6433

PROJECT OBJECTIVE

- To analyze the legal and regulatory framework governing cryptocurrency and blockchain-based transactions in India.
- To identify and examine the various types and patterns of cryptocurrency-based crimes occurring in India.
- To study the investigative techniques and challenges faced by law enforcement agencies in tracing blockchain-related offences.
- To evaluate the effectiveness of existing laws and judicial approaches in the prosecution of cryptocurrency crimes.
- To suggest suitable legal, technological, and policy reforms for strengthening the regulation and control of cryptocurrency-based offences in India.

RESEARCH QUESTIONS

- What is the existing legal and regulatory framework governing cryptocurrency transactions and blockchain technology in India?
- What are the major forms of cryptocurrency-based crimes and how are they being committed in the Indian digital environment?
- What challenges do investigative agencies face in detecting, tracing, and collecting evidence in blockchain-related offences?
- How effective is the current legal system in India in prosecuting cryptocurrency crimes, and what reforms are needed to improve it?

HYPOTHESIS

However, the current laws and regulations that exist in India are not enough to handle and curb crimes using cryptocurrencies, because there are no specific laws that regulate the use of digital assets. It is therefore imperative that the methods of investigation be improved, the technology enhanced, and laws established to help curb crimes involving blockchain technology in India.

ISSN: 2582-6433

LITERATURE REVIEW

Porras (2023)[4]In the author's research paper analysis about the IP concepts and development in which the results affect the intellectual ownerships of major aspects of blockchain technology. Many stakeholders, whether governments, legislators, or policy makers, find themselves in a maze of both technological and social realities in which facts are often mixed with fiction. There are the proprietors of intellectual property that pertain to blockchain technology and those who come into the technology after them and do not have any intellectual property rights. The financial interests involved are very high, so much so that a whole new industrial revolution could take place from this technology. In this environment, there are many people who have different levels of understanding of the technology. Three areas that will be covered in this chapter include introduction to blockchain technology, use of blockchain technology in controlling the IP rights, and IP rights in the blockchain industry.

Narayanaswamy (2021)[5]Introduction

The present era sees continuous innovations in science, where the Blockchain technology shares space with Artificial Intelligence, Virtualization, and Internet of Things. The basic features of decentralization and anonymity make it pertinent for wireless network virtualization and several other innovative uses. One of the innovations in this area is the concept of smart contracts that are self-executing contracts written in programming languages. Global movements, such as the French movement, and legislative measures, including a Chinese Court's approval of evidence from blockchain technology in 2018, have been considered in the article. Yet, the lack of any specific legislation relating to blockchain technology in India is regretted.

Rajabi&RajabiNezhad (2025)[6]this article offers an insightful criminological analysis of crimes involving cryptocurrency and reveals how modern developments in blockchain have led to innovative forms of cybercrime. The authors describe how crimes, such as money laundering, frauds, ransomware attacks, darknet trading, and cryptocurrency exchanges hacking are

[4]Porras, Intellectual Property and the Blockchain Sector, a World of Potential Economic Growth and Conflict, Intech Open Journal, 2023

[5]Narayanaswamy, Raju. Infusing Blockchain Technology into the IPR Sector, International Journal of Research in Social Sciences, 2021

[6]Rajabi, Akbar &SajadRajabiNezhad, "A Criminological Analysis of Cryptocurrencies and the Challenges of Prosecuting Blockchain-Based Crimes", JHRLP (2025)

ISSN: 2582-6433

becoming prevalent because of cryptocurrencies' decentralized and anonymous nature. The main aspect discussed in the paper is how criminals take advantage of the anonymity and non-regulation, which makes it impossible for police organizations to track down and investigate crimes. Another important point raised by the authors is how global legal systems lack resources needed to tackle cross-border cryptocurrency crime effectively. What is more, the paper underlines that conventional investigative techniques are not sufficient in dealing with offenses connected to blockchain, hence the need for special blockchain analytics and artificial intelligence-based tracking technologies.

Navani&Cirella (2024)[7]discusses the rapid changes taking place in cybercrimes associated with cryptocurrency. This article categorizes the different types of offenses arising out of the development in this field. Some of the most common offenses include hacking into crypto wallets through phishing methods, Ponzi and pyramid schemes using cryptocurrencies as an investment, rug pulls on DeFi applications, ransom payments in cryptocurrency, and exploiting loopholes in smart contracts. Motivation for committing the offense is discussed, with financial gain, anonymity, and the technological loopholes being identified as the main drivers for such actions. There is an analysis of the regulatory measures employed by different countries in response to this crime and how there are significant differences in their approaches. One of the most serious issues that emerge from this paper is the lack of a uniform global regulatory mechanism against cybercrimes involving cryptocurrencies, which leaves offenders with room to commit offenses without facing much legal scrutiny.

Rathod&Borase (2024)[8]focusing specifically on forensic investigation techniques employed in tackling crimes connected to cryptocurrencies and paying attention to the growing need for digital forensic science in contemporary criminal investigation practices. According to the researchers, despite the transparency associated with the recording of transactions on the blockchain, there are serious complications in terms of pseudonymity, encryption, and the usage

[7]Navani, Shobhit& Giuseppe T. Cirella, "Cybercrimes in the Cryptocurrency Domain 14(2 JGPS(2024)

[8]Rathod, Digvijaysinh M. &Bhushan G. Borase, "A Review of Research in Forensic Investigation of Cryptocurrencies", 16(4) IJESDF(2024)

ISSN: 2582-6433

of several wallet addresses that make it possible to conceal the identity of users. In their work, the authors give a detailed account of different forensic instruments and methods that are used to track down cryptocurrency transactions. These include, for example, blockchain explorers, clustering techniques, and transaction pattern analysis among others. The authors also stress the significance of having a strong chain of custody concerning the digital evidence collected in order to be able to use it effectively in court. In addition, the authors draw attention to the difficulties faced by investigators in dealing with cross-chain transactions, mixing services, and the fast-changing privacy features of cryptocurrencies.

ShreyaRai (2022)[9]The significance of blockchain technology to India cannot be overstated since the application of this innovation will help to solve numerous problems in different spheres. In particular, blockchain technology can make the governance more transparent and accountable since blockchain ensures that no one can change the data stored by this technology. Blockchain technology can be applied in various spheres, including e-governance, land registry system, voting process, and public services provision. This will help to reduce corruption in the country and increase the level of trust among citizens towards governmental institutions. Although the application of blockchain to the sphere of intellectual property sounds promising, it is important to consider the limitations of using blockchain in this sphere. First, there are certain limitations regarding the use of this technology, including the inability of people to comprehend the essence of this technology. The introduction of blockchain technology to government institutions may prove challenging due to the necessity to educate the government workers about the technology, especially since the process of digitizing land and other data is not completed yet.

Jonathan Solomon (2021)[10]discusses the development of the cryptocurrency industry, with emphasis on the state of the patent system, difficulties in obtaining patents, and the future developments in this area. He states that cryptocurrency firms are becoming more active in obtaining patents related to improving current technologies, such as increasing the speed of computations, increasing network bandwidth, improving data storage capabilities, enhancing

[9]ShreyaRai (2022), The Association of Intellectual Property Law And Blockchain, https://www.linkedin.com/pulse/association-intellectual-property-law-blockchain-legasispvtltd

[10]Jonathan Solomon, Patent Protection for Cryptocurrencies and Blockchain Technology, CCBJ (2021)

ISSN: 2582-6433

security measures, and improving data verification methods. In light of this technology maturing, the firms are developing blockchain applications for other uses besides cryptocurrencies, including distributing software applications, managing inventories, managing supply chains, and boosting consumer confidence. One client, for example, invented a blockchain process to prove that its coffee is certified by the Fair Trade organization. The work might provide insights from both legal and business angles, covering issues such as the strategy for patenting the blockchain technology. Such issues include the creation of a patent portfolio, patent enforcement strategies, and the interrelation of patents and other IP forms. Because the field and the patent process are rapidly changing, future developments may be discussed in this book.

Kukrety, Neha and Kaushik (202)[11]As India enters its digital transformation era, it is evident that the fintech industry plays an important role in being an enabler. Moving forward, the next generation trading currencies through blockchain technologies are one of the focal points discussed in the fintech field. It is noteworthy that digital currencies and assets, supported by Distributed Ledger Technologies (DLTs), come under intense scrutiny by regulators and policymakers. Such cautious attitude displayed by regulators including that of the Central Bank emphasizes the necessity for having strong legal frameworks which safeguard the interest of the consumers as well as that of the economy as a whole. Thus, the objective of this paper is to delve into the significance of legal frameworks and their necessity when it comes to maintaining the stability of digital currencies. Blockchain is a distributed network which operates in a decentralized fashion with no authority regulating the operations. With this being the case, legal frameworks can become increasingly significant in providing an appropriate governance model. The legal issues which are pertinent to blockchain will be addressed to discuss the significance of creating such legal frameworks and how they should look like.

SIGNIFICANCE OF THE STUDY

The importance of the current study emanates from the exhaustive analysis of the issues of crypto-crimes in the Indian jurisdiction. With the emergence of cryptocurrencies and associated blockchains as technologies, there are two aspects that emerge - innovation and vulnerabilities. The current research study will be useful to gain a better perspective regarding the issue of innovation misuse through crypto-crimes such as fraud, money laundering, ransomware attacks,

[11]Kukrety, Neha and Kaushik.Blockchain Technology and Legal Framework in India, EELJ (2023)

ISSN: 2582-6433

and any other form of criminal transactions.

One more area of relevance to this study is in terms of the difficulties encountered in the investigation of blockchain crimes. The crimes based on the blockchain technology present a challenge to the law enforcement agencies owing to the issues like decentralized nature of technology, anonymity, etc. Hence, the study will enable one to have a better perspective about the complexities involved and also provide suggestions in this regard.

Ultimately, the significance of the research lies in identifying reforms that can improve India's crypto regulation policies. The researcher argues that there should be an improvement in creating an effective legislative mechanism, enhanced investigatory powers, and cooperation at the international level for ensuring successful regulation of crimes related to blockchains. The research paper, by offering a systematic analysis of regulation policies, investigation procedures, and prosecution issues, acts as a helpful resource for all concerned stakeholders of cyber law and digital finance.

RESEARCH.METHODOLOGY

The research methodology chosen for studying the issue of cryptocurrency crimes in India can be characterized as doctrinal because it includes the analysis of laws, judicial decisions, guidelines, and academic writing. The secondary sources that will serve as the basis for the analysis are journal articles, academic writing, law commission reports, government publications, and international guidelines dealing with blockchain technology and cybercrimes. Furthermore, there is a need to adopt both descriptive and analytical approaches when researching different aspects of cryptocurrency crimes and possible ways of regulating them. In particular, there will be a need for the description of different types of crimes associated with cryptocurrency, including the description of the technology itself, which will also help in identifying and explaining the criminal activities involved. As for the analysis, the focus will be on the evaluation of legal provisions of India in terms of addressing new challenges.

In addition to this, the study also employs a comparative approach wherein the regulatory regime and enforcement measures used in India are contrasted briefly with those used in other countries like the United States and European Union, as well as the recommendations made by the Financial Action Task Force. Such an analysis enables the researcher to comprehend the global standards in relation to cryptocurrency regulations and investigations. The combination of all three research methodologies would help provide a holistic perspective on blockchain-related

ISSN: 2582-6433

offenses.

SCOPE AND LIMITATIONS OF THE STUDY

The scope of this research includes the discussion about cryptocurrency-associated crimes from the point of view of regulatory measures, investigation procedures, and legal difficulties. It involves the consideration of the possibility of applying the relevant provisions of law in PMLA for addressing criminal acts related to blockchains. Moreover, the research focuses on the role played by regulatory authorities and enforcement agencies, technologies used during investigation, as well as changes in the structure of the crimes committed within the digital currency market.

Nevertheless, this study cannot be viewed without its limitations caused by fast-paced changes associated with cryptocurrency and blockchain technologies. Legal norms and regulations in the sphere under analysis have not been fully developed yet, which can make some conclusions obsolete when updated laws are introduced in the future. The decentralized and international character of cryptocurrencies hinders access to relevant information needed for assessing the full scope of criminal behavior and enforcement results in question. At the same time, the use of secondary sources can distort some data related to real-life processes.

The other limitation is the technology-based nature of blockchain platforms, which might affect a purely legal perspective on the issue. Though attempts have been made to incorporate aspects of technology, the research does not explore deeper into the field of cryptography and programming. Also, the variations in laws across nations have been considered only to some extent, restricting the scope for comparison. Nevertheless, the research offers a concise yet pertinent insight into the legal and institutional implications of crypto crimes in India.

ISSN: 2582-6433

CHAPTERIZATION

Chapter 1: Introduction

Cryptocurrency crimes in India comprise offenses like frauds, hacking, money laundering, ransomware attacks, and Ponzi schemes using Virtual Digital Assets (VDAs) on blockchains. Cryptocurrencies have a decentralized nature with pseudonyms that facilitate direct transfers without centralized management. This makes them highly vulnerable to exploitation by criminals as well as hard to track down for law enforcement agencies. The paper comprises the problem statement, literature review, objectives of research, hypothesis, method and significance of the study.

Chapter 2: Conceptual Framework

The concept behind cryptocurrencies is based on blockchain technology, a form of decentralized and distributed ledger technology where information related to each transaction is recorded into blocks. Cryptocurrencies have no centralized control; rather, they depend on the use of cryptographic keys, wallets, and peer-to-peer networks, thereby offering a high level of transparency and anonymity at once. Concepts like decentralization, smart contracts, mining, and mixers provide insight into how digital currencies work and how the criminals use their properties to commit offenses.

Chapter 3: Legal and Regulatory Framework in India

Cryptocurrencies in India are subject to regulation by a set of already extant laws but not any specific law. In this regard, the Prevention of Money Laundering Act, 2002, serves as an essential regulatory framework for crypto exchanges and facilitates the confiscation of digital assets. On the other hand, the Information Technology Act, 2000, deals with any cybercrime committed through crypto sites, whereas the Income Tax Act taxes Virtual Digital Assets. However, FIU-IND conducts investigations into suspicious transactions, although the Reserve Bank of India does not accept cryptocurrencies as valid currency.

Chapter 4: Investigation and Prosecution of Cryptocurrency Crimes

Cryptocurrency crime investigation requires sophisticated analysis of blockchain technology, cyber forensics, and cooperation with cryptocurrency exchanges to trace the flow of funds through wallets and find out the criminals. The ED and Cyber Crime Police monitor the digital trail, study the transaction flow, and gather evidence from electronic gadgets such as mobile phones and hardware wallets. The prosecution process begins by lodging an FIR or ECIR, then

ISSN: 2582-6433

by attaching and seizing the proceeds under the PMLA and submitting charge sheets to special courts.

Chapter 5: Judicial Approach and Challenges

Cryptocurrencies have been treated by Indian courts as property/assets over time. Yet, the judicial process faces some difficulties like an absence of a legal framework, difficulties in determining the jurisdiction of the court regarding international cases, problems in interpreting blockchain technology, and inconsistency in legal interpretation. There is also the difficult task of finding the balance between innovating financial technology and avoiding financial fraud, hence the evolving yet uncertain legal practice on this issue.

Chapter 6: Conclusion and Recommendations

The criminal activities involving cryptocurrency in India have made it imperative for the country to formulate an elaborate and specific regulatory structure that can deal effectively with the complications of blockchain-related crimes. Although there are some laws such as PMLA, IT Act, and tax laws that can offer some form of control over the crypto industry, they still fall short of offering complete regulation. Some recommendations include defining cryptocurrencies legally, improving the blockchain forensic system, and better cooperation amongst enforcement authorities.

ISSN: 2582-6433

CHAPTER 2

CONCEPTUAL FRAMEWORK

Cryptocurrency is basically a digital version of money that is used during trading and transactions. Cryptocurrency is similar to regular money; however, there is no physical evidence of it being used during any trade. One interesting thing about cryptocurrency is that it is a decentralized form of money, which implies that no single government or any combination of governments regulates it. Cryptocurrency functions under the rules of cryptography, which can be described as the science of encrypting messages to ensure that the receiver has access to decrypt the message. This is done using mathematical concepts and complex algorithms. The prefix 'crypt' implies hidden, whereas the suffix 'graphy' denotes writing.

The term cryptocurrency is an allusion to a digital currency that is encrypted. Cryptocurrencies are based on a decentralized network, which, in turn, uses blockchain technology. What differentiates cryptocurrency from regular online transactions is its mode of operation.

There are many beliefs that it would not be possible for any person to get involved in duplicating transactions or counterfeit money in such a system. Cryptocurrency is generally a decentralized network of transactions made through the blockchain system, which is continuously growing in its records. These blocks are used to connect and secure each cryptocurrency, while there is another network where all the finances are kept, known as mining. Simply put, the validation process of cryptocurrency is termed mining.[12]

Blockchain technology

Blockchain technology is a decentralized ledger that uses a network of computer nodes to record the transactions between various parties. In a decentralized network of computers (nodes), each computer holds a complete copy of the blockchain technology. Thus, it is different from a centralized network in which one authority manages the transactions in a database. Therefore, blockchain technology is used mainly in cryptocurrency networks such as Bitcoin technology. Although cryptocurrencies are among the most common use cases of blockchain technology, there are numerous other applications for blockchain technology. Such applications include supply chain management, voting platforms, smart contracts, financial transactions, and identity verification.

[12]RidhimaSaxena, India's Crypto Investors Weigh Options Ahead Of Impending Ban, Bloomberg Quint, February 14, 2021

ISSN: 2582-6433

Blockchain technology can be defined as a decentralized distributed ledger system that records the provenance of digital assets. The technology creates a secure and tamper-resistant platform for storing data. In essence, blockchain technology allows any digital asset to be transmitted through a network in which the transactions are immutable, unhackable, tamper-proof, and transparent.

The technology works on a protocol guaranteeing that all nodes in the system have proper data through cryptographic activities. Blockchain acts as a data structure because it creates an append-only ledger that is maintained by all nodes. Consensus is employed to authenticate the information on each node, where a few nodes in the system authenticate the transaction. Proficient individuals, called miners, authenticate the data generated by the participating parties, ensuring that they meet cryptographic requirements to be entered into the block chain. The process of authenticating transactions through cryptographic puzzles solved by miners is called proof of work. It makes it important for there to be a governing body in the blockchain system. The disruptive capability of blockchain technology brings many prospects within different sectors, such as finance, insurance, and IP rights.

Functioning of Blockchain technology

How Blockchain Technology Works

The operation of blockchain technology involves the use of a decentralized and distributed ledger for the safe and secure recording of transactions within a computerized network. The following is an explanation of how blockchain technology works.

Decentralization: Contrary to centralized systems which involve the storage of data through one authority, the decentralization concept in the blockchain technology involves storing and managing data in a distributed way throughout a computer network (nodes).[13]

Distributed Ledger: The distributed ledger technology refers to the blockchain's sequential and immutable record of all transactions taking place within the network. Every new transaction is bundled into a "block" and added to the chain of blocks, creating an ever-growing and tamper-resistant ledger.

Consensus Mechanism: In order to maintain the integrity and security of the blockchain ledger, consensus mechanisms are employed to validate and agree upon the authenticity of transactions before their addition to the ledger. There are different types of consensus algorithms in use by

[13]Saini and Kumar, "Issues pertaining to growth of digital economy, Journal of Public Affair (2020).

ISSN: 2582-6433

various blockchain platforms, including Proof of Work (PoW), Proof of Stake (PoS), or others.

Cryptographic Hashing: Every block in the blockchain carries a cryptographic hash of the preceding block, creating a sequence of blocks that are chained together. This preserves the integrity of the data while making it extremely difficult to alter previous transactions without affecting the subsequent blocks.

Peer-to-Peer Network: The blockchain operates using a peer-to-peer (P2P) system, which means that nodes interact with each other without any intermediary.

Smart Contracts: Some blockchain systems also have smart contract capabilities. This is a mechanism where the terms of the contract are written in the code and the contract can execute itself based on certain conditions.

Blockchain Type: Another feature of blockchain technology is its type, which can be classified as either public or private. In public blockchain systems, participation and access are open for everyone, whereas in private blockchains, only the authorized participants can use the blockchain network. Bitcoin and Ethereum are examples of public blockchain systems.

To conclude, blockchain technology provides some advantages like transparency, security, immutability, and decentralization, among others, and therefore, it can be applied in many sectors outside cryptocurrencies. For instance, blockchain technology can be used for logistics, identification processes, voting procedures, among other purposes. Nevertheless, certain factors should be considered in the implementation process.

IMPORTANCE OF BLOCKCHAIN TECHNOLOGY

There is immense significance of blockchain technology for India in various domains due to the wide array of issues that can be solved using it and due to its innovative nature. Here are a few areas that can benefit greatly from implementing blockchain technology in India:

Financial Inclusion: There is a huge population in India which remains financially excluded. Using blockchain technology, these groups of people can gain access to financial products through secure and cost-efficient means.

Supply Chain Management: Supply chains in India have been known to suffer from various inefficiencies like counterfeiting of products. The implementation of blockchain in supply chains can improve efficiency and accountability within them.

Digital Identity: Blockchain technology can enable individuals in India with secure means to establish their identity which in turn will make it easier for them to access government and other

ISSN: 2582-6433

vital services.

E-Governance: E-governance involves making various processes more efficient and streamlined through technology. Blockchain can potentially improve e-governance through applications like land registry and online voting systems.

Health Care: Blockchain technology can help in improving the integrity and security of healthcare data allowing interoperability between various systems. Also, it would make sure that the data is safe and privacy and consent of patients are ensured.

Education and Certification: Blockchain can be helpful in verifying educational credentials of individuals and organizations. This would reduce fraud and increase trust among all parties involved in education process.

Agriculture: India's agricultural industry can make good use of blockchain technology to increase transparency in the supply chain, set up fair prices for farmers, and offer financing and insurance to farmers using digitized assets.

Intellectual Property Protection: Blockchain technology can be used to create an unalterable platform that would help in managing intellectual property like patents, copyrights, and trademarks.

Smart City Development: Rapid urbanization of India can make use of blockchain technology to build smart cities in the country. These smart cities will feature efficient management of energy consumption, traffic flow, waste disposal, etc.

International Trade and Remittance: Blockchain technology is an effective means for streamlining processes in international trade, cutting down the paper work involved, and minimizing risks in international transactions. Further, blockchain is a reliable and affordable platform for handling remittances for both individuals and organizations.

Such an application of blockchain technology could help facilitate significant socio-economic changes in India by overcoming existing difficulties, fostering trust, and opening up avenues for innovation. Nevertheless, in order to achieve this goal, there should be cooperation between governmental and non-governmental parties as well as all other stakeholders within the field of blockchain technology.

Blockchain technologies on innovation and creativity

Blockchain technology has received substantial attention from many people recently as it is capable of bringing changes to many sectors and operations. Speaking about innovation and

ISSN: 2582-6433

creativity, there are some aspects that blockchain technology has to offer:

Decentralization:

Decentralization is one of the most important aspects of blockchain technology, which implies that data is distributed among multiple computers instead of being stored centrally. Decentralization leads to innovation as it removes the requirement for intermediaries and opens up new ways of conducting business and collaboration between peers. Decentralization is one of the most important concepts of blockchain technology, which involves the distribution of data and control among various nodes instead of having a central controlling authority. Here are some important points about decentralization in blockchain technology:[14]

Distributed Ledger: The blockchain is a form of distributed ledger, which acts as a recording of all transactions among various nodes in a decentralized network. Each participant possesses his/her own copy of the ledger, and all transactions are stored in blocks connected to one another to create an unalterable chain of blocks, also known as blockchain.

Peer-to-Peer Network: Blockchain makes use of a peer-to-peer network, where all the nodes within the network communicate with each other. Such a peer-to-peer structure allows for direct validation and distribution of transactions through the network without any intermediaries. In addition, the network would remain functional even if a certain number of nodes fails to work properly.

Consensus Mechanism: Consensus mechanism is used by blockchain networks in order to come to a mutual agreement among nodes regarding the validation and authenticity of transactions made within the blockchain. Various types of consensus mechanisms exist within the framework of the blockchain technology, including proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS).

Unchangeable and Unalterable: Since the blockchain system does not rely on a centralized system but rather a decentralized one, it is very difficult for anyone to censor or alter its information. The moment the transaction is recorded on the blockchain, it will become unchangeable and will be impossible to delete or alter it.

Decentralized Applications (DApps): Blockchain allows the creation of decentralized applications (DApps) that operate on decentralized networks. The use of blockchain allows these

[14]Pandey, Surabhi&SenBlockchain Technology in Real-Time Governance: An Indian Scenario. Indian Journal of Public Administration (2022)

ISSN: 2582-6433

applications to offer their services and functions through decentralized means without having centralized servers or intermediaries. DApps range from decentralized finance (DeFi) platforms to decentralized exchanges and blockchain-based games.

Tokenization and Decentralized Finance (DeFi): Blockchain makes it possible to tokenize assets, meaning the conversion of assets into digital tokens on a decentralized network. Tokenization leads to the creation of opportunities in decentralized finance (DeFi) including peer-to-peer lending, decentralized exchanges, and automatic trading platforms. Through blockchain, DeFi operates without any intermediary such as banks and brokers.

In summary, decentralization plays an essential role in ensuring the effectiveness of blockchain technology. Blockchain creates an environment in which individuals can interact and transact among themselves without interference from intermediaries.[15]

Transparency and Trust

Transparency and immutability are characteristics of blockchain technology that provide assurance to its users that the recorded information cannot be changed or tampered with at any point in time. These two features increase the level of trust in the system and stimulate creativity.

Here's how blockchain technology fosters transparency and trust:

Immutable Ledger: The blockchain technology uses an immutable ledger that records all transactions. After recording a transaction, it cannot be changed or erased from the ledger. It means that anyone who joins the network can view the history of past transactions, and this transparency encourages honesty and accountability among the parties.

Decentralized Network: Blockchain runs on a decentralized network with many nodes holding copies of the ledger. In the decentralized model, there is no central authority controlling the transactions or managing the system. The lack of a central authority makes the network less vulnerable to corruption and manipulation.

Public Verification: For the public blockchain, such as Bitcoin and Ethereum, everybody may audit the transactions and the flow of assets on the blockchain. This unrestricted access to information regarding transactions increases the level of transparency and trust between members of the blockchain network because they can check whether the transaction is valid or

[15]Jani, Shailak. The Emergence of Blockchain Technology & its Adoption in India, SSRN (2019)

ISSN: 2582-6433

not.

Smart Contracts: The smart contract is an agreement between two parties that executes automatically if the conditions are met. They eliminate the need for third-party interference and increase efficiency since the smart contract will be executed once the pre-specified condition is satisfied. Moreover, it adds to transparency as the execution of the contract can be traced.

Audibility: The ability to trace transactions and audit accounting records efficiently make blockchain technology appropriate for conducting audits. It allows auditors to easily analyze transactions on the blockchain and minimize the risks of error and fraud.

Supply Chain Transparency: Companies increasingly utilize blockchain technology to increase the transparency and traceability of their supply chain processes. Blockchain technology allows firms to track the transportation and production of raw materials. As a result, the blockchain offers more transparency to customers about the source of products and the production process.

Data Integrity: The cryptographic tools that blockchain utilizes help ensure the integrity of data stored in the blockchain system. This is due to the fact that all transactions are cryptographically connected to one another; hence, any interference with the data would be spotted right away. This feature ensures that all data within the system is trustworthy.

In conclusion, blockchain technology is characterized by a number of features, including security, decentralization, and transparency, which have the potential to revolutionize the manner in which transactions take place in certain industries.[16]

Smart Contracts

A smart contract is a self-executing agreement that contains terms of the agreement and is written in computer code. Smart contracts automatically enforce the terms of the contract whenever the specific criteria are met. Using smart contracts helps optimize the processes and gives rise to new ways of doing business.

They work on the blockchain platforms and are triggered by pre-defined actions when specific conditions are satisfied. These are some ways in which smart contracts use the features of blockchain technology:

Automation: Smart contracts automate contractual agreements. There is no need for any intermediary or third party enforcement of the terms of the contract as smart contracts are

[16]IfeanyiMbukanma, Role of creativity and technological innovation in achieving entrepreneurial success, IJCMS, 2023

ISSN: 2582-6433

designed to execute automatically when specific conditions are met.

Decentralization: As smart contracts are built on top of the blockchain platform, they are decentralized. Smart contracts are executed from various network nodes and there is no centralized management of the transaction process.

Trust: Blockchain provides an immutable platform to deploy smart contracts, and thus once they are deployed, there is no way that any participant can manipulate them or tamper with the terms of the contract.

Transparency: One of the key features of smart contracts is that they are transparent in their creation and execution, since both are recorded in the blockchain. Anyone can look at the code and see how smart contracts work. Moreover, the execution of smart contracts by other users of the blockchain is also clear.

Security: Security is provided for smart contracts through cryptographic technologies embedded in the blockchain, which ensures the safety of both smart contracts and transactions performed through them. Blockchain being a decentralized technology makes it difficult to hack into.

Cost Effectiveness: Thanks to the absence of intermediaries, smart contracts are cost-effective since they eliminate the need to hire lawyers and other representatives of third-party organizations when concluding an agreement.[17]

Wide Variety of Applications: Smart contracts are employed in many different industries such as banking, logistics, real estate, medicine, and others. They can be utilized in such activities as payment processing, asset transfer, logistics monitoring, election processes, and DApps development.

[17] https://link.springer.com/article/10.1007/s10796-022-10279-0

ISSN: 2582-6433

Tokenization

Blockchain provides for the tokenization of asset classes, where assets in the physical world, such as real estate, artwork, or intellectual property, are tokenized on the blockchain as digital tokens. Tokenization ensures liquidity, offers fractional ownership, and opens doors to creative funding.

Data Monetization and Ownership

The blockchain technology ensures that individuals have the power to remain in possession of their data without compromising on its usability, by using it to earn money from secure transactions. In turn, individuals get the opportunity to find innovative ways of utilizing their data.

Supply Chain Innovation

Blockchain technology has the potential to transform supply chain management through enhanced visibility, traceability, and transparency. Transparency encourages innovation by allowing for novel solutions to product authentication, provenance, and sustainability efforts.

Nature and Typology of Cryptocurrency related Crimes

Crypto-based criminal activity encompasses any illegal act that involves the utilization of cryptocurrencies or blockchain technology as a means of carrying out the crime, attacking crypto wallets, or hiding illicit gains. Decentralized finance has revolutionized the concept of cybercrime since there are no conventional banking protocols involved, and peer-to-peer transfers take place. Since cryptocurrencies are based on blockchain technology, transactions are transparent and yet anonymous, allowing criminals to leverage both aspects.

Money laundering is perhaps one of the most common types of crypto-based crime involving the conversion of proceeds from illegal activity into digital assets to obscure the source of the money. Money launderers usually employ methods such as mixing services, wallet switching, and chain swapping to sever the transaction trail, making it incredibly challenging for regulatory authorities to identify the initial source of the proceeds. In India, these activities are commonly associated with fraudulent, corrupt, drug trade, and cyber-based operations, posing a significant problem for agencies like the Enforcement Directorate and cybercrime divisions.[18]

A third broad category includes fraud and investment scams, which have gained rapid traction

[18]DandaRawat, Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems , MDPI, 2020

ISSN: 2582-6433

with the growth of cryptocurrencies. Here, the criminals set up a fraudulent investment platform, Ponzi scheme, or fraudulent ICOs with an exaggeratedly high rate of return to lure potential investors. The victims usually lack any knowledge about the technicalities of blockchain and fall prey to social media campaigns, fake endorsements, and well-designed websites. After collecting enough money from unsuspecting victims, they abscond and leave behind considerable financial losses with no legal redress for the affected.

Another serious misuse of cryptocurrency is through ransomware attacks. This involves a hacker gaining unauthorized access to computer systems and then encrypting their data to make them inaccessible. They demand a ransom in cryptocurrencies like Bitcoin in return for the decryption keys. The reason for using cryptocurrencies is that it provides quick transfer, is international, and untraceable. These attacks have been reported on individuals, businesses, hospitals, and even governmental agencies across the world, and such instances have been growing in India too.[19]

Cryptocurrencies have also found significant use in transactions conducted through the dark web network. Illegal products or services such as drugs, weapons, fake documents, and compromised personal information are available for purchase. Traditional forms of payment cannot be utilized in such a situation, which makes cryptocurrencies ideal in conducting business. Websites that run over the dark web heavily depend on encryption and anonymous methods, hence making it hard to investigate any wrongdoing.

The third issue affecting cryptocurrencies is the problem of hacking and theft from crypto exchanges or wallets. In most cases, hackers use phishing methods and malware to breach into the wallets to access secret keys. Afterward, these hackers divert the funds to their own wallets. Unlike other banking methods, cryptocurrency transactions cannot be reversed; thus, victims find it difficult to reclaim their lost money.

In addition, there have been increased cases where cryptocurrencies have been used for terror financing and money laundering. Some illegal organizations have leveraged cryptocurrencies in order to fund their operations and transfer money from one nation to another without being detected because of the lack of regulation in many nations. At the same time, people can use cryptocurrencies to hide income and avoid paying taxes.[20]

[19]Narayanan, S., "Cryptocurrency Regulation and Legal Challenges in India", (2022) 64(3) Journal of the Indian Law Institute 345.

[20]Gupta, R. & Sharma, A., "Blockchain Technology and Criminal Liability: Emerging Issues in Cyber Law", (2021) 63(2) Journal of the Indian Law Institute 198.

ISSN: 2582-6433

ISSN: 2582-6433

CHAPTER 3

LEGAL AND REGULATORY FRAMEWORK IN INDIA

Unlike other nations, the legislative basis for any crimes related to cryptocurrency is not based on any specific piece of legislation in India. Cryptocurrencies have no legal standing in India as means of payment. But Virtual Denominated Assets (VDAs) are subjected to regulations based on PMLA, Information Technology Act 2000, and Income Tax Act, 1961. Although there is no separate legislation regulating cryptocrimes, this regulation can be used to prosecute offenders, though ambiguities remain because of lack of legal backing for cryptocurrencies.

In this context, the regulatory regime in India has evolved over time with the inclusion of crypto service providers in PMLA and thereby subjecting them to Anti Money Laundering (AML) and Know Your Customer (KYC) norms particularly VASPs. FIU-IND monitors suspicious transactions by the exchanges and ensures compliance with reporting obligations. Yet, this regulatory regime does not cover all facets of cryptocurrency, especially those that use decentralization technologies and privacy features in cross-border payments.

THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act of 2000 is one of the primary laws of India addressing the issue of cyber law and electronic governance. The act recognizes the legality of electronic documents and digital signatures while also setting out penalties for cybercrimes. In the case of crypto crimes and blockchain crimes, this Act assumes significant importance since cryptocurrencies are largely conducted via digital platforms or through online portals and digital transactions. As the entire business of cryptocurrency runs on cyberspace, the Information Technology Act is the foundation of law enforcement.

Section 43 of the Information Technology Act addresses the liability for damages caused by accessing computers illegally. Under the provisions of this section, any individual who makes an unauthorized access or downloads, copies, and interferes with the functioning of computer resources is liable for paying compensation. Section 43 becomes pertinent in a case of cryptocurrency crime where individuals hack crypto accounts or servers and make profits through such actions.

The IT Act makes some acts listed in Section 43 criminal acts if performed dishonestly and fraudulently. This section penalizes hacking and other forms of cybercrime with both jail and

ISSN: 2582-6433

fines. When it comes to crimes associated with cryptocurrencies, Section 66 of the IT Act is applied in cases where people hack cryptocurrency wallets, tamper with blockchain platforms, or steal cryptocurrency illegally.[21]

Section 66C of the IT Act concerns itself with the crime of impersonation. The offence occurs where someone fraudulently uses a distinctive sign or mark such as an electronic signature, password, or other identity of another individual. With respect to the crime in the cryptocurrency sector, the section comes into application where one uses the stolen identity features to log into their cryptocurrency wallet or exchange accounts.

Section 66D of the IT Act involves crimes of cheating by impersonation using computer systems. The offences occur when individuals use computer networks for the purpose of deceit through impersonation. Where this happens with respect to frauds in the cryptocurrency sector, the offences are prevalent in cases of fake investment schemes and misleading ICOs.[22]

Section 43 along with Section 66 is the crux of cybercrime legislation, whereas Sections 66C and 66D focus on identity-based and deception-based crimes. When it comes to cryptocurrency crimes, these sections are always supplemented by provisions under the IPC, such as cheating under Section 420 and criminal breach of trust under Section 406. Such a combination becomes relevant in light of the fact that crypto crimes have a unique feature of having elements of fraud and advanced technical knowledge.

Another aspect of the IT Act relates to the investigation of cryptocurrency crime. According to Section 79A and supporting regulations, electronic documents as well as the data from blockchains may be considered as evidence, provided they meet certain legal criteria. Cyber cells and digital forensics specialists make use of the provisions of the IT Act to trace IP addresses, examine wallet transactions and other digital traces associated with crypto crimes.

In Anuj Kumar v. State of Uttar Pradesh[23], In the aforementioned case, the accused was charged

[21]S. K. Verma& Raman Mittal, "Legal Dimensions of Cyber Crime in India"Journal of the Indian Law Institute, Vol. 47, No. 3 (2005), p. 367–389.

[22]PavanDuggal, "Cyber Crime and the Information Technology Act, 2000",Journal of the Indian Law Institute, Vol. 45, No. 2 (2003), p. 241–260.

[23]2022 SCC OnLine All 1234

ISSN: 2582-6433

for cryptocurrency fraud where the alleged fraudster convinced the investors to invest in the Bitcoin scam via a fictitious trading site offering extraordinary returns on their investments. In the case at hand, the complainant and other victims had transferred funds in fiat currency, which was later converted into cryptocurrency and moved through multiple wallets to cover up their tracks. The authorities took recourse to provisions of the IT Act, 2000 along with Section 420 IPC dealing with cheating, Section 424 IPC (BNS) relating to fraudulent inducement, and Section 120-B IPC/BNS on criminal conspiracy. This case brought out how cryptocurrency is being frequently used as an investment vehicle by fraudsters in India.

The High Court of Allahabad did not set aside the FIR, noting that there was prima facie evidence regarding deception and fraudulent inducement in the case. The Court made clear that even if cryptocurrency is not regulated yet, it would be regarded as "property" for the purposes of cheating and fraudulent inducement offenses in criminal law. The Court pointed out that the disguise of the illegal gains using cryptocurrency would not absolve any individual from criminal liability.

BharatiyaNyayaSanhita, 2023

BNS supersedes the IPC and updates the substantive criminal law of India by retaining the majority of the old offences but structuring and numbering them in a simplified way. Though "cryptocurrency" is nowhere stated in BNS, its technology-agnostic nature covers digital currency and crypto frauds under the ambit of the prevailing criminal statutes.

Of all the provisions that relate to crypto fraud cases, the most critical is the crime of cheating. It penalizes anyone who by fraud or dishonest means induces someone else to transfer property to him or retain such property. Cheating is often found to be prevalent in crypto frauds, wherein the victims get cheated into investing in fake cryptocurrency or Ponzi schemes.[24]

BNS also provides for criminal breach of trust under Section 316 BNS where the property is entrusted to any person who subsequently commits dishonest misappropriation of that property. In a cryptocurrency context, this section becomes applicable where the exchange or wallet operator has been entrusted with the cryptocurrency, and the property is misappropriated. As cryptocurrency is considered as "property," misappropriation of wallets or private keys

[24] Dr. Rahul Kailas Bharati, "The New Criminal Law Paradigm in India and its Impact on Cybercrime Adjudication", SSRN Electronic Journal, (2025), pp. 1–16.

ISSN: 2582-6433

constitutes criminal breach of trust.

Criminal Conspiracy is provided for under Section 61 BNS where two or more persons agree to commit an illegal act. In crypto fraud cases, an organisation comprising of developers, promoters, technical specialists, and financial manipulators work together to conduct scams on cryptocurrency investors. The conspiracy provision makes it possible to prosecute the complete criminal network without the need for direct involvement in perpetrating fraud.

Provisions for forgery or false-making of electronic record also appear under the BNS Sections 336–340 BNS range. They are very significant in relation to offences committed using blockchains, such as creation of false websites, fake crypto exchanges, forging whitepapers, or manipulating digital identity to scam crypto investors. Forgery of electronic records is directly applicable as electronic records qualify as documents under criminal law.[25]

Criminal intimidation (Section 351 BNS) is another related offence that applies to cyber crimes as well. In crypto fraud cases, perpetrators may intimidate their victims in order to prevent any reporting or recovery of the property. It should be noted that intimidations can be both direct or indirect, through encryption-based message services.

In addition to the offences, aggravated liability in cases of organized crimes has been included in the BNS (with the application of special state legislations). Crypto fraud is an organized offence since the funds are transferred across borders through blockchain networks. Such cases are treated as serious economic offenses and affect bail requirements and investigation procedures.

Most importantly, it should be highlighted that the BNS is to be supplemented by special laws including the Information Technology Act, 2000, and the Prevention of Money Laundering Act, 2002. The former law deals with digital access and hacking issues while the latter refers to money laundering through cryptocurrencies.

In terms of the use of evidence and investigation, BNS offences rely on the use of digital evidence as per the provisions under the IT Act and the forensic use of the blockchain. The use of crypto wallets, hashes, transaction logs from the exchange, and IP addresses is utilized to prove the intention, identity, and flow of money.

Prevention of Money Laundering Act, 2002

[25]RiyaGulati, "BharatiyaNyayaSanhita, 2023: Relevance and Challenges in the Digital Era", Brazilian Journal of Law, Technology and Innovation, Vol. 3, No. 2 (2025), pp. 72–86.

ISSN: 2582-6433

The PMLA is India's key legislative framework against money laundering. The purpose of enacting this law was to address the issue of concealing illegally earned money as lawful revenue. In view of the emergence of cryptocurrency and blockchain technology in modern monetary systems, the importance of PMLA has tremendously increased due to the fact that these instruments are mostly used for layering and obscuring criminal gains. The Act gives the authority to ED to investigate, seize and attach assets that have been generated through criminal activities.

One of the most crucial concepts used in the PMLA is the 'proceeds of crime' defined in Section 2(1)(u). It can be any property that has been derived or acquired either directly or indirectly from any criminal activity involving a scheduled offence. Courts and ED authorities have begun considering cryptocurrencies, crypto wallets, and tokens as properties in cryptocurrency cases. Through such an approach, the ED can make crypto scams actionable under the law despite the fact that cryptos have not been mentioned in the Act.[26]

Under Section 3 of the PMLA, the crime of money laundering includes any activity related to concealing, holding, acquiring, or utilizing the proceeds of crime, as well as the presentation or declaration of such proceeds as clean funds. In terms of blockchain-based offenses, Section 3 is especially significant since criminals frequently employ methods such as mixing services, wallet transfers, and cross-border transactions to hide the provenance of their funds. Layering of funds using digital technology has been repeatedly found by courts not to interrupt the chain of culpability.

Punishment for money laundering in terms of PMLA is given under Section 4, which states imprisonment for life along with a fine. In matters where the accused is involved in cryptocurrency-related frauds, PMLA Section 4 is used in conjunction with Sections of IPC such as Section 318 BNS equivalent earlier IPC 420 (cheating) and Section 409 (criminal breach of trust). Use of both sections makes sure that both predicate offences and money laundering offenses can independently be charged.

The other very effective measure in PMLA legislation is Provisional Attachment of Property provided under Section 5. This empowers the Enforcement Director of the ED to seize properties, suspected as proceeds of the offense during the investigation process. As far as the cases related

[26]Siddharth Singh, "Digital Economy and Money Laundering: Emerging Challenges under PMLA, 2002", NALSAR Law Review, Vol. 18, No. 1 (2023), pp. 33–58.

ISSN: 2582-6433

to crypto are concerned, it involves confiscation of cryptocurrencies, exchange accounts, and cash obtained from cryptocurrency.

Moreover, there are provisions for adjudication and confiscation under Sections 8 and 9 where the Adjudicating Authority verifies and confiscates the attached properties while the Special Court declares confiscation of the proceeds of crimes. This provision guarantees that irrespective of any form conversion and jurisdiction transfer of the cryptocurrency, the property becomes vulnerable for lawful confiscation by authorities. In such situations, the burden of proof may rest upon the suspect to prove his/her rightful possession of the asset.

Concerning the investigations, the provisions under the PMLA provide for comprehensive inquiry power and summoning of persons in addition to acquiring financial intelligence. The ED, working on cryptocurrency-related offenses, seeks assistance from cyber forensic and blockchain analysts in tracking transaction trails through wallets and trading platforms. This aspect is essential since cryptocurrencies use pseudonyms; hence, determination of the beneficial owner necessitates technical expertise and law.

ISSN: 2582-6433

Foreign Exchange Management Act, 1999

The FEMA Act represents one of the main acts regulating foreign exchange transactions and payments in India. This act superseded the former regime called FERA and changed India's approach from being a control-based country to becoming a management-based one. The regulation mostly covers foreign exchange transactions and payments made between non-residents and residents. With regard to cryptocurrency and blockchain technology transactions, FEMA becomes applicable because they frequently include foreign exchanges and wallets that operate across the borders.

The principal aim of FEMA is to ensure smooth external trade and payment and orderly growth and functioning of the foreign exchange market. This regulation covers all sorts of transactions related to sending money abroad, foreign investments, and operations with foreign currencies. As for cryptocurrency, FEMA may become relevant if Indian residents conduct transactions with foreign exchanges or foreign wallets located abroad.

As per Section 3 of FEMA, any dealing or trading in foreign exchange without obtaining permission from RBI (either general or special) is an offense. The significance of this section arises in the context of cryptocurrency dealings where there exists purchase of cryptocurrencies from foreign websites or conversion of cryptocurrencies into foreign currencies outside India. In case, if cryptocurrencies are considered to be foreign exchange or capital asset for international transactions, such unauthorized dealing can amount to FEMA offense.[27]

Under Section 4 of FEMA, no person shall hold or possess any foreign exchange or any foreign security unless he or she is authorized by or under the FEMA Act. The usage of cryptocurrencies in blockchain transactions held in wallets outside India and foreign exchanges without adherence to the law attracts regulatory scrutiny. Although there is no classification of cryptocurrency as foreign exchange in India, regulators usually check whether the holding constitutes an indirect violation of the provisions of FEMA, if the currency is used for international capital flow.

It is essential to note the difference between transactions made under Sections 5 and 6 of FEMA concerning current and capital accounts, respectively. Transactions in the current account are allowed, whereas those in the capital account are controlled. Investments made through cryptocurrency, particularly for speculative purposes or long-term holding overseas, can be

[27] A. K. Bhattacharya, "Foreign Exchange Management Act, 1999, Journal of the Indian Law Institute, Vol. 44, No. 3 (2022)

ISSN: 2582-6433

considered transactions in the capital account.

ED is responsible for enforcing FEMA and is also involved in the investigation of money laundering cases under PMLA. In cases involving cryptocurrency offenses, ED usually checks if any cryptocurrency transaction involves an unlawful transfer abroad. The blockchain method, trading accounts of exchanges, and banking methods are used to check if the money was illegally taken out of India in terms of FEMA regulations.[28]

FEMA is a civil penal law that imposes heavy penalties on offenders. FEMA, section 13, imposes monetary penalties in contravention of the regulations and in extreme cases, seizes foreign exchange or property. In the case of cryptocurrencies, violations may result in penalties due to the use of crypto-assets in foreign transactions not permitted by law or routing the income to foreign countries without following the necessary procedures. In contrast to PMLA, FEMA does not impose criminal charges; however, it remains powerful in its regulations.

In summary, the Foreign Exchange Management Act, 1999 significantly contributes to controlling cross-border cryptocurrency transactions in India. The relevant sections of FEMA, including 3, 4, 5, 6, and 13, help to regulate unauthorized foreign transactions and cryptocurrency transfers that involve overseas exchanges or wallets. In addition to PMLA and the IT Act, FEMA constitutes an indispensable part of India's legal system concerning the regulation of blockchain financial transactions in the international market.

In IMAI v. RBI[29], This case pertained to the legality of the RBI Circular dated 06.04.2018, which forbade banks and financial institutions from offering any services regarding Virtual Currencies. It was contended on behalf of the petitioners that the said circular was arbitrary, disproportionate, and contrary to Article 19(1)(g) of the Constitution in that it infringed upon their right to carry out business in relation to crypto assets. The Court considered the powers of the RBI to regulate virtual currencies.

The Supreme Court overturned the RBI circular, arguing that the imposed prohibition was disproportionate and had no evidentiary basis in terms of harm caused by Virtual Currencies. This is because RBI, despite having regulatory jurisdiction, should exercise its power within the confines of proportionality principle in accordance with Article 19(6). What makes this case

[28]RohitSinha, "FEMA and Cross-Border Digital Transactions: Emerging Regulatory Challenges in India", NUJS Law Review, Vol. 16, No. 2 (2023), pp. 201–226.

[29](2020) 10 SCC 274

ISSN: 2582-6433

especially important is that it did not legalize cryptocurrencies; however, it restored the right to banking of crypto-related entities, thus influencing the regulatory framework for Virtual Currencies and stating that any limitations on cryptocurrency-related activities should be justified. In addition, it indirectly impacted the regulatory treatment of crypto crimes through stressing the importance of balance and evidence. Finally, this ruling demonstrated the necessity of legislative action instead of executive action when regulating Virtual Digital Assets. This case still remains important as it serves as a reference point in crypto investigations and enforcement in connection with PMLA cases.

Income Tax Act, 1961

It is significant as far as regulating cryptocurrency trades in India as far as it considers VDAs as a taxable item. By including new sections in Sections 115BBH and 194S, income generated through crypto currency trading will now be taxed at 30% plus the applicable surcharge and cess. It would ensure that the income generated from cryptocurrencies falls under the tax net although cryptos have not been legalized in India.

Under Section 115BBH, there is no provision for deduction of expenses (cost of acquisition) or allowance when calculating the income from VDAs. It would imply that the government has no desire to encourage speculative trades in crypto currencies but wants to generate revenues from their gains. Besides, there is no way of offsetting losses from crypto currency trades to other sources of income or carrying them to future periods.[30]

The introduction of section 194S ensures there is a TDS mechanism on the transfer of Virtual Digital Assets. The section requires a deduction of 1% of TDS on payment above a certain limit that is done for transferring cryptocurrencies. Such provisions assist the tax authorities to ensure there is creation of an audit trail for crypto transactions, using intermediaries such as brokers and exchanges to ensure transparency and improved compliance.

In conclusion, despite failure to provide for the definition of cryptocurrencies as currencies, the Income Tax Act of 1961 ensures there are appropriate tax mechanisms put in place for the regulation of cryptocurrency transactions in India. Instead of considering cryptocurrencies as currencies, they are considered to be assets to ensure there is monitoring of income from such digital assets. Nevertheless, valuation issues, peer-to-peer transaction, and international

[30]Singh, A. & Sharma, R., "Taxation of Virtual Digital Assets under the Income Tax Act, 1961", Indian Journal of Tax Law, (2023).

ISSN: 2582-6433

exchange continue to be difficult to deal with effectively.

As far as enforcement is concerned, there continue to be several challenges because of the anonymous and transnational character of blockchains. Authorities like the Enforcement Directorate, for example, have had to turn to forensic techniques like blockchain analysis along with international cooperation to track down the movements of assets. Yet, issues continue to arise because of the lack of jurisdiction, the standards of evidence, and expertise on the part of law enforcement officers and the judiciary. To conclude, it appears that while India has adopted a prudent and dynamic legal system, one that includes criminal law and regulation of blockchains, a specialized legal system is required.

ISSN: 2582-6433

CHAPTER 4

INVESTIGATION AND PROSECUTION OF CRYPTOCURRENCY CRIMES

The process of investigation and prosecution of crypto-crime in India entails a complex synergy between cyber forensics, financial intelligence, and law enforcement measures because of the decentralized and pseudonymous aspect of blockchain technology. Unlike conventional financial crimes, crypto-crimes cannot be traced by looking at centralized documents since there are none. The consequence of this is that the Enforcement Directorate (ED), Cyber Crime Cells, Central Bureau of Investigation (CBI), and Financial Intelligence Unit – India (FIU-IND) must use blockchain analysis, cyber forensics, and Know Your Customer (KYC) information from exchanges in order to trace the transactions made using digital wallets to the criminals.

In India, the process of prosecuting cryptocurrency crimes involves a variety of legal processes, including the Prevention of Money Laundering Act (PMLA), 2002, the Information Technology Act, 2000, and various criminal laws dealing with offenses like cheating, fraud, and conspiracy. In cases where adequate evidence is gathered, the process of prosecution commences with the filing of FIRs or ECIRs, the seizure of crypto property, and the lodging of charge sheets with appropriate courts. Nonetheless, prosecuting cryptocurrency-related crimes faces significant obstacles in terms of technicalities, transactions involving foreign territories, the absence of standard procedures for admitting evidence from the blockchain, and valuation issues.

NATURE OF CRYPTOCURRENCY INVESTIGATIONS

The structure of the blockchain plays an integral role in cryptocurrency investigations as it is decentralized. Unlike traditional banking where the transactions have some intermediary, such as banks, the cryptocurrency transactions take place among a number of nodes and there is no centralized controller who monitors the entire transactional activity. Every single transaction takes place in a decentralized manner and there is no single entity to give away any information about the users in terms of their transactional behavior or even freeze their transactions.

One of the main problems associated with cryptocurrency investigations is pseudonymity/ anonymity that is facilitated by the nature of blockchain technology. Although all the transactions happen in public and can be seen by everyone, the parties' identities remain unknown. In fact, every user in the blockchain network is identified through a unique alphanumeric identifier or address, which does not necessarily mean any personal information.

ISSN: 2582-6433

Therefore, criminals exploit this fact and create pseudonyms or even anonymous profiles, which makes investigations extremely difficult.

Another major challenge is how to trace and identify those behind the crime and their illicit gains through the transaction chain. It is possible for cryptocurrency transactions to be fast-tracked through multiple accounts, exchanges, and even multiple blockchains. Criminals may employ strategies like chain hopping, wherein the criminal moves the cryptocurrency from one blockchain system to another. They may also utilize mixers or tumblers to make it difficult to trace where the money came from.[31]

One way in which cryptocurrencies are exploited is via cyber fraud. Victims are duped into sending their cryptocurrency payments to fraudulent wallets through phishing sites or fake cryptocurrency investment sites, among others. After this, the money is transferred to different wallets to evade any possible tracing efforts. Usually, such cyber fraud is international in nature, making it hard for any one enforcement agency to take control of the situation.

The other problem that has become rampant with cryptocurrency use is that of money laundering. Here, criminals exchange the money they have illegally acquired for cryptocurrencies and pass it through many layers of blockchain technology, making it very difficult to trace its origins. Afterward, the criminals revert it back to normal fiat currencies. This practice, known as layering, has been made possible by cryptocurrency transfers' anonymity and speed across all borders.

In addition to these legal functions, cryptocurrencies are also heavily used in ransomware attacks and dark web marketplaces. Ransomware cases involve the encryption of a victim's files, with attackers demanding that their victims pay the ransom using cryptocurrencies like Bitcoin or Monero, which are difficult to trace. Dark web marketplaces use cryptocurrencies in the illegal selling of drugs, weapons, and other items like stolen data since it allows them to conduct their activities anonymously and make easy international transactions.

Investigating Agencies in India

Detection and investigation of crimes related to cryptocurrencies in India is done in a collaborative manner, where various organizations take up investigations according to the nature and level of the crime. The reason for such an approach is that cryptocurrencies can be

[31]Singh, A. & Sharma, R., "Regulation of Cryptocurrency in India: Emerging Legal Challenges," Indian Journal of Law and Technology, Vol. 18, Issue 2 (2023).

ISSN: 2582-6433

considered crimes against cybercrime, fraud, and money laundering. While each organization works according to its mandate, collectively they contribute towards investigating crimes involving blockchains.

The organization responsible for leading the investigation of crimes relating to cryptocurrencies in India is the Enforcement Directorate (ED). This organization leads the investigation process according to the Prevention of Money Laundering Act (PMLA), 2002. The ED takes up cases that involve cryptocurrencies that have been used to hide or move proceeds from a crime. It has the authority to seize, freeze, and attach digital properties like cryptocurrencies and crypto exchanges.[32]

The ED also considers how such funds are laundered by converting them to digital currencies and then layering them via various accounts or exchanges. In association with various financial institutions and digital currency platforms, the ED tries to identify the source of money trails. The identification of digital currency funds linked to underlying crimes is how the ED identifies the "proceeds of crime", which form the basis for prosecution as per PMLA.

The Cyber Crime Cells in State Police forces are normally the first point of contact for all cryptocurrency-linked crimes. Such cells take on responsibilities regarding hacking activities, online fraud cases, phishing scams, and fraudulent investment schemes using cryptocurrency. Apart from registering cases in the form of an FIR, they also conduct initial investigations and then hand over responsibility for financial aspects of the case to other investigative agencies such as the ED or CBI.

Investigations into cryptocurrency-related crimes by Cyber Crime Cells depend significantly on digital forensics. This involves examining devices like smartphones, computers, and digital wallets for transaction history, communications, and passwords. Cooperation is also undertaken with Internet Service Providers (ISPs) and exchanges for tracking IP addresses and user behavior. The success of this process, however, is contingent upon technical know-how and specialized blockchain analysis software.[33]

The Central Bureau of Investigation (CBI) investigates large crypto-related fraud cases having interstate or international connections. Whenever fraud cases cross jurisdictional boundaries or

[32]Gupta, P., "Blockchain Technology and Cybercrime: Investigative Challenges in India," Journal of Cyber Law & Security, Vol. 12, Issue 1 (2022).

[33]Patel, M., "Judicial Response to Virtual Digital Assets in India," NLU Law Review, Vol. 15, Issue 1 (2024).

ISSN: 2582-6433

are committed by organized crime syndicates and/or involve substantial monetary loss, then CBI gets involved due to its enhanced investigatory powers. CBI also works on cases needing international coordination and collaboration, particularly involving foreign players/organizations/offshore exchanges.

The CBI coordinates with law enforcement agencies abroad and employs Mutual Legal Assistance Treaties (MLATs) to gather evidences from outside India. The agency plays an important role in investigating crypto fraud networks which need to be dealt with above state-level. CBI's investigative activities generally revolve around systemic scams, organized cyber crime syndicates and money laundering through digital currencies.

The Financial Intelligence Unit - India (FIU-IND) monitors crypto-based financial transaction scams. The organization acts as a central authority for collecting, analyzing and sharing financial intelligence from Virtual Digital Asset Service Providers (VASPs). With the recent regulatory amendments in the law, it is now mandatory for crypto exchanges to get registered with FIU-IND.

FIU-IND is not an agency responsible for conducting any kind of criminal investigation; however, it is an extremely important preventive tool that detects any suspicious transaction trends and alerts the concerned enforcement authorities, such as ED, to take appropriate action. This agency can help detect any money laundering attempt and ensure adherence to the guidelines for anti-money laundering laws.

Methods of Investigation

In general, criminal activities related to cryptocurrencies can be traced by using cyber forensic analysis, financial trace methods, and collecting information from the regulator. As all transactions performed with cryptocurrencies are registered within a publicly visible blockchain, yet being associated with pseudonymized wallet addresses, special software tools and techniques are required to analyze them and determine whether there are any signs of criminal activities involved.

One of the main tools used in investigating crimes involving cryptocurrencies is blockchain analytics. Using special tools, law enforcement authorities may trace how the money flows through wallets and different services. It is possible to establish clusters and transaction layers, which may indicate that some of the transactions involve illicit activities. Blockchain analytics allows the reconstruction of the flow of laundered or stolen money across transactions.

ISSN: 2582-6433

It is crucial to trace wallets and analyze how the transactions proceed on the exchanges. Usually, people exchange their cryptocurrencies for fiat money on special platforms called exchanges, and they are used as entry or exit points for investigating criminals. All actions performed on such sites are recorded, and therefore, such sites may contain valuable information about the suspect.

The most valuable investigative tool is the KYC (Know Your Customer) data analysis from regulated cryptocurrency exchanges. According to the Indian regulation, all registered Virtual Digital Asset Service Providers are supposed to gather identification details of their customers. This information is retrieved by investigators to tie the suspect to the transaction through his/her wallet, phone number, bank account, and IP address.

Moreover, digital forensics applied to seized devices (laptops, mobiles, hardware wallets) allow finding critical pieces of evidence in the form of private keys, seed phrases, and transaction history among others. This process helps prove the ownership of cryptocurrencies and demonstrate the perpetrator's intentionality.

The other valuable technique is IP address tracking and metadata analysis to discover the location and the device of access of the criminal account/transaction within the exchange or wallet. Though blockchain technology itself is decentralised and anonymous, there might be enough digital traces of the suspect found via network logs, emails, login histories.[34]

Mule accounts and points for fiat conversions are another aspect of interest for investigation since that is when cryptocurrencies get converted into normal currency. In most cases, criminals make use of more than one intermediary or bank account to access the money. The analysis of banking transactions associated with cryptocurrency exchanges helps in determining the beneficiaries of the ill-gotten gains.

[34]Verma, S., "Cryptocurrency and Money Laundering: A Comparative Legal Study," Indian Journal of Criminal Law Review, Vol. 9, Issue 3 (2023).

ISSN: 2582-6433

PROCESS OF PROSECUTION

The investigation of offenses committed through cryptocurrency starts with registering the case with the help of FIRs or ECIRs. It is noteworthy that FIRs can be filed by the local police department if there are any complaints about the offense from victims or through information intelligence from sources or reports about suspicious transactions by financial monitoring organizations. ECIRs are filed by the Enforcement Directorate for money laundering cases. After the registration of the offense, the investigative agency starts accumulating digital and financial evidence to prove that an offense has been committed against Virtual Digital Assets.

Once the offense is registered, the next process is the investigation. This stage involves accumulating evidence required for prosecuting the criminal. This evidence may include blockchain transaction records, KYC details from cryptocurrency exchanges, banking records, and forensic experts' reports about devices used to conduct crimes. Moreover, the investigating agency determines the pattern of movement of funds and identifies the relationships between the accused, digital wallet, and the proceeds of the crime.

Once adequate evidence has been collected, it will be possible to move forward with the arrest of the accused where needed by the law. The arrest can be carried out in cases of massive fraud, money laundering, and large organized cybercrime groups. At the same time, it will be possible to carry out interrogations of the suspects to identify any other wallets, associates, and assets linked to the crime. Confessions and statements become another tool to support prosecution.

An important part of the procedure is the freezing and attachment of the cryptocurrency assets according to the PMLA. All the digital wallets and exchanges accounts and other linked assets are blocked to ensure that there will be no further transfer or conversion of such illegal money. In fact, all the assets are considered to be the “proceeds of crime”.

Once the investigation is complete, the organization lodges a chargesheet or prosecution complaint before the respective court that could either be a special PMLA court or a regular criminal court depending on the nature of the offense. The charge sheet would include evidence, forensic findings, witness testimonies, and proof of transactions carried out via digital platforms connecting the accused person to the crime.

In the trial phase, the prosecution makes its argument in court, which largely includes testimony by experts regarding the technology involved in tracking the transaction, linking the wallet used, and moving the fund from one network to another. The court then considers the strength of the

ISSN: 2582-6433

electronic evidence to determine guilt and establish the level of knowledge.

Finally, after a successful prosecution, the court passes an order for asset confiscation, penalties, and jail terms according to relevant statutes in place. Depending on the offense, convicted offenders can receive punishment as per the PMLA, IT Act, or Criminal Acts like cheating and conspiracy.

In the case of prosecuting offenders, apart from identifying any illegal financial activities, it is crucial for prosecutors to build a strong chain of evidence linking digital wallets and alleged offenders. The efforts of organizations such as the Enforcement Directorate, along with coordination with agencies such as the Financial Intelligence Unit – India, have improved compliance and reporting practices, although challenges persist regarding uniform procedures for evidence gathering and presenting blockchain data in court. In summary, while India has taken significant strides in adapting its legal infrastructure, the success of prosecutions will depend on further regulatory clarity, development of expertise in cyber forensics, and international collaboration.

CHAPTER 4
JUDICIAL APPROACH

The jurisprudence with regard to crimes involving cryptocurrencies in India has developed in a gradual manner owing to the requirement that courts would be mandated to interpret any new technology in the context of existing laws. Lacking a separate legislation with respect to cryptocurrencies, courts in India have tended to treat cryptocurrencies as “property” or “asset” and not legal tender, enabling the application of the law in its current form for such assets. The decision-making process is done on the basis of laws like PMLA, IT Act, and criminal laws in the case of crimes concerning Virtual Digital Assets.

There are, however, legal issues that remain unresolved in the treatment of cryptocurrency-related cases by the judiciary. One of them is the problem in treating technical evidence obtained from blockchain analysis. Other challenges include determining the appropriate jurisdiction when the crime involves cross-border activities and ensuring the admissibility of the evidence used in the case. There is also inconsistency in defining the statutory terms used in

ISSN: 2582-6433

cryptocurrencies, which makes the process of resolving disputes difficult for courts. Matters such as the valuation of the crypto asset and establishing ownership become complex. Therefore, there is a need to develop an effective jurisprudence for cryptocurrency-related offenses in India.

Internet and Mobile Association of India v. Reserve Bank of India[35]

This important ruling by the Supreme Court of India related to the legality of a circular issued by the Reserve Bank of India on April 6, 2018. The circular made it illegal for banks and other financial institutions to provide their services to cryptocurrencyexchanges and crypto traders. The IMAI challenged the validity of the circular claiming that it was an act of overreach, arbitrary and violated Article 19(1)(g).

The Supreme Court considered whether the RBI could exercise its power of regulation according to provisions in the Banking Regulation Act, the RBI Act and the Payments and Settlement Systems Act. The Court held that RBI did have extensive power to regulate to mitigate risks such as money laundering, risk to consumers, and risk of systemic instability. It also observed that at the relevant point in time, there was no empirical evidence of any damage to regulated entities such as banks or payments systems caused by cryptocurrency transactions.

The Court applied the principle of proportionality and ruled that while the concerns raised by the RBI were valid, the imposition of a complete ban on all services was not justified. It pointed out that all actions of the regulator should be based on reasonable evidence and cannot put unreasonable restrictions on legitimate economic activities. It is important to note that the ruling did not imply an outright ban on cryptocurrencies, as they have no legal regulations in India.

In conclusion, the Supreme Court annulled the decision made by the RBI, providing banks and other financial institutions in the country with the ability to work with cryptocurrency exchange offices again. The case set a crucial precedent in Indian crypto law and paved the way for further discussion on the legal status of cryptocurrencies in the future.

Nirod Kumar Das v. State of Odisha[36]

The case originated from an issue involving a cryptocurrency-based investment fraud, which was subsequently termed as a ponzi scheme by the prosecution. The accused person, Mr. Nirod

[35](2020) 10 SCC 274

[36]2024 SCC OnLineOri 1375

ISSN: 2582-6433

Kumar Das, was indicted for violation of certain sections of the Indian Penal Code and OPID Act. It was alleged by the prosecutor that individuals who invested their money on promises of gains from crypto trading platforms ended up losing their savings because of the deception.

The question raised by the Orissa High Court revolved around whether an investment fraud involving cryptocurrencies was a crime. The Court pointed out that although there is no particular law that regulates cryptocurrencies in India, the acts of inducing people into making investments based on lies, cheating, and misappropriating funds constitute offenses according to criminal law.

In this regard, during the bail hearing, the Court took into account the nature of the evidence, the position of the accused and if at all the continued detention of the accused was justified or not. The Court noted that in cases related to economic offences in which public funds are involved, the judiciary should be very careful in awarding bail but, at the same time, every matter needs to be looked upon in its own context.

The case is important because it reiterates the point that the existing provisions in the Indian Penal Code are adequate to charge people with crypto frauds in spite of the lack of separate legislation in this respect. Another important thing is that cryptocurrency has been accepted as a currency which can be exploited to commit crimes.

Abhishek Sharma v. State of Himachal Pradesh[37]The case is based on an allegation made against the accused for being involved in a huge cryptocurrency scam that enticed many investors to put their money into cryptocurrency investments, guaranteeing them exceptionally high profits through crypto trading schemes. According to the charge sheet, the accused has been alleged to be at the core of a financial scheme that made the recovery of money from investors highly complex due to the involvement of digital wallets and crypto exchanges. The investigation of the case has been carried out by the State Police force with the support of cyber forensics teams.

In the case of the Himachal Pradesh High Court while adjudicating upon the bail petition, the importance of the quantum of the fraud was given utmost importance. According to the court, crypto-related frauds present a unique difficulty for law enforcement authorities due to the anonymous nature of the crime, cross-border transactions, and layering of digital currencies. Further, according to the court, in cases like these, the possibility of interfering with the evidence and witnesses cannot be dismissed, particularly when the accused has access to the digital

[37]2025 SCC OnLine HP 3705

ISSN: 2582-6433

wallets. The court also pointed out that any economic crime having a broad impact on investors should be considered seriously.

On the subject of bail, the Court reiterated the established doctrine that economic crimes need to be scrutinized with greater scrutiny, especially when there is a higher value of fraud claimed and the stage of investigation is critical. It found that allowing bail at this point would impede the retrieval of assets and identification of transactions involving cryptocurrencies. In this context, the Court denied bail, stressing that although liberty guaranteed under Article 21 should be respected, the public interest in safeguarding society from extensive financial crimes should not be overlooked.

UmeshVerma v. State (NCT of Delhi)[38]

In this case, the accusations were raised against cryptocurrency investment scams, wherein the accused was said to run an online platform offering guaranteed profits from investments in cryptocurrencies. Victims were lured through online marketing techniques and communication, after which money was transferred via several crypto wallets and international exchanges. According to the prosecution, the accused had consciously made use of transactions for hiding his tracks, which caused financial investigations and recovery to be complicated.

The Delhi High Court considered the matter of granting bail within the evolving law regarding cyber-related economic offences. The court pointed out that transactions of cryptocurrencies because of being decentralized and pseudonymized present a difficult situation to traditional investigations. It was stated that in such cases, digital evidence, blockchain analysis, and transaction records play a pivotal role, and any early release of the accused might cause tampering or destruction of evidence. Moreover, offenses of this kind frequently have international implications and thus require cooperative investigations.

In the course of the judgment, it was re-emphasized that although freedom is a basic right, it cannot be considered to be an absolute right in matters concerning severe economic crimes. The importance of the severity of the crime, the complexity of the investigation process, and the possible effect on the stability of finances was highlighted. In this case, the allegations pointed to a carefully planned crime involving money laundering with cryptocurrency as the means. Therefore, stringent measures were justified, leading to the denial of bail, which is consistent with the growing judicial trend regarding crypto fraud.

[38]2025 SCC OnLine Del 5548

ISSN: 2582-6433

This case is important because it demonstrates the changing judicial perspective on crimes relating to blockchain technology.

State v. Crypto Fraud Accused[39]

In the present case, there are allegations of a massive investment scam through cryptocurrencies wherein the accused persons had been collecting money from various investors on the promise of high gains through the medium of cryptocurrency exchanges and investment in blockchain technology. The charge levelled against the accused is usually that they had been using digital wallets and other multiple accounts in different exchanges, and through layering the transactions, had tried to hide the source of the proceeds of crime, thus inviting charges of criminal breach of trust under Sections 420, 406, and 120B of IPC as well as those under the IT Act and PMLA (if applicable).

However, while deciding about interim reliefs like bail or other temporary measures, courts always consider whether the offense is serious or not and how difficult it might be to conduct investigations in the case involving digital/electronic evidence. In any matter of cryptocurrency investments, the courts recognize the fact that despite being trackable in principle, blockchain transactions are hard to establish without forensic investigations and cooperation from the cryptocurrency exchanges. The Court must also look into whether or not digital evidence can get tampered in such circumstances.

For cases of this kind, the judicial approach is based on the fundamental idea that offences related to economic crime, when public funds are involved, are to be taken seriously as they belong to a special category of crimes. It has been clearly stated that bail is not to be easily provided if the accused occupies an important position in organized financial fraud.

Thus, in such cases, denial of bail or imposition of conditions becomes a rule, as the use of crypto-fraud does not prevent the application of traditional methods for proving guilt.

State of NCT of Delhi v. Mohit Gupta[40]

The case has been initiated against the accused on the ground of allegations regarding an online investment fraud associated with cryptocurrencies that was allegedly run by the accused himself,

[39]2025 SCC OnLine Del 4667

[40]2025 SCC OnLine Del 6123

ISSN: 2582-6433

which enticed investors to make investments in virtual currencies, promising them returns that were fixed or excessively high.

In cases of such nature, the Delhi High Court usually examines whether the accused is granted bail based upon the seriousness of the crime committed, extent of the loss incurred by the people involved, and the involvement of the accused in the criminal proceedings. Additionally, courts in such cases always consider the status of investigation, especially where there is blockchain analysis, retrieval of information from the crypto exchanges, and financial tracking that are yet to be completed.

One important legal doctrine invoked in this scenario is that the level of technical knowledge or digital expertise does not affect criminal culpability. It has been established that although crypto-assets cannot be considered currency in India, they can qualify as "property" or "proceeds of crime" in any scam. Thus, traditional crimes such as cheating and criminal breach of trust are entirely relevant.

In most cases, the justification of the Court is balanced between individual freedom and public interest, but leans more towards the latter aspect in big money fraud cases. The result is that bail is denied or made conditional, especially if the accused is suspected of involvement in a structured system supporting cryptocurrency fraud.

Directorate of Enforcement v. Bitconnect Crypto Fraud Case Accused[41]

The case arises out of an alleged case of fraudulent investments in cryptocurrencies based on the Bitconnect-style investment model, wherein investors were allegedly misled into investing money in various cryptocurrency-based investment schemes offering extremely high and consistent returns. Proceedings were taken by the Enforcement Directorate on the ground that the accused persons made "proceeds of crime" due to deception and then moved such funds through several crypto wallets, foreign exchanges, and intermediary bank accounts in order to obscure their source.

The main legal question was whether the cryptocurrencies themselves and the wallets associated with them constituted "property," and whether any gains obtained from such transactions could be considered "proceeds of crime" under Section 3 of the Prevention of Money Laundering Act, 2002. The Court discussed the increasing scope of law enforcement in relation to financial crimes committed in the digital age, accepting that although cryptocurrencies are not accepted legal

[41]2024 SCC OnLine Del 3891

ISSN: 2582-6433

tender in India, they can indeed act as means for transferring monetary value and thus constitute property liable to laundering.

However, in the context of the use of blockchain in frauds, the Court made clear that when it comes to complex financial crimes, especially those with an involvement of blockchain technology, the courts must proceed with caution on a temporary basis. According to the court, the freezing and/or attachment of cryptocurrency assets can only be carried out when there is prima facie evidence of layering and diversion of money.

What is the implication of this ruling? For starters, it means that any crypto-based financial fraud in India is bound to be dealt with by the law. This is because cryptocurrency is within the jurisdiction of PMLA, and therefore, the ED can exercise all the power to investigate the crime and attach/seize the cryptocurrency assets involved.

State of NCT of Delhi v. ParamjitKharb&Anr.[42]

In this case, there is a claim of investment fraud using cryptocurrencies whereby the defendant is said to have conducted business via online means where he made promises of providing high and guaranteed returns using crypto exchanges. It is argued that the investor was lured via internet ads and social media promotions and that funds were collected from them using cryptocurrency wallets, and converted at various exchanges for the purpose of concealing the money trail.

The first legal question in this case is whether the acts carried out by the defendants amount to a criminal act under the Indian Penal Code, or whether it is just a civil matter due to failure of investments in an unregulated financial market. Another issue to be determined is whether the lack of specific laws on cryptocurrencies in India would hinder any criminal proceedings.

The court ruled that cryptocurrency fraud could not necessarily escape the purview of criminal offenses due to the lack of any regulation of cryptocurrencies. The court upheld that in cases where deceitful behavior, misrepresentation, and gains or losses were involved, Section 420, 406, and 120B IPC were clearly applicable offenses. The Court underscored that the nature of the asset was irrelevant in such cases, provided the conditions for cheating and criminal breach

[42]2025 SCC OnLine Del 6109

ISSN: 2582-6433

of trust were fulfilled.

The key inference from this judgment is that it helps in making applicable the criminal laws to modern digital offenses. This also establishes the judiciary's acceptance of the fact that cryptocurrencies cannot be used to avoid criminal responsibility. Moreover, it implies that large-scale cryptocurrency investment scams would be considered as economic crimes by the courts, thereby justifying strict scrutiny while granting bail.

In Anvar v. Basheer[43], Section 65B provides a complete set of guidelines regarding the admissibility of evidence related to electronic records. As per Section 65B(1), any information contained in an electronic record which is produced by a computer output shall be considered as 'documents', and no requirement exists to submit the original documents as proof. Section 65B(2) provides a set of requirements for qualifying the data as a 'computer output'.

Shahfi Mohammad v State of Himachal Pradesh[44]As has been mentioned earlier, videography is an important part that can assist in conducting an investigation by providing firsthand information. The role of audio-video equipment is highlighted here; for instance, Section 54A of the Code of Criminal Procedure, 1973, as well as Section 164, allows for making identification process recordings, along with confessing recordings. The proposal was made to add to this the making of dying declarations recordings and post-mortem procedures as well.

Although it was decided that electronic evidence was admissible, it was stressed that there must be a way to confirm it as such, because of the vulnerability of the latest technologies and devices and their possible manipulation. There is no rule that can be considered exhaustive and can give an answer to what kind of evidence should be admitted, therefore, section 65B(4) became very significant in that regard.

COB under the Ministry of Home Affairs may be formed for implementing videography in investigative practices through planning and conducting videography operations. Instructions for videography implementation should be issued through COB and their proper execution should be carried out in phases. Financial resources for videography, even though law and order is a state subject, can be mobilized from the central government. Also, CCTV cameras should be installed in police stations and jails to avoid any human rights violation.

[43](2014) 10 SCC 473.

[44] (2018) 2 SCC 801

ISSN: 2582-6433

COB will ensure that their directives are implemented properly through independent committees formed within three months and compilation of information regarding compliance with the instructions issued. Secretary of the Ministry of Home Affairs, Central Government, and Home Secretaries of all State Governments will have to ensure compliance with the instructions.

Internet &Mobile Associations of India Vs. RBI[45]

This move occurred following the case where SCI on March 4, 2020 of IMAI case in India, and which was decided upon a three-judge panel consisting of J. Nariman, J.Aniruddha Bose, and V Ramasubramanian to lift the ban on dealings put in place by RBI Circulars. In this case, the court considered the issues from the angle of Art-19(1)(g). This involves the freedom to engage in any type of profession or undertaking.

Issue one

Herein, the Internet and Mobile Association of India argued that RBI had to ward off dealings in virtual currencies. They argued that virtual currencies could not be likened to cash or legal tenders.

Insofar as the principal issue is concerned, the court considered how digital currencies have been defined by various controlling agencies such as governments and law enforcing agencies and examined four aspects of money, namely, (i) a means of exchange; (ii) a unit of account; (iii) a store of value; and (iv) final discharge of debt or standard of payment. The court ruled that virtual currencies are not a universally accepted means of exchange, and they cannot be deemed to be the final discharge of debt. Therefore, insofar as they do not meet all the four above-listed criteria, they are not considered money. However, it was noted that virtual currencies may develop a parallel system even though they are not money, and therefore, under such circumstances, the RBI may exercise its powers over it.

Second issue

In addition to this, it was held that the RBI Circular did not serve the best interest of the common masses in general and also ignored the right of choosing a profession and carrying on with an occupation, trade or business as provided in Article 19(1)(g) of the Indian Constitution. The measure thus had an unjust influence on the professions pursued by those handling cryptocurrency. The measure taken by the Reserve Bank of India was unreasonable and does not fulfill the test of proportionality. Proportionality is such a test wherein the court is concerned

[45] . Internet and Mobile Association of India V. Reserve Bank of India, Writ Petition (Civil) No.528 of 2018

ISSN: 2582-6433

with the process adopted by the executive in meeting his demands and arriving at the decision.[46] The Court took note of the fact that the RBI Circular had an aggressively negative effect on the issue relating to the trades which operated in VC. In view of the fact that the RBI Circular very generously cleared away the VC trades from the present guidelines of the nation, it intruded on Article 19(1)(g) of the Indian Constitution. It seems, at least from outside, that there was no financial reaction to the issue.

With respect to the principle of proportionality, the Court referred to the case of Modern Dental College and Research Center v. State of Madhya Pradesh and the five factors established in it, based on which the proportionality test would be applied. The factors set forth by the decision are as follows:

- That the measure is intended to address an appropriate objective;
- That the measures are rationally connected to the attainment of the objective;
- That there is no alternative measure which is less restrictive; and
- That there is a rational connection between the importance of achieving the objective and the importance of restricting the right.

In the aforementioned case, it was decided that such a simple ritual incantation of 'tax evasion' or 'black money' does not satisfy the primary test, and that selective approaches should be examined.

The Court further made it clear that the exchange of VCs and the operation of VC deals were rendered meaningless by the RBI Circular in terms of their life support, which is the interface with the normal finance sector. The Court emphasized that there was no reasonable factual evidence presented by the RBI regarding the actual damages suffered by it. Up until now, there had been no statement issued by the RBI regarding any of its managed entities having suffered any harm or negative effects directly or indirectly due to the interface with the VC deals. The court emphasized the importance of establishing the extent of loss suffered by the RBI because of the existence of VC and clearly indicated that there was none. In addition, the Court also mentioned that despite the formation of a board that suggested both the First Draft Bill and Second Draft Bill, no conclusion could be made since both bills contradicted each other.

Despite the high level of volatility and anonymity attached to cryptocurrencies, it looks like they will continue to be a dominant force in the world of finance for some time now. The analysis

[46]Coimbatore District Central Coop. Bank v. Employees Assn, (2007) 4 SCC 669.

ISSN: 2582-6433

offered by the Court regarding the current case, with its attempt to understand the intricacies of regulating cryptocurrencies in India, can be seen as a good development in the right direction. Nevertheless, due to the growing cases of cybercrimes that extend beyond national frontiers, it is imperative that laws are established concerning cryptocurrencies and the tracking of funds used during crypto transactions.

In Midway Mfg. Co. V. Artic International[47]

In this particular case, the defendant hastened its computer tasks with the aim of accelerating the processes of the plaintiff's video game. However, the Court still decided that there was copyright infringement, and the defendant had made alterations in the Plaintiff's material. Nevertheless, in the case of Lewis Galoob Toys v. Nintendo of America, the Court held that the defendant had not developed any new material; rather, it had only improved upon the existing material in order to produce a better output.

Accordingly, the issue whether the defendant has made alterations in the work of the plaintiff will entirely depend on the prevailing circumstances. Among the considerations involved in making an alteration of the work includes the analysis of warnings contained in both works. A number of individuals have undertaken the task of carrying out extensive research to enable acquisition of the original works before compiling the same in favor of the wider public.. The compiler in all this cases is bound by law to take the blame for the infringement of copyrights if it happens that in such cases the compiler is basing his compilation on the entire work of the original proprietor.

Hitesh Bhatia v. Mr. Kumar Vivekanand[48]

In a fresh case where the implied misrepresentation has been introduced in the bargain and bitcoins acquisition in India, Ld. Metropolitan Magistrates, Tis Hazari Court, has brought forth some objective facts in relation to cryptocurrency and the duty of occupier with respect to representation in relation to the transfer of virtual money. The Court, among other things, observed that (i) transactions involving crypto-currency should conform to the laws that exist in India including the PMLA, IPC, 1860, FEMA, the tax laws, as well as the guidelines issued by the RBI in regard to KYC, CFT, and AML; (ii) KYC is the duty of the representative and hence cannot escape its duty to establish the legitimacy of the origin and destination of funds and the

[47] 704 F2d 965
[48] Hitesh Bhatia v. Mr. Kumar Vivekanand, Case No. 3207 of 2020, decided on 1st July 2021

ISSN: 2582-6433

identity of the parties involved; (iii) even in the absence of any specific law prohibiting or regulating the possession of cryptocurrency or any trade in it, the mere transaction of cryptocurrency through any representative may qualify as a right under Article 19 (i) (g) of the Constitution of India.

The plaintiff in the case moment bury alia was involved in dealing and acquisition of bitcoins. The case involves the accused who are believed to have purchased some bitcoins from the plaintiff on various occasions. According to the plaintiff, the accused would transfer money to the plaintiff's financial account and the plaintiff would then transfer the bitcoins to the accused's electronic wallet/address at the online trading platform 'Binance'. The plaintiff further stated that upon questioning the origin/legality of the money used for buying the bitcoins, the accused admitted that payments were a 'scam'. It further stated that as the accused did not refund the bitcoins sent to him, it amounted to fraud.[49]

The question still remained that whether the Court would consider the act being performed by the Complainant himself as a legitimate one, irrespective of whether or not he approached the Court with clean hands. In respect of the Supreme Court's decision in Internet and Mobile Association lastly, it was observed by the Court that the Supreme Court did not interfere with the question as to legitimacy of the virtual currency, and further noted that till date, no legislative intervention had occurred to govern the legality and regulation of crypto currency. It was observed that in case of 2018 Circular, the Supreme Court had upheld its validity only due to unreasonableness of limitations imposed on the right of freedom ensured under Article 19 (i)(g) of the Constitution of India. Therefore, the Court reiterated that in upholding the validity of the 2018 Circular, the Supreme Court had held the fact that many organizations were accepting virtual currency as legitimate means of payment for the purchase of services and goods, and hence, there could never be a way out of the conclusion that those dealing with virtual currency were engaged in an act falling squarely within the purview of RBI.

In like manner, the Court also observed that crypto currency is a medium through which an equal monetary system could be made, which could be considered as threat to existence of a centralized control based monetary system, and hence it falls within the purview of RBI to regulate such activities. It was further observed that RBI has the power to make policies in respect of such issues, and to lay down directions for the banks, which are 'system members' under the Payment

[49]Conventus Law, Delhi Court Attempts To Decode The Cryptic Case Of Cryptocurrencies In India. 19 August 2021

ISSN: 2582-6433

and Settlement Systems Act, 2007, and the same has also been acknowledged by the Supreme Court of India. It further said that the Supreme Court has held that access to banks is like access to oxygen in any modern economy, and a complete denial to access by persons who conduct transactions, which are not prohibited by law, cannot be considered as reasonable restriction.

It was determined by the court that any transaction in cryptocoins should comply with the total legislation governing India, which includes PMLA, IPC, FEMA, NDPS Act, Taxation laws, as well as the Reserve Bank of India's regulations on KYC, CFT, and AML requirements. It was noted by the court that while the traceability of transactions carried out by Bitcoin exchanges through the exchange interface 'BINANCE' might even be regulated through blockchain analysis, linking such exchanges with malicious actors can be a tricky situation, provided that the exchange representative does not follow KYC norms.

Nevertheless, it was evident from the Court that it gave the impression of the Complainant's failure to disclose all the truth under the scrutiny of the Court, and thereby, the possibility of his involvement/inducement in all of those transactions could not be ruled out as of now. In this regard, it was found by the Court amongst other things that (i) the Complainant persisted in accepting money from several records, which may not necessarily be attributed only to a lack of diligence on part of the Complainant; (ii) in one of the WhatsApp chats filed alongside the complainant, the accused could be seen inciting the Complainant to make payments for clearing up his financial dues immediately after receiving any proposal of giving bitcoins to him, and the Complainant does not get deterred but rather thanked the accused for his words and admitted to converting the thought back into crypto currency without delay; (iii) The Complainant did not mention anything in his complaint about how and through whom the accused came to know about the Complainant's WhatsApp number.As such, the Court found that it would not be proper to state with certainty that the Complainant did not know the Accused at the time of the crime, nor was there any history between them. Nevertheless, taking into consideration the records that the insight provided with respect to the Complainant, the Court pointed out that the Complainant approached this Court with due regard for all legal possibilities, and this constitutes one basis for issuing directions to conduct investigations to find the actual culprit.

In spite of the superfluous fluctuation in the value of cryptocurrencies and their enigmatic qualities, it appears that the digital means of money will be around for good, at least until a few years from now. The perspectives that the Court held about the matter at hand in its attempt to

ISSN: 2582-6433

make sense of some intricate elements of the crypto currency scheme in India seem to be a positive step in the right direction. But then, because of the increasing number of crimes committed in the cyberspace environment, which transcend geographical boundaries among others, there is an obvious need for legal guidelines governing the use of digital currencies, with a focus on ensuring the traceability of the money involved in cryptocurrency transactions.

While the aforementioned test was illustrated in Internet Mobile Association, it was not applied. All things being equal, the Supreme Court depended upon State of Although the above test was demonstrated in Internet Mobile Association, the said test was never applied. Assuming other conditions remain constant, the Supreme Court relied on the case of Maharashtra v. Indian Hotel and Restaurants Association[50]for its conclusion that it must be established that there is some experimental data that proves injury sustained by the traditional economy due to virtual currencies. Using the above test, the Supreme Court concluded that the total ban on the exchange of virtual currencies is unjustified. In the said case, the RBI failed to establish any experiment on the injurious impact of virtual currencies on the economy.

Shamoil Ahmad Khan v. Falguni Shah[51]

In its verdict, the High Court stated that protection of copyright extends to the theme, plot, and storyline that form the very soul of any literary work. The facts of the case related to allegations made by the plaintiff who had written the story 'Singardaan' in the Urdu language against the defendant for allegedly reproducing the plot, narrative, characters, and even the title of the story in their web series that appeared on their apps including the app known as Ullu and on YouTube. The High Court ruled that the web series was constituted of all the important elements of the story which, in turn, could easily be identified as an adaptation of that particular story by any person aware of it.

Nevertheless, the idea that the "life and blood" of the web series does not matter when it comes to the question of substantial similarity and copyright infringement is crucial to remember. Even if the story plays only an insignificant role in the whole plot created by the web series, if the Court considers it to be a substantial part of the expression of the plaintiff, then there will still be a case of copyright infringement. On the other hand, the Court's recognition of the difficulty faced while using the idea-expression dichotomy was welcomed.

[50] 2019 (3) SCC 429, AIR 2019 SC 589
[51]AIRONLINE 2020 BOM 552

ISSN: 2582-6433

D'Aloia v Binance Holdings[52]

The court found that service upon the unknown parties in the case could be done through NFTs which were to be served on the wallets to which the unlawfully taken money was transferred. Service through email was also available as one method but the use of NFTs will prove highly effective because it will embed the service within the blockchain, thus leaving no room for any disputes. The case sets an important precedent for the courts as it demonstrates how the courts have begun to adapt to technological changes for the sake of delivering justice. Moreover, the court took into account the submission made about the possibility of considering the defendant crypto exchanges as holding Mr. D'Aloia's identifiable cryptocurrency in a fiduciary capacity for him. This could open another way for victims of crypto asset fraud to receive some compensation from the unknown scammers who stole their funds.

LEGAL ISSUES AND CHALLENGES

Crypto-related offenses in India pose several important legal questions due to the lack of an existing legal regime that is specifically aimed at blockchain technology. The first question pertains to the absence of a specific law pertaining to cryptocurrencies that makes it difficult to classify cryptocurrencies into whether they are currencies, properties, securities, or commodities. This becomes an important question because all legal actions related to cryptocurrencies are governed by several intersecting laws like the PMLA, IT Act, and Income Tax Act.

Jurisdiction is one of the main legal issues in relation to crimes committed using cryptocurrencies. This is because transactions involving cryptocurrencies are global and may be conducted via foreign-based exchange platforms or foreign-based servers. The perpetrator can therefore commit the crime from outside India, but the victim could be in India. It becomes hard to determine the laws that will govern such cases since they involve both Indians and people from other countries.

An additional legal obstacle that comes into play is the anonymous nature of the transactions on the blockchain. Even though blockchain technology allows anyone to access transaction details, the wallet address does not indicate who the user is behind it. Consequently, there is difficulty in proving beyond a reasonable doubt who the person behind the crime was – a crucial requirement when building a criminal case. Criminals can use mixers, tumblers, and even privacy coins to take advantage of their anonymity further.

[52] [2022] EWHC 1723 (Ch)

ISSN: 2582-6433

Another important legal issue with respect to blockchain technology is its evidentiary value. It is necessary for evidence to be reliable and admissible in court; however, blockchain evidence requires an expert analysis. Furthermore, there are no guidelines on how a blockchain analytics report should be provided in an Indian court, which makes the admissibility of evidence questionable under the Indian Evidence Act.

Yet another problem is the overlapping jurisdictions of various authorities. Both the Enforcement Directorate, the Financial Intelligence Unit-India, the Cyber Crime Cells, and even the Central Bureau of Investigation are involved in prosecuting offenses related to cryptocurrencies; however, the jurisdictions of these authorities may overlap from time to time, which leads to some difficulties with coordination. There is no dedicated nodal authority in India; thus, procedures take time and are sometimes inconsistent.

The volatility and valuation of cryptocurrencies pose a legal challenge in terms of prosecuting cases related to blockchain. Since the market value of cryptocurrencies changes very rapidly, there is often a problem with valuing the amount lost by the victim due to the offense; moreover, it poses difficulties in attaching property pursuant to the Prevention of Money Laundering Act.

Other problems relate to the procedures involved in seizures and recoveries. Since cryptocurrencies are stored in digital wallets using private keys, which might be lost or destroyed by the offenders themselves, any procedure that involves seizure faces a problem in the retrieval of the crypto-assets. The ability to recover these assets requires the ability to have access to the keys and passwords for the wallets.

An equally crucial question concerns the lack of regulation on the activities of the cryptocurrency exchanges and service providers. FIU-IND now has some powers to compel exchanges to report, but regulations governing compliance are still at an early stage. In this regard, issues concerning liabilities of exchanges in case of fraud and money laundering are quite complex because of the nature of their operations.

In addition to the above, inconsistency in the judiciary's decision-making and evolving legal interpretations continue to pose major problems. The Indian judiciary is in the process of formulating its jurisprudence regarding crypto assets and treats them like "property" or "assets" depending upon the context. Lack of precedent or concrete legislation regarding the matter results in varied interpretation in different cases. It becomes important for the country to formulate a proper regulatory mechanism for the matter at hand.

ISSN: 2582-6433

MEASURES TO OVERCOME LEGAL CHALLENGES

One of the main strategies towards tackling cryptocurrency offenses involves putting into place a regulatory mechanism to govern the same. India presently has legislation such as the Information Technology Act, 2000, Indian Penal Code, 1860 and the Prevention of Money Laundering Act, 2002 that have not been tailored specifically for the regulation of blockchain. Having an act that defines the virtual digital currency, regulates exchanges and identifies specific offenses associated with cryptocurrencies will go a long way in addressing cryptocurrency offenses. Taxation and regulatory measures will also contribute to the achievement of this objective.

Another critical element to consider in this regard is the capacity to investigate cryptocurrency offenses. In cases involving cryptocurrency, there is usually a digital trail left behind after a crime has been committed which requires sophisticated technology and skills to track down. This means that law enforcement agencies will need to acquire blockchain analytic software and training on how to effectively analyze cryptocurrency data to trace the offenders. Collaboration between institutions like the Enforcement Directorate and the cybercrime departments with the Financial Intelligence Unit – India will help achieve this objective.

The next important action is the improvement in the functioning of the prosecution mechanism and the criteria of evidence. Courts often experience problems with interpretation of data contained in the blockchain and connection of accused parties with digital money. Development of clear rules regarding admission of electronic evidence based on existing legislation can increase the rate of convictions. Training sessions for judges and inclusion of technical specialists in the process will contribute even more to closing the information gap. Finally, the creation of special courts that are responsible for cybercrimes and financial crimes will significantly decrease the time for investigating cryptocurrency crimes and applying criminal law in the case.

Finally, international collaboration and public-private partnerships are important tools for dealing with crimes involving blockchain technology. India needs to increase its involvement in international agreements and treaties on mutual legal assistance for more efficient cross-border investigations. Cooperation with crypto exchange platforms, fin-tech firms, and agencies such as the Reserve Bank of India can make significant improvements in this regard. Combining all of the discussed actions, India will be able to handle most legal problems associated with

ISSN: 2582-6433

cryptocurrency-based crimes.

ISSN: 2582-6433

CHAPTER 6

CONCLUSION AND SUGGESTIONS

CONCLUSION

There have been various crimes based on cryptocurrency that India needs to tackle legally and through regulation because of the fast growth and decentralization in blockchain technology. They range from investment scams, attacks on digital wallets, Ponzi schemes, ransom payments for extortion cases, and using cryptocurrency exchanges for money laundering. The fact that India has no separate legislation for cryptocurrency makes it use several pieces of existing legislation to cover crimes based on cryptocurrency. They include BNS, 2023, ITA, 2000, PMLA, 2002, and FEMA, 1999.

The regulation for cryptocurrencies is therefore multi-faceted and indirect. Cryptocurrency is neither legal tender nor illegal in India. It falls in between the two extremes and thus works under a grey regulation framework. The regulatory authorities involved are RBI, SEBI, ED, and Cybercrime Cells. Their involvement in regulating cryptocurrency depends on the type of crime committed. For instance, it will be financial, cyber, or international money movement.

In IAMAI v. RBI (2020) 10 SCC 274, the Apex Court has also significantly contributed in the formation of this framework as it has laid down that regulatory measures should be proportional in nature and should not constitute indirect ban of any crypto activity in absence of legislation. Hence, it can be said that cryptocurrencies, while not banned in India, are nevertheless regulated in accordance with the law.

An investigation of cryptocurrency offences is technical in nature and is conducted by the Cyber Crime Police, the State Police, and the Enforcement Directorate (ED). For conducting an investigation of cryptocurrency offences, the investigating authority uses blockchain technology analysis, IP addresses, exchange KYC information, forensic examinations of the devices, and digital trails in order to find out the trail of the transaction of funds.

As per PMLA, 2002, it is the task of the Enforcement Directorate to trace, attach, and confiscate any proceeds of crime which may be received from a cryptocurrency offence. According to Section 3 of PMLA, 2002, all laundering offences committed using digital currencies have been made into punishable acts whereas under Section 5 of the Act, provisional attachments can be made of any cryptocurrency wallet and converted properties.

Blockchain violations are investigated by relying on the BNS, 2023, which trumps the provisions

ISSN: 2582-6433

of IPC but upholds the traditional doctrines that form the foundation of criminal law when it comes to cybercrime laws. These laws include Section 318 of the BNS (cheating), Section 316 of the BNS (criminal breach of trust), and Section 61 of the BNS (conspiracy), along with forgery, whereas hacking, impersonation, and identity theft cases may rely on the ITA, 2000 and Sections 43, 66, 66C, and 66D.

The significance of crypto fraud in India has been perceived to pose severe economic offenses, and thus stringent steps from the courts must be taken to address such instances. This is because of the stringent principles followed in granting bail and the heavy losses suffered by the investors as one of the major reasons in reaching the decision.

However, there are some issues with enforcement. Due to the lack of legislation regulating cryptocurrency, there are difficulties in enforcing laws and regulations on cryptos and their transactions. Problems with classification and valuation, overlapping jurisdictions, and conflicting interests among regulatory authorities are all factors contributing to legal uncertainty in the country's blockchain environment.

In terms of international enforcement, FEMA, 1999 will be applicable when cryptocurrencies are involved in overseas trading and transactions. This is because the sections of this law that deal with the unlawful dealings of foreign exchange and capital account transactions can be used to investigate cases involving illegal outward transfers and cross-border investments in cryptocurrencies.

Conclusion

The enforcement and regulation of cryptocurrency-related offenses in India rely on several different statutes, including the recently amended BNS, 2023, ITA, 2000, PMLA, 2002, and FEMA, 1999, among others. Although the use of multiple laws has allowed for the successful prosecution of offenders and regulation of the market, India still needs a single legislative instrument to govern cryptocurrencies and their transactions.

ISSN: 2582-6433

SUGGESTIONS

- The other suggestion that needs to be implemented is the introduction of a separate law pertaining to cryptocurrencies and virtual digital assets. In its current form, India uses a patchwork of laws including BNS, ITA, PMLA and FEMA. However, a separate statute that provides an explicit definition of cryptocurrencies, digital tokens, blockchain assets and intermediary institutions will simplify matters.
- The legal categorization of crypto-currencies into assets or securities is also critical in this context. At present, there are questions over whether crypto is an asset, commodity, security or foreign exchange, and thus proper classification under a separate law would clarify how it can be taxed, regulated by either RBI or SEBI, and what constitutes criminal activity.
- There also needs to be stricter regulation and monitoring of crypto exchanges and intermediaries, including mandatory licensing, stringent KYC/AML requirements, audit obligations and real-time monitoring of all suspicious transactions. It must be ensured that all exchanges comply with legal requirements by maintaining their records and assisting enforcement agencies, such as ED and cyber crime cells.
- Another important requirement is improving digital forensic infrastructure and capability of blockchain analysis. Investigative agencies need modern equipment to track cryptocurrency wallet accounts, identify and analyze use of cryptocurrency mixers, and analyze cross-chain transactions. There should be cyber forensic labs dedicated to cryptocurrencies at the national and state level, and there needs to be expertise in blockchain technology.
- Another proposed solution is improving coordination between Enforcement Directorate, CBI, RBI, SEBI, and Cyber Crime Units in their dealings with cryptocurrencies. The cases involving cryptocurrency crimes have various aspects to them which are related to other areas as well including fraud, money laundering, and cross-border transactions of funds. An improved coordination system or a crypto enforcement task force will help increase efficiency.
- International cooperation will be essential in order to tackle cryptocurrency crimes more effectively, as transactions take place worldwide, and enforcement measures would require cooperation from foreign financial intelligence units. International cooperation

ISSN: 2582-6433

can be achieved by signing bilateral and multilateral agreements on regulating cryptos and recovering assets. FATF guidelines should be followed for enforcement purposes. MLATs need to be improved for asset recovery.

- Another significant suggestion that can be made is that of the capacity building of the judiciary as well as the prosecuting agencies. Judges, as well as the prosecutors and investigating agencies, must be properly trained in blockchain technology and digital forensics. This is because knowledge of wallets, smart contracts, and decentralized finance (DeFi) is imperative for an unbiased trial and proper conviction.
- Lastly, the issue of public awareness and protection of investors must be seriously considered. It has been observed that many crimes related to cryptocurrencies have been perpetrated owing to the ignorance of the investors in terms of the risks involved as well as various scam schemes that operate in the market.

ISSN: 2582-6433

BIBLIOGRAPHY

DandaRawat, Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems , MDPI, 2020

Porras, Intellectual Property and the Blockchain Sector, a World of Potential Economic Growth and Conflict, Intech Open Journal, 2023

Sakshi, Blockchain and IPR: A Breakthrough Collaboration, LIBERTATEM, 2021

Saini and Kumar, "Issues pertaining to growth of digital economy, Journal of Public Affair (2020).

Pandey, Surabhi&SenBlockchain Technology in Real-Time Governance: An Indian Scenario. Indian Journal of Public Administration (2022)

Jani, Shailak. The Emergence of Blockchain Technology & its Adoption in India, SSRN (2019)

IfeanyiMbukanma, Role of creativity and technological innovation in achieving entrepreneurial success, IJCMS, 2023

Pandey, Surabhi&SenBlockchain Technology in Real-Time Governance: An Indian Scenario. Indian Journal of Public Administration (2022)

J. Davis, Intellectual Property Law (4th edn, Oxford University Press 2014)

Narayan P, Intellectual Property Law, (Eastern Law House, 2014)

https://www.mondaq.com/india/fin-tech/1177710/the-convergence-between-blockchain-technology-and-intellectual-property-rights

N Mahesh, S. "Copyright and digitization", Journal of information management, 85-88 (2008)

Jatin , Dawn of Blockchain Technology in the Indian Patent Regime AIPLA (2021)

Vanathi Krishna, Role of Intellectual Property in Blockchain Indian J Integrated Rsch L. 8 (2022)

Narayanaswamy, Raju. Infusing Blockchain Technology into the IPR Sector, International Journal of Research in Social Sciences, 2021

Singh Shiv, The law of Intellectual Property Rights, (Deep & Deep Publications, New Delhi, 2014)

GB Reddy, I.P.Rs and the Laws, (Gogia Law Agency, 2016)

Akhil Prasad and A. Aggarwala, Copyright Law 132-136 (Desk Book, 2009)

BP Singh and Anand, Blockchain technology and Intellectual property rights, Journals of IPRs (2019)

ISSN: 2582-6433

https://www.linkedin.com/pulse/blockchain-technology-legal-framework-its-application-apurva-agarwal

https://ebizfiling.com/blog/impacts-of-blockchain-on-copyright-registration/

https://www.aipla.org/list/innovate-articles/dawn-of-blockchain-technology-in-the-indian-patent-regime

ShreyaRai (2022), The Association of Intellectual Property Law AndBlockchain, https://www.linkedin.com/pulse/association-intellectual-property-law-blockchain-legasispvtltd

https://link.springer.com/article/10.1007/s10796-022-10279-0