VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CRYPTOCURRENCY AND ECONOMIC CRIME IN INDIA: STUDYING THE LEGAL CHALLENGES AND REGULATORY GAPS

- Srusty Surachita Dhal[1]

ABSTRACT

The surged in the development of cryptocurrency has transformed the global financial platform, offering exceptional opportunities for emerging technologies and digitally-mediated transactions. However, the same features that make cryptocurrency such as decentralization, obfuscated identity and cross-jurisdictional transfer, also identify it as an effective mechanism for committing economic crimes. In India, where even if the application and trading of cryptocurrencies have surged and expanded drastically, a clear regulatory framework to administer the digital assets are still significantly lacking. Vulnerabilities in the financial sector has led to economic crimes such as fraud, money laundering, Ponzi schemes and various cross border transfers due to the very gap in the legal governance of digital assets.

This research paper identifies the regulatory gaps in the Indian laws regarding crypto regulations and weak regulatory frameworks in the integration of cryptocurrency and related offences even under the pre-existing laws like the Prevention of Money Laundering Act (PMLA). The paper evaluates Indian legal approach to treat crypto offences, following the evolved jurisprudence post the Supreme Court's judgement on the *Internet and Mobile Association v. RBI*[2] case and other landmark cases such as the GainBitcoin scam[3] and Enforcement Directorate seizures[4] under the Prevention of Money Laundering Act (PMLA). It further includes comparative study of the legislations

[1] Student at KIIT School of Law

[2] Supreme Court of India. (2020, March 4). *Internet and Mobile Association of India v. Reserve Bank of India*, Writ Petition (Civil) No. 528 of 2018.

[3]Moneycontrol. (2022, July 12). *GainBitcoin scam: A cryptocurrency fraud of over Rs 20,000 crore that's still unfoldin*

[4] Press Information Bureau. (2023, March 15). *ED seizes crypto assets worth ₹907 crores under PMLA*

including the international frameworks of the European Union's MiCA[5] regulations, the regulatory model of the U.S.[6], and the licensing system for crypto entities of Singapore[7].

India's cryptocurrency regulation has gone through evolution over the past few years characterised by a series of critical developments.[8]

INTRODUCTION

Socio-economic crimes or termed as white-collar crimes, often confine with non-violence and they are rather financially motivated crimes that are committed by entities in the position of authority and trust. These include offences like fraud, tax evasion, money laundering, and embezzlement, pose significant ultimatum to economic momentum and public trust. These are the offences which violate the laws and regulations that govern the social and economic well-being and activity of the society. And one such surging issue in India is the rise of such offence in the digital financial sector with the evolution of the new technologies.

Cryptocurrency is a digital currency which used the technique of cryptography to make secured transactions. Cryptography is the technique of the conversion of the information using algorithms and mathematical concepts into unreadable format called as cipher-texts. Cryptocurrencies arte decentralized which thus implies that they are not regulated by any central authority such as the government or the bank. They are thus different from the traditional form currencies which are controlled by the banks and government. It has three certain features; anonymity, decentralized and borderless transfer which have significantly contributed in its surge in popularity in the recent decade. However, the given features also made cryptocurrencies, significant tools for unlawful activities.Time and again, the same has been proven on the global jumbo-tron when cryptocurrencies have been used in financial terrorism, money laundering and to execute large-scale cross-border frauds. Despite uncertain regulatory frameworks the adoption of cryptocurrency has surged within India as well. *"India has also got a fairly wide spread level of adoption across different assets of crypto despite restrictions, implying new participants to crypto would have been participating via services that were not banned. Now we've started to*

[5] European Commission. (2023). *Markets in Crypto-Assets (MiCA) regulation*
[6] U.S. Securities and Exchange Commission. (n.d.). *Spotlight on crypto assets*.
[7] Monetary Authority of Singapore. (2024). *Payment Services Act and digital payment token services.*
[8] IMPRI India. (n.d.). *Crypto in India: The regulatory framework*. Retrieved April 18, 2025

see some of those restrictions get rolled back, for example with Binance, which is probably just going to amplify adoption in the country.[9]" said Eric Jardine, research head at Chainalysis.

The legal landscape of India's regulatory framework has however been at the standpoint of ambiguity. The Reserve Bank of India (RBI) imposed a banking ban on crypto transactions in 2018, which was later repealed in 2020 by the Supreme Court. The Finance Ministry then covered crypto transactions under the ambit of the Prevention of Money Laundering Act (PMLA), however a legal comprehension and exhaustive legislation still remains oblivious. Overlapping of the economic crimes and cryptocurrency thus gives rise to unique crimes and challenges for more evolving legal regulatory bodies and law enforcement. Given India's drastic digitalization and surging adoption of the cryptocurrencies into the financial sector, there is an urgent call for more evolving laws and regulations to address these challenges.

India's approach to regulate cryptocurrency has gone under a notable transformation in recent years.

This paper aims to study the application of cryptocurrencies in the financial system and their utilization in the occurrence of the economic offences in India. The study also aims to identify the prevailing legal and regulatory gaps in the financial landscape of India.

LITERATURE REVIEW

The study of crimes has always found a way back to understanding their sociological roots. Thus understanding the evolution and growth of economic offences and their transition into the digital age too requires a comprehensive understanding of their sociological roots. Edwin H. Sutherland's theory of white-collar crime, given in 1930s is one of the most foundational contributions of the socio-economic understanding in this field. The prevailing concept that crime is associated with poverty and social disadvantage was rejected and challenged by Sutherland[10]. He strongly claimed that crime

[9]Reuters. (2024, September 11). *India leads in crypto adoption for second straight year, report shows*. Based on the 2024 Geography of Cryptocurrency Report by Chainalysis.

[10]Geis, G. (1992). *Geis, Sutherland and white-collar crime*. University of California, Irvine – Center for Law and Society.

Gil Geis was a fundamental criminologist and a close companion scholar of Edwin H. Sutherland who first conceptualized white-collar crimes in 1939. In the given paper, Geis emphasizes on the evolution of Sutherland's ideas and their influence on corporate crimes scholarship, highlighting a retrospective which

can even be committed by individual in the positions of stewardship and power through deception for monetary gains[11]. He specifies that offences like fraud, embezzlement and insider trading committed by business professionals, executives and corporate actors could be as harmful, if not more, as conventional as street crimes. He drew a connection between white-collar crime and his own differential association theory which emphasizes that criminal behaviour is learn through interaction and association with immediate peer groups. He emphasized that the lack of enforcement of prosecution in the elite crime area thus allows such offences to thrive rampant and unchecked. In the context of the current times, Sutherland's theory helps in understanding how crypto-related offences, laundering schemes and digital scams are modern versions of white-collar crimes often committed by the tech-savvy, socially respectable and trusted individuals. Cryptocurrency provides anonymity and decentralization, aligning along with Sutherland's observation that the privileged entities commit offences under the guise of legality or technological errors[12]. Thus there is an urgent need for the criminologists to focus on the institutional accountability, regulatory negligence and the refinement of the economic crimes which are highly valid in the cryptocurrency crimes. This is particularly prevailing in the countries like India where there is a drastic surge in the adoption of cryptocurrencies eventually leading to rise in crypto crimes outpacing the laws.

The Financial Action Task Force (FATF) has played an important role in addressing the money laundering and digital financial assets terrorism. In the regulatory documents, of 2019 and 2021, the FATF emphasized the "Travel Rule" which gives the virtual asset service providers (VASPs) an access to collect and share the user information when conducting transactions, to enhance the transparency and accountability[13][14]FATF warned of the increasing risk in crypto activities in India due to India's slow progress in

---

abridges traditional criminology theories and modern elite deviance and the prolonging failure in the regulatory framework.

[11]Geis, G. (1992), ibid.

[12] Simpson, S. S. (2019). *Reimagining Sutherland 80 years after white-collar crime*. Criminology, 57(2), 189–207.

Simpson is a leading scholar on corporate crime and this article is based on her 2018 Sutherland Address at the American Society of Criminology. It critically revaluates Edwin Sutherland's original thesis of white-collar crimes, offering insights into constructive comprehensive challenges and the contemporary validity.

[13]Financial Action Task Force (FATF). (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Paris: FATF/OECD.

[14]Financial Action Task Force (FATF). (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Paris: FATF/OECD.

incorporating effective laws and proactive enforcement of Anti-Money Laundering Standards (AML).

RESEARCH OBJECTIVES

The main objective of this paper is identifying the regulatory and enforcement gaps in the current legal framework which governs the relationship between cryptocurrencies and socioeconomic crimes in India.

To study how the characteristics of cryptocurrencies such as their decentralization, anonymity, and cross-border transfer, make them vulnerable to abuse in financial frauds, money laundering, Ponzi schemes and financial terrorism.

To assess India's present cryptocurrency governance legal environment, with a focus on the incorporation and use of the Prevention of Money Laundering Act (PMLA) in offences pertaining to cryptocurrencies.

RESEARCH GAP

Even though cryptocurrencies have drawn a lot of attention from around the world, especially for their part in changing digital finance, academic and regulatory attention in India is still dispersed and lacking, particularly when it comes to their link to economic crimes. The majority of the literature currently in publication is either global in scope, ignoring the complex legal and enforcement issues unique to India, or technical, focusing on block-chain technology and its financial ramifications. Sutherland's theory of white-collar crime provides a strong sociological framework for comprehending crimes committed by powerful and trusted individuals, but there is hardly any current scholarly discussion that applies it to India's growing cryptocurrency offenses.

Furthermore, it is still unclear how effective these legal changes are at stopping and prosecuting economic crimes involving cryptocurrencies, even in light of historic rulings like the Supreme Court's 2020 overturning of the RBI's 2018 crypto ban and the inclusion of virtual assets under the Prevention of Money Laundering Act (PMLA).

There are also very few comparative studies that examine India's regulatory response in comparison to global models, such as Singapore's VASP licensing scheme, the EU's MiCA framework, and the U.S. SEC's strategy. Empirical studies assessing the

effectiveness of law enforcement organizations such as the ED and FIU in combating intricate crypto frauds, scams, and money laundering schemes are also lacking.

RESEARCH QUESTIONS

- How have socioeconomic crimes like fraud, money laundering, and cross-border financial crimes increased in India as a result of the rise of cryptocurrencies?
- How well-suited are the Prevention of Money Laundering Act (PMLA) and other current Indian laws to deal with offenses involving cryptocurrencies?
- Which significant regulatory gaps exist in India's cryptocurrency laws?
- How does India's approach compare to international regulatory models like the US framework and the EU's MiCA?
- What legislative changes are required to guarantee that economic crimes involving cryptocurrency are effectively regulated in India?

METHODOLOGY

In order to investigate the legal and regulatory framework governing cryptocurrency-related socio-economic offenses in India, this study combines a comparative legal analysis with a qualitative doctrinal approach. In addition to academic articles, reports, and policy papers from reputable organizations like the Financial Action Task Force (FATF), Reserve Bank of India (RBI), and international regulatory bodies, the study is based on secondary sources such as statutes, court rulings, government notifications, and international conventions.

In order to investigate the Indian legal response to cybercrimes, the paper critically examines important pieces of legislation such as the Information Technology Act of 2000 and the Prevention of Money Laundering Act (PMLA), 2002. The study focuses in particular on the Supreme Court's historic ruling in Internet and Mobile Association of India v. Reserve Bank of India (2020), which overturned the RBI circular from 2018 that prohibited cryptocurrency transactions and established a standard for the regulation of digital finance.

The Markets in Crypto-Assets (MiCA) Regulation of the European Union, the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) frameworks of the United States, and Singapore's Virtual Asset Service Provider (VASP)

licensing program under the Payment Services Act, 2019 are among the other regulatory frameworks that are evaluated through comparative legal research. The purpose of this comparison is to evaluate how India's changing legal system might benefit from international best practices.

High-profile Indian cases like the GainBitcoin scam and Enforcement Directorate actions pertaining to crypto-assets are also examined using the case-study method. The gaps and real-world difficulties in applying the available legal tools to digital financial crimes are demonstrated by these case studies.

In order to suggest a strong and flexible legal framework suited to India's quickly growing digital economy, the research eventually seeks to integrate doctrinal insights with policy-oriented findings.

BROAD STRUCTURE OF THE DISCUSSION

In order to thoroughly examine the legal and regulatory issues surrounding cryptocurrency-related socioeconomic offenses in India, the discussion in this research paper is divided into several interconnected sections. An outline of white-collar crimes and how they have spread to the digital sphere via cryptocurrencies is given at the outset. The changing legal position in India is then examined, along with significant court rulings and the implementation of the Prevention of Money Laundering Act (PMLA). A critical analysis of well-known Indian cryptocrime cases is then presented in order to draw attention to enforcement issues. A comparative legal analysis is then provided by looking at international regulatory frameworks like Singapore's licensing model, the EU's MiCA, and the US SEC-CFTC approach.The conversation ends with particular suggestions for India that centre on the necessity of a specific legal framework for virtual assets, institutional readiness, and legislative clarity.

DISCUSSION

Understanding Cryptocurrency an its Legal Landscape

Financial transactions have been transformed by cryptocurrency, a decentralized digital asset that uses blockchain technology to facilitate peer-to-peer exchanges without the need for middlemen. Its fundamental qualities: decentralization, anonymity, and borderless transfer have made it easier for it to be quickly adopted everywhere, including

in India.[15] Nonetheless, legal and regulatory frameworks face serious difficulties as a result of these same characteristics.[16]There has been uncertainty surrounding the legal status of cryptocurrencies in India. The cryptocurrency market was essentially suppressed in 2018 when the Reserve Bank of India (RBI) issued a circular banning banks from facilitating cryptocurrency transactions. Due to disproportionate restrictions on the cryptocurrency industry, the Supreme Court overturned the RBI's directive in 2020 after this ban was challenged.[17]

Even though cryptocurrency trading started up again after 2020, there was still no complete regulatory framework in place. In an attempt to acknowledge cryptocurrency assets but fall short of formal regulation, the government implemented a 30% tax on cryptocurrency gains and a 1% Tax Deducted at Source (TDS) on transactions.[18] The Ministry of Finance required adherence to anti-money laundering regulations in March 2023 by bringing Virtual Digital Assets (VDAs) under the purview of the Prevention of Money Laundering Act (PMLA).[19] Cryptocurrencies are not fully regulated or accepted as legal tender in spite of these steps. Businesses and investors continue to face uncertainty due to the lack of clear regulations on topics like consumer protection, dispute resolution, and the classification of cryptocurrency assets.This regulatory gap has consequences for both market development and the prevention of illegal acts assisted by cryptocurrency.

Economic Crimes Using Cryptocurrency

Cryptocurrencies are appealing tools for a variety of economic crimes due to their inherent qualities, which include pseudonymity, ease of cross-border transactions, and lack of centralized oversight.[20] Money laundering, fraud, and Ponzi schemes are among the crypto-related offenses that have significantly increased in India.[21]Cryptocurrency

[15]Ghosh, S. (2022). *Cryptocurrency regulation in India: A regulatory vacuum or a balancing act?* Journal of Financial Crime, 29(1), 23–40.
[16]Narayanan, A., Bonneau, J., Felten, E., Miller, A., &Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
[17]Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.
[18]Ministry of Finance, Government of India. (2022). *Union Budget 2022–23: Taxation of Virtual Digital Assets*.
[19]Press Information Bureau. (2023, March 7). *Virtual digital assets brought under the purview of the Prevention of Money Laundering Act, 2002*.
[20]FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Financial Action Task Force.
[21]Reserve Bank of India. (2021). *Report on Currency and Finance 2020-21: Reviewing the Monetary Policy Framework*.

money laundering entails turning illegal funds into digital assets, sending them across international borders, and then turning them back into fiat money to hide the money trail. Because cryptocurrency transactions are decentralized, it is more difficult to monitor and intercept them.

The number of fraudulent investment schemes has also increased. Scammers use phony cryptocurrency investment platforms or tokens to entice investors with promises of large returns. It is frequently only after suffering large financial losses that victims become aware of the fraud. The susceptibility to such scams is increased by a lack of investor awareness and regulatory oversight.

Ponzi schemes that use cryptocurrency have surfaced, in which the capital of new investors is used to pay returns to previous investors, giving the appearance of profitability.[22] Participants in these schemes suffer significant losses when the flow of new investments stops.Cryptocurrency anonymity also makes it easier for ransomware attackers to demand cryptocurrency payments in order to unlock victims' data. The fact that these transactions are untraceable gives cybercriminals more confidence.

In addition to causing monetary losses for victims, these economic crimes also present larger threats to national security and financial stability. The difficulties in identifying, looking into, and prosecuting such offenses highlight the necessity of strong legal and regulatory frameworks that are adapted to the particular characteristics of cryptocurrencies.

Case Studies

a. *GainBitcoin Scam*[23]: Amit Bhardwaj was the mastermind behind the GainBitcoin scam, one of the largest cryptocurrency Ponzi schemes in India. He enticed investors with the promise of 10% monthly returns from Bitcoin mining. More than 8,000 investors in India and overseas contributed more than ₹2,000 crore between 2015 and 2017. In addition to routing money through a network of international wallets and shell corporations, Bhardwaj established a network of businesses, including GBMiners and GainBitcoin.

[22]Europol. (2022). *Cryptocurrencies and Ponzi Schemes: Crime Trends and Challenges*. European Union Agency for Law Enforcement Cooperation.
[23]*Amit Bhardwaj v. State of Maharashtra &Anr.*, Bail Application, 2020 SCC Online.

Issues: This case revealed significant weaknesses in India's digital asset laws and regulations. Tracking peer-to-peer (P2P) cryptocurrency transfers and recovering digital funds hidden overseas presented technical challenges for authorities.

Status: In 2018, Bhardwaj was taken into custody. Several FIRs were submitted in various states.The fact that recovery actions and court proceedings are still pending as of 2024 illustrates how slowly the legal system is reacting to crypto-related cyber-financial frauds.

b. *Bhogapuram Fake Call Centre Scam*[24]*:* In 2022, a phoney call center with more than 200 employees in Atchutapuram, Andhra Pradesh, was exposed for posing as US tax authorities. In the United States, victims were duped into purchasing gift cards or sending money using cryptocurrency, which was subsequently laundered through online channels.

Issues: This scam demonstrated the lack of real-time collaboration between Indian and foreign law enforcement agencies and the use of cryptocurrencies in cross-border frauds.

Currents Status: Although arrests were made in accordance with the IT Act and the IPC, the pseudonymous nature of cryptocurrency transactions made cross-border fund recovery challenging.

c. *Jaipur Engineering Student Scam*[25]*:* After tricking people with fictitious job offers, a 21-year-old student abducted them and forced them to send ₹4.5 lakh in cryptocurrency.

Issues: This case demonstrated how traditional crimes and digital tools can coexist, creating special difficulties for law enforcement and forensics. Judgement & Current Status: The accused was taken into custody and charged with kidnapping and extortion under the IT Act and sections of the IPC. The cryptocurrency hasn't fully recovered yet, though.

d. *Stock Advisory Scam – IIT Hacker Case*[26]*:* By pretending to be authorized stock advisors, an IIT graduate and his associate defrauded investors out of ₹22 lakh.

[24]State v. Unknown Accused (Fake Call Centre Scam, Atchutapuram), Crime registered under Sections 419, 420, 467, 468, 471 IPC and Sections of the IT Act, 2000, Bhogapuram Police Station, Andhra Pradesh (2022).
[25]State v. RohitMeena, Sections 364, 384, 420 IPC and relevant sections of the Information Technology Act, 2000, Jaipur Police, Rajasthan.
[26]State v. Rahul Sharma &Anr, Sections 66C, 66D IT Act and Sections 420, 120B IPC, Delhi Police Cyber Crime Cell, in connection with Cambodia-based fraudulent stock advisory ring.

Money was obtained through phony companies and transferred via cryptocurrency into wallets connected to Cambodia.

Issues: The fraud exposed gaps in fintech regulation and the circumvention of Indian financial regulations through foreign platforms.

Status &Judgment: Although the two were arrested in 2023, the case brought attention to the pressing need for legislative changes that are specific to cyberspace and cryptocurrency.

Regulatory Challenges

India has taken a cautious and incremental approach to regulating cryptocurrencies. The Supreme Court's reversal in 2020 after the RBI's initial ban in 2018 illustrates the regulatory ambivalence surrounding digital assets. Even though the PMLA's 2023 inclusion of cryptocurrencies was a big step, there are still a number of issues.[27]

- Absence of Complete Law: India does not have a specific legal framework that addresses cryptocurrencies. Current laws, such as the Information Technology Act and the PMLA, are applied to offenses involving cryptocurrency, but they were not created with digital assets in mind, which creates ambiguities in their interpretation.
- Regulatory Fragmentation: The Ministry of Finance, the RBI, and the Securities and Exchange Board of India (SEBI) are among the organizations whose jurisdictions overlap with regard to certain aspects of cryptocurrency regulation.
- Technological Complexity: New crypto instruments and blockchain technologies are developing at a faster rate than regulations can keep up with. Regulators frequently lack the resources and technical know-how necessary to properly monitor and control these developments.
- Enforcement Challenges: Enforcement efforts are made more difficult by the anonymity and international reach of cryptocurrencies. Tracing transactions, identifying offenders, and gaining cooperation from foreign jurisdictions are all difficult tasks for law enforcement agencies.
- Investor Protection: Investors are at risk of fraud and scams due to the lack of explicit rules regarding consumer rights, dispute resolution procedures, and redressal forums.

[27]Ministry of Finance. (2023, March 7). *Virtual digital assets brought under anti-money laundering law*. Press Information Bureau, Government of India.

- Taxation Ambiguities: Although the government has levied taxes on cryptocurrency gains, it is still unclear how to classify cryptocurrencies for taxation purposes, which makes compliance difficult.

Comparative Legal Approaches

European Union (EU): The Markets in Crypto-Assets (MiCA) Regulation was adopted by the European Union (EU) with the goal of establishing a thorough legal framework for crypto-assets.[28]MiCA creates consumer protection measures, requires transparency, and imposes licensing requirements on crypto service providers. In order to promote innovation and mitigate risks like money laundering, market manipulation, and investor fraud, it aims to standardize regulations among member states. The EU offers a model for balanced oversight that may be instructive for India by establishing a clear and consistent regulatory environment.

United States (U.S.): The U.S. regulates cryptocurrencies in a disjointed manner. Various facets of the industry are supervised by organizations like the Internal Revenue Service (IRS), Commodity Futures Trading Commission (CFTC), and Securities and Exchange Commission (SEC).[29] Certain cryptocurrency assets are treated as securities by the SEC and must be disclosed. Nonetheless, there is still regulatory uncertainty, particularly with regard to token classification and the scope of state and federal laws. Numerous lawsuits and demands for extensive federal legislation have resulted from this.

Singapore: One of the most crypto-friendly jurisdictions is thought to be Singapore. Under the Payment Services Act, the Monetary Authority of Singapore (MAS) oversees crypto service providers, placing a strong emphasis on compliance with anti-money laundering and counter-terrorism financing laws.[30]While preserving strong protections against unauthorized use, the government actively encourages blockchain innovation. Its licensing system boosts investor confidence and clarifies regulations.

Japan: One of the first nations to legalize cryptocurrencies and set up an exchange licensing system was Japan. Regulations were tightened following the 2018 Coincheck

[28]European Commission. (2023). *Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in Crypto-assets (MiCA)*. Official Journal of the European Union.
[29]U.S. Government Accountability Office. (2023). *Blockchain in finance: Legislative clarity and coordination needed for oversight of crypto assets*. GAO-23-106842.
[30]Monetary Authority of Singapore. (2022). *Payment Services Act 2019: Regulatory framework for digital payment token services*.

hack, requiring crypto exchanges to register with the Financial Services Agency (FSA) and requiring internal security controls.[31] Japan is now a safe and alluring market for crypto innovation as a result of this proactive approach.

Recommendations

By implementing a balanced regulatory strategy that promotes innovation while safeguarding investors and upholding financial integrity, India can take a cue from these models. Important first steps include creating a technologically advanced regulatory body, coordinating tax policy, and guaranteeing interagency cooperation. India needs a thorough and progressive regulatory approach because of the intricate relationship between cryptocurrency and economic offenses. The following suggestions are put forth:

- India ought to enact a thorough law that defines cryptocurrencies, establishes their legal standing, and lays out precise guidelines for use, trading, and taxation. Stakeholders will benefit from clarity and a reduction in ambiguity.
- To keep an eye on the sector, guarantee adherence, and work with law enforcement, a central authority with knowledge of blockchain and crypto-assets should be established.
- Give law enforcement the equipment and instruction they need to look into cybercrimes. Tracking capabilities can be improved through collaborations with blockchain analytics companies.
- To streamline cross-border investigations and standardize regulatory requirements, cooperate with international organizations and crypto-friendly jurisdictions.
- Start awareness-raising initiatives to inform investors about the dangers and frauds associated with cryptocurrencies. Provide a grievance redressal system for scams involving cryptocurrency.
- Enforce stringent Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures for all cryptocurrency exchanges doing business in India in order to reduce anonymity and illegal use.

CONCLUSION

[31]Financial Services Agency (Japan). (2023). *Approach to crypto-asset exchange service providers and regulation under the Payment Services Act*.

The emergence of cryptocurrencies has allowed for quick, decentralized, and international transactions, completely changing the financial system. However, in India, this innovation has also been used for a variety of socioeconomic offenses, from extortion and Ponzi schemes to international cyber frauds. Fake call center scams, kidnapping for cryptocurrency ransom, and the GainBitcoin scam are just a few of the case studies that demonstrate the variety and increasing complexity of crimes made possible by virtual currencies. India's current legal and regulatory system is still ill-prepared to handle the problems caused by offenses involving cryptocurrencies. Because there is no comprehensive law that specifically governs digital assets, there is a gap in the law that criminals can take advantage of.Enforcement and prosecution are made more difficult by the anonymous nature of cryptocurrencies, the implementation of encrypted communication, and the presence of unregulated offshore exchanges.

Furthermore, Indian law enforcement organizations frequently lack the technical know-how and resources required to successfully cooperate with foreign jurisdictions, track down cryptocurrency transactions, and retrieve stolen money. Due to the novelty of these offenses and the lack of standardized legal principles that apply to crypto crimes, judicial responses have also been sluggish and uneven.

There are conflicting reactions to cryptocurrencies in the international legal system; some nations have welcomed them with robust regulatory frameworks, while others have completely banned them. India must strike a balance between innovation and security at this pivotal moment.A more comprehensive legislative and institutional framework is desperately needed, even though the government has implemented taxation and anti-money laundering (AML) regulations for virtual digital assets.

This study emphasizes the necessity of a multifaceted strategy. It demands the adoption of a specific cryptocurrency law, the development of cybercrime units' capabilities, international agreements for the tracking of digital assets, and public awareness initiatives to stop victimization. To protect investors and maintain national security, the RBI, SEBI, and law enforcement must coordinate their regulatory oversight.

To sum up, there are advantages and disadvantages to cryptocurrencies. The abuse of virtual assets for financial crimes will continue to present serious socio-legal issues in the years to come unless India implements proactive and flexible legal measures.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/