FROM BITCOIN TO BUST: UNDERSTANDING THE IMPACT OF PMLA ON THE INDIAN CRYPTOCURRENCY MARKET

Written by ***Amisha Mittal* & Shubhi Agrawal*****

**5th year BA LLB Student, Jindal Global Law School, Haryana, India*

*** 5th year BA LLB Student, Jindal Global Law School, Haryana, India*

Orcid: 0009-0007-9628-8529

ABSTRACT

As a popular form of investment and payment, cryptocurrency has grown exponentially in recognition in recent years. However, it additionally has grown into an opportunity for money laundering and other financial crimes simply due to its decentralized and anonymous nature. The Prevention of Money Laundering Act (PMLA) along with other regulations are being brought into effect by the Indian government to curb such crimes. The following paper aims to provide an in-depth analysis of the PMLA's regulation of cryptocurrencies along with how it affects the Indian cryptocurrency market by analysing its provisions, difficulties, and ramifications.

RESEARCH OBJECTIVE

This research paper's primary objective is to study how the Prevention of Money Laundering Act (PMLA) regulates cryptocurrencies. With the aim of understanding the effectiveness of the current regulatory frameworks and recommending areas for reform, the research paper analyses the state of cryptocurrency regulations currently while considering how this impacts the prohibition of money laundering. further, using a combination of case studies and examples from around the globe, the paper will also evaluate the advantages and drawbacks of PMLA's applicability to cryptocurrencies.

OVERVIEW OF CRYTOCURRENCY

A cryptocurrency is an electronic form of decentralized virtual currency. The most well-known cryptocurrencies, including Bitcoin, Binance Coin, Ethereum, Dogecoin, and Litecoin, that have been developed on blockchain technology, which enables users to transact anonymously and is encrypted[i]. The way that we handle money, trade, conduct financial transactions, and most importantly, assess, evaluate, and reduce the dangers linked to using cryptocurrencies might all be revolutionized by Bitcoin. The distributed ledger system on which blockchain technology has its foundation, stores, and transmits data in 'blocks' connected by a chain. Then, such data is securely and impermanently synchronized using the cryptography algorithm. One of the factors that constrain and limit the adoption of cryptocurrency is its possibility of abuse[ii].

Moreover, a cryptocurrency is traded by using a digital platform, crypto-wallet, or any comparable digital technique and does not have backing by any physical assets. A cryptocurrency's value is purely determined by the views of its users.

Furthermore, with a market valuation of more than $2 trillion as of April 2021, the cryptocurrency industry has experienced remarkable growth in recent years. Prices tend to fluctuate dramatically in reaction to developments and shifts in the market, regulations, and consumer demand[iii]. Such fluctuations are an inherent characteristic of market dynamics. Growth in the market has been fuelled by rising consumer and business acceptance rates as well as the advent of new use cases and applications.

INTRODUCTION

The emergence of cryptocurrencies as an internationally recognized trend has showcased both opportunities and challenges for financial systems all over the globe. While cryptocurrencies have benefits like efficiency, global accessibility, and decentralization, they additionally involve risks like the possibility of money laundering and other illegal financial activity. Governments across the world have started implementing rules to cater to these kinds of concerns that pertain to potentially fraudulent use of cryptocurrencies. The Prevention of Money Laundering Act (PMLA) serves as the basis in India for regulating cryptocurrency-related activities while minimizing the risks involved. The main goals of the PMLA are primarily to establish an exhaustive legal structure for preventing money laundering and terrorist financing; enhancing the integrity of the financial system by placing into place strict anti-money laundering (AML) regulations; and enabling global coordination and cooperation to combat international money laundering[iv].

Even, the Italian securities regulator, Commissione Nazionale per le Società e la Borsa (Consob) head, Paolo Savona, has expressed concern about the rising popularity of cryptocurrencies given their lack of defined regulatory guidelines. Savona expressed such an opinion while presenting Consob's annual report, stating that the absence of explicit laws and regulations, thus gives criminals a chance to use cryptocurrency for illegal purposes. According to Paolo Savona, ***"Without proper oversight, there could be a worsening in market*** transparency***, the basis of legality and rational choice for (market) operators[v]."***

Moreover, the government of India has also recognized the need to tackle financial crimes like money laundering and terrorism financing with the introduction of the Prevention of Money Laundering Act. The PMLA accentuates the importance of effective anti-money laundering control measures in numerous industries while providing a legal framework for the prevention, detection, and investigation of such activities. The PMLA required to include regulations that specifically addressed the special difficulties associated with these digital currencies and assets in relation to the recent development and growing popularity of cryptocurrencies.

Cryptocurrency is a form of digital and virtual currency that deploys the technique of cryptography to secure and authenticate, and confirm transactions, in addition to regulating the

creation of new units. Some of the most widely used cryptocurrencies include Bitcoin, Ethereum, and Ripple.

Cryptocurrency is decentralized, which essentially implies that no single entity, like a bank or a government authority, possesses a position of power to control it. Rather, it operates on a peer-to-peer network where transactions are encrypted, verified by network nodes, and subsequently added to a blockchain, a public ledger.

While cryptocurrencies offer several benefits, including decentralization, anonymity, and speedy transactions, they have additionally grown to be a target for financial crimes such as money laundering. Therefore, the Indian government has enacted an array of laws and regulations, specifically the PMLA, that aim to discourage such crimes. The term "*proceeds of crime*[vi]" under the PMLA act, is defined as, any kind of property derived from criminal activity, which includes digital, or cryptocurrency gained fraudulently and illegally. Since "reporting entities" are bound to the legislation's requirements, the PMLA primarily applies to bitcoin[vii] exchanges, intermediaries, and other entities that are involved in cryptocurrency transactions.

Bitcoin, Ethereum, and other cryptocurrencies work on decentralized networks and use cryptographic technology to ensure the security of transactions. Cryptocurrencies are appealing to cybercriminals attempting for ways to take advantage of the financial system due to their decentralized nature and users' anonymous identities[viii].

Some of the threats associated with cryptocurrencies include money laundering, tax evasion, fraud, terror financing, and encouragement of illegal, criminal activities. The PMLA has been extended to encompass cryptocurrency exchanges, trading platforms, and other intermediaries involved in cryptocurrency transactions in an effort to help mitigate such risks.

MONEY LAUNDERING AND CRYPTOCURRENCY

Money laundering is the process of concealing criminal gains, 'proceeds of crime' to make it look legal and acceptable. Placement, layering, and integration are the typical three steps. Placement refers to the actual placement of illicit money into the financial system, Layering refers to the use of intricate financial instruments and transactions to conceal the source of the

funds, and Integration refers to the re-entry of the funds into the legal financial economic system[ix].

Thus, cryptocurrencies are particularly appealing to money launderers because of their decentralized structure and anonymity. Cryptocurrencies can be used by money launderers for transferring money across borders covertly, making it challenging for law authorities to identify and confiscate illegal finances. Also, through the use of complicated transactions and strategies like tumbling and mixing, cryptocurrency can also be used to cover up the actual origin of funds. Thus, upon considering their distinct characteristics and capacities, it can be said that cryptocurrencies and money laundering are related[x].

Additionally, considering cryptocurrency transactions are globally connected in nature, money launderers are able to indulge in regulatory arbitrage by taking advantage of varying degrees of regulation of cryptocurrencies in different countries. Money launderers can participate in illegal activity with a lower risk of being identified and prosecuted by utilizing counties with weak or non-existent cryptocurrency rules.

Combating against money laundering is made more difficult by the cryptocurrency market's continuing development and the advent of currencies that prioritize confidentiality. Monero and Zcash are few examples of digital privacy coins that offer improved privacy and anonymity features, thus, making it even harder for law enforcement to track down illegal transactions and identify the persons involved[xi].

Therefore, globally, the connection between cryptocurrencies and money laundering poses a serious challenge for regulators and law enforcement organizations.

REGULATION OF CRYPTOCURRENCY UNDER THE PMLA ACT

Several nations have adopted the Prevention of Money Laundering Act (PMLA) legislations as a legal safeguard against money laundering and other financial crimes. The main goal of the PMLA is to prevent and control money laundering activities through the establishment of procedures for the identification, investigation, and prosecution of money laundering crimes. The Act provides a framework for legal proceedings to locate, seize, and identify criminally, and illegally generated proceeds of crime[xii].

The PMLA normally includes a number of regulations requiring designated non-financial companies and professions (DNFBPs) and financial institutions to take proactive measures against money laundering. The Act specifies the responsibilities that the reporting entities must fulfil, such as performing customer due diligence (CDD), keeping track of all transactions, and notifying the appropriate authorities of any suspicious activity[xiii].

The Prevention of Money Laundering Act aims to stop financial crimes including money laundering. Banks, money exchangers, and other businesses that conduct financial transactions are subject to regulation by the legislation, along with other financial institutions. The act under its ambit, includes all cryptocurrency-related activity. The Indian government aims to address the possible potential risks associated with cryptocurrencies used in money laundering and other illegal activities by introducing them under the PMLA's scope[xiv]. The intention includes encouraging transparency and enhancing due diligence while making it easier for law enforcement to investigate and prosecute incidents of cryptocurrency-related money laundering.

Many jurisdictions have recently widened the PMLA's application to include cryptocurrency-related activities. Much like traditional financial institutions, cryptocurrency exchanges, wallet providers, and other virtual asset service providers (VASPs) are now required to adhere to AML and CDD regulations. By extending the PMLA, the goal is to include cryptocurrencies under regulation and prevent the coins from being used for money laundering[xv].

Anti-Money Laundering (AML) and Know Your Customer (KYC) methods must be followed by cryptocurrency exchanges and trading platforms because they are deemed "reporting entities" under the PMLA. The steps they take involve verifying their clients' identities, maintaining an eye on transactions, and notifying the correct authorities of any suspicious activities.

Thus, with the intent of safeguarding transaction anonymity and ensuring transaction transparency, KYC requires verifying the identity of clients, collecting necessary information, along with performing customer due diligence. Further, the identification and prevention of potential money laundering operations in the cryptocurrency industry also depend on anti-money laundering (AML) mechanisms, such as monitoring and reporting doubtful and unclear transactions.

ENFORCEMENT AND IMPLEMENTATION CHALLENGES

Extending the PMLA's provisions to incorporate cryptocurrencies is a positive move, but putting these conditions into effect while maintaining them in force will continue to remain challenging. Many of these challenges arise from the distinctive characteristics of cryptocurrencies, such as their decentralized form, anonymity, and cross-border transactions, which have a bearing on the efficient application of the PMLA's anti-money laundering (AML) requirements[xvi].

The issues and challenges in effective implementation of Anti Money Laundering (AML) requirements involves:

Technological Complexity-

The PMLA's Section 12(2) underlines the significance of identifying, tracking down, and recognizing the proceeds of crime. But it's challenging to monitor and analyse these transactions efficiently due to the technological complexity surrounding cryptocurrencies, especially blockchain-based transactions. Cryptocurrencies are decentralized, as identified in Section 12(3), thereby making it more challenging to identify the individuals who are engaged in money laundering activities.

Cross Border Transactions-

The PMLA's Section 2(u)[xvii] describes "proceeds of crime" as any asset produced from criminal activity, regardless of where it is geographically located. The cross-border nature of Bitcoin transactions, however, makes it more challenging for governments to enforce AML laws. As stated in Section 2(vi), it is difficult to establish jurisdiction and coordinate efforts among many countries because there is no centralized regulatory body for cryptocurrencies.

Anonymity and Pseudonymity-

Cryptocurrencies give users variable levels of anonymity and pseudonymity, making it challenging to identify and connect certain users against specific transactions. The PMLA's Section 3[xviii] specifies that reporting companies keep records of transactions, including customer identity information. However, as noted in Section 3(x), the anonymous character of

Bitcoin transactions makes it difficult to determine the real identity behind wallet addresses, impeding the effective execution of AML requirements.

Regulatory Divergence-

The PMLA's Section 13[xix] is concerned with international cooperation and mutually exclusive legal assistance in instances that involve money laundering. Regulative divergence results from the realization that the regulatory framework and legislations for cryptocurrencies differs between nations. In addition, in Section 13(2)[xx], inconsistent legislation and different standards of strictness in different nations create the door to regulatory arbitrage while making it more difficult to stop money laundering through international networks.

Lack of Standardization-

The PMLA's Section 12(1)[xxi] highlights the responsibility of reporting entities to ensure and verify the identification of clients whilst maintaining monitoring of their transactions. The absence of standardized procedures and regulations in the cryptocurrency sector, however, makes it difficult to execute AML controls effectively. Cryptocurrency exchanges and service providers' varying degrees of compliance with AML requirements, as noted in Section 12(3), create gaps in the AML framework's broader effectiveness.

A broad extensive approach must be devised to tackle these enforcement and implementation issues. As stated in Section 12(2)(c), policymakers and regulatory bodies must improve technology capabilities to track and analyse Bitcoin transactions. To overcome jurisdictional barriers and successfully combat cross-border money laundering in the cryptocurrency arena, promoting global cooperation and information exchange is essential, as emphasized in Section 13(1). Further, with the intention of assuring compliance and preventing money laundering, cryptocurrency gateways, and facilitators must be subject to the strict AML regulations set forth in Sections 12(1)(a) and 12(1)(b).

Additionally, in order to cater to changing market conditions and emerging problems, Section 14[xxii] of the PMLA Act mandates that ongoing monitoring, auditing, and updating of AML legislation is significant[xxiii]. It will be possible to identify any violations and make necessary modifications that are needed to enhance the AML framework with periodic reviews of the PMLA regulations in connection with cryptocurrencies.

Moreover, Section 13(3)[xxiv] of the PMLA also highlights the significance of encouraging global collaboration in the discovery and prosecution of money laundering offences. By exchanging information, coordinating investigations, and assisting in the recovery of illegal funds, regulatory authorities, law enforcement agencies, and international organisations can work together to increase the effectiveness of AML protections.

Also, programmes for education and awareness-raising also play a significant role in dealing with enforcement and implementation issues, in addition to legislative and regulatory measures. To enable reporting entity workers better understand their AML obligations, Section 12(4)[xxv] of the PMLA recognises the importance of training programmes for the employees and other entities. A marketplace for cryptocurrencies that is safer and more compliant can be achieved by imparting knowledge to people in general about the risks of cryptocurrencies, their responsibilities under the PMLA, and the value of responsible financial practices.

Thus, the policymakers and regulatory bodies can build extensive detailed strategies and frameworks that effectively address money laundering in the cryptocurrency arena by recognizing and analysing these enforcement and implementation problems considering the relevant aspects under the PMLA. The following requires maximizing technology, encouraging global collaboration, establishing standardized practices, and assuring continuing improvements to the AML regulatory framework. The enforcement and application of the PMLA can only be strengthened by the deployment of all these comprehensive approaches that seek to triumph over the unique challenges that arise from cryptocurrencies and their tendency to facilitate illegal financial transactions and money laundering.

JURISDICTIONAL APPROACHES TO CRYPTOCURRENCY REGULATIONS

Around the world, there are many different jurisdictional approaches to cryptocurrency regulations. While some nations have taken a more supportive and sympathetic approach, several adopted strict regulatory guidelines, or outright prohibitions on cryptocurrencies. India falls within the latter category as in 2018, the Reserve Bank of India (RBI)[xxvi] issued a blanket ban on banks providing services to cryptocurrency exchanges,

however, the same circular was subsequently revoked by the Supreme Court in 2020 in the case the Internet and Mobile Association of India v Reserve Bank of India[xxvii].

The Prevention of Money Laundering Act (PMLA) and the Securities and Exchange Board of India[xxviii] (SEBI) regulations are the primary agencies in responsible for regulating cryptocurrencies in India. The PMLA imposes reporting obligations on reporting entities, including banks, financial institutions, and intermediaries, to conduct customer due diligence, keep records, and promptly notify the Financial Intelligence Unit (FIU) of suspicious transactions. Initial coin offerings (ICOs) and cryptocurrencies are regulated by the SEBI[xxix] as securities, pursuant to its regulations on public offers.

With varying interpretations of the PMLA and a lack of specific regulatory authority for cryptocurrencies, India's regulatory environment for cryptocurrencies is still uncertain. Investors are exposed to fraud and financial crime owing to the lack of regulatory clarity, which has raised concern among cryptocurrency businesses and hampered the industry's growth.

On the contrary, several nations have taken a more progressive stance when it comes to cryptocurrency regulations. For instance, the Financial Crimes Enforcement Network (FinCEN)[xxx] oversees AML/CFT compliance, the Securities and Exchange Commission (SEC) regulates securities offerings, and the Commodity Futures Trading Commission (CFTC) oversees derivatives trading. Thus, the United States government has developed a comprehensive regulatory framework for cryptocurrencies.

Even the Financial Services Agency (FSA) in Japan has established a licensing mechanism for Bitcoin exchanges, and it is responsible for monitoring compliance with AML/CFT laws. This approach adopted by Japan has led to the development of a regulated cryptocurrency market and improved investor safety[xxxi]. Also, Initial coin offerings (ICOs) and cryptocurrency trading activities are strictly prohibited in China. These various approaches reflect upon the various regulatory goals and risk assessment procedures of each jurisdiction.

Further, the diverse approaches to regulating cryptocurrencies demonstrate the importance of a well-balanced strategy that secures investors and fosters innovation. In the Bitcoin industry[xxxii], the PMLA offers a solid foundation for preventing money laundering and terrorist financing. However, in conjunction with the most recent Supreme Court decision[xxxiii], its enforcement and execution call for greater precision, details, and uniformity.

In addition, there can be seen numerous instances that serve to provide insight into the opportunities and challenges that cryptocurrencies bring in the context of AML/CFT regulations. For instance, in Amit Bharadwaj case[xxxiv], the arrest of Amit Bhardwaj in connection with a multi-million-dollar Bitcoin Ponzi scheme provides as an additional reminder of the potential risks linked to unregulated cryptocurrency schemes, the case underlines the need for more robust enforcement measures to protect investors, and the need for increased public awareness.

Likewise, in Coinsecure hack case, in April 2018, one of India's top cryptocurrency exchanges, CoinSecure[xxxv], experienced a serious security breach in which thieves took 438 Bitcoin, which was back reportedly worth around $3.3 million. The exchange traced the compromise on its Chief Security Officer (CSO), who they claimed was in responsible for keeping the private keys to the exchange's wallets on his personal computer. The CSO refuted the accusations and alleged negligence on the part of the exchange. The case emphasizes the significance of robust internal controls and cybersecurity measures for preventing and identifying financial crimes in the digital currency bitcoin area.

Moreover, in another cryptocurrency exchange based in India, Koinex[xxxvi], closed its operations in June 2019 due to regulatory uncertainties and financial challenges. Due to the RBI's[xxxvii] prohibition against banks providing services to cryptocurrency businesses, the exchange had been experiencing issues processing deposits and withdrawals. The case also underlines the difficulties faced by cryptocurrency businesses due to the lack of a well-defined regulatory framework and the requirement for greater regulatory clarity to promote innovation and growth in the digital currency industry.

In outcome, although India has adopted a more conservative stance towards cryptocurrency legislation, it still needs to continue to develop its regulatory framework to address the unique challenges presented by cryptocurrencies. The construction of a comprehensive and efficient regulatory framework for cryptocurrencies in India can be influenced by the incorporation of jurisprudence and comparative analysis and can offer an insightful understanding of nations with different regulatory frameworks.

ANALYSIS OF CRYPTOCURRENCY REGULATION UNDER PMLA

Exchanges for cryptocurrencies have endured substantial changes to the manner in which businesses operate as an outcome of the wider application of PMLA laws. Nowadays, cryptocurrency exchanges must adopt strict KYC policies, confirm customers' identities, and keep track of transactions. By enhancing transparency and accountability, these measures are making it harder for money launderers to take advantage of exchanges for illegal activities. Exchanges are also required to notify the appropriate authorities concerning any suspicious transactions, enabling to identify and prevent money laundering schemes[xxxviii].

Although the inclusion of cryptocurrencies in the PMLA's legal framework was an important step in a positive direction, there are still number of issues that must be resolved. Firstly, the PMLA's definition of "virtual currency" is broad and includes a variety of digital assets, such as tokens and coins that cannot always serve as a form of payment transaction. This lack of definition may cause misunderstanding and uncertainty when it comes to its application[xxxix].

Additionally, the PMLA's CDD and record-keeping requirements impose an intense compliance burden on cryptocurrency intermediaries. This may end up in higher compliance fees, which might ultimately hinder India's adoption of cryptocurrencies.

Thirdly, the carrying out of the confiscation and seizure provisions of the PMLA in the context of cryptocurrencies might prove to be challenging. Since they are decentralized, cryptocurrency can be owned by anybody that holds a private key. The identification and seizure of cryptocurrencies used in money laundering or terrorism financing become increasingly difficult as an aftermath for law enforcement agencies.

COMPARISION WITH OTHER JURISDICTIONS

The regulatory landscape for cryptocurrencies is more complex in other regions, like the United States and Europe. For instance, cryptocurrencies are governed by state and federal laws in the US, with many regulatory bodies in charge of every aspect of cryptocurrency regulation. Further, a robust regulatory framework for cryptocurrencies has been provided in Europe by the Fifth Anti-Money Laundering Directive (5AMLD).

CHALLENGES AND AREAS OF IMPROVEMENT

Despite substantial progress, there are still issues and need for improvement in the regulation of cryptocurrencies under AML frameworks. These consist of:

1. **Technological Difficulties**: Regulating cryptocurrencies demands knowledge of the underlying technology as well as the flexibility to adjust to changes in that technology. To successfully monitor and control bitcoin transactions, regulators must consistently improve their expertise and knowledge of technology.
2. **International Cooperation**: Since cryptocurrencies operate internationally, international coordination is essential in fighting against money laundering. The effectiveness of AML controls will be increased by adopting unified regulatory approaches and improving cooperation among jurisdictions.
3. **Privacy coins and Mixing Services:** The advent of privacy-focused cryptocurrencies and mixing services is a challenge for anti-money laundering (AML) initiatives. For authorities to address the threats posed by these technologies and strike a balance between privacy and AML goals, regulators must seek new approaches.
4. **Education and Knowledge**: It's necessary for promoting awareness regarding the risks of money laundering among Bitcoin users, businesses, and authorities. Training programs may help in promoting compliance within the bitcoin community and a greater understanding of AML duties.
5. **Innovation**: Considering the constantly changing nature of cryptocurrencies, regulators should adopt a flexible and adaptive approach to regulatory frameworks. Growing challenges could be effectively addressed by embracing regulatory sandboxes, interacting with industry stakeholders, and encouraging innovation.

CONCLUSION

For governments to address the issues of money laundering connected with digital assets, it is essential to regulate cryptocurrencies under the Prevention of Money Laundering Act (PMLA)[xl]. Transparency, accountability, and traceability within the Bitcoin industry have been improved by the PMLA's expansion to include cryptocurrency exchanges and intermediaries.

Regulators must adapt and create efficient methods to reduce the risk of money laundering, regardless of whether regulating cryptocurrencies presents difficulties due to technological complexity, international cooperation, and changing privacy aspects. Maintaining consistent regulatory frameworks and promoting the integrity of financial systems require ongoing cooperation between regulators, industry stakeholders, and international organizations.

Regulators can help create an environment that minimizes the potential misuse of cryptocurrencies for money laundering by implementing strong KYC and AML safeguards, monitoring suspicious actions, and promoting education and awareness. The regulation of cryptocurrencies under PMLA can promote a more safe and more open financial marketplace through continuous review and development.

ENDNOTES

[i] Raza, S. (2019). "An Overview of Cryptocurrency Regulation in India". Journal of Money Laundering Control, 22(4), 407-414.
[ii] Lipton, A. (2018). Money laundering risks in cryptocurrency and initial coin offerings. Columbia Business Law Review, 2018(2), 331-362.
[iii] Raza, S. (2019). "An Overview of Cryptocurrency Regulation in India". Journal of Money Laundering Control, 22(4), 407-414.
[iv] Aloysius, J. A. (2018). A Legal and Regulatory Analysis of Cryptocurrencies under the Prevention of Money Laundering Act. International Journal of Science and Research, 7(10), 1035-1040.
[v] Reuters Staff and Paolo Savona, "Unregulated Spread of Cryptocurrencies a Concern, Says Italian Regulator" Reuters (June 14, 2021) <https://www.reuters.com/article/us-cryptocurrency-italy-consob-idCAKCN2DQ> accessed May 4, 2023
[vi] Section 2(1)(u), Prevention of Money Laundering Act, 2002; "*Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property [or where such property is taken or held outside the country, then the property equivalent in value held within the country] [or abroad]*"
[vii]Bitcoin [FAQs], Reserve Bank of India (last visited Apr. 28, 2023),https://www.rbi.org.in/Scripts/FAQView.aspx?Id=119.
[viii] Financial Stability Board. (2019). Decentralised financial technologies: Report on financial stability, regulatory and governance implications. Retrieved from https://www.fsb.org/wp-content/uploads/P151119.pdf
[ix] Badev, A., & Chen, M. (2018). Cryptocurrency, financial crime and money laundering: A review of the literature. Journal of Financial Crime, 25(4), 1094-1105.
[x] Ciaian, P., Rajcaniova, M., & Kancs, D. A. (2021). How cryptocurrencies impact money laundering and financial crime. European Journal of Law and Economics, 1-36.
[xi] Fatima, S., & Fatima, S. (2020). The intersection of cryptocurrency and anti-money laundering laws in India. In S. H. Ali & A. Karjiker (Eds.), The Routledge Handbook of Financial Crime in Asia (pp. 166-184). Routledge.
[xii] Hashmi, A. (2019). "Bitcoin in India: A Study of Legal Framework and Regulatory Challenges", Asian Journal of Multidisciplinary Studies, 7(1), 43-48.
[xiii] Anwar, S., & Adnan, S. (2020). Bitcoin, money laundering and terrorist financing risks: Emerging trends and regulatory measures. Journal of Financial Crime, 27(4), 1177-1191.
[xiv] Hashmi, A. (2019). "Bitcoin in India: A Study of Legal Framework and Regulatory Challenges", Asian Journal of Multidisciplinary Studies, 7(1), 43-48.

[xv] International Organization of Securities Commissions. (2019). Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms. Retrieved from https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf

[xvi] Park, J. H., & Cha, J. H. (2019). AML/CFT regulation and cryptocurrencies: A case study of South Korea. Journal of Financial Crime, 26(2), 501-514.

[xvii] Section 2(1)(u), Prevention of Money Laundering Act, 2002; "*Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property [or where such property is taken or held outside the country, then the property equivalent in value held within the country] [or abroad]*"

[xviii] Section 3, Prevention of Money Laundering Act, 2002; "*Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the 1[proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming] it as untainted property shall be guilty of offence of money-laundering".*

[xix] Section 13, Prevention of Money Laundering Act, 2002; *The Director may, either of his own motion or on an application made by any authority, officer or person, [make such inquiry or cause such inquiry to be made, as he thinks fit to be necessary, with regard to the obligations of the reporting entity, under this Chapter].*

[xx] Section 13(2), Prevention of Money Laundering Act, 2002; "*If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may— (a) issue a warning in writing; or (b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or (c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or (d) by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."*

[xxi] Section 12, Prevention of Money Laundering Act, 2002; "*Reporting entity to maintain records—(1) Every reporting entity shall— (a) maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions; (b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed*;"

[xxii] Section 14, Prevention of Money Laundering Act, 2002; *"No civil or criminal proceedings against reporting entity, its directors and employees in certain cases—Save as otherwise provided in section 13, the reporting entity, its directors and employees shall not be liable to any civil or criminal proceedings against them for furnishing information under clause (b) of sub-section (1) of section 12."*

[xxiii] Park, J. H., & Cha, J. H. (2019). AML/CFT regulation and cryptocurrencies: A case study of South Korea. Journal of Financial Crime, 26(2), 501-514.

[xxiv] Section 13(3), Prevention of Money Laundering Act, 2002; "*The Director shall forward a copy of the order passed under sub-section (2) to every banking company, financial institution or intermediary or person who is a party to the proceedings under that sub-section.*"

[xxv] Section 12, Prevention of Money Laundering Act, 2002; "*The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later*."

[xxvi] The Reserve Bank of India. (2018). "Prohibition on dealing in Virtual Currencies (VCs)". Retrieved from https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243&Mode=0

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

[xxviii] The Securities and Exchange Board of India. (2019). "Report of the Committee on the Regulatory Framework for Digital Tokens". Retrieved from https://www.sebi.gov.in/reports/reports/mar-2019/report-of-the-committee-on-the-regulatory-framework-for-digital-tokens_42299.html

[xxix] The Securities and Exchange Board of India. (2019). "Report of the Committee on the Regulatory Framework for Digital Tokens". Retrieved from https://www.sebi.gov.in/reports/reports/mar-2019/report-of-the-committee-on-the-regulatory-framework-for-digital-tokens_42299.html

[xxx] Financial Action Task Force. (2021). FATF Report on Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing. Retrieved from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/virtual-assets-red-flag-indicators.html

[xxxi] McKeon, A. (2019). Money laundering risks of cryptocurrencies: How the FATF is responding. Journal of Money Laundering Control, 22(4), 489-504.

[xxxii]Bitcoin [FAQs], Reserve Bank of India (last visited Apr. 28, 2023), https://www.rbi.org.in/Scripts/FAQView.aspx?Id=119.
[xxxiii]Internet and Mobile Association of India v. Reserve Bank of India, Writ Petition (Civil) No. 528 of 2018, Supreme Court of India, (Mar. 4, 2020)
[xxxiv] State of Maharashtra v. Amit Bhardwaj, Criminal Application No. 2989 of 2018 (Bombay High Court)
[xxxv] Coinsecure Exchange v. Officer-In-Charge, Cyber Cell, Economic Offences Wing, Delhi Police, Criminal Complaint No. 1764 of 2018 (Delhi High Court)
[xxxvi] Koinex Trading Pvt. Ltd. v. Union of India, Writ Petition (Civil) No. 373 of 2019 (Bombay High Court)
[xxxvii] The Reserve Bank of India. (2018). "Prohibition on dealing in Virtual Currencies (VCs)". Retrieved from https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243&Mode=0
[xxxviii] Janczewski, M., & Amiraslani, H. (2019). An analysis of anti-money laundering in the Bitcoin system. In M. Janczewski (Ed.), Handbook of Research on Blockchain Technology (pp. 295-320). IGI Global.
[xxxix] Lipton, A. (2018). Money laundering risks in cryptocurrency and initial coin offerings. Columbia Business Law Review, 2018(2), 331-362.
[xl] The Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2002 (India).