



ANTI-MONEY LAUNDERING LAWS AND CRYPTOCURRENCY TRANSACTIONS

Souham Sarkar*

ABSTRACT

This paper explores the intersection of cryptocurrency and money laundering, highlighting the challenges posed to traditional Anti-Money Laundering (AML) frameworks. While money laundering has long been a method for criminals to disguise illicit financial gains, the rise of cryptocurrencies has introduced new complexities due to their decentralised, pseudonymous, and borderless nature. Features such as anonymity, global transfers, and digital storage have made cryptocurrencies attractive tools for laundering illicit funds, facilitated further by mixers, unregulated exchanges, and online gambling platforms. The study examines India's regulatory response, particularly through the Prevention of Money Laundering Act (PMLA) 2002 and the Financial Intelligence Unit–India (FIU–IND) guidelines, which extend AML obligations to Virtual Digital Assets (VDAs). Enhanced Know Your Customer (KYC) norms, due diligence requirements, and restrictions on anonymity-enhancing tools reflect India's effort to align with global standards set by the Financial Action Task Force (FATF). Ultimately, the paper underscores the urgent need for adaptive and technologically advanced AML policies to counter evolving laundering techniques. It calls for stronger enforcement capacity, international cooperation, and collaboration among regulators, financial institutions, and service providers to ensure cryptocurrencies serve as instruments of economic innovation rather than vehicles for illicit finance.

Keywords: Anti-Money Laundering, Cryptocurrencies, Virtual Digital Assets, Financial Intelligence Unit-India, Know Your Customer.

*GRADUATE.

INTRODUCTION

This article aims to take a fresh perspective towards the major issue of money laundering and the use of cryptocurrency by money launderers, criminals or organisations, as a modern way of facilitating money laundering and other financial crimes and its various challenges to Anti-money laundering (AML) regulations.

The main issue or problem of profit-driven criminals is not the making of money, but is hiding the money and the illicit activities that generated such money, because every dollar is recorded and tracked by authorities. Due to this issue, criminals are not able to use the illegally obtained money, as its use can expose or connect them to the crime. To resolve this problem, criminals use money laundering. Money laundering involves masking of financial assets or proceeds of illicit business and integrating them into a nation's legitimate financial systems. The purpose is to use the illegally gained monetary proceeds by disguising them as obtained from a legitimate source.

Money laundering makes it challenging for the financial authorities to find out where undocumented money comes from, to stop crime, prosecute criminals, and seize the illegally earned money and assets. However, with the passing of time and the emergence of more safety and security protocols and procedures, this method of money laundering has become old and traditional in this modern world, and many criminals are being apprehended by the authorities. To evade these apprehensions, criminals began to search for new modern methods for money laundering, and the search ended in the use of cryptocurrency.

CRYPTOCURRENCY - A NEW ATTRACTION FOR MONEY LAUNDERERS

What Is Cryptocurrency?

Cryptocurrencies are a technical and financial innovation as a response to the various flaws and instability in the traditional financial system, which was realised particularly around the time of the 2008 global financial crisis. The cryptocurrency gained rapid recognition in the financial market mainly due to its decentralised nature, meaning it does not rely on middle-man meaning they're generally not backed, controlled, or owned by any government, central bank, or corporation, making it highly potential for the global economy. The Indian rupees on the other hand, is backed by the Indian government, having its seal and is regulated and documented by the Reserve Bank of India.

Cryptocurrency is a digital currency that is free from and does not depend upon any banks for verifying transactions. It does not exist in physical form like paper money or coins because it runs on a virtual network in a peer-to-peer system that enables anyone to send and receive payments across the world. However, it also gained high usage in criminal networks due to its unique features and also in the absence of effective regulations.

REASON FOR THE ATTRACTIONS OF CRYPTO CURRENCY BY MONEY LAUNDERERS

In the current economy, where the financial systems are evolving and greatly relying on digitisation for more strict and detailed tracking and documentation of money, traditional money laundering has become difficult. However, cryptocurrency comes with its unique features appealing to launderers more and more to opt crypto currency for their illicit businesses.

Decentralisation: Cryptocurrencies reduce tracking, procedure and regulations as it excludes the interference of regulatory authorities.

Anonymity: Crypto transactions operate on blockchain technology, which is publicly visible, but the identities of the participants can remain pseudonymous, making it difficult to trace the origin of funds and their history.

Global Transfers: As crypto transactions run over the internet, cross-border transfer becomes easy, minimising the cost and bypassing traditional financial systems. This enables international transfers, thereby easy facilitation of cross-border money laundering.

Easy Storage: Physical money like cash requires huge space or storage and requires carrying around and exchanging hand-to-hand, making it easily visible and trackable by authorities, increasing the risk factor and might lead to seizure. This issue is now solved by the use of cryptocurrency, as they are stored digitally over online databases called crypto wallet each describing specific transactions, negating the need for physical space.

The inception of this revolutionary payment system that allows secure, encrypted transactions has advanced into a widespread mode of payment and transfer of funds. At the same time, increased criminal use of this virtual currency over the past few years in terms of volume has also caused serious regulatory concerns. The absence of efficient control has also made

accessible and established various crypto tools and services accessible and established, dedicated to channelling such criminal profits. These tools and services have further broadened the sphere of their usage beyond cybercrime activities and are now used in all types of criminal activities that require the transmission of money.

CRYPTOCURRENCY AND MONEY LAUNDERING

The cryptocurrency has seen substantial acceptance by consumers, global banks and financial organisations since the introduction of Bitcoin in 2009 due to factors like easy cross-border exchanges and low exchange rates. As a result, the number of crypto transactions has increased over the years. The integration of this virtual currency into the financial market has, at the same time, increased the risk of money laundering and thereby drastically changed the criminal landscape. Over the past decade, cryptocurrency has become more favoured by illegal enterprises and criminals, and unlawful organisations have thus become more sophisticated and professionalised in their operations to help criminal networks to launder their illicit money in large scale with the use of crypto.

In 2025, illicit crypto volume has skyrocketed by nearly 145% to approximately USD 157 billion, a sharp increase compared to 2024, which was only USD 64 billion. This has been facilitated by the utilisation of various tools available at the hands of fraudsters for hiding the origin of such illicit funds.

Mixing Services: Mixers or tumblers are used by launderers to conceal the true origin of the illegal gains by mixing or blending the cryptocurrencies of several users or from various addresses. It is also to be noted that there are times when not all digital assets are dubious, but are mixed together with the illicit ones to hide the owner of such funds.

Unregulated Exchanges: Money launderers often use exchanges which less AML restrictions. Such crypto exchanges require fewer user identity verifications, making them suitable for laundering illicit digital assets.

Online Casino and Gambling Platforms: Online gaming platforms have been seen to be booming for laundering cryptocurrencies, as criminals use stolen coins for bets and withdraw the gained coins, thereby transforming them into real cash.

ENFORCING AML REGULATIONS – COUNTERING MONEY LAUNDERING

In the past decade, cryptocurrencies have gained huge popularity as a means of payment by the people, but it also attracted criminals to use them for various illegal activities. Traditional AML (Anti-money laundering) regulations and processes were not made for cryptocurrency money laundering. This gave various criminals in the cyber world an open field to continue laundering activities, fraud and other unlawful activities using different types of cryptocurrencies.

In India, the fight against money laundering and other unlawful commercial activities has marked by a length of regulatory modifications and amendments. Investigations of various offences of money laundering come under the jurisdiction of various central agencies – the ED (Enforcement Directorate), the Ministry of Finance and the Government of India under the enacted Prevention of Money Laundering Act 2002 (PMLA).

India's financial system always aimed to achieve higher levels of transparency and reliability. This transparency has been greatly heightened by the enactment of the PMLA (Prevention of Money Laundering Act), which has made different institutions handling financial matters and other organisations adhere to its various provisions and implement and execute various actions and procedures to prevent instances of money laundering. In addition to the above, other regulators such as the Reserve Bank of India ("RBI"), the Securities and Exchange Board of India ("SEBI") and the Insurance Regulatory and Development Authority of India ("IRDAI") are empowered to deal with issues relating to money laundering activities and lay down guidelines on anti-money laundering ("AML") standards. These guidelines, read with the PMLA and PML Rules, form the core of the legal framework for AML law and enforcement in India.

The PMLA 2002 also provide for extraterritorial jurisdiction to such authorities to counter cross-border money laundering and has given power to seize the earnings of crime and such persons who commit the offence.

However, it is said that criminals always find loopholes in the systems and devise creative and innovative ways to evade the authorities to continue their criminal activities. The same is the case for money launderers, as they began to adopt advanced technologies like cryptocurrencies to continue laundering activities. This posed a great risk to the financial sector.

AML REQUIREMENT FOR CRYPTOCURRENCY IN INDIA

With the rapid growth in the use of cryptocurrency in money laundering activities and other financial frauds, conventional AML regulations needed to be more stringent. To curb financial crimes in India's cryptocurrency network, the financial intelligence unit- Indian (FIU – IND) has introduced stricter guidelines for that purpose for digital virtual assets (VDA). Virtual digital assets have been statutorily defined under Section 2 (47A) of the Income Tax Act, 1961, inserted by the Finance Act, 2022 and include cryptocurrencies along with others such as NFTs- Non-Fungible Tokens, utility tokens and other security tokens which have been generated through Cryptographic means carrying with them some digital value.

These guidelines regulate entities or organisations that provide services related to Virtual Digital Assets (VDA) and carry on businesses on various Crypto-assets at both international and domestic levels within the country. They have upgraded the KYC compliance to be more stringent by employing mandatory multi-layer verification requirements for new customers by the service providers (SPs) for their own protection from state and non-state actors who misuse them for financing terror groups and money laundering. Now the SPs are also required to carry out re-KYC of their existing customers. This has been done by combining the mandatory PAN requirement with secondary identification (such as Adhaar card or a passport) with separate email verification.

Enhanced due diligence norms are also introduced, requiring the SPs to examine large transactions and report unusual patterns of exchanges or transfers that seem to be unlawful or lack economic justification. Business relationships with potentially risky clients such as PEPs - politically exposed persons (defined under rule 2(1) (db) of PMLR), and natural and legal persons from higher risk jurisdictions specifically with countries designated as tax-havens and those on the FATF grey and black lists are required to be monitored and tracked by the SPs whether their activities or transaction are facilitating and increasing the risks of money laundering or financial criminal organisations and file a suspicious transaction report (STR) for any non-compliance.

Further, new FIU guidelines strongly restrain the conduct of Initial Coin/Token Offerings and prohibit anonymity-enhancing crypto tokens and products/services (such as tumblers/mixers) due to ML/TF risks. The Guidelines also cover smart contract technologies and the facilitation

of VDA transfers to/from un-hosted wallets by crypto-exchanges, while clearly defining related liabilities.

Because of the rising challenges associated with potential increased anonymity and privacy of VDA or cryptocurrency financial flows, such crypto activities are put in the category of high ML/TF risks. The Financial Action Task Force (FATF) has further improved the AML regulation. The FATF is a premier body responsible for actively implementing global standards for countering money laundering and curbing financial terrorism. India became a full member of FATF in 2010. In recent years, FATF has made many changes to its recommendations. It has brought cryptocurrencies and other virtual assets within the purview of AML regulations and made compliance procedures mandatory for VA and VASPs. For analysing and recognising money laundering and terrorist financing activities associated with cryptocurrency transactions, FATF has also given various red flag indications – transaction size and frequency, anonymity, sources of funds, geographical risks, sender & recipient information and transaction patterns.

CONCLUSION

The innovative nature of cryptocurrency has revolutionised the global financial ecosystem by ensuring decentralised and seamless anonymity and cross-border transactions. Parallely, it has also attracted criminals who have developed advanced tools to hide their illegally gained funds. This unlawful usage of the digital currency has made the intersection between cryptocurrency and money laundering highly challenging for the financial authorities, underscoring an urgent need for policy amendments. Legislators or policymakers are therefore required to balance the speed of this technological progress and safeguard financial integrity. With the continued emergence of new cryptocurrencies, Anti-money laundering regulations are also required to be kept updated and regularly adapted to meet the requirements of the modern financial system.

Stricter Know Your Customer (KYC) and due diligence standards are required to prohibit tools such as mixers and tumblers. Curbing Illicit cross border exchanges necessitates international cooperation, adoption of Financial Action Task Force (FATF) recommendations and cross-jurisdictional intelligence sharing to close gaps or loopholes used for facilitating money laundering across countries. In India, the Prevention of Money Laundering Act, 2002 and the Financial Intelligence Unit – India (FIU – IND) guidelines mark a significant step towards defining and regulating Virtual Digital Assets (VDA), but there is also a necessity of enhancing

the enforcement capacity and technological expertise. Cooperation and collaborations between regulators, financial institutions and service providers are required for monitoring and reporting suspicious patterns of money laundering. Lastly, a modern and enhanced policy approach and system is necessary to ensure that cryptocurrencies and other VDAs serve as an instrument of economic enhancement of a country rather than tools for illicit finance.