MONEY LAUNDERING USING CRYPTOCURRENCIES: LEGAL RESPONSE IN INDIA AND IN THE USA

Rahee Chaudhari, Symbiosis Law School, Pune

1. Introduction

The dynamic cat and mouse game between the thieves and the investigating agencies has been brought to the forefront during the 21st century. Technology such as and cryptocurrency has supercharged the age-old concept of simple fraud.

The magnitude of this new threat is enormous. Cryptocurrency crime is estimated to be around 40.9 billion USD in 2024 and with the increasing financial crimes, losses in the United States alone may be as high as 40 billion USD by 2027[1]. To this end, in Europe, the case of DIN SISTERS who built a gigantic drug business with crypto and technological sophistication should be mentioned. In this instance, it was encrypted devices that were used to move drugs and payments made through anonymous crypto accounts[2].

By contrast, the USA has enacted a GENIUS act which is the first crypto-specific act enacted and signed into law. The USA has already launched a battle against the adverse use of these great technologies in the first step by recognizing them and then trying to track and control them. Evidently, the country has already brought in multiple acts on artificial intelligence but have not passed a federal comprehensive artificial intelligence act.

2. Statement of the Problem

Cryptocurrency networks function as a double-edged sword: on one side, rapid innovation has been harnessed for legitimate financial activity, while on the other side criminals increasingly use these systems to evade authorities.

3. Literature Review

3.1 Foundational Doctrinal Literature

Foundational doctrinal work on money laundering, economic offences and transnational

[1] Chainanalysis, Crypto Crime Report 2025
[2] Geoff White, *From Cartels to Crypto: How the tech industry washes money for the world* (2024)

financial crime predates cryptocurrencies but still shapes how regulators and courts conceptualise illicit finance and design counter-measures. Stessens' *Money Laundering: A New International Law Enforcement Model*[3] traces the evolution of money laundering from a derivative offence connected to drug trafficking into a central policy concern that justified criminalisation of handling criminal proceeds, the introduction of far-reaching confiscation regimes and preventive obligations on financial institutions. Stessens analyses jurisdiction, mutual legal assistance and banking secrecy, highlighting how the cross-border movement of value undermines traditional territorial notions of criminal law and necessitates cooperative enforcement techniques that are now being adapted—often imperfectly—to crypto-asset environments.

Parallel literature in *Crime, Law and Social Change*[4] and related journals, including work by Levi[5] and co-authors, documents the growth of economic and cyber-enabled frauds and examines the limitations of traditional criminal-justice responses. These studies show that fraud and economic crime statistics are chronically under-reported; that many police and prosecution agencies have not increased their capabilities in proportion to changing fraud patterns; and that a purely reactive, case-by-case criminal-justice model struggles to cope with mass, low-value but cumulatively high-impact offences facilitated by digital infrastructures. This insight is highly relevant to crypto-enabled offences, where the volume of small, automated or cross-border transactions can overwhelm investigative capacity and call for public-health or risk-based approaches rather than traditional "offender-by-offender" strategies.

3.2 Modern jurisprudence of Cryptocurrency

De Filippi and Wright address the decentralised nature of blockchain architectures in their article, "Blockchain and the Law" which refers to the tension between code-based governance and government regulation. Their discussion is essential to comprehend the regulatory issues that arise due to the decentralised finance (DeFi) and mixers[6].

Brümmer provides a more in-depth analysis on legal classification, prudential regulation,

[3] GUY STESSENS, *MONEY LAUNDERING: A NEW INTERNATIONAL LAW ENFORCEMENT MODEL* (Cambridge Univ. Press 2000).
[4] Springer Nature, Crime, Law and Social Change, https://link.springer.com/journal/10611.
[5] Michael Levi et al., *Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research*, 67 Crime L. & Soc. Change 77 (2017).
[6] Primavera De Filippi & Aaron Wright, *Blockchain and the law: The rule of Code* (Harvard University Press. 2018)

market integrity and sanctions in the edited volume "Crypto-assets". It sheds light on the jurisdiction of various jurisdictions and the way cryptocurrencies are dealt with under current financial regulations[7].

3.3 Policy and Regulatory Reports

Policy and regulatory reports are essential in the description of activities and regulatory frameworks that influence the operations of companies around the world. Guidance of a Risk-Based Approach to Virtual Assets and VASPs (2019) which suggested ideas for risk assessment has later focused updates established by FATF to create the global AML/CFT minimum standard when it comes to virtual assets, such as the Travel Rule and DeFi risks. These reports have significant impact on Indian and U.S. regulatory responses.

Regulatory pronouncement on Digital Payments Fraud and VDA reporting obligation are available in Indian RBI Annual Reports (2018-2025) [8] and guidance notes issued by FIU-IND on the subject matter of Digital Payments Fraud and VDA reporting obligation. The procedures of incident reporting and data retention are introduced in CERT-In Directions (2022) and subsequent advisories.

Since 2019, FinCEN[9] guidance has clarified the nature of the BSA application to virtual currency actors in the United States and the Sanctions Compliance Guidance to the Virtual Currency Industry (2021) by OFAC has established the sanctions-screening requirements for crypto platforms. U.S. Treasury DeFi Illicit Finance Risk Assessment[10] (2023) and Illicit Finance Strategy (2024) are sophisticated regulatory thought on risks with regards to compounds.

3.4 Academic Articles and Practitioner Research

The analyses of work by Micheal Levi (2021) [11] discuss how financial cybercrime has evolved and emphasize on social engineering and regulatory gaps, as well as their exploitation. Wall proposes that the science of criminology should be re-theorized to deal with crimes of the

[7] Chris Brummer, Cryptoassets: Legal, Regulatory, and Monetary Perspectives (Oxford University Press. 2019)
[8] Reserve Bank of India, *Annual Report (2018-2025);* Financial Intelligence unit – India, *Guidance Notes on VDA Reporting (2023)*
[9] FinCEN, *Applications of FinCEN's Regulations to persons administering, exchanging, or using Virtual currencies (*2019)
[10] OFAC, *Sanctions Compliance Guidance for the virtual currency industry (2021)*
[11] Micheal Levi, *Financial Cybercrime and Regulatory Evasion, 45 Crime L. & Soc. Change 89 (2021)*

digital-native. [12] Arun Sukumar's scholarship is dedicated to the topic of intermediary liability and the regulation of platforms in India, which is directly applicable to the attribution of responsibility of the services provided by crypto. [13]

3.5 Synthesis and Gaps that are identified

The relationship between the criminals and law enforcement officials is complicated. The problem is that the complexity of the crime and the regulators' response is increasing. The use of crypto currencies and block chain can enable today's economic bad guys to create adaptive and intelligent systems that can automatically detect vulnerabilities and carry out sophisticated economic crimes, while also adjusting their attacks in real-time to evade detection.

Fragmentation of regulatory Frameworks:

The problem is that there is a lack of harmony of regulatory approaches among jurisdictions, a lack that is made particularly apparent when one looks at the difference between developed legal systems like the United States and India. The absence of international regulations on cryptocurrency crimes is an opportunity for regulatory arbitrage, which is the ability of cryptocurrency criminals to evade punishment due to the different regulations in countries.

Lack of Risk Assessment and Management

Emerging analytic tools could in principle help identify layered transaction patterns and support earlier intervention, but these remain underdeveloped relative to the sophistication of criminal techniques.

Limits on Enforcement across borders

Let us also note that planning and coordination of the intent and goals of the criminals in the various parts of the world has been developed sufficiently to carry out the crimes and to evade investigators. This criminality is global and it needs to be supervised by a globalised or at least internationally linked investigating agency to prosecute cross-border economic crimes and conduct investigations of crimes. The variation in policies of various nations and countries has rendered inconsistency in the regulation of crypto governance. This has not only caused

[12] David S. Wall *Cybercrime in the Digital era: Rethinking Criminology, 58 Brit. J. Criminology 1 (2020).*
[13] Arun Sukumar, *Intermidiary Liability and Tech Regulation in India, Carnegie India Papers* (2021)

conflict of jurisdiction but has contributed to the gaps in enforcement.

A major problem in the realm of effective investigation of complex crypto-enabled crimes is the disconnect between the technology needed to investigate such offences and the legal frameworks and institutional capacities that support these investigations.

The insufficiency of preventative mechanism

The lack of comprehensive and coherent laws specifically governing cryptocurrencies has also weakened the preventive function of criminal law and the signalling effect of sanctions designed to discourage participation in such offences.

4. Research Gaps

a) **The multiplication of evasion methods** of criminals with the help of Crypto currencies: Numerous studies consider the use of Crypto currencies in the financial crime detection.

b) **Lack of proper strategy to allocate resources towards development of properly supervising Cryptocurrency**. Current studies show that there are gaps in terms of the distribution of the right resources that were deployed to control and resolve these complex economic offenses and create the infrastructure required to address the offenders.

c) Lack of comprehensive, self-contained legislative frameworks to control and govern cryptocurrency and related virtual-asset activities. Comparative legal analysis of how various jurisdictions, especially developed systems such as the United States and developing regulatory systems such as India, are modifying their legal frameworks to deal with technologically sophisticated crypto-enabled offences remains limited.

5. Research Questions

1. Which technological characteristics of cryptocurrency systems applications are being used to commit economic crimes, and what are the ways that such mechanisms make legal enforcement difficult?

2. How well is the current Indian legal and regulatory framework equipped to deal with crypto-enabled economic offences?

3. What is the effectiveness of the institutional mechanisms and enforcement strategies used by Indian authorities to detect, investigate and prosecute such offences, especially those that have a cross-border dimension?

4. What is the legal, regulatory, and enforcement framework that exists in the United States to regulate economic offences involving cryptocurrency, and how the legal, regulatory, and enforcement frameworks operationalised in practice?

5. What is the comparison between the U.S. structure and the Indian one in legislative clarity, regulatory proactiveness, capacity of institutions, and inter-agencies cooperation in the fight against economic offences in the sphere of new technologies?

6. Research Objectives

1. To understand and reproduce new trends in cryptocurrency-related economic crimes, including the identification of new criminal typologies, the study of patterns of technological convergence, and an evaluation of the magnitude, complexity and consequences of these crimes in the global financial systems.

2. To Explore risk mechanisms and vulnerabilities that cryptocurrency integration generates to research the economic crimes, including assessing the risks of compounds, examining the existing risk assessment frameworks, as well as creating overall risk typologies unique to technologically mediated financial crimes.

3. To critically assess of the sufficiency of current legal frameworks to combat cryptocurrency economic crimes, both in India and in the United States, and analysis of the legislative frameworks and regulatory mechanisms, enforcement abilities, and identification of any gaps and limitations in the law.

4. To relate a systematic comparative study of Indian and the United States approaches to economic crimes that are carried out with the assistance of cryptocurrency.

7. Research Methodology

The researcher will adopt a secondary research methodology on this research as well as content analysis. The scholar will be conducting a thorough study (qualitative research) of what is available in terms of its doctrines. The following modes have been selected by the researcher to carry out this research.

8. Limitations

1. **Legal Ambiguity**: the statutory, jurisdictional, judicial and legal ambiguity which exist because of the lack of formal acts on the economic offences does not enable the investigating machinery or the independent agencies to probe freely.

2. **The economic offences being limited to the crimes which have been committed with Cryptocurrency**.

3. **Indecisive judicial standpoint**: The judicial standpoints have remained indeterminate to interpret as part of an effort to ensure that the industry is an inclusionary nature and this has contributed to the confusing state of the study.

9. Analysis

9.1 Trends and typologies in cryptocurrency-related economic crimes

The first dimension of the analysis relates to the growing trends and typologies of cryptocurrency-related economic crimes and its scale which define the risk landscape that India and the United States regulators and enforcement authorities need to tackle. Cryptocurrencies do not in themselves create new categories of offences, but rather provide new infrastructure through which existing offences can be more quickly carried out, across borders and more automated, and familiar offences like fraud, cheating, breach of trust, Ponzi schemes and money laundering can be performed.

Empirical practitioner reports, such as the Chainalysis Crypto Crime Report 2025, show that despite the fact that the share of illicit transactions has fallen as a percentage of total on chain volume, the total value of crypto activity associated with illicit activity has been in the tens of billions of US dollars per year. These streams are indicative of the proceeds of ransomware

operations, darknet markets, major investment frauds, online scams, and sanctions evasion activities, and are laundered through a mixture of centralised exchanges, decentralised protocols and informal off-chain arrangements. Therefore, criminal use of cryptocurrencies is an intrinsic part of the digital financial system and not a fringe phenomenon.

In this general context, clear patterns of crime typologies have emerged. A large category is ransomware and digital extortion, where the attackers use malware to encrypt a victim's system and ask for ransom money, often in cryptocurrency, with the difficulty of tracing crypto addresses and the quick movement of crypto between chains making it easy to hide one's tracks. The other typology is investment related fraud, involving the use of "pig butchering" schemes where fraudsters use social engineering and fake trading platforms or impersonated exchanges to trick victims into depositing fiat funds and transferring funds to wallets under their control. The third typology relates to professionalised laundering and sanctions evasion, with the systematic use of mixers, tumblers, cross chain bridges, stablecoins and privacy enhancing coins to clean money or to transfer funds across jurisdictions to evade financial controls.

These typologies are even more complex by technological convergence. The automation of many transactions made possible through programmable smart contracts and decentralised finance (DeFi) protocols, such as flash loan driven exploits and cross chain swaps, can significantly hinder tracing and attribution. Meanwhile, blockchain analytics tools enable public and private businesses to map networks of addresses and look for patterns, creating a dynamic "arms race" between the criminals and the analytics companies that improve as criminals get more sophisticated.

These trends translate into distinct and yet converging risk profiles in India, and the United States. Large scale token scams and Ponzi type crypto investment schemes that target retail investors have had a particular impact on India, which typically are based on informal networks and lightly regulated offshore exchanges. Meanwhile, the United States – due to having large crypto markets and being a key part of the global financial system – has been a key jurisdiction for significant ransomware attacks, mixer-oriented laundering operations and enforcement against service providers. Yet, both jurisdictions face the same facts: crypto related economic crime is pervasive, cross-border and technology-driven, and not a transient or secondary issue.

9.2 Risk mechanisms, vulnerabilities and risk assessment frameworks

The second strand of analysis is the particular risk mechanisms and vulnerabilities sparked by cryptocurrencies and if current anti money laundering (AML) and risk assessment frameworks are sufficient to capture these. The traditional AML regimes, including the Financial Action Task Force (FATF) Recommendations, were based on the concept that risk could be managed by putting onus on regulated, centralised entities like banks and other financial institutions to implement prevention duties. Customer due diligence, monitoring and reporting are all premised on the existence of a clearly identifiable "gatekeeper" institution.

Cryptocurrencies attack this model in three ways at least. First, addresses are pseudonymous and users are able to hold their assets outside of regulated intermediaries, at the point of transfer, which makes the implementation of customer due diligence and "know your customer" measures associated with account based systems less effective. Secondly, there are "regulation light" environments which are structurally created by decentralised protocols, such as automated market makers, peer to peer exchanges and cross chain bridges, where users can move value, swap tokens, and access liquidity without any single entity having comprehensive control of the onboarding, monitoring, or reporting processes. Third, crypto transactions are naturally cross-border: a resident of India can have direct access to an unregulated exchange or DeFi protocol in the world, removing the need to obtain local licenses and supervision, thus rendering domestic risk assessments incomplete by design.

In recognition of these features, both India and the United States have started to update their risk frameworks. The recent inclusion of some virtual digital asset (VDA) service providers in the Prevention of Money Laundering Act (PMLA) and the introduction of record keeping and reporting requirements are important developments in India to incorporate crypto into the country's local AML framework. While FIU IND guidance, RBI's take on digital payments fraud and CERT In's incident reporting guidance have all contributed to the evolution of crypto risk management, internal risk frameworks of many entities continue to be rule-driven and largely dependent on static KYC which are unable to account for on chain typologies.

Risk frameworks in the United States are generally more well developed and also vary by institution. FinCEN's guidance includes many typologies of virtual asset businesses as money service businesses and is required to be registered and fulfill AML obligations, and Treasury's DeFi and virtual currency risk assessments explicitly address typologies like ransomware,

mixer based laundering, and sanctions evasion. Adoption of advanced blockchain analytics and typology based red flag indicators is not consistent across the lower and/or offshore exchanges, while a concern is with the use of proprietary analytics and the coverage of privacy preserving technologies.

The analysis under this heading indicates that general, technology agnostic risk frameworks are not sufficient to address crypto-specific risks. Risk assessment needs to be made explicit "crypto aware", and involve on chain analytics, typology mapping, dynamic red flag indicators (e.g., repeated engagement with high risk services or known illicit service clusters), and a knowledge of the AML risk associated with certain protocol designs. Guidance and regulation in India and the US have started to catch up, but there's still a disconnect between theory and practice, particularly in smaller banks and new markets.

9.3 Legal comparative study of Indian and US

The third category of analysis examines the extent to which the existing Indian and US legal framework (both substantive and procedural) would suffice to tackle cryptocurrency related economic crimes and conduct a comparative analysis of the approaches of both the Indian and the US legal frameworks. This involves looking at the statutory provisions, the regulation documents, the roles of the institutions and the practical experience of enforcement.

The key substantive provisions of PMLA 2002 for addressing money laundering, including crypto cases, are the criminalization of the conduct of money laundering as the property of scheduled offenses and the authority to attach and confiscate. Exchanges and some intermediaries are now included as 'reporting entities' under PMLA and thus fall under a robust AML compliance regime. However, there is no specific and comprehensive legislation which clearly defines the legal framework of cryptocurrencies, sets licensing requirements for exchanges and custodians and specifies the complete set of responsibilities for all types of virtual asset intermediaries. This patchwork fashion can cause legal uncertainty on both sides, that is for regulators and the regulated.This patchwork can create legal insecurity for the regulators and regulated and may hinder coherent development of case law.

On the procedural side, the Indian agencies such as the Enforcement Directorate, FIU IND, CERT In, Reserve Bank of India and state police cyber crime units have gradually been beefing up their capacities to process investigations related to cryptocurrencies. They have proven to

be capable of tracing the flows, freezing the balances on local platforms, and interacting with foreign exchanges as needed, such as in the case of the HPZ token and GainBitcoin scams. Despite this, there are challenges: the length of time that can be taken to assist in investigations through mutual legal assistance procedures, lack of fully standardised approach to the collection, preservation and presentation of blockchain evidence, technical forensic capacity is not equal across all locations outside of major metros and overlapping mandates between agencies can result in duplication and/or gaps.

The legal setting is more detailed but disjointed in the United States. On the substance, multiple federal laws are applicable to crypto activities, including the Bank Secrecy Act and related regulations for anti-money laundering, wire fraud and securities fraud laws, and sanctions laws administered by the OFAC, and recent legislation like the GENIUS Act, aimed at creating a federal framework for payment stablecoins. The FinCEN guidance and OFAC's guidance on sanctions compliance for virtual currency providers provide some clarity on the applicability of these regimes to virtual asset businesses.

Procedurally, US enforcement has units in the Department of Justice, FBI, IRS CI and others, and has plenty of experience investigating complex financial crime. The now reformed National Cryptocurrency Enforcement Team and other internal preparations signal institutional willingness to pursue crypto cases, while US courts have started to establish case law on how blockchain evidence is admissible, what tokens are and who is liable, and how intermediaries can be held liable. Meanwhile, the murky overlap of recent jurisdictional claims, particularly as they relate to token classification, and the enforcement by guidance or litigation as opposed to detailed ex ante legislation has introduced a grey zone for good-faith actors looking for clarity.

Both systems are partially sufficient in comparison. The US has more mature institutions, more specific instructions and more extensive case law, while facing issues of fragmentation and regulatory competition. Although India has strong confiscatory powers and a centralised enforcement, it does not have equivalent statutory clarity and consistently high level forensic capacity. The analysis thus indicates that neither jurisdiction has yet fully reached a coherent and comprehensive and technologically sensitive construction of the legal regime of crypto facilitated economic offences; and that both have strengths to draw on that can contribute to the reform process in the other jurisdiction.

9.4 Legal, regulatory and policy recommendations for strengthening India's response

The final analytical category brings together comparative lessons from the Indian and US experiences and establishes reform-oriented recommendations for India, within its constitutional and institutional context. The comparative discussion points to the fact that the models of the USA cannot be simply transferred to India, but direction and design guidance can be drawn from the same.

It would be advantageous for India to have a statutory framework for crypto assets and their services based on activities, instead of relying mainly on a slew of executive instruments and PMLA extensions. This law could specify the regulated activities, including exchange, custody, issuance, operating some kinds of DeFi interfaces, mixing or privacy services; include licensing conditions and fit and proper requirements; set out core obligations as customer due diligence, record keeping, travel rules and sanctions screening. Would provide improved enforcement and compliance baseline and decrease to date reliance on interpretive guidance and enforcement action.

As far as institutional design is concerned, India needs to formalise and enhance inter agency coordination among ED, FIU IND, CERT In, RBI, MeitY and police cybercrime units in the form of joint task forces, common analytics platforms, and standard operating procedures for cryptocases. The creation of a National Crypto Intelligence Hub to centralise blockchain forensic insights, typology information and red flag indicators could lead to more proactive detection and prioritisation of high-risk cases. Ongoing training for investigators, prosecutors and judges on crypto evidence and typologies would help to ensure that good cases result in long-term convictions.

US practice indicates that lessons learned on risk and supervision include the need for clear, explicit, and public guidance on typologies and risk indicators, and systematic interactions with the private sector to harmonize expectations and to share intelligence. India can replicate the same by releasing more specific FIU IND and RBI guidelines on crypto specific red flags and by urging domestic exchanges and service providers to introduce blockchain analytics in their AML programmes with a due consideration for privacy and data protection measures.

Internationally, India should strive to increase its involvement in international bodies and fora for establishing standards and practices, and, in addition to complying with the FATF

standards, provide its experience of successful large scale retail scams and informal networks to influence the norms and standards on virtual asset supervision and cooperation. This will involve discussing expedited channels of cross-border information sharing, asset freezing in crypto cases, US-India cooperation, and multilateral mechanisms.

Lastly, reforms should be targeted to prevent unintended side effects. Excessively restrictive policy measures, such as de facto exclusion of compliant domestic exchanges, could push users to less transparent and more difficult to regulate exchanges and peer to peer markets abroad. On the other hand, too loose or vague standards might make regulatory arbitrage and the drawing of illegal flows possible. The analysis therefore tends to point towards a balanced model: strong licensing & AML standards for domestic intermediaries, focused measures on the activities with highest risk (unregulated intermediaries/mixers, non-transparent cross chain services) and proportionate responses to non-compliance, within a constitutional culture with a strong sense for proportionality, privacy and due process.

10. Conclusion

As mentioned above, cryptocurrencies have not only introduced a new payment mechanism into the financial system but have also completely changed the infrastructure for planning, carrying out and hiding economic offences, especially money laundering offences. In short, rather than a passing technological novelty, crypto-enabled crime has become an established element of today's financial landscape, with unique typologies that feature ransomware monetisation, investment and “pig butchering” scams, and advanced sanctions evasion and laundering schemes that incorporate mixers, cross chain bridges, privacy enhancing tools and stablecoins. These advances have created a qualitatively new “criminogenic” environment where the characteristics of decentralised networks like speed, global reach, programmability – far exceed the design of legacy anti money laundering (AML) frameworks.

The paper has also highlighted the distinctive risk mechanisms of cryptocurrencies that are not well captured by traditional, institution-centred risk models. The effectiveness of account-based customer due diligence and transaction monitoring systems is also undermined by pseudonymous addresses, the use of non-custodial wallets and the decentralised nature of the protocols, and the fact that on chain transfers are inherently cross-border in nature makes purely national risk assessments incomplete. While both India and the United States have started to adjust their frameworks (e.g., by introducing virtual asset service providers as reporting entities

under the Prevention of Money Laundering Act in India and through guidance from FinCEN and the U.S. Treasury), this adjustment process is uneven and, in important ways, reactive rather than anticipatory.

Concerning legal and institutional reactions, the comparative study shows that both jurisdictions are partially sufficient. While India has a robust confiscatory regime in PMLA and has taken key steps such as extending the AML regime to certain VDA service providers, a comprehensive, activity based primary legislation for crypto assets is missing, and there are also disparities in forensic capabilities and inter agency coordination. In contrast, the United States has more established institutions, guidance from regulators, and an ever-evolving body of judicial interpretations, including the recent issuance of the GENIUS Act as the first significant legislative framework for payment stablecoins, but still has significant issues stemming from the fragmentation of the regulatory landscape and overlapping jurisdiction claims that frequently have been addressed by enforcement action because of the lack of clear guidance ex ante in the law.

In this context, the paper has called for a reform agenda for India that is grounded in but not simply in line with, the US experience. Some of the key elements in this agenda are: the implementation of a statutory framework that specifies the functions of regulated crypto assets and the obligations of the reporting entities, establishment of a National Crypto Intelligence Hub for integration of on chain analytics and crypto specific red flag indicators in agencies' risk assessment practices, formalization of inter-agency coordination via joint task forces and SOP, and the development of blockchain forensic capabilities. The paper has also highlighted the importance of India's active involvement in developing new norms for the regulation and cooperation on virtual assets at the international level instead of just the execution of the norms set by others.

Finally, this research's main finding is that a successful approach to money laundering with cryptocurrencies is not possible by "bolting-on" legacy AML tools. They need legal doctrine, regulatory design and institutional practice to be radically rethought along the lines of the structural characteristics of decentralised, programmable and borderless value networks. This means that for India, it is no longer about episodic, seizure centric enforcement but a technologically literate, intelligence informed, constitutionally sound approach in which the crypto asset ecosystem is seen as a legitimate part of the financial system, and not an aberration

at the fringes. In doing so, India can not only save its own financial integrity but also make a meaningful contribution to the changing landscape of economic crime control in the digital age, globally.

Bibliography

- Chainanalysis, Crypto Crime Report 2025
- Geoff White, From Cartels to Crypto: How the tech industry washes money for the world (2024)
- GUY STESSENS, MONEY LAUNDERING: A NEW INTERNATIONAL LAW ENFORCEMENT
- MODEL (Cambridge Univ. Press 2000).
- Springer Nature, Crime, Law and Social Change, https://link.springer.com/journal/10611.
- Michael Levi et al., Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research, 67 Crime L. & Soc. Change 77 (2017).
- Primavera De Filippi & Aaron Wright, Blockchain and the law: The rule of Code (Harvard University Press. 2018)
- Chris Brummer, Cryptoassets: Legal, Regulatory, and Monetary Perspectives (Oxford University Press. (2019)
- Reserve Bank of India, Annual Report (2018-2025); Financial Intelligence unit – India, Guidance Notes on VDA Reporting (2023)
- FinCEN, Applications of FinCEN's Regulations to persons administering, exchanging, or using Virtual currencies (2019)
- OFAC, Sanctions Compliance Guidance for the virtual currency industry (2021)
- Micheal Levi, Financial Cybercrime and Regulatory Evasion, 45 Crime L. & Soc. Change 89 (2021)
- David S. Wall Cybercrime in the Digital era: Rethinking Criminology, 58 Brit. J. Criminology 1 (2020).
- Arun Sukumar, Intermediary Liability and Tech Regulation in India, Carnegie India Papers (2021)