INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

ISSN: 2582-6433

BLOCKCHAIN-BASED FINANCIAL CRIMES: LEGAL CHALLENGES AND EVOLVING PROSECUTORIAL STRATEGIES IN CRYPTOCURRENCY-RELATED OFFENCES

AUTHORED BY - HAROON RASHID S
Student, School of Law
Vels Institute of Science, Technology & Advanced Studies (VISTAS)

CO-AUTHOR - AKHIL SAJEEV
Assistant Professor, School of Law
Vels Institute of Science, Technology & Advanced Studies (VISTAS)

ABSTRACT

The rapid proliferation of blockchain technology and cryptocurrency has engendered a paradigm shift in the architecture of financial crime. From money laundering orchestrated through decentralised exchanges to large-scale investment fraud enabled by smart contracts, blockchain-based financial crimes present unprecedented challenges for legal systems across jurisdictions. This paper examines the intersection of distributed ledger technology and criminal law, critically analysing the legal lacunae that facilitate illicit activity and the evolving prosecutorial strategies deployed to counter them. Drawing upon international case law, legislative frameworks, and interdisciplinary scholarship, the paper argues that effective prosecution of cryptocurrency-related offences demands a coordinated response integrating advanced forensic analytics, harmonised international legal standards, and adaptive domestic legislation. The paper further evaluates the Indian regulatory landscape, tracing its development from judicial interventions to the Virtual Digital Assets framework, situating it within the global anti-money laundering matrix. Ultimately, the paper contends that while technological innovation has outpaced legal architecture, emerging prosecutorial tools and international cooperation mechanisms are progressively closing the enforcement gap.

Keywords: *Blockchain, Cryptocurrency, Financial Crimes, Money Laundering, Prosecutorial Strategy, FATF, Virtual Digital Assets, AML, Decentralised Finance.*

ISSN: 2582-6433

I. INTRODUCTION

The advent of blockchain technology, first operationalised through the Bitcoin protocol in 2008, was celebrated as a transformative innovation promising decentralised, transparent, and immutable financial transactions.[1] Yet, the very attributes that render distributed ledger technology revolutionary ,pseudonymity, permissionless access, cross-border operability, and resistance to censorship ,have simultaneously made it an instrument of choice for sophisticated financial criminals. Within less than two decades of Bitcoin's genesis, cryptocurrency has become deeply embedded in the architecture of money laundering, terrorist financing, ransomware, market manipulation, and large-scale investment fraud.

The Financial Action Task Force (FATF) has identified virtual assets as a significant and growing vector for money laundering and terrorism financing, urging member states to extend their anti-money laundering (AML) and counter-terrorism financing (CTF) obligations to virtual asset service providers (VASPs).[2] Europol's Internet Organised Crime Threat Assessment has similarly catalogued the deepening penetration of cryptocurrency into organised crime ecosystems, ranging from dark web marketplaces to ransomware syndicates.[3] The United Nations Office on Drugs and Crime has estimated that billions of dollars in criminal proceeds are laundered annually through cryptocurrency networks.[4]

These developments impose acute pressures on legal systems designed for a pre-digital era of financial regulation. Traditional prosecutorial frameworks premised upon identifiable financial institutions, traceable paper trails, and territorial jurisdiction sit uncomfortably with blockchain's decentralised architecture, pseudonymous transacting, and borderless operations. The result is an enforcement deficit that criminal actors have been quick to exploit.

This paper proceeds in five principal parts. Following this introduction, Part II examines the typology of blockchain-based financial crimes and the enabling characteristics of cryptocurrency. Part III analyses the principal legal challenges encountered by prosecutors.

[1]Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 10 April 2025.
[2]Financial Action Task Force (FATF), 'Virtual Assets and Virtual Asset Service Providers' (Updated Guidance, 2021) <https://www.fatf-gafi.org> accessed 10 April 2025.
[3]Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2021' (European Union Agency for Law Enforcement Cooperation, 2021) 40–45.
[4]United Nations Office on Drugs and Crime (UNODC), 'Money Laundering and the Financing of Terrorism Through Cryptocurrency' (UN, 2020) 12.

ISSN: 2582-6433

Part IV surveys evolving prosecutorial strategies and enforcement innovations. Part V considers the Indian regulatory and prosecutorial landscape. The paper concludes with recommendations for a coherent legislative and enforcement architecture.

II. TYPOLOGY OF BLOCKCHAIN-BASED FINANCIAL CRIMES

Blockchain-based financial crimes are not monolithic. They encompass a diverse and evolving range of predicate offences, each exploiting distinct features of distributed ledger technology. A coherent prosecutorial response requires precise taxonomical understanding of these offence categories.

A. Money Laundering Through Cryptocurrency

Money laundering represents the most pervasive category of cryptocurrency-enabled financial crime. The three-stage typology of placement, layering, and integration maps onto cryptocurrency ecosystems with notable facility. Criminals convert illicit fiat currency into cryptocurrency (placement), conduct rapid sequences of transactions across multiple wallets, mixing services, and chain-hopping protocols to obscure the audit trail (layering), and ultimately convert cryptocurrency back into legitimate assets (integration).[5]

The prosecution of *US v Ulbricht*[6] illustrated the operationalisation of cryptocurrency-enabled money laundering through dark web platforms. The Silk Road marketplace processed over 1.2 million transactions involving an estimated 9.5 million bitcoins before its dismantling in 2013. 'Tumbling' or 'mixing' services ,which aggregate and redistribute cryptocurrency to obscure transactional origin ,present particular evidentiary challenges, as they deliberately fragment the blockchain's otherwise transparent record.[7]

B. Cryptocurrency Fraud and Investment Scams

The explosive growth of cryptocurrency markets has furnished fertile ground for investment fraud. Initial coin offering (ICO) scams, rug pulls in decentralised finance (DeFi) protocols, Ponzi schemes denominated in cryptocurrency, and celebrity-endorsed pump-and-dump schemes have collectively caused billions of dollars in investor losses. OneCoin, perhaps the

[5]Chainalysis, 'Crypto Crime Report 2023' (Chainalysis Inc, 2023) <https://go.chainalysis.com/crypto-crime-2023.html> accessed 10 April 2025.
[6]US v Ross Ulbricht, No 14-CR-68 (KBF) (SDNY 2015). Ross Ulbricht was convicted of money laundering, drug trafficking, and continuing a criminal enterprise through the Silk Road dark web marketplace.
[7]Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (Center on Sanctions and Illicit Finance, 2018) 7.

ISSN: 2582-6433

largest cryptocurrency fraud in history, defrauded investors of an estimated USD 4 billion globally.[8] Such schemes frequently exploit the information asymmetry between technologically sophisticated promoters and retail investors unfamiliar with blockchain mechanics.

C. Ransomware and Cybercrime Financing

Ransomware attacks, in which malicious software encrypts victim data and demands cryptocurrency ransom for decryption, represent a rapidly escalating cyber-financial threat. The mandatory use of cryptocurrency in ransomware payments is not incidental; it reflects deliberate exploitation of cryptocurrency's pseudonymous and borderless characteristics to insulate criminal proceeds from seizure. The Colonial Pipeline ransomware attack of 2021 resulted in a USD 4.4 million ransom payment in Bitcoin, a significant portion of which was subsequently recovered by the United States Department of Justice through blockchain tracing, demonstrating both the vulnerability and the recoverability of such proceeds.

D. Terrorist Financing Through Virtual Assets

Terrorist organisations have increasingly turned to cryptocurrency to circumvent international financial sanctions and correspondent banking restrictions. While the aggregate quantum of terrorist financing through cryptocurrency remains modest relative to traditional channels, its potential for rapid, borderless transfer renders it a significant security concern. FATF has specifically highlighted the use of virtual assets by designated terrorist groups, urging enhanced monitoring and targeted financial sanctions against virtual asset addresses associated with such entities.[9]

III. LEGAL CHALLENGES IN PROSECUTING CRYPTOCURRENCY-RELATED OFFENCES

A. Definitional and Classificatory Ambiguity

A foundational challenge confronting cryptocurrency prosecution is the absence of settled legal definitions for cryptocurrency and its associated instruments. Whether a cryptocurrency constitutes 'money', 'property', a 'commodity', or a 'security' determines which regulatory authority holds jurisdiction, which offences apply, and what evidentiary standards govern. This

[8]Ruja Ignatova, the self-styled 'Cryptoqueen', raised approximately USD 4 billion through OneCoin, a fraudulent scheme. See US v Ruja Ignatova, No 17-CR-630 (ER) (SDNY 2019).

ISSN: 2582-6433

definitional uncertainty has spawned fragmented regulatory architectures across jurisdictions.[10] In *US v Harmon*[11] the District of Columbia Federal District Court held that Bitcoin constitutes 'money' within the meaning of the DC Money Transmitters Act, enabling prosecution of unlicensed cryptocurrency exchange operations. Conversely, the *SEC v Ripple Labs*[12] litigation has animated protracted judicial examination of whether XRP tokens qualify as investment contracts under the *Howey* test, with profound implications for the regulatory classification of thousands of similar tokens. The European Union's Markets in Crypto-Assets Regulation (MiCA) represents the most comprehensive legislative attempt to date to resolve these classificatory uncertainties through harmonised definitions.[13]

B. Pseudonymity and the Identification Problem

Blockchain transactions are recorded under alphanumeric wallet addresses rather than verified identities. This pseudonymous architecture, distinguishable from full anonymity but substantially more opaque than conventional financial transactions, significantly complicates the identification of criminal actors. Privacy-enhancing cryptocurrencies such as Monero and Zcash deploy advanced cryptographic techniques including ring signatures and zero-knowledge proofs to achieve near-complete transactional anonymity.[14] The identification of beneficial owners across chains of pseudonymous transactions demands forensic capabilities substantially beyond those required in conventional financial investigations.

Mixing services, commonly known as 'tumblers', compound the identification problem by aggregating and redistributing cryptocurrency across multiple wallets, deliberately severing the transactional chain. The prosecution in *US v Sterlingov*[15], targeting the Bitcoin Fog mixing service, demonstrated that blockchain analytics can, with sufficient computational resources, reconstruct transactional chains even through tumbling operations, albeit at considerable evidentiary complexity.

[10]Andres Guadamuz and Chris Marsden, 'Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies' (2015) 20(12) First Monday <https://firstmonday.org/article/view/6105/4969> accessed 10 April 2025.
[11]US v Larry Dean Harmon, 497 F Supp 3d 1 (DDC 2020). The court held that bitcoin constitutes 'money' under the DC Money Transmitters Act, significantly expanding the regulatory scope.
[12]SEC v Ripple Labs Inc, No 20-cv-10832 (SDNY, filed 22 December 2020). This case raised foundational questions about whether XRP qualifies as a security under the Howey test.
[13]Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets [2023] OJ L150/40 (MiCA Regulation).
[14]Zerocash protocol (ZEC) and Monero (XMR) utilise zero-knowledge proofs and ring signatures respectively to achieve near-complete transaction anonymity; see Eli Ben-Sasson and others, 'Zerocash: Decentralized Anonymous Payments from Bitcoin' (2014) IEEE Symposium on Security and Privacy 459.
[15]US v Sterlingov, No 21-cr-399 (RDM) (DDC 2021). This Bitcoin Fog case demonstrated the prosecutorial use of blockchain analytics to trace transactions through mixing services.

ISSN: 2582-6433

C. Jurisdictional Fragmentation

Blockchain's inherently transnational character renders territorial conceptions of jurisdiction largely inadequate. A single money laundering transaction may involve a perpetrator in one jurisdiction, a mixing service hosted in a second, an exchange registered in a third, and a victim in a fourth. The applicable law, evidentiary standards, and enforcement competencies of each jurisdiction may differ substantially, creating opportunities for regulatory arbitrage that sophisticated criminal actors readily exploit.[16]

Mutual legal assistance treaty (MLAT) mechanisms, while theoretically available, are characterised by glacial response times often spanning months to years, rendering them impractical for rapidly evolving cryptocurrency investigations.[17] The Budapest Convention on Cybercrime provides some expedited mechanisms for the preservation and disclosure of stored data, but its ratification remains incomplete across key cryptocurrency-hosting jurisdictions.[18]

D. Evidentiary Challenges

The admissibility and interpretation of blockchain evidence present novel evidentiary challenges. Unlike conventional bank records which carry established hearsay exceptions, blockchain transaction records require expert testimony to explain their technical generation, storage, and immutability. Courts must grapple with questions of whether blockchain outputs constitute hearsay, what authentication standards apply, and whether blockchain forensic tools are sufficiently reliable to meet evidentiary standards analogous to those applicable to forensic scientific evidence under frameworks such as the *Daubert* standard in the United States.[19]

The privacy dimensions of blockchain evidence also generate constitutional tensions. In *US v Gratkowski*[20] the Fifth Circuit held that the third-party doctrine, established in *Smith v Maryland* and analogically applied, diminishes Fourth Amendment protections in respect of blockchain records voluntarily shared with exchanges. However, commentators have argued that the Supreme Court's decision in *Riley v California*[21] signals a trajectory toward heightened

[16]Kevin V Tu and Michael W Meredith, 'Rethinking Virtual Currency Regulation in the Bitcoin Age' (2015) 90 Washington Law Review 271, 302.
[17]Mutual Legal Assistance Treaties (MLATs) remain the primary mechanism for cross-border evidence sharing; however, the average MLAT response time ranges from 10 months to 3 years, creating substantial delays in cryptocurrency investigations.
[18]Council of Europe Convention on Cybercrime (Budapest Convention) (2001) ETS 185, art 29–35 (expedited preservation and disclosure of stored computer data).
[19]Jaideep T Venkatesan, 'Prosecutorial Challenges in Cryptocurrency Cases: Jurisdiction, Evidence and Anonymity' (2021) 74 Stanford Law Review 188, 205.
[20]US v Gratkowski, 964 F3d 307 (5th Cir 2020). The Fifth Circuit held that users have no Fourth Amendment reasonable expectation of privacy in blockchain transaction records disclosed to a virtual currency exchange, applying the third-party doctrine.
[21]Riley v California, 573 US 373 (2014). The Supreme Court held that warrantless searches of digital information

ISSN: 2582-6433

constitutional protection for comprehensive digital records, potentially unsettling the application of third-party doctrine to blockchain investigations.

E. Asset Recovery and Seizure Complexities

The recovery and forfeiture of cryptocurrency assets presents distinct legal and technical challenges. Unlike fiat currency held in bank accounts, cryptocurrency may be secured by private keys accessible only to the owner. Where a suspect refuses to disclose private keys, prosecutors must navigate competing considerations of compelled self-incrimination and the practical imperative of asset recovery. Furthermore, the volatile valuation of cryptocurrency introduces complications in quantifying proceeds of crime and determining appropriate forfeiture values for sentencing purposes.[22]

IV. EVOLVING PROSECUTORIAL STRATEGIES

A. Blockchain Forensic Analytics

The most consequential development in cryptocurrency prosecution has been the maturation of blockchain forensic analytics. Specialised firms including Chainalysis, Elliptic, and CipherTrace have developed sophisticated tools capable of tracing transactional flows across complex blockchain networks, identifying clustering patterns that associate multiple wallet addresses with a common entity, and flagging addresses associated with known criminal infrastructure.[23] These tools have been deployed in major prosecutions globally, enabling investigators to reconstruct transactional histories that appear opaque to conventional analysis. The Chainalysis Reactor platform, widely used by United States federal agencies and international law enforcement partners, enables investigators to visualise blockchain transactional flows and identify exposures to high-risk entities.[24] Such tools were instrumental in the recovery of approximately USD 3.6 billion in cryptocurrency linked to the 2016 Bitfinex hack ,the largest cryptocurrency seizure in United States history at the time of its announcement,demonstrating the transformative investigative potential of blockchain analytics.

on cell phones violated the Fourth Amendment, providing an analogical framework for digital privacy rights in cryptocurrency investigations.

[22]US Department of Justice, 'Attorney General's Cyber Digital Task Force: Cryptocurrency: An Enforcement Framework' (DOJ, 2020) 30–35.

[23]Chainalysis Reactor is a blockchain analysis tool used by law enforcement agencies globally; see Chainalysis, 'Government Solutions' <https://www.chainalysis.com/government/> accessed 10 April 2025.

ISSN: 2582-6433

B. Know Your Customer and Travel Rule Compliance

A central pillar of cryptocurrency AML enforcement is the extension of Know Your Customer (KYC) and Customer Due Diligence (CDD) obligations to VASPs. FATF's 2019 Recommendation 16 ,the 'Travel Rule' ,mandates that VASPs collect and transmit originator and beneficiary information for virtual asset transfers above designated thresholds, effectively replicating the correspondent banking information requirements that constitute a cornerstone of traditional financial crime prevention.[25] Compliance with the Travel Rule creates transactional records that substantially augment the evidentiary resources available to prosecutors.

In *HM Revenue & Customs v Coinbase Europe Ltd*[26] the English High Court affirmed the power of revenue authorities to compel disclosure of user transaction records from cryptocurrency exchanges, establishing an important precedent for tax-related criminal investigations. The FinCEN guidance of 2013 similarly extended Bank Secrecy Act obligations to cryptocurrency money transmitters, requiring registration, KYC implementation, and suspicious activity reporting.[27]

C. International Enforcement Cooperation

Recognising the inherent transnationality of blockchain-based crime, enforcement agencies have progressively developed cooperative mechanisms to transcend jurisdictional barriers. The United States Department of Justice's National Cryptocurrency Enforcement Team (NCET), established in 2021, provides a dedicated institutional focus for cryptocurrency criminal enforcement and facilitates inter-agency cooperation.[28] Interpol's Financial Crime unit and Europol's European Cybercrime Centre (EC3) similarly provide multilateral platforms for coordinated cryptocurrency investigation.

The OFAC cryptocurrency sanctions framework represents a parallel enforcement track, enabling the designation of cryptocurrency addresses associated with sanctioned actors and VASPs, thereby chilling illicit transactional flows through compliance pressure on regulated exchanges.[29] The intersection of criminal prosecution and sanctions enforcement has become

[25]Travel Rule, Financial Action Task Force, Recommendation 16; see also FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (Updated, 2021) 55.
[26]HM Revenue & Customs v Coinbase Europe Ltd [2020] EWHC 1997 (Admin). The UK High Court upheld a notice requiring Coinbase to disclose user transaction data exceeding GBP 5,000 for tax enforcement purposes.
[27]Financial Crimes Enforcement Network (FinCEN), 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies' (Guidance FIN-2013-G001, 2013).
[29]Office of Foreign Assets Control (OFAC), Treasury Department, 'Sanctions Compliance Guidance for the Virtual Currency Industry' (2021) <https://ofac.treasury.gov> accessed 10 April 2025.

ISSN: 2582-6433

an increasingly integrated feature of the global cryptocurrency enforcement landscape.

D. Undercover Operations and Controlled Transactions

Law enforcement agencies have adapted conventional undercover investigation techniques to cryptocurrency environments. Investigators have created pseudonymous blockchain identities to engage with criminal marketplaces, participate in illicit transactional networks, and gather evidence through controlled transactions. The legal and ethical parameters of such operations, including entrapment doctrines, agency authority, and chain-of-custody protocols for digital evidence, remain subjects of developing jurisprudence.[30] Such methods proved crucial in dismantling darknet markets including AlphaBay and Hansa Market through coordinated multinational law enforcement operations in 2017.

E. Tax Enforcement as a Prosecutorial Gateway

Drawing upon a prosecutorial tradition dating to the conviction of Al Capone for tax evasion, enforcement agencies have deployed tax offence prosecution as a gateway to broader cryptocurrency financial crime enforcement. The IRS Criminal Investigation division has recorded substantial success in prosecuting cryptocurrency tax evasion, frequently using such investigations as entry points into wider money laundering and fraud conspiracies.[31] This approach exploits the requirement that cryptocurrency income be reported for tax purposes, creating a legal obligation that, when violated, establishes an independently prosecutable predicate offence while simultaneously generating evidence of underlying illicit activity.

V. THE INDIAN REGULATORY AND PROSECUTORIAL LANDSCAPE

India's engagement with cryptocurrency regulation has been characterised by oscillation between prohibitionary impulse and pragmatic accommodation, tracing a trajectory from the Reserve Bank of India's 2018 banking prohibition to the judicial intervention of the Supreme Court and the subsequent legislative construction of a Virtual Digital Assets (VDA) framework.

In *Reserve Bank of India v Internet and Mobile Association of India*[32] the Supreme Court of

[30]Nicolas Christin, 'Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace' (2013) Proceedings of the 22nd International Conference on World Wide Web 213.
[31]IRS Criminal Investigation, 'CI Annual Report 2022' (Internal Revenue Service, 2022) 8–10. The report details successful prosecutions of tax evasion facilitated through cryptocurrency transactions.
[32]Reserve Bank of India v Internet and Mobile Association of India (2020) 10 SCC 274. The Supreme Court set

ISSN: 2582-6433

India set aside the RBI's circular prohibiting regulated entities from providing services to cryptocurrency businesses, holding it disproportionate in the absence of demonstrated harm. This judgment, while framed in proportionality analysis rather than recognition of a fundamental right to transact in cryptocurrency, effectively restored institutional banking access to the sector and precipitated a regulatory recalibration.

The Finance Act 2022 introduced a VDA taxation framework, imposing a thirty percent flat tax on gains from virtual digital assets and a one percent tax deducted at source on transfers, while prohibiting the set-off of losses.[33] While these provisions were principally directed at revenue generation rather than financial crime prevention, they created a formal legal characterisation of VDAs as taxable property, providing a definitional foundation for subsequent regulatory and prosecutorial engagement.

Most significantly for financial crime enforcement, the 2023 amendment to the Prevention of Money Laundering Act extended PMLA obligations to VDA service providers, requiring registration, KYC compliance, suspicious transaction reporting, and record maintenance.[34] The Supreme Court's validation of broad PMLA enforcement powers in *Vijay Madanlal Choudhary v Union of India*[35] has furnished the Enforcement Directorate with substantial coercive authority potentially applicable to cryptocurrency financial crime investigations.

Notwithstanding these developments, India's prosecutorial architecture for cryptocurrency financial crime remains nascent. The Enforcement Directorate and specialised Economic Offences Wings of state police forces lack the technical capacity, forensic tool access, and specialised training to prosecute sophisticated blockchain-based financial crime with consistent efficacy. The absence of a comprehensive, standalone cryptocurrency legislation, analogous to the EU's MiCA framework, continues to generate definitional uncertainty that impedes regulatory and prosecutorial coherence.[36]

aside the RBI's circular prohibiting banks from providing services to cryptocurrency entities, holding it disproportionate.

[33]Virtual Digital Assets (VDA) framework introduced under Finance Act 2022 (India), inserting ss 115BBH and 194S into the Income Tax Act 1961; see also Central Board of Direct Taxes, Circular No 13 of 2022.

[34]Prevention of Money Laundering (Maintenance of Records) Amendment Rules 2023 (India); the Ministry of Finance notification extending PMLA obligations to Virtual Digital Asset Service Providers.

[35]Prevention of Money Laundering Act 2002 (India), s 3; see also Vijay Madanlal Choudhary v Union of India AIR 2022 SC 3914 where the Supreme Court upheld the constitutional validity of PMLA provisions.

[36]Kiran Raj and Aarav Mehta, 'Decentralised Finance (DeFi) and Regulatory Arbitrage: Challenges for Global AML Frameworks' (2022) 37(2) Journal of International Banking Law and Regulation 78, 90.

ISSN: 2582-6433

VI. CONCLUSION AND RECOMMENDATIONS

Blockchain-based financial crime represents one of the most technically complex and jurisdictionally challenging frontiers of contemporary criminal law enforcement. The pseudonymous architecture of distributed ledger technology, its permissionless global accessibility, and its capacity to obscure beneficial ownership through sophisticated layering techniques have created enforcement deficits that demand coordinated legislative, regulatory, and prosecutorial responses.

The foregoing analysis yields several conclusions. First, the definitional fragmentation that characterises cryptocurrency's legal treatment across jurisdictions, as property, money, commodity, or security, must yield to harmonised international standards, whether through frameworks such as MiCA or through coordinated FATF-driven adoption of common definitional standards. Second, the extension of AML/CTF obligations to VASPs through Travel Rule compliance, KYC mandates, and suspicious transaction reporting creates the evidentiary infrastructure upon which effective prosecution increasingly depends.[37]

Third, blockchain forensic analytics has demonstrated transformative potential as a prosecutorial tool, capable of reconstructing transactional chains that appear opaque to conventional analysis. Investment in law enforcement capacity for these technologies, and in the legal frameworks governing their admissibility as evidence, is essential. Fourth, international enforcement cooperation must be deepened and expedited, with MLAT reform and the expansion of real-time information sharing protocols to address the mismatch between the speed of cryptocurrency transactions and the pace of traditional mutual assistance mechanisms.

For India specifically, the paper recommends: first, the enactment of comprehensive standalone virtual assets legislation that resolves definitional ambiguity and establishes clear regulatory competencies; second, capacity investment in the Enforcement Directorate and state-level economic offence investigation units for blockchain forensic capabilities; third, expedited bilateral and multilateral mutual legal assistance arrangements with major cryptocurrency-hosting jurisdictions; and fourth, engagement with FATF peer review processes to benchmark

[37]Basel Committee on Banking Supervision, 'Prudential Treatment of Crypto-asset Exposures' (BIS, 2022); see also Financial Stability Board, 'Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets' (FSB, 2022).

ISSN: 2582-6433

domestic AML/CTF standards against international best practices.

The governance of blockchain-based financial crime ultimately demands legal architecture that is simultaneously technically sophisticated, institutionally adaptive, and internationally coordinated. The evolutionary pace of blockchain innovation means that no static legal framework will suffice; what is required is a regulatory ecosystem characterised by principled flexibility, continuous institutional learning, and genuine multilateral cooperation. While the enforcement gap remains significant, the trajectory of prosecutorial strategy, marked by forensic innovation, international coordination, and adaptive legal interpretation, suggests a measured but meaningful convergence between the demands of justice and the architecture of the blockchain.