Page: 1283-1314 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.55

THE DARK SIDE OF AI: CRYPTOCURRENCY AND CYBERCRIME: REGULATORY GAPS IN DIGITAL ASSET TRACING

Vishwajeet Singh[1] & Dr. Mudra Singh[2]

I. ABSTRACT

This paper examines how artificial intelligence is reshaping cryptocurrency-enabled cybercrime and why Indian regulatory architecture still struggles to trace, freeze, and prosecute virtual digital asset flows at speed. It maps the modern crime stack, from AI-assisted phishing and social engineering to ransomware, pig butchering, mixer use, and cross-chain laundering. It then evaluates India's compliance perimeter under the PMLA notification covering VDA service activities, FIU-IND reporting obligations, CERT-In incident directions, and the evidentiary demands for electronic records under the Bharatiya Sakshya Adhiniyam, 2023 and procedural safeguards under the Bharatiya Nagarik Suraksha Sanhita, 2023. The analysis identifies persistent gaps: inconsistent Travel Rule implementation, weak governance for unhosted wallets and DeFi control points, uneven forensic readiness across platforms, and cross-border delays that allow rapid dissipation of value. The paper argues for traceability as infrastructure, not paperwork, and proposes a reform roadmap that combines minimum technical standards for logs and attribution artefacts, risk-tiered controls for high-risk transfers, stronger supervisory testing, and faster international cooperation mechanisms. The goal is a rights-respecting model that improves recovery for victims while preserving due process and data protection. It also situates these reforms within FATF standards and comparative models to ensure interoperability, predictability, and resilient prosecutions across jurisdictions globally.

[1] LLB 3rd year (6th semester) Student at Amity Law School, Lucknow Campus (India). Email: vishwjeet.singh1@s.amity.edu
[2] Assistant Professor at Amity Law School, Lucknow Campus (India). Email: msingh5@lko.amity.edu

 (ISSN: 2583-7753)

II. KEYWORDS

AI-enabled cybercrime, virtual digital assets, AML/CFT compliance, blockchain analytics and tracing, digital evidence and attribution

III. INTRODUCTION

A. Context: AI, crypto-economy, and evolving cybercrime

AI has shifted cybercrime from craft to production. Offenders now generate phishing lures, deepfake voice scripts, and persuasive scam chats in bulk. They also automate reconnaissance and victim profiling. This lowers entry barriers and increases attack volume. It also compresses the time between compromise and monetisation. Criminal groups therefore behave like service operators with tooling, customer support, and rapid iteration. Law enforcement assessments already treat AI as a key enabler of cyber-attacks and online fraud at scale.[3]

The crypto-economy makes this monetisation portable. It moves value across borders with fewer friction points and with fast finality. That is attractive in ransomware, extortion, investment fraud, and account takeover. Illicit actors rarely stop at simple receipt of funds. They route proceeds through exchanges, brokers, and other services that provide liquidity. They also layer through chain hops and rapid fragmentation to blunt tracing. Empirical research shows that illicit addresses still send large volumes to services, confirming that cash-out often depends on intermediated venues, not only peer transfers.[4]

International standards try to close the identity gap but implementation remains uneven. FATF Recommendation 15 and its interpretative note expect countries to apply AML and CFT controls to virtual assets and VASPs, and to operationalise Travel Rule style

[3] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (2024), https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (last visited Mar. 4, 2026).
[4] Chainalysis Team, 2023 Crypto Money Laundering: Key Trends (Feb. 15, 2024), https://www.chainalysis.com/blog/2024-crypto-money-laundering/ (last visited Mar. 4, 2026).

information sharing for transfers. Yet jurisdictions differ in speed, supervision, and enforcement intensity. Criminals exploit these differences as routing strategy. They choose weak nodes. They then bridge and swap to widen distance from the predicate offence. This global unevenness amplifies the local enforcement challenge in India.[5]

India's compliance architecture has begun to harden around VDA service providers as reporting entities, with FIU-IND positioned as the AML and CFT regulator for covered VDA services. The framework emphasises KYC and customer due diligence, ongoing monitoring, suspicious transaction reporting, and record retention. It also treats higher risk transfers, including certain unhosted wallet exposures, as requiring enhanced controls. Still, the evidentiary value of tracing depends on how platforms preserve logs and attribution artefacts during live incidents, and many systems remain not fully forensic-ready yet.[6]

B. Research questions

1. How does AI amplify cryptocurrency-linked cybercrime in India across ransomware, fraud, and laundering typologies?
2. Do India's AML/CFT and KYC frameworks adequately enable digital asset tracing and timely interdiction?
3. What evidentiary and procedural bottlenecks weaken investigation and prosecution of crypto-cybercrime?
4. Which comparative models and international instruments best support cross-border tracing, freezing, and recovery?

[5] Fin. Action Task Force (FATF), Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (July 9, 2024), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (last visited Mar. 4, 2026).

[6] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (updated Jan. 8, 2026), https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf (last visited Mar. 4, 2026).

C. Research objectives

1. To map AI-enabled threat vectors and explain how they increase scale, speed, and attribution complexity in VDA offences.
2. To assess the effectiveness of PMLA-based VDA coverage, FIU-IND compliance architecture, and the FATF Travel Rule interface for traceability outcomes.
3. To evaluate admissibility and proof requirements for electronic records and identify reforms that improve chain of custody and courtroom reliability.
4. To derive implementable best practices from FATF standards and select foreign regimes to strengthen India's cooperation and supervisory design.

D. Research methodology

This study adopts a doctrinal legal research method with a focused comparative layer. It analyses Indian statutory and regulatory materials governing VDAs, AML/CFT, cyber incidents, digital evidence, and procedural safeguards, alongside leading judicial doctrine on electronic records and due process. It then triangulates the legal analysis with secondary empirical material from reputable institutional reports on crypto crime, laundering patterns, and AI-enabled fraud to ground the discussion in operational reality. A comparative review of FATF standards and select foreign approaches to Travel Rule supervision, VASP governance, and cross-border assistance is used to identify gaps, measure interoperability, and craft a reform roadmap that is legally feasible, enforceable, and rights-respecting.

IV. CONCEPTUAL & TECHNICAL FOUNDATIONS

A. A. Cryptocurrency ecosystem and transaction architecture

Public blockchains run as distributed ledgers. They record transactions in blocks and secure them through cryptography and consensus. Users control funds through private keys, while the network validates transfers through linked data structures and

verification rules. This design removes a single trusted intermediary, but it also makes transaction history durable and globally visible, which matters for both crime and proof.[7]

Transaction architecture varies by design. Bitcoin follows an unspent transaction output model, so every spend links earlier outputs to new outputs. Account-based systems like Ethereum record balances and execute smart contracts that can bundle transfers, swaps, and lending logic in a single chain event. These layers allow decentralised exchanges, bridges, and mixers to route value quickly across networks, often with weak identity hooks. That technical choice creates tracing friction because investigators must follow both on-chain hops and off-chain service records.[8]

Indian law now touches this ecosystem through activity-based regulation, not by treating every token as "currency" in the classic sense. FIU-IND circulars for Virtual Digital Asset Service Providers list exchange, transfer, safekeeping, administration, and participation in financial services related to an issuer's offer or sale as compliance-triggering activities. This approach targets the control points where a person converts, custody-holds, or moves VDAs for another, even when code executes the front end.[9]

The enforcement signal is already visible. A 2025 PIB release records FIU-IND notices for non-compliance to offshore VDA service providers and also refers to takedown related notices under the IT Act framework, alongside the point that VDA service providers entered the AML-CFT framework under PMLA in March 2023. This shows a policy

[7] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf (last visited Mar. 4, 2026).
[8] Fin. Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct. 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf (last visited Mar. 4, 2026).
[9] Fin. Intelligence Unit-India, Ministry of Finance, Dep't of Revenue, 3rd Revision of Circular for Registration of Virtual Digital Asset Service Providers (VDA SPs) in FIU India as Reporting Entity (RE) (Sept. 15, 2025), https://fiuindia.gov.in/pdfs/downloads/VDASP15092025.pdf (last visited Mar. 4, 2026).

preference for forcing traceability through platform obligations, even when a service sits outside India but serves Indian users.[10]

B. AI in cybercrime: automation, obfuscation, and scale

AI compresses skill barriers. It helps offenders draft targeted phishing, automate social engineering at scale, and industrialise malware workflows through "crime-as-a-service" markets. Europol's IOCTA 2024 flags that AI and machine learning tools have become prominent commodities for cybercriminals, including the emergence of malicious LLM offerings that support phishing and cyber-attacks. That trend matters for crypto crime because the first breach often begins with credential capture and device compromise.[11]

AI also upgrades obfuscation. Deepfake audio and video can impersonate founders, compliance officers, or even investigators. This supports business email compromise, investor fraud, and coercive extortion. Europol's deepfakes report recognises deepfakes as an operational tool for fraud and manipulation in online interactions, which makes KYC and transaction authorisation weaker if institutions rely on visual checks or voice calls. Small mistakes in verification becomes costly.[12]

Scale now becomes the core risk, not novelty. Chainalysis reports that 2023 saw a drop in value received by illicit crypto addresses to a lower-bound estimate of $24.2 billion, while also noting growth in ransomware and darknet market activity. This mixed pattern matters for Indian policy because the harm concentrates in a smaller number of high-

[10] Press Info. Bureau, Gov't of India, Ministry of Finance, Financial Intelligence Unit (FIU IND) Issues Notices for Non-Compliance to 25 Offshore Virtual Digital Assets Service Providers (VDA SPs) (Oct. 1, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758 (last visited Mar. 4, 2026).
[11] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (2024), https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (last visited Mar. 4, 2026).
[12] Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (Observatory Report from the Europol Innovation Lab) (2022) (version published Jan. 2024), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf (last visited Mar. 4, 2026).

impact campaigns, which then launder through stablecoins, exchanges, and cross-chain tools.[13]

Hard loss figures also underline the attack surface. Reuters reported that losses from crypto hacks rose to about $2.2 billion in 2024, and highlighted major incidents including a large theft from an India-linked exchange. These events show how AI-assisted targeting and key theft convert directly into traceable on-chain outflows, but only if investigators act fast and preserve logs and wallet intelligence early.[14]

C. Digital asset tracing: attribution, clustering, and evidentiary value

Digital asset tracing starts with a simple reality. Many blockchains publish transaction graphs openly. Analysts therefore use graph methods to infer control relationships, identify service clusters, and follow value through time. Meiklejohn and co-authors show how heuristic clustering can group wallets based on evidence of shared authority and then support re-identification attacks when combined with real-world touchpoints like merchant payments or exchange deposits. That is not perfect science, but it is operationally powerful.[15]

Attribution usually needs an off-chain bridge. Investigators link addresses to persons through KYC records, IP logs, device data, exchange support tickets, and seized devices. Clustering then helps them map "same-entity" behaviour through transaction patterns, such as multi-input spends and change-output behaviour. This is where Indian compliance rules become evidence enablers, because recordkeeping obligations create the join between a pseudonymous address and a legal identity.

---

[13] Chainalysis Team, 2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth (Jan. 18, 2024), https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (last visited Mar. 4, 2026).
[14] Losses from Crypto Hacks Jump to $2.2 Bln in 2024, Report Says, Reuters (Dec. 19, 2024), https://www.reuters.com/technology/losses-crypto-hacks-jump-22-bln-2024-report-says-2024-12-19/ (last visited Mar. 4, 2026).
[15] Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, in Proceedings of the 2013 Internet Measurement Conference (2013), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (last visited Mar. 4, 2026).

Tracing has limits, and offenders exploit them. Address clustering rests on heuristics that can fail when wallets randomise behaviour or when services deliberately try to break linkability. Möser and Narayanan show that clustering techniques need careful evaluation because false positives can cause "cluster collapse," and change-address identification errors can pollute an investigation narrative. Privacy tools, mixers, and cross-chain bridges increase this risk, so investigators must treat clustering as an inference and not as identity proof by itself.[16]

Indian courts then test tracing output through evidence rules, not through technical confidence. The Supreme Court in *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 and in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 required proper certification for admissibility of electronic records. The Bharatiya Sakshya Adhiniyam, 2023 reinforces this structure through its provisions on proving contents of electronic records and admissibility conditions, including certificate requirements and hash-related particulars in the Schedule. So blockchain analytics must arrive with clean acquisition notes, device provenance, and certification hygiene, else the court may reject it outright.[17]

Cross-border design makes tracing legally international. FATF continues to evaluate implementation of Recommendation 15 and its interpretative note for virtual assets and VASPs, and it flags uneven compliance and emerging risks. For Indian investigators, this means MLAT delay and platform non-cooperation can break the attribution chain even when the on-chain trail stays intact. Therefore, policy must push interoperable disclosure standards and faster lawful access, while still respecting due process and data protection duties.[18]

---

[16] Malte Möser & Arvind Narayanan, Resurrecting Address Clustering in Bitcoin (2021), https://fc22.ifca.ai/preproceedings/87.pdf (last visited Mar. 4, 2026).
[17] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 62–63, sched. (India).
[18] Fin. Action Task Force (FATF), Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (July 9, 2024), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html (last visited Mar. 4, 2026).

V. CYBERCRIME TYPOLOGIES INVOLVING CRYPTO AND AI

A. Ransomware, extortion, and crypto laundering chains

Ransomware groups run a repeatable playbook. They buy access through malware loaders, stolen credentials, or phishing at scale. They then encrypt systems and force downtime. Next, they add data theft. They threaten leaks. This is now routine double extortion. Many crews also add pressure through repeated calls, DDoS, or direct messages to clients and vendors. They demand payment in cryptocurrency because it settles fast and moves across borders without banking friction. Chainalysis observed record-setting ransomware receipts in 2023 and also linked the rebound to adaptation by attackers, even when defenders improved backups and incident response.[19]

Laundering chains often look modular. The attacker first consolidates inflows into a small set of addresses. Then the actor layers funds through swaps, chain hops, or nested services. They prefer high-liquidity assets like stablecoins because these convert quickly and travel through many venues. They also use mixers and rapid fragmentation to break clean tracing. FATF has described recurring red flags that fit this pattern, including rapid layering across multiple VASPs, the use of anonymity-enhancing services, and transaction behaviour that does not match an apparent customer profile.[20]

Sanctions and law enforcement data also show how laundering chains reuse infrastructure across campaigns. The U.S. Treasury described Sinbad as a mixer used to launder proceeds from major theft events and cross-ecosystem hacks. It also noted laundering of stolen funds linked to bridge compromises. This typology matters because bridge exploits create large, sudden outflows, then the actor breaks them into smaller

[19] Chainalysis Team, Ransomware Hit $1 Billion in 2023 (Feb. 7, 2024), https://www.chainalysis.com/blog/ransomware-2024/ (last visited Mar. 4, 2026).
[20] Fin. Action Task Force (FATF), Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing (Sept. 2020), https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html (last visited Mar. 4, 2026).

flows for cash-out. That pattern can overwhelm first-responder tracing unless a platform freezes quickly.[21]

Indian enforcement theory usually maps ransomware into two tracks. First, cyber intrusion and data damage under the Information Technology Act framework. Second, extortion and intimidation under the general penal law. The Bharatiya Nyaya Sanhita, 2023 expressly places extortion under § 308 and criminal intimidation under § 351. These provisions fit ransomware threats because the offender compels payment by fear of injury to property, reputation, or business continuity. The same facts also create a money trail, so PMLA exposure can arise when the actor projects illicit proceeds as clean value through VDA routes.[22]

Operationally, the first hours decide recoverability. CERT-In directions require entities to report specified cyber incidents within 6 hours of noticing them, and also require secure log retention for a rolling 180 days within Indian jurisdiction. These obligations can convert a ransomware event into usable evidence. They help preserve exchange logs, VPN logs, system time coherence, and endpoint traces. Without that, tracing degrades into guesswork and delayed letters rogatory.[23]

India's VDA compliance layer now turns laundering chains into reportable conduct. FIU-IND's registration and compliance framework for VDA service providers positions exchanges and custodians as reporting entities for suspicious patterns. That creates a legal hook for STR generation, record retention, and quicker identification. It does not solve offshore non-cooperation, but it improves domestic choke points.[24]

---

[21] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency (Nov. 29, 2023), https://home.treasury.gov/news/press-releases/jy1933 (last visited Mar. 4, 2026).
[22] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 308, 351 (India).
[23] Indian Comput. Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022) (India).
[24] Fin. Intelligence Unit-India, Ministry of Finance, Dep't of Revenue, 3rd Revision of Circular for Registration of Virtual Digital Asset Service Providers (VDA SPs) in FIU India as Reporting Entity (RE) (Sept. 15, 2025), https://fiuindia.gov.in/pdfs/downloads/VDASP15092025.pdf (last visited Mar. 4, 2026).

B. Fraud, phishing, pig butchering, and synthetic identity scams

Fraud campaigns now blend social engineering with crypto rails. Phishing steals credentials, then attackers empty wallets or drain exchange accounts. Investment fraud goes further. It builds a narrative, shows fake dashboards, and uses small early withdrawals to create trust. The FBI's 2024 Internet Crime Report data shows that investment fraud involving cryptocurrency produced the highest reported losses, crossing billions of dollars, and it sits alongside phishing and extortion as top complaint categories. This scale signals that crypto fraud is not peripheral anymore.[25]

AI increases throughput. Attackers generate tailored scripts, fake identities, and multilingual chats in minutes. They test many variants and keep what converts. Europol's IOCTA 2024 flags that AI tools expand the reach of fraudsters and improve social engineering quality, including investment platform fraud at industrial scale. When the victim pays in crypto, the scammer can move funds instantly and irreversibly, which turns persuasion into a final settlement event.[26]

Pig butchering fits this model but adds patience. Offenders cultivate relationships through dating apps or social platforms, then pivot to "investment" in crypto, forex, or token presales. UNODC's 2024 convergence report describes cryptocurrency-based pig butchering scams as a flagship revenue stream for transnational criminal ecosystems in Southeast Asia. These networks also integrate laundering services and underground banking. So the scam is not just deception, it is a supply chain with recruitment, coercion, and financial engineering.[27]

---

[25] Press Release, Fed. Bureau of Investigation, FBI Releases Annual Internet Crime Report (Apr. 23, 2025), https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report (last visited Mar. 4, 2026).

[26] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (2024), https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (last visited Mar. 4, 2026).

[27] U.N. Office on Drugs & Crime (UNODC), Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Illicit Online Markets in Southeast Asia (2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (last visited Mar. 4, 2026).

Synthetic identity scams sit at the edge of both fraud and compliance breach. The offender uses forged documents, deepfake KYC, or rented accounts to open exchange profiles and payment rails. Deepfake audio can also defeat call-based verification. Europol's deepfakes analysis frames this as a rising operational threat because deepfakes reduce trust signals that institutions relied on for onboarding and approvals. The legal risk is clear. Weak KYC becomes an enabler of laundering and victimisation, not a mere procedural lapse.[28]

The Indian response must treat these frauds as evidence-heavy crimes. Victims often hold only screenshots and chat logs. The money trail sits on-chain and on exchange servers. Therefore investigators must seize devices, preserve chats, and rapidly obtain KYC and withdrawal logs. That is where due process meets speed. Delay allows the fraudster to hop chains and cash out through offshore brokers, then restitution becomes remote.

C. Darknet markets, mixers, privacy coins, and cross-chain bridges

Darknet markets still monetise trust through escrow, vendor ratings, and dispute systems. They accept crypto because it supports remote settlement and pseudonymity. Chainalysis has repeatedly noted that darknet markets remain a prominent crypto crime category, and that revenues rose in 2023 even when overall illicit inflows appeared lower. These markets also drive demand for privacy tools and laundering services, since vendors need reliable cash-out.[29]

Mixers act as laundering utilities. They pool and shuffle assets to break attribution links. Regulators treat them as high-risk when they become a default exit route for stolen funds. The U.S. Treasury's 2022 designation of Tornado Cash described laundering volumes in the billions and linked its use to major theft proceeds. This matters for typology because

[28] Europol Innovation Lab, Facing Reality? Law Enforcement and the Challenge of Deepfakes (Observatory Report) (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf (last visited Mar. 4, 2026).
[29] Chainalysis Team, 2024 Crypto Crime Trends (Jan. 18, 2024), https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (last visited Mar. 4, 2026).

many cyber thefts now show a "theft to mixer" hop early in the chain, before the cash-out exchange step.[30]

European enforcement treats large mixers as organised crime infrastructure. Europol and partners announced the takedown of "Cryptomixer" and framed it as a service suspected of facilitating cybercrime and laundering. This enforcement posture supports a practical point. When states hit mixers, they aim to disrupt the laundering layer, not merely punish a single theft event. That can change attacker cost models, though it can also push laundering into smaller and more fragmented services.[31]

Privacy coins and cross-chain bridges complicate tracing in different ways. Privacy coins reduce on-chain observability. Bridges create chain discontinuity and jurisdictional confusion. OFAC's 2023 action against Sinbad cited laundering tied to major thefts and specifically referenced bridge-linked incidents. This is not abstract. In many investigations, the bridge hop is the moment the trail becomes colder, because the attacker changes asset type, chain analytics vendor, and sometimes legal venue at once.[32]

VI. REGULATORY LANDSCAPE AND COMPLIANCE ARCHITECTURE

A. AML/CFT obligations, KYC norms, and FATF "Travel Rule" interface

India placed core VDA service activities inside the PMLA compliance perimeter through a Central Government notification dated 7 March 2023. It treats exchange, transfer, safekeeping or administration, and issuer-related financial services as "designated" activities when done for or on behalf of another person in course of business. This move

[30] Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 (last visited Mar. 4, 2026).
[31] Press Release, Europol, Europol and Partners Shut Down "Cryptomixer" (Dec. 1, 2025), https://www.europol.europa.eu/media-press/newsroom/news/europol-and-partners-shut-down-cryptomixer (last visited Mar. 4, 2026).
[32] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency (Nov. 29, 2023), https://home.treasury.gov/news/press-releases/jy1933 (last visited Mar. 4, 2026).

shifts crypto tracing from a purely technical exercise to a legally enforceable compliance duty.[33]

FIU-IND then operationalised this perimeter through AML and CFT guidelines for reporting entities providing VDA-related services. The framework pushes deterrence through KYC and CDD, detection through monitoring and suspicious transaction reporting, and discipline through structured recordkeeping. It also links VDA compliance with UAPA and WMDA screening, so sanctions and prohibited-entity risks stay in view, not optional. Some service providers still treat this as paperwork, that approach fails in practice.[34]

FATF standards supply the common vocabulary for cross-border co-operation, especially on virtual assets. FATF's travel rule supervision work clarifies that the Travel Rule requires VASPs and financial institutions to obtain, hold, and transmit specified originator and beneficiary information "immediately and securely" for VA transfers, much like wire transfers. This interface matters because Indian investigations often depend on foreign platform data, and foreign platforms demand Travel Rule compatible requests.[35]

FIU-IND's VDA guidelines translate the Travel Rule into Indian operational terms by treating many VDA transfers on the lines of "wire transfers." It requires originator and beneficiary information and sets content expectations like PAN or national ID, verified originator name, and wallet addresses. It also flags unhosted wallet transfers as high risk

[33] Ministry of Finance (Dep't of Revenue), Notification S.O. 1072(E), Gazette of India, Extraordinary, Part II, Section 3(ii) (Mar. 7, 2023) (India).
[34] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023), https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf (last visited Mar. 4, 2026).
[35] Fin. Action Task Force (FATF), Best Practices in Travel Rule Supervision (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf (last visited Mar. 4, 2026).

and allows added controls. This creates an auditable chain of custody for identity data, if platforms actually implement it without gaps.[36]

KYC norms also arrive through the RBI's Master Direction on KYC for regulated entities, including banks that provide fiat on-ramps and custody-linked services. It defines officially valid documents, recognises Central KYC Registry workflows, and emphasises beneficial ownership and risk-based customer due diligence. Therefore exchanges cannot treat banking KYC as "outside" crypto. Weak KYC upstream contaminates the entire tracing chain downstream.[37]

Tax law quietly strengthens traceability too. Finance Bill 2022 inserted section 115BBH for VDA income taxation and section 194S for TDS on consideration for transfer of a virtual digital asset. The TDS design pressures platforms and counterparties to capture PAN and transaction identifiers, because deduction and reporting fail without identity hooks. So taxation becomes a compliance rail, not merely revenue collection.[38]

B. Virtual Asset Service Providers: duties, liabilities, and supervision gaps

VASP duties in India now track the reporting entity model under PMLA and PMLR. A reporting entity must run an internal AML program, appoint a Principal Officer, design escalation pathways, and file reports in prescribed form. It must also avoid tipping-off and preserve transaction trails for later investigative demands. In a cybercrime case, these duties decide whether law enforcement can freeze value in time.[39]

---

[36] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023), https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf (last visited Mar. 4, 2026).

[37] Reserve Bank of India, Master Direction - Know Your Customer (KYC) Direction, 2016 (Feb. 25, 2016), https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.pdf (last visited Mar. 4, 2026).

[38] Gov't of India, Finance Bill, 2022 (2022), https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf (last visited Mar. 4, 2026).

[39] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023), https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf (last visited Mar. 4, 2026).

Liability is not theoretical. The Government publicly recorded FIU-IND action against offshore VDA service providers for non-compliance under section 13 of the PMLA, 2002, including notices to 25 offshore entities. This illustrates the supervision strategy. India is trying to extend compliance to platforms that serve Indian users, even when the platform sits abroad. Still, service of process and enforcement remain hard at the edges.[40]

Supervision gaps cluster around three fault lines. First, offshore platforms and fragmented corporate structures. Second, unhosted wallets and peer to peer flows. Third, fast-evolving products like DeFi routing and cross-chain bridges. FATF's targeted update on implementation notes uneven progress across jurisdictions, persistent Travel Rule challenges, and rising risks from stablecoins and DeFi style arrangements. This unevenness creates regulatory arbitrage that criminals exploit with almost no friction.[41]

C. Platform governance: exchanges, wallets, and DeFi protocols

Exchanges and wallet-hosting platforms also sit inside India's intermediary governance logic. Section 79 of the Information Technology Act, 2000 grants conditional safe harbour to intermediaries, but it ties protection to due diligence and lawful conduct. When a platform ignores obvious laundering patterns, it risks losing the protective shield and invites layered liability exposure. The Supreme Court's proportionality reasoning in *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274 also signals a wider point. Regulators must target risk with calibrated measures, not blunt bans.[42]

The Intermediary Rules, 2021 deepen operational duties through grievance, takedown processes, and user-facing compliance. Crypto platforms often behave like financial firms

[40] Press Info. Bureau, Ministry of Finance, Financial Intelligence Unit (FIU IND) Issues Notices for Non-Compliance to 25 Offshore Virtual Digital Assets Service Providers (VDA SPs) Under Section 13 of the Prevention of Money Laundering Act (PML) Act, 2002 (Oct. 1, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758 (last visited Mar. 4, 2026).
[41] Fin. Action Task Force (FATF), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs (2024), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (last visited Mar. 4, 2026).
[42] Information Technology Act, No. 21 of 2000, § 79 (India).

and tech intermediaries at same time. That dual character creates compliance tension. For example, aggressive takedowns may protect users but also destroy evidence if logs and wallet metadata are not preserved properly. The platform must design governance so that enforcement and evidence can co-exist.[43]

Wallet governance splits into hosted and unhosted. Hosted wallets give the platform control, hence greater compliance ability and also more accountability. FIU-IND classifies transfers to or from unhosted wallets as higher risk because the counterparty wallet may not sit with an obliged entity. It places the compliance onus on the obliged entity where the hosted wallet sits and permits added limitations or controls. This is where many laundering chains deliberately migrate, since controls are weaker there.[44]

DeFi governance forces the hardest legal question. Who is responsible when "code runs it." FATF's 2021 guidance still expects countries to identify persons who maintain control or sufficient influence over VA arrangements, even if smart contracts execute the transactions. Admin keys, governance chokepoints, front-end operators, and fee collectors can convert "decentralised" claims into accountable perimeter. Platforms should run ML and TF risk assessment before launch and after upgrades, else they import systemic compliance debt.[45]

Personal data compliance now overlays every KYC and Travel Rule workflow. DPDP Rules 2025 require reasonable security safeguards like encryption, masking, logging, and also mandate breach intimation to affected Data Principals without delay and reporting to the Board, including detailed updates within seventy-two hours. The same Rules address cross-border transfer of personal data subject to Government specified

[43] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[44] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023), https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf (last visited Mar. 4, 2026).
[45] Fin. Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct. 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf (last visited Mar. 4, 2026).

requirements. After *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, these safeguards also carry a constitutional colour of necessity and proportionality.[46]

VII. REGULATORY GAPS IN DIGITAL ASSET TRACING

India's AML perimeter for VDAs rests on an activity list under Notification S.O. 1072(E) dated 7 March 2023, which covers exchange, transfer, safekeeping or administration, and issuer-linked financial services. Yet, the notification does not prescribe traceability standards. It does not mandate minimum telemetry, wallet attribution controls, or audit trails for cross-chain hops. This leaves tracing quality uneven across platforms, even when the legal duty exists on paper.[47]

FIU-IND's updated AML CFT guidelines for VDA-related reporting entities consolidate compliance expectations and push a risk based model for KYC, ongoing monitoring, sanctions screening, and recordkeeping. Still, the framework leaves a practical gap on unhosted wallets, DeFi routing, and smart-contract mediated transfers, where the service boundary is disputed. AI makes this gap sharper, because it automates layering patterns and creates rapid typology shifts that a slow rulebook cannot match.[48]

Cross-border supervision remains the largest enforcement fault line. The Government itself recorded FIU-IND notices to 25 offshore VDA service providers under section 13 of PMLA for non-compliance. This shows intent to regulate by market access. Yet it also shows the dependency on extra-territorial cooperation, platform presence, and local enforcement capacity. In fast-moving laundering chains, a delayed freeze order often means the asset is already bridged and dispersed.[49]

---

[46] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India).
[47] Ministry of Finance (Dep't of Revenue), Notification S.O. 1072(E) (Mar. 7, 2023) (India).
[48] Fin. Intelligence Unit-India, *AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets* (Updated Jan. 8, 2026), https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf (last visited Mar. 4, 2026).
[49] Press Info. Bureau, Ministry of Finance, *Financial Intelligence Unit (FIU IND) Issues Notices for Non-Compliance to 25 Offshore Virtual Digital Assets Service Providers (VDA SPs) Under Section 13 of the Prevention of Money Laundering Act (PML) Act, 2002* (Oct. 1, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758 (last visited Mar. 4, 2026).

Stablecoins add a special compliance asymmetry. Reuters reported that Tether stated it had frozen about $4.2 billion of USDT linked to illicit activity, reflecting issuer-level control that can support law enforcement outcomes. Indian tracing often depends on such issuer cooperation, but Indian law does not directly bind offshore stablecoin issuers to respond within defined time limits. So, recovery sometimes turns on voluntary action, not enforceable duty, and the victim pays the price.[50]

Data protection adds another boundary line. DPDP Rules, 2025 expect security safeguards and structured breach handling, while KYC and Travel Rule style sharing require extensive identity datasets and cross-border transmission. After *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, investigators and regulators must justify collection and retention through necessity and proportionality. This creates a governance gap when platforms over-collect data without minimisation, or under-collect data and later fail attribution. Both paths create litigation risk.[51]

VIII. INVESTIGATION, EVIDENCE, AND PROSECUTION

Crypto-cybercrime investigations succeed or fail on early preservation. CERT-In Directions dated 28 April 2022 impose tight incident reporting timelines and also require log retention and time synchronisation duties on covered entities. In a VDA theft or AI fraud incident, these logs link the on-chain outflow to the off-chain actor through IP, device, admin events, and withdrawal approvals. Without these artifacts, tracing remains a graph without a person behind it.[52]

BNSS hard-wires technology into procedure. Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023 requires audio-video recording of search and seizure processes and quick forwarding of recordings to the Magistracy. This directly strengthens the chain of custody for seized mobiles, seed phrase notebooks, hardware wallets, and exchange

[50] Tether Says It Has Frozen $4.2 Billion of Its Stablecoin Over Crime Links, Reuters (Feb. 27, 2026).
[51] Digital Personal Data Protection Rules, 2025 (India).
[52] Indian Comput. Emergency Response Team (CERT-In), *Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000* (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 4, 2026).

access devices. It also reduces later defence claims of planted devices or altered seizure memos, a frequent pain point in cyber cases.[53]

Admissibility then turns on electronic evidence discipline. Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 requires certification particulars for electronic records, and the Schedule specifies the certificate content expectations. The Supreme Court has treated certificate compliance as a threshold rule in *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, and it clarified the certificate pathway again in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, AIR 2020 SC 4908. Therefore, blockchain analytics output, screenshots, and exchange emails must come with proper certification and provenance. Else the court may reject them at admission.[54]

Prosecution often proceeds on two parallel tracks. The predicate offence track uses the IT Act, 2000 for identity theft and cheating by personation via computer resources, along with BNS offences like cheating, forgery, extortion, criminal intimidation, and conspiracy depending on the fact pattern. The proceeds track then uses PMLA when the accused projects or layers "proceeds of crime" through VDAs. The Supreme Court in *Vijay Madanlal Choudhary v. Union of India*, 2022 SCC OnLine SC 929 affirmed the statutory architecture of PMLA and its enforcement logic, so investigators must build a clean predicate narrative and a clean money trail. If the predicate collapses, the laundering case weakens too.[55]

Finally, courts will scrutinise blockchain tracing methods as expert opinion, not as identity proof by default. Academic work on clustering shows that heuristics can generate false positives and unstable clusters when wallets adapt or when mixing and change-address behaviour misleads the model. So investigators should disclose methodology, preserve raw transaction graphs, and avoid overclaiming attribution. This

[53] Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 105 (India).
[54] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 (India).
[55] *Vijay Madanlal Choudhary v. Union of India*, 2022 SCC OnLine SC 929.

improves credibility under cross-examination and reduces wrongful implication risks, which courts treat seriously.[56]

IX. COMPARATIVE AND INTERNATIONAL APPROACHES

The EU has moved toward harmonised licensing plus traceability. Regulation (EU) 2023/1114 (MiCA) creates a structured regime for crypto-asset service providers and stablecoin style issuances, while Regulation (EU) 2023/1113 applies Travel Rule style information requirements to transfers of certain crypto-assets and flags risks around self-hosted addresses. This model treats compliance as market infrastructure, not optional platform policy. India can borrow the idea of uniform supervisory baselines and cross-provider interoperability.[57]

FATF continues to act as the global alignment layer. Its Best Practices on Travel Rule Supervision (2025) gives practical supervisory approaches, including thematic reviews, solution adoption checks, and enforcement escalation for non-compliance. This matters for India because MLAT requests and exchange-to-exchange information sharing work better when counterpart jurisdictions apply the same data fields and transmission timing standards. Fragmented implementation invites criminals to route through weak nodes.[58]

The United States frames many virtual currency business models through the AML lens of money services businesses. FinCEN's 2019 guidance consolidates how administrators and exchangers of convertible virtual currency trigger registration, AML program duties, and suspicious activity reporting expectations. For Indian policy, this shows a clear

[56] Malte Möser & Arvind Narayanan, *Resurrecting Address Clustering in Bitcoin* (2021), https://fc22.ifca.ai/preproceedings/87.pdf (last visited Mar. 4, 2026).
[57] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA).
[58] Fin. Action Task Force (FATF), *Best Practices on Travel Rule Supervision* (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf (last visited Mar. 4, 2026).

compliance hinge. If a platform intermediates value, law should treat it like an obliged entity, even if it brands itself as "tech."[59]

The United Kingdom uses registration and fit-and-proper screening to gate AML entry. The FCA states that cryptoasset businesses within scope must register under the Money Laundering Regulations before operating. This creates supervisory leverage through refusal, conditions, and ongoing compliance checks. India's FIU registration approach is moving in a similar direction, but it still needs stronger cross-border enforceability and consistent supervisory depth.[60]

For international cooperation, UNTOC supports mutual legal assistance, confiscation cooperation, and transnational organised crime coordination, which fits large pig-butchering networks and laundering rings. The Budapest Convention on Cybercrime provides a detailed framework for expedited preservation and cross-border assistance in cyber investigations. Even where India relies mainly on bilateral MLATs, these instruments illustrate what "fast cooperation" looks like in treaty form, and they offer drafting cues for modern crypto evidence requests.[61]

X. FINDINGS AND DISCUSSION

India brought key VDA service activities into the AML perimeter through Notification S.O. 1072(E) dated 7 March 2023. Yet the instrument stays activity-focused. It does not prescribe baseline traceability standards. It does not set minimum audit trails for cross-chain hops. This creates uneven evidence quality across platforms for the same offence pattern.[62] FIU-IND's updated AML and CFT guidelines for reporting entities providing

[59] FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019), https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (last visited Mar. 4, 2026).
[60] Fin. Conduct Auth., *Cryptoassets: Who Needs to Register* (Oct. 24, 2023), https://www.fca.org.uk/firms/cryptoassets-aml-ctf-regime/cryptoassets-who-needs-register (last visited Mar. 4, 2026).
[61] United Nations Convention against Transnational Organized Crime, Nov. 15, 2000, U.N.T.S. vol. 2225, p. 209.

[62] Ministry of Finance (Dep't of Revenue), Notification S.O. 1072(E), Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Mar. 7, 2023) (India).

VDA services consolidate KYC, monitoring, recordkeeping, and reporting expectations. Still, practical gaps remain on unhosted wallet interactions and fast DeFi routing. Platforms often treat compliance as form filling and not as attribution engineering. That weakens post-incident tracing.[63]

FATF's targeted update confirms uneven global implementation of Recommendation 15 and its interpretative note. Travel Rule adoption remains inconsistent across jurisdictions. Criminals exploit that unevenness as a routing map. AI then reduces the time window for interdiction by automating the laundering choreography.[64] FATF's Best Practices on Travel Rule Supervision shows why "law on paper" fails without supervision in practice. Supervisors struggle to verify whether VASPs actually transmit required originator and beneficiary information in time and in full. Weak testing and weak enforcement degrade interoperability. This is the exact point where cross-border attribution breaks.[65]

Chainalysis reported that illicit addresses sent about $22.2 billion worth of cryptocurrency to services in 2023. The data supports a choke-point finding. Laundering still seeks service exits such as exchanges, brokers, and other venues. India's model can work only if those services preserve high-grade attribution artefacts and respond fast to lawful requests.[66] CERT-In Directions of 28 April 2022 impose fast incident reporting and log retention expectations on covered entities. Crypto investigations still lose momentum when platforms do not standardise forensic readiness. Logs arrive late, incomplete, or

[63] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023), https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf (last visited Mar. 4, 2026).

[64] Fin. Action Task Force (FATF), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs (July 2024), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (last visited Mar. 4, 2026).

[65] Fin. Action Task Force (FATF), Best Practices on Travel Rule Supervision (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf (last visited Mar. 4, 2026).

[66] Chainalysis Team, 2023 Crypto Money Laundering: Key Trends (Feb. 2024), https://www.chainalysis.com/blog/2024-crypto-money-laundering/ (last visited Mar. 4, 2026).

without integrity notes. That leaves investigators over-dependent on screenshots and summaries. Defence then attacks reliability.[67]

Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023 mandates audio-video recording of search and seizure and prompt forwarding to the Magistracy. In crypto cases this matters because seed phrases, hardware wallets, and recovery keys are fragile evidence. Proper recording and sealing reduces disputes on planting and tampering, which otherwise derail trials.[68] Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 sets the admissibility pathway for electronic records, including certification particulars. Blockchain analytics outputs, exchange emails, and server logs must therefore travel with compliant certificates and provenance details. Otherwise courts may treat them as inadmissible at the threshold.[69]

The Supreme Court in *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 treated statutory certification as a condition precedent for admissibility of secondary electronic evidence. Crypto prosecutions must therefore avoid casual printouts and informal exports. Investigators must build certification into the evidence lifecycle from day one.[70] The Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, AIR 2020 SC 4908 reaffirmed *Anvar* and clarified the limited circumstances around the certificate requirement. This is central in VDA cases because key proof sits with third-party platforms. Investigators must use lawful process quickly so platform-origin records can be certified correctly.[71]

XI. RECOMMENDATIONS AND REFORM ROADMAP

FIU-IND should publish minimum traceability and forensic-readiness standards for VDA reporting entities. The standards should specify baseline logs, retention format,

[67] Indian Comput. Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 4, 2026).
[68] Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 105 (India).
[69] Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 63 (India).
[70] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[71] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, AIR 2020 SC 4908.

withdrawal telemetry, and audit trails for chain hops. This converts tracing from vendor discretion into enforceable compliance. It also makes later court scrutiny more predictable.[72] India should harden Travel Rule compliance from "policy expectation" to "tested control." Supervisors should run thematic inspections, verify message completeness, and require interoperable solution adoption. Enforcement escalation should be real, not symbolic. FATF's supervisory practices provide a ready blueprint.[73]

A tiered framework for unhosted wallet interactions should become explicit. Platforms should apply enhanced scrutiny for high-value unhosted withdrawals, including proof-of-control checks and calibrated transaction delays where risk spikes. This keeps proportionality while closing the identity gap that laundering chains exploit.[74] India should adopt a "control-point" approach for DeFi compliance triggers. If a person or group controls admin keys, upgrades, front ends, or fee flows, then duties should attach. This prevents decentralisation labels from becoming a liability shield. FATF's implementation findings already support this risk framing.[75]

CERT-In reporting and FIU suspicious reporting should link into a standard fast-track case package. The package should carry incident timestamps, wallet addresses, transaction hashes, ticket IDs, and key log extracts. This reduces duplication across agencies and speeds freezing. It also improves chain-of-custody quality early.[76] Police training should focus on court survivability of electronic proof. Standard certificate

[72] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Updated Jan. 8, 2026), https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf (last visited Mar. 4, 2026).
[73] Fin. Action Task Force (FATF), Best Practices on Travel Rule Supervision (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf (last visited Mar. 4, 2026).
[74] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Updated Jan. 8, 2026), https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf (last visited Mar. 4, 2026).
[75] Fin. Action Task Force (FATF), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs (July 2024), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (last visited Mar. 4, 2026).
[76] Indian Comput. Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 4, 2026).

templates should align with the statutory particulars under the Bharatiya Sakshya Adhiniyam, 2023. Investigators should preserve reproducible raw transaction graphs and platform exports, not only PDF summaries. This makes expert testimony defensible under cross-examination.[77]

DPDP Rules, 2025 compliance must run alongside KYC and Travel Rule programs. Platforms should implement minimisation, role-based access, encryption, and breach handling. Clear internal separation between KYC stores and telemetry stores reduces misuse risk while preserving lawful attribution capability.[78]

India can borrow the EU's uniform supervisory baselines through a domestic equivalent of harmonised licensing and transfer information rules. MiCA shows how a consolidated regime can reduce regulatory arbitrage across service providers. India need not copy the text, but it can copy the discipline of uniform metrics.[79] The EU transfer-information regulation extends information obligations to certain crypto-asset transfers, including compliance expectations around self-hosted address risk. This supports a practical lesson. Traceability improves when transfer rules and service rules speak the same language. It also improves MLAT cooperation.[80]

XII. CONCLUSION

Digital-asset tracing now sits inside a race condition. AI compresses planning, targeting, and laundering into minutes. Attackers run parallel playbooks. They phish, drain, swap, bridge, and cash out with very little human friction. Meanwhile, global compliance remains uneven and Travel Rule adoption still varies by jurisdiction. That asymmetry creates predictable laundering corridors, and criminals use them like highways.[81]

---

[77] Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 63 (India).
[78] Digital Personal Data Protection Rules, 2025 (India).
[79] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, 2023 O.J. (L 150) 40.
[80] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets, 2023 O.J. (L 150) 1.
[81] Fin. Action Task Force (FATF), Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (July 9, 2024), https://www.fatf-gafi.org/content/dam/fatf-

India has already taken the right structural step by pulling core VDA service activities into the AML perimeter and by assigning FIU-IND a central regulatory role for VDA service providers. Yet the ecosystem still treats compliance as form rather than function. A platform can tick KYC boxes and still preserve weak attribution artefacts. That weakens tracing later, and it weakens prosecution even more. India therefore needs compliance to behave like tracing infrastructure, not a quarterly ritual.[82]

Cross-border cases expose the sharpest gap. Investigators often know where the funds went but they cannot compel fast disclosure abroad. Here the Travel Rule becomes the practical bridge between identity and transaction flow. But the Travel Rule only helps when supervisors test it and enforce it, and when VASPs use interoperable messaging standards. Without that, platforms will "collect" data but never transmit it at speed. Then, the chain breaks at the border and the victim loses recovery chances.[83]

The first hours after a crypto incident decide the file. If logs survive and time is consistent, attribution becomes feasible. If logs vanish or arrive late, the case becomes a pure graph story. CERT-In directions already push rapid reporting and structured log retention for specified entities. Yet many VDA actors still lack forensic readiness. They do not lock audit trails quickly. They also do not preserve withdrawal approval metadata cleanly. This creates avoidable evidentiary holes, and some holes never close.[84]

Prosecution does not run on chain analytics alone. Courts ask for admissible electronic records, clean provenance, and procedure that survives challenge. BNSS recording of searches and seizures strengthens the custody narrative for devices and keys. Bharatiya

gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (last visited Mar. 4, 2026).

[82] Fin. Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Updated Jan. 8, 2026), https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf (last visited Mar. 4, 2026).

[83] Fin. Action Task Force (FATF), Best Practices on Travel Rule Supervision (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf (last visited Mar. 4, 2026).

[84] Indian Comput. Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 4, 2026).

Sakshya Adhiniyam certification discipline then decides admissibility of platform exports and logs. The Supreme Court's approach in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, AIR 2020 SC 4908 makes the point plain. The State must prove the record properly, not merely narrate it.[85]

Finally, the system must keep rights and security in balance. KYC and Travel Rule data collection is intrusive by design. It creates large identity stores that criminals will try to breach. The DPDP regime expects lawful processing, safeguards, and accountability, while constitutional privacy doctrine demands proportionality. Platforms must therefore minimise, secure, and segregate identity data. They must also document lawful access pathways so investigators can obtain what they need without turning every case into a privacy dispute. A clean governance model helps both enforcement and trust, even if it feels slower at first.[86]

XIII. BIBLIOGRAPHY

A. Indian Statutes, Rules, and Subordinate Legislation

1. Information Technology Act, 2000 (India).
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
3. Prevention of Money Laundering Act, 2002 (India).
4. Bharatiya Nyaya Sanhita, 2023 (India).
5. Bharatiya Nagarik Suraksha Sanhita, 2023 (India).
6. Bharatiya Sakshya Adhiniyam, 2023 (India).
7. The Digital Personal Data Protection Act, 2023 (India).
8. Digital Personal Data Protection Rules, 2025 (India).

[85] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, AIR 2020 SC 4908.
[86] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India).

9. Income-tax Act, 1961 (India) (including § 115BBH; § 194S).

10. Finance Act, 2022 (India) (VDA taxation and TDS framework as enacted).

B. Indian Government Notifications, Circulars, and Official Guidance

1. Ministry of Finance (Dep't of Revenue), Notification S.O. 1072(E) (Mar. 7, 2023) (India), https://egazette.gov.in/WriteReadData/2023/244184.pdf (last visited Mar. 4, 2026).

2. Financial Intelligence Unit-India, AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (updated Jan. 8, 2026), https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf (last visited Mar. 4, 2026).

3. Financial Intelligence Unit-India, 3rd Revision of Circular for Registration of Virtual Digital Asset Service Providers (VDA SPs) in FIU-IND as Reporting Entity (Sept. 15, 2025), https://fiuindia.gov.in/pdfs/downloads/VDASP15092025.pdf (last visited Mar. 4, 2026).

4. Press Information Bureau, Ministry of Finance, FIU-IND Issues Notices for Non-Compliance to 25 Offshore VDA SPs (Oct. 1, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758 (last visited Mar. 4, 2026).

5. Indian Computer Emergency Response Team (CERT-In), Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited Mar. 4, 2026).

6. Reserve Bank of India, Prohibition on Dealing in Virtual Currencies (VCs), RBI/2017-18/154, DBR.No.BP.BC.104/08.13.102/2017-18 (Apr. 6, 2018), https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT154ML060418.PDF (last visited Mar. 4, 2026).

7. Reserve Bank of India, Master Direction: Know Your Customer (KYC) Direction, 2016 (Feb. 25, 2016) (as amended), https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.pdf (last visited Mar. 4, 2026).

8. Government of India, Finance Bill, 2022 (official text), https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf (last visited Mar. 4, 2026).

9. Ministry of Electronics & Information Technology, Digital Personal Data Protection Rules, 2025 (portal page), https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025 (last visited Mar. 4, 2026).

10. Press Information Bureau, DPDP Rules, 2025 Notified: A Citizen-Centric Framework (Nov. 17, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf (last visited Mar. 4, 2026).

11. Ministry of Home Affairs, Annual Report 2023-24 (PDF) (India), https://xn--i1b5bzbybhfo5c8b4bxh.xn--11b7cb3a6a.xn--h2brj9c/sites/default/files/AnnualReport_27122024.pdf (last visited Mar. 4, 2026).

12. Ministry of External Affairs, Treaty Between India and the United States of America on Mutual Legal Assistance in Criminal Matters (Oct. 17, 2001) (PDF), https://www.mea.gov.in/Portal/LegalTreatiesDoc/US01B0634-1-1.pdf (last visited Mar. 4, 2026).

C. International Standards, Regional Regulations, and Instruments

1. Financial Action Task Force (FATF), Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct. 2021),

https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf (last visited Mar. 4, 2026).

2. Financial Action Task Force (FATF), Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (July 9, 2024), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (last visited Mar. 4, 2026).
3. Financial Action Task Force (FATF), Best Practices on Travel Rule Supervision (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf (last visited Mar. 4, 2026).
4. Financial Action Task Force (FATF), Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (Sept. 2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf (last visited Mar. 4, 2026).
5. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA), 2023 O.J. (L 150).
6. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets (recast), 2023 O.J. (L 150).
7. United Nations Convention against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.
8. Convention on Cybercrime (Budapest Convention), Nov. 23, 2001, ETS No. 185.
9. FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN-2019-G001) (May 9, 2019), https://www.fincen.gov/system/files/2019-

05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (last visited Mar. 4, 2026).

D. Academic and Technical Literature

1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf (last visited Mar. 4, 2026).

2. Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, in *Proceedings of the 2013 Internet Measurement Conference* (2013), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (last visited Mar. 4, 2026).

3. Malte Möser & Arvind Narayanan, Resurrecting Address Clustering in Bitcoin, in *Financial Cryptography and Data Security* (2022) (preprint), https://fc22.ifca.ai/preproceedings/87.pdf (last visited Mar. 4, 2026).