Blockchain and Virtual Digital Assets

India, the UAE and Singapore

BY

Chandan Goswami

Partner, AT & Partners

Important Notice & Disclaimer

This guide is intended for general information and professional education only. It is not legal advice, does not create an attorney–client relationship, and must not be relied upon as a substitute for tailored advice on any specific matter. The law governing virtual digital assets is unusually fluid in each of the jurisdictions surveyed; provisions, regulator positions and case law can and do change within months. The commentary characterising the arguments of any regulator or enforcement agency reflects the author's reading of publicly reported positions and pleadings, and is offered to assist the readers in advising and, where necessary, in contesting such positions — not as a statement of any agency's official view.

Nothing in this guide should be read as encouraging or facilitating any breach of law in any jurisdiction. Cross-border structuring in this sector engages tax, exchange-control, securities, anti-money-laundering and insolvency regimes simultaneously, and specific advice should be taken before any step is implemented. *All statutory and case references should be verified against the primary sources as in force on the relevant date.*

Contents

ABOUT AT & PARTNERS

AT & Partners was built on a simple idea: the most important legal questions of the coming decade will not sit neatly within traditional boundaries. They arise where law meets technology. The practice is focused there — artificial intelligence, blockchain and cryptocurrency, Web3, space law and technology contracts — alongside a full-service corporate and commercial litigation practice, because advisory work changes once you have seen how things fall apart in court.

Research is the foundation of the practice rather than a support function: in technology law, where statutes are drafted years after the technology they govern has matured, that commitment is not optional. The firm publishes international-grade research guides, of which this is one, and writes in The Hindu, Mint and elsewhere.

Its base of operations is New Delhi, with partners and senior counsel regularly present in Dubai, Singapore, London, Bangalore, Hyderabad and Kolkata, and clients across Singapore, London, the UAE, Panama and the United States.

AREAS OF PRACTICE

Artificial Intelligence

AI governance frameworks, liability for AI errors, IP ownership in AI-generated outputs, AI contract structuring, EU AI Act compliance for India-based companies, and advisory on AI deployment in regulated sectors including financial services, healthcare, and insurance.

Space Law

IN-SPACe authorisation and engagement, advisory under the Indian Space Policy 2023 and NGP 2024, remote sensing data commercialisation under RSDP 2011, insurance structuring for space activities, and international space treaty implications for private operators.

Cryptocurrency & Blockchain

Token structuring and regulatory classification, exchange compliance and FIU-IND registration, AML/KYC programme design, DAO frameworks, jurisdictional regulatory navigation, and representation in crypto-related regulatory inquiries.

Technology Contracts

SaaS and technology services agreements, AI-specific contract provisions, software development and IP assignment, DPDP Act compliance in commercial agreements, data processing agreements, and procurement contracts for technology companies.

Web3 & Digital Assets

Platform documentation and IP frameworks, smart contract legal structures, DeFi regulatory advisory, digital asset transaction documentation, deal structuring, hack response and recovery.

Corporate & Commercial Litigation

Technology sector disputes, commercial arbitration, contract disputes, IP litigation, regulatory enforcement response, and crisis management across sectors including technology, FMCG, petroleum, and financial services.

FOREWORD

India is building fast in blockchain and digital assets, and Indian founders are working at a pace that consistently outstrips the development of the legal frameworks designed to govern them. In most jurisdictions the law follows technology by a decade or more. In India, that gap is both a challenge and an opportunity.

This guide is written for the people in that gap — founders, operators, in-house counsel, and the lawyers who advise them, building at the intersection of virtual digital assets and law, often without a clear map of the terrain.

It is not a comprehensive treatise but a guide, written from over a decade of advising companies through token structuring, exchange compliance, hack response and recovery, enforcement inquiries, and the quiet legal crises that most founders encounter too late.

It is anchored in India, where the sector is taxed and policed but not regulated, and is therefore defined by enforcement rather than by licensing. Part 2 sets out the Enforcement Directorate's statutory toolkit, the arguments the agency actually advances, and the doctrinal answer to each. The chapters on the UAE and Singapore are here for contrast, and for the structuring questions that follow — what a licence-led regime looks like, what a mature activity-based one looks like, and what an Indian-origin business genuinely gains and loses by moving.

The principles that run through it are consistent: understand the framework before you build; never assume that regulatory silence means regulatory permission; and remember that a migration offshore does not extinguish an Indian nexus.

Where the law is genuinely uncertain, I have said so. Where a position is contestable, I have set out both sides — the agency's, and the answer. I hope you find it useful.

CHANDAN GOSWAMI

1. Summary

Three of the most consequential jurisdictions for digital-asset businesses in the Asia–Gulf corridor — India, the United Arab Emirates and Singapore — have arrived at strikingly different equilibria. This guide maps all three, but it is anchored in India, where the defining feature of the landscape is not a regulatory statute but an *enforcement* posture: the sector is taxed heavily, brought within anti-money-laundering law, and policed vigorously, yet it remains without a dedicated legislative framework.

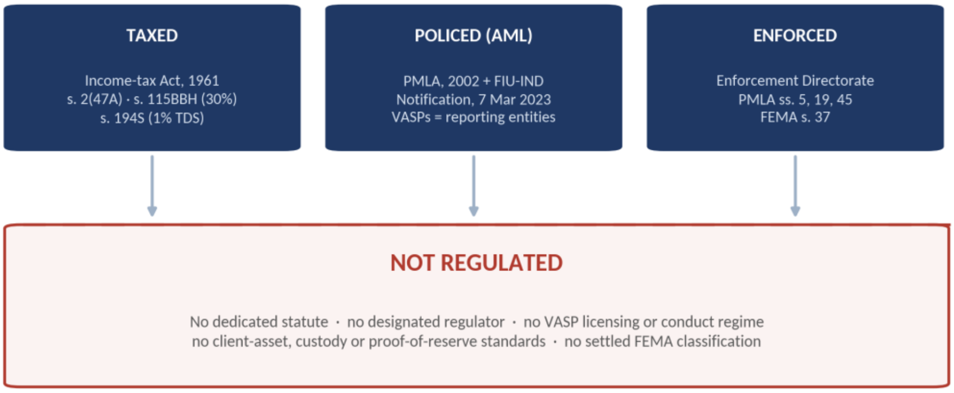

Figure 1 — India's VDA architecture — three hooks, and no statute.

India recognises virtual digital assets (**VDAs**) only obliquely — through the tax definition in section 2(47A) of the Income-tax Act, 1961 — while declining to treat them as legal tender. A flat 30% tax on transfers, a 1% tax deducted at source, and a bar on set-off of losses discourage domestic activity; the March 2023 notification bringing VDA service providers within the Prevention of Money Laundering Act, 2002 (**PMLA**) supplies the compliance spine; and the Enforcement Directorate (**ED**) supplies the teeth. By the Government's own account, the ED had by December 2025 attached, seized or frozen proceeds of crime worth roughly ₹4,190 crore in crypto-linked matters. A parallel FEMA theory — that moving value across borders in stablecoins is an unauthorised transfer of foreign exchange — has opened a second, and arguably more destabilising, front.

The guide's central Indian contribution is a litigator's map of that enforcement effort: the statutory toolkit the ED wields, the specific arguments it advances (proceeds of crime, the exchange as facilitator, provisional attachment, extraterritorial reach, and the FEMA "hawala" analogy), and the doctrinal answers to each — the scheduled-offence requirement, the preventive and civil character of attachment recognised in *Vijay Madanlal Choudhary*, the identification and valuation problems intrinsic to on-chain assets, the certification conundrum that public-blockchain evidence poses under section 63 of the Bharatiya Sakshya Adhiniyam, 2023, and the single most powerful structural objection: that the State cannot simultaneously tax crypto as an asset, deny that it is currency, and prosecute its cross-border movement as though it were money.

Against India's enforcement-first model, the **UAE** offers a licence-led, multi-regulator architecture — federal (CBUAE and the SCA) layered over Emirate-level (Dubai's VARA) and free-zone regimes (ADGM's FSRA and DIFC's DFSA) — now consolidated by Federal Decree-Law No. 6 of 2025, which extends Central Bank oversight to on-chain activity and ends the "just code" defence for decentralised finance. **Singapore** offers a mature, activity-based regime under the Payment Services Act 2019 and the Securities and Futures Act 2001, tightened in 2025 by the digital-token-service-provider regime under Part 9 of the Financial Services and Markets Act 2022, which effectively closes the door on Singapore-incorporated firms serving only offshore clients.

For the Indian founder, the practical consequence is a well-worn migration to Dubai or Singapore — a move that solves the domestic regulatory vacuum but creates fresh exposure under India's exchange-control and round-tripping rules, and, as the WazirX collapse demonstrates, leaves Indian users exposed to a cross-border insolvency system India has not fully equipped itself to engage. The guide closes with a comparative matrix and a concrete reform agenda for India.

2. INDIA: THE ENFORCEMENT-FIRST REGIME

India presents a paradox that no amount of drafting has yet resolved: a market of well over one hundred million users and among the highest grass-roots adoption rates in the world, governed by no dedicated statute, yet subject to one of the heaviest tax burdens and one of the most active enforcement machineries applied to the asset class anywhere. The Indian position is therefore best understood not as a coherent regulatory scheme but as the sum of three overlapping impulses — to *tax* the sector, to bring it within *anti-money-laundering* discipline, and to *police* it — operating in the continued absence of the fourth impulse, to regulate it. This Part maps each layer, then turns to the enforcement effort that dominates practice.

2.1 The definitional and taxonomy framework

The only operative statutory definition of a virtual digital asset in Indian law sits in tax legislation. Section 2(47A) of the Income-tax Act, 1961, inserted by the Finance Act, 2022, defines a VDA expansively across three limbs: any information, code, number or token (not being Indian or foreign currency) generated through cryptographic means and capable of being transferred, stored or traded electronically; a non-fungible token or similar token; and any other digital asset the Central Government may notify.[1]

Here are the two consequences that follow. First, the definition is functional and technology-agnostic. It captures cryptocurrencies, stablecoins (including fiat-referenced tokens such as USDT and USDC), and NFTs, regardless of label. The Finance Act, 2025 further widened the language to place beyond doubt that any crypto-asset relying on cryptographically secured distributed-ledger technology falls within scope, and introduced a dedicated transaction-reporting obligation and the treatment of undisclosed VDA holdings within search and block-assessment provisions.[2] The Central Board of Direct Taxes has, by notification, carved

[1]Income-tax Act, 1961, s. 2(47A), inserted by the Finance Act, 2022, w.e.f. 1 April 2022. The Central Government has power to notify further assets and to exclude specified assets by notification.

[2]Finance Act, 2025 — amendments to s. 2(47A) and related provisions; introduction of a prescribed reporting obligation for crypto-asset transactions (aligned in design with the OECD Crypto-Asset Reporting Framework) and inclusion of VDAs within the block-assessment machinery for undisclosed income.

out of the NFT limb those tokens whose transfer effects a legally enforceable transfer of ownership of an underlying tangible asset.[3]

Second, and critically important, the definition does not confer legal status on a VDA. A VDA is neither legal tender nor currency; it cannot be insisted upon as a means of payment protected by law. What is permitted is private dealing — the purchase, sale and holding of VDAs by individuals and entities is lawful. India has thus chosen neither prohibition nor recognition, but a narrow tax-law acknowledgment that leaves the asset class in a defined-but-unregulated space.

2.2 Regulation by taxation

In the vacuum left by the absence of a regulatory statute, tax policy has functioned as de facto regulation — and, many would argue, as deliberate friction. Three features define the regime introduced by the Finance Act, 2022:

- **Flat 30% tax on transfers.** Section 115BBH charges income arising on the transfer of any VDA at a flat 30% (plus applicable surcharge and cess), with no deduction permitted other than the cost of acquisition.[4]
- **No set-off of losses.** Loss from the transfer of a VDA cannot be set off against income under any other head, nor carried forward — so gains and losses across tokens cannot be netted. This is punitive by design and has no analogue in the treatment of shares, commodities or other capital assets.
- **1% tax deducted at source.** Section 194S imposes a 1% TDS on the consideration for transfer of a VDA above prescribed thresholds. Although modest as a rate, TDS on every transaction creates a continuous, granular reporting trail and materially impairs the economics of high-frequency trading.[5]

Reporting is channelled through the dedicated Schedule VDA in the income-tax return. The compliance dividend of this architecture is now visible in enforcement data: in December 2025 the Government told Parliament that the CBDT had detected undisclosed income of approximately ₹888.82 crore from VDA transactions in search operations, and had issued

[3] CBDT Notification No. 75/2022 dated 30 June 2022 (excluding from the NFT definition tokens whose transfer results in a legally enforceable transfer of ownership of an underlying tangible asset).

[4] Income-tax Act, 1961, s. 115BBH.

[5] Income-tax Act, 1961, s. 194S, w.e.f. 1 July 2022; failure to deduct is addressed by ss. 271C and 276B.

more than 44,000 communications to taxpayers who had traded in VDAs without reporting in Schedule VDA.[6]

Layered on top for offshore holdings is the Black Money (Undisclosed Foreign Income and Assets) Act, 2015. A resident holding VDAs on a foreign exchange or in a foreign wallet must disclose them in Schedule FA of the return; non-disclosure exposes the holder to the Black Money Act's severe penalty and prosecution provisions, wholly independent of the income-tax consequences.[7]

Taxation is not recognition. That VDAs are taxed as assets does not, of itself, resolve their status under exchange-control, securities or evidence law — and, as Part 2.6 develops, the mismatch between how the same asset is treated under the Income-tax Act and under FEMA is a live and exploitable inconsistency in the State's own position.

2.3 The regulatory architecture and the missing statute

2.3.1 The banking-ban litigation

The RBI has been consistently sceptical of private virtual currencies, cautioning the public as early as 2013 and, in April 2018, directing regulated entities not to deal with or provide services to any person or business dealing in virtual currencies. That circular was challenged and set aside by the Supreme Court in *Internet and Mobile Association of India v. Reserve Bank of India*, the single most important Indian authority in the field.[8]

The Court held the measure disproportionate under Article 19(1)(g): although the RBI possessed ample power to act pre-emptively in defence of the financial system, it had not demonstrated that regulated entities had suffered any measurable harm, and had effectively banned a lawful trade absent any legislative prohibition of that trade. *IAMAI* judgment thus stands for two propositions that continue to structure the field: there is no legislative ban on dealing in VDAs in India; and disproportionate administrative action against the sector is subject to be challenged. Interestingly, the RBI's posture has since shifted to a parallel strategy — advancing its own central bank digital currency (CBDC) as a sovereign,

[6]Minister of State for Finance, written reply, Lok Sabha, 8 December 2025 (undisclosed income of ~₹888.82 crore detected from VDA transactions; 44,057 communications issued to non-reporting taxpayers).

[7]Black Money (Undisclosed Foreign Income and Assets) Act, 2015 — foreign VDA holdings are reportable as foreign assets; non-disclosure attracts penalty and prosecution.

[8]Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.

controllable alternative, while senior officials continue to characterise private crypto-assets as lacking intrinsic value.[9]

2.3.2 SEBI, IFSCA and the emerging multi-regulator idea

No securities regulator has been formally designated as the crypto regulator, but the contours of a division of labour are emerging. The Securities and Exchange Board of India (SEBI) has signalled a willingness to supervise tokens that exhibit the characteristics of securities — instruments conferring rights to returns, profit participation or governance — leaving payment-type tokens such as Bitcoin and Ether to be treated as commodities. In inter-ministerial deliberations, a *multi-regulator* model has been floated, under which different authorities would supervise different functional categories of VDA rather than a single monolithic regulator.[10]

The most concrete regulatory innovation has come from the International Financial Services Centres Authority (IFSCA) at GIFT City, which has advanced a framework for the tokenisation of real-world assets within its regulatory sandbox, including conditional approvals for tokenised-asset marketplaces. IFSCA's posture demonstrates that risk-calibrated experimentation is achievable within India's borders where a purpose-built regulator with a clear remit exists.[11]

2.3.3 The statute that is yet to arrive

It is an open secret that a comprehensive VDA law has been anticipated for years but has not yet materialised. A discussion paper on the Government's policy stance, expected in 2024, was deferred, th1en in December 2024 the Ministry of Finance told Parliament that no timeline was anticipated for comprehensive regulatory guidelines. In May 2025 the Supreme Court, hearing a related matter, publicly questioned the absence of clear regulation and urged the framing of a coherent policy — following which the CBDT invited stakeholder feedback on whether a dedicated VDA law is needed.[12]

---

[9]The RBI's CBDC pilots have expanded materially since 2022; the central bank's stated preference is for a sovereign, programmable digital currency rather than private tokens.

[10]A functional, multi-agency supervisory model — with SEBI supervising security-like tokens, the RBI addressing systemic and payment-token risk, and the FIU-IND retaining the AML mandate — has been reported as under consideration; it remains a policy proposal rather than an enacted allocation of jurisdiction.

[11]IFSCA consultation on tokenisation of real-world assets (February 2025) and subsequent regulations enabling sandbox-based experimentation at GIFT City IFSC.

[12]The Supreme Court's observations of May 2025 on the regulatory gap; the Ministry of Finance's December 2024 statement in Parliament that no timeline was anticipated; and the subsequent CBDT stakeholder-

The consistent judicial refrain — that the design of a regulatory framework is the domain of the legislature and the executive — was reiterated when the Supreme Court declined, in April 2025, to entertain a writ petition brought by aggrieved users seeking directions to frame such a framework.[13] The result is a policy stasis in which the sector is taxed and policed but not regulated — the precise condition that makes the enforcement analysis in the sections that follow so consequential.

2.4 The the PMLA and FIU-IND

If tax is the friction and enforcement is the teeth, the March 2023 notification under the PMLA is the connective tissue between them. By a notification dated 7 March 2023, the Ministry of Finance designated persons carrying on specified VDA-related activities as "reporting entities" under the PMLA, ending the regulatory ambiguity that had insulated the sector from formal AML obligations.[14]

The notification captures five activities where carried on for or on behalf of another person in the course of business:

- exchange between VDAs and fiat currencies;
- exchange between one or more forms of VDA;
- transfer of VDAs;
- safekeeping or administration of VDAs, or of instruments enabling control over VDAs; and
- participation in, and provision of, financial services relating to an issuer's offer and sale of a VDA.

A reporting entity must register with the Financial Intelligence Unit–India (FIU-IND), verify customer identity, maintain prescribed records, appoint a Designated Director and Principal Officer, and file the reports the PMLA and its Rules require — including suspicious-

feedback exercise. The Government has indicated that its final posture will be informed by evolving global standards, including developments in the United States and the recommendations of the FSB, IMF and FATF.

[13]In April 2025 the Supreme Court dismissed a criminal writ petition arising out of the WazirX matter, observing that framing a regulatory regime falls within the domain of the legislature and the executive.

[14]Ministry of Finance Notification dated 7 March 2023, issued under s. 2(1)(sa)/(wa) of the PMLA, bringing specified VDA activities within the definition of a person carrying on a designated business or profession (a reporting entity).

transaction and prescribed-transaction reports. Non-compliance attracts monetary penalty for each failure, in addition to any other action available under the Act.[15]

2.4.1 From domestic registration to offshore enforcement

Once domestic exchanges registered, enforcement turned outward. In December 2023, the FIU-IND issued show-cause notices to nine major offshore exchanges — among them Binance, KuCoin, Huobi, Kraken, Gate.io, Bittrex, Bitstamp, MEXC Global and Bitfinex — for operating without registration. As a result,non-compliant platforms faced URL-blocking that cut off easy access for Indian users.[16] The pressure produced results and penalties. In June 2024, the FIU-IND penalised Binance for operating without registration and for KYC/AML failures, and in January 2025 Bybit was penalised approximately ₹9.27 crore. In parallel, the Directorate General of GST Intelligence pursued Binance for unpaid GST of some ₹722 crore — a reminder that indirect-tax exposure runs alongside the AML and exchange-control fronts.[17]

"The 7 March 2023 notification casts a wide net and applies a single, one-size compliance template to a spectrum of very different actors. Its application to genuinely decentralised finance is unsettled: the notification does not distinguish centralised entities from DeFi protocols, and a bare self-description as 'decentralised' is not a safe harbour. The better view is that decentralisation lies on a spectrum, and only protocols that are demonstrably and sufficiently decentralised — with no controlling operator, front-end curator or fee-taker — can credibly claim to fall outside the regime. Front-end operation, token-listing curation and fee capture are the accountability hooks a regulator will reach for."

CHANDAN GOSWAMI

[15]Prevention of Money-Laundering (Maintenance of Records) Rules, 2005; FIU-IND registration and reporting obligations. Penalty for a reporting-entity failure is not less than ₹10,000 and may extend to ₹1,00,000 for each failure.

[16]FIU-IND show-cause notices to nine offshore VASPs, December 2023, followed by URL-blocking of non-compliant platforms.

[17]FIU-IND penalty order against Binance (June 2024); penalty of approximately ₹9.27 crore on Bybit Fintech Limited (January 2025); DGGI show-cause notice to Binance alleging GST of approximately ₹722.43 crore (August 2024). Several of these platforms subsequently registered with the FIU-IND and resumed India-facing operations.

2.5. The Enforcement Directorate

The Directorate of Enforcement is the single most important actor a VDA business or investor is likely to encounter in India. It operates two statutes of very different character — the PMLA, a penal anti-money-laundering law with sweeping attachment and arrest powers, and FEMA, a civil exchange-control law. Noticeably, it has begun to deploy both against the sector. Understanding the toolkit is the precondition to contesting its use.

2.5.1 The statutory toolkit

Under the PMLA, the offence of money-laundering in section 3 is drawn in deliberately wide terms — it percolates to anyone who directly or indirectly attempts to indulge in, knowingly assists, is knowingly a party to, or is actually involved in any process or activity connected with the proceeds of crime, including its concealment, possession, acquisition, use, or projection as untainted.

The ED's principal powers are: provisional attachment of property under **section 5** (on a recorded "reason to believe", initially for up to 180 days); adjudication and confirmation of attachment by the Adjudicating Authority under **section 8**; search and seizure under **sections 17 and 18**; arrest under **section 19**; the reverse burden in **section 24**; the twin bail conditions in **section 45**; and the power to summon and record admissible statements under **section 50**. Proceedings are opened by an internal Enforcement Case Information Report (ECIR), the analogue of an FIR.[18]

Under FEMA, Section 3 prohibits dealing in or transferring foreign exchange, and making payments to or for the credit of a person resident outside India, otherwise than through an authorised person. Section 13 provides for penalties up to three times the sum involved (or ₹2,00,000 where the amount is not quantifiable), with a continuing penalty for ongoing default, and section 37 confers investigative powers. It is noteworthy to mention that FEMA contraventions are civil, and are compoundable under section 15 of the Act which is a structural distinction from the PMLA.[19]

[18] Prevention of Money-Laundering Act, 2002, ss. 3, 5, 8, 17, 18, 19, 24, 45 and 50. Punishment under s. 4 is rigorous imprisonment of three to seven years (extendable to ten where the scheduled offence relates to the Narcotic Drugs and Psychotropic Substances Act).

[19] Foreign Exchange Management Act, 1999, ss. 3, 13, 15 and 37. Unlike its predecessor FERA, FEMA decriminalised exchange-control contraventions; they are adjudicated civilly and are ordinarily compoundable.

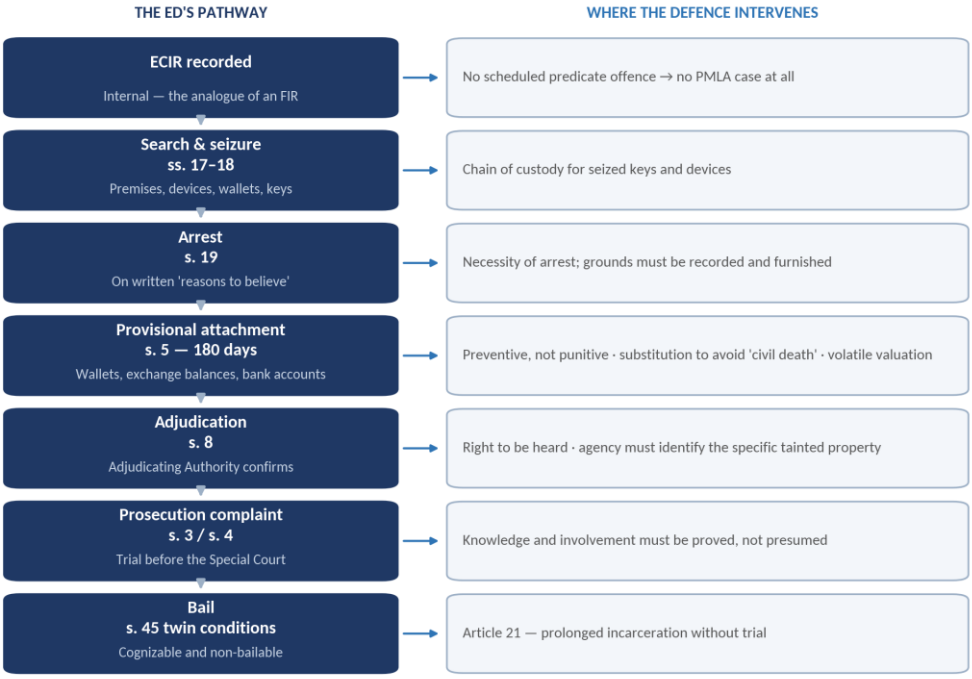

Figure 2 — The ED's PMLA pathway, and where the defence intervenes.

2.5.2 The numbers

The trajectory of the ED's crypto effort is visible in successive Parliamentary answers. Attachments in crypto-linked matters stood at roughly ₹907 crore in December 2022 and ₹936 crore by January 2023; by December 2025 the Government reported that the ED had attached, seized or frozen proceeds of crime of approximately ₹4,189.89 crore in crypto-related cases, with 29 arrests, 22 prosecution complaints filed, and one accused declared a Fugitive Economic Offender.[20] The headline figure should be read with a structural caveat that applies to PMLA enforcement generally. Across all PMLA matters, the ratio of assets attached to eventual convictions has historically been very large, which underscores a persistent gap between provisional seizure and proven guilt.

[20] Minister of State for Finance, written reply, Lok Sabha, 8 December 2025 (₹4,189.89 crore attached/seized/frozen; 29 arrests; 22 prosecution complaints; one Fugitive Economic Offender). Earlier Parliamentary answers recorded ₹907.48 crore (December 2022) and approximately ₹936 crore (January 2023).

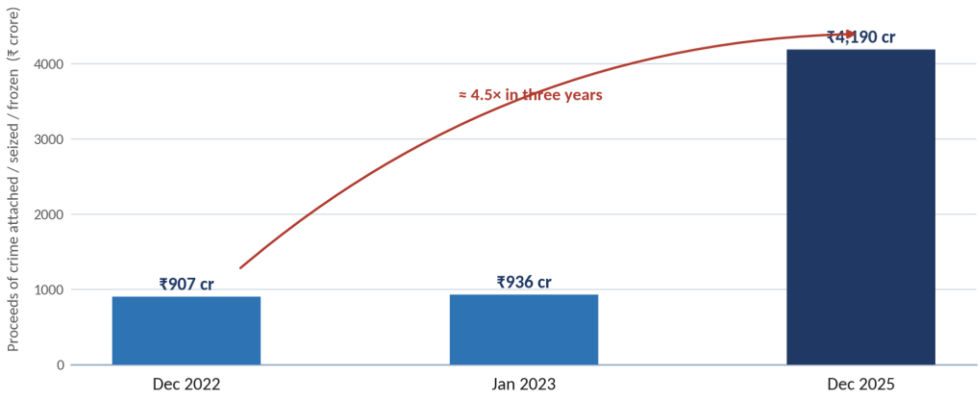

Figure 3 — Proceeds of crime attached, seized or frozen in crypto-linked cases (₹ crore).

Figure 4 — The enforcement scoreboard — position as reported to Parliament, December 2025.

2.5.3 Case study : Adnan Nisar v. Directorate of Enforcement

The leading Indian authority on the ED's jurisdiction over cross-border crypto fraud is the Delhi High Court's decision in *Adnan Nisar v. Directorate of Enforcement* (17 September 2024). The matter arose from a cryptocurrency fraud uncovered on a complaint by a victim in the United States; the ED, acting on a Mutual Legal Assistance Request, moved against WazirX accounts and then opened its own investigation, mapping the foreign conduct to cheating and related offences under the Indian Penal Code and the Information Technology Act to satisfy the scheduled-offence requirement.[21]

The Court held that an offence committed abroad can constitute a predicate offence under the PMLA where it has cross-border implications and the proceeds have travelled back into Indian territory, since money-laundering is then deemed to be committed in India. Crucially, however, it reaffirmed the outer limit. It said that the ED must anchor its case to a corresponding scheduled offence recognised under Indian law, even where the underlying fraud occurred overseas. The accused's reliance on *Vijay Madanlal Choudhary* and *P.*

[21]Adnan Nisar v. Directorate of Enforcement, Hon'ble The High Court of Delhi, judgment dated 17 September 2024. The accused's conduct was mapped to ss. 420 and 424 IPC and to the extraterritorial-application provision of the Information Technology Act, 2000.

Chidambaram — that prosecution presupposes a clearly established scheduled offence — was the correct doctrinal frame, and remains the first line of any defence.[22]

2.5.4 FEMA

A newer and more structurally significant line of enforcement recasts cross-border crypto flows as unauthorised foreign-exchange transactions. In June 2026, the ED conducted searches at premises in Bengaluru under section 37 of FEMA, targeting several on-ramp and payment-infrastructure companies over allegedly unauthorised cross-border transfers exceeding ₹2,500 crore effected using VDAs, and froze bank balances linked to the transactions.[23]

The ED's premise is that transmitting stablecoins directly to a foreign counterparty moves value across the border outside the regulated banking channel — a variant, in its view, of hawala; and that routing the fiat leg through a bank typically requires a misleading declaration of purpose, itself a contravention. The significance lies less in the specific allegations than in the breadth of the premise. Read expansively, it reaches virtually every India-facing platform that sources liquidity offshore, and potentially every over-the-counter cross-border VDA transaction. This front is analysed, and answered, in Part 2.6.

2.5.5 Case study — the unfortunate WazirX collapse and the cross-border vacuum

The July 2024 WazirX breach in which roughly US$235 million (about ₹2,000 crore) was drained from a multi-signature wallet operated under a third-party custody arrangement, in an attack widely attributed to the Lazarus Group, is the defining case study of what happens when a hack meets a regulatory vacuum. The Indian response was hobbled by the very gap this Part describes: the Delhi High Court, hearing petitions by aggrieved users, issued notices to the ED, the FIU-IND, the RBI and SEBI, directed the cyber unit to file a status report, and ordered production of the operator's arrangements but expressly observed that, crypto being unregulated, it could not itself direct an investigation into the hack.[24]

---

[22]The Court relied on the deeming effect of s. 2(2)/s. 3 PMLA for cross-border proceeds, while affirming that a corresponding scheduled offence under Indian law is indispensable — consistent with Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929, and P. Chidambaram v. Directorate of Enforcement, (2019) 9 SCC 24.

[23]ED searches in Bengaluru under s. 37 FEMA (June 2026) targeting on-ramp/payment-infrastructure providers over alleged unauthorised cross-border VDA transfers exceeding ₹2,500 crore; associated bank balances of approximately ₹6 crore frozen.

[24]2024 WazirX breach; petitions before the Delhi High Court (including the Jaivir Bains matter, W.P.(C) 14571/2024) with notices to the ED, FIU-IND, RBI and SEBI, and directions to the Delhi Police cyber unit (IFSO)

The recovery itself played out not in India but in Singapore, because the operating entity was domiciled there. A scheme of arrangement under Singapore's Insolvency, Restructuring and Dissolution Act 2018 was ultimately sanctioned by the Singapore High Court in October 2025 (after an earlier rejection and a re-vote), with the platform resuming operations and returning the bulk of user balances. The episode exposes a jurisdictional fault-line that recurs throughout this guide. Indian users, an Indian-facing business, an offshore parent, and an insolvency conducted under a foreign statute with India's own cross-border-insolvency machinery not yet fully in force to give Indian creditors a coordinated seat at the table.[25]

2.6 Mock arguments and answers

This section states, as fairly as the author can, the arguments the ED may have, and then sets out the mock answer to each. It is written for a general understanding on the issues. The arguments and answers are not be taken as legal advice or opinion on the subject matter.

(a) "The VDAs are proceeds of crime, and therefore tainted property liable to attachment."

The ED contends that VDAs derived from, or used to launder, the fruits of a scheduled offence are "proceeds of crime" within the meaning and ambit of section 2(1)(u), and that their conversion into or through crypto is precisely the "process or activity" of concealment and layering that section 3 targets; the point at which crypto meets fiat on an exchange is the tainted transaction the Act reaches.

In defence it may be argued that the offence of money-laundering in the above context has no independent existence. Since it is dependent on a scheduled predicate offence there must be *'property'* derived from criminal activity relating to a scheduled offence, and the prosecution must establish that link. Where there is no scheduled offence, or where the accused is discharged or acquitted of it, the PMLA case cannot survive. A generalised assertion that crypto is "anonymous" or "untraceable" is not a substitute for tracing and the

to file a status report; the Court's observation that it could not direct an investigation given the unregulated status of crypto. The Supreme Court declined a related users' writ petition in April 2025.

[25] Scheme of arrangement sanctioned by the Singapore High Court (October 2025) under the Insolvency, Restructuring and Dissolution Act 2018, following an initial rejection and a re-vote; distribution routed through an India-based FIU-registered entity. See Part 5 on the cross-border-insolvency gap and India's partial adoption of the UNCITRAL Model Law.

burden is on the agency to identify the specific tainted property and connect it to the specific predicate.

(b) "The exchange or service provider is a facilitator and is knowingly party to the laundering."

The ED contends that a VASP which onboarded the accused (or is an accued), executed the conversions, or held the assets, participated in the process connected with proceeds of crime, and that as a reporting entity it is fixed with heightened responsibility.

In defence it may be argued that, Section 3 requires knowledge or involvement, not the mere provision of a regulated service. A compliant VASP that performed KYC, filed suspicious-transaction reports where indicated and maintained records has, if anything, discharged precisely the statutory function the AML regime imposes. Therefore, treating compliance as complicity inverts the scheme.

The reporting-entity obligations are supervisory and carry their own graded penalties under the PMLA Rules and are, therefore, not a conduit for converting a service provider into a launderer absent proof of the requisite *mens rea*. The correct question is whether this provider knowingly assisted this laundering which is a fact to be proved and not presumed from the nature of the business.

(c) "Provisional attachment is justified to prevent dissipation."

The ED contends that under section 5 it may attach property it has reason to believe are proceeds of crime and are likely to be dealt with in a manner that would frustrate confiscation. That the volatility and transferability of crypto make dissipation acute, warranting swift attachment of wallets, keys and linked bank balances.

In defence it may be argued that attachment is a preventive, civil measure — not punishment — and is hedged with safeguards that must be enforced. The "reason to believe" must be recorded in writing and must rest on material in possession, not suspicion. The attachment is provisional and must be placed before, and confirmed by, an independent Adjudicating Authority under section 8, at which the affected person is entitled to be heard. Two further defences are of particular value to operating businesses. First, proportionality and the avoidance of "civil death." Courts have accepted a doctrine of substitution, permitting attached assets to be released against unencumbered property of equivalent value (including a bank guarantee), so that securing the State's interest does not needlessly destroy a going concern. Second, valuation. Crypto's price volatility makes the *quantum* of any *"value equivalent"* attachment genuinely contestable, and over-attachment measured at a peak price is challengeable.

(d) "The ED has jurisdiction even where the underlying fraud occurred abroad."

The ED contends that where proceeds have entered India, money-laundering is deemed committed in India, and its extraterritorial reach exercised through mutual legal assistance extends to conduct and accounts connected to foreign predicate offences.

In defence it may be argued that the reach is real but bounded. As *Adnan Nisar* holds, the ED must still anchor its case to a corresponding scheduled offence under Indian law and it cannot investigate a foreign predicate in the abstract. Where an attachment or investigation is founded on a mutual-legal-assistance request confined to freezing specified accounts, the agency cannot bootstrap that limited mandate into a free-standing domestic investigation of conduct abroad without the domestic scheduled-offence foundation. The scope of the request, and the presence of a genuine Indian scheduled offence, are both contestable.

(e) "Moving crypto across borders outside the banking channel violates FEMA."

The ED contends that transmitting stablecoins to a foreign counterparty, or sourcing crypto from abroad without routing value through an authorised dealer, is an unauthorised dealing in or transfer of value across the border under section 3 of FEMA — economically indistinguishable from an informal money-transfer (hawala) arrangement.

In defence it may be argued that it is internally inconsistent. FEMA regulates *foreign exchange*, and a VDA is neither a currency nor a foreign currency, and therefore cannot be equated as foreign exchange within FEMA's own definitions. Moreover, the RBI itself has confirmed it does not classify crypto as currency. Moreover, the Government cannot hold three incompatible positions at once i.e. taxing crypto as an asset under the Income-tax Act, denying that it is currency in court, and prosecuting its cross-border movement as though it were money under FEMA**.** If crypto is property rather than currency, its cross-border transfer is not a foreign-exchange transaction at all. At most it engages the treatment of cross-border dealings in an asset.. Even where a FEMA contravention is made out, the consequences are civil, penalty-based, and compoundable under section 15.

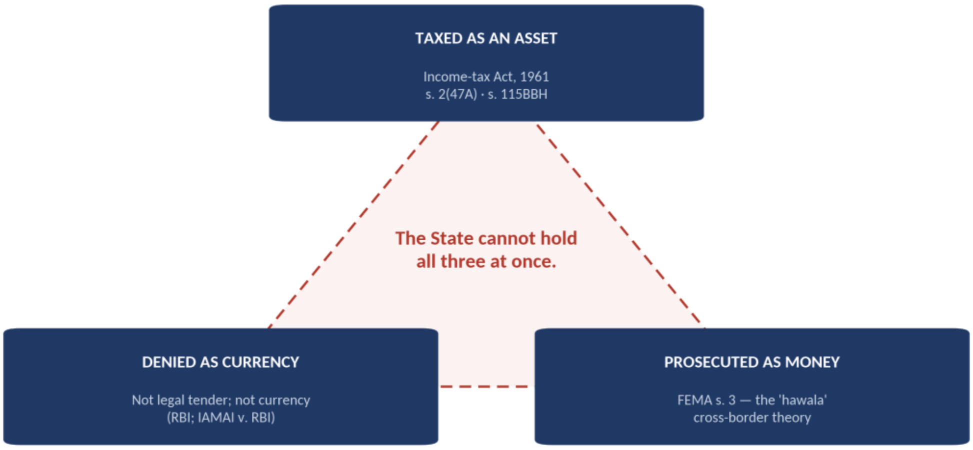

Figure 5 — The three inconsistent positions.

(f) "The on-chain record proves the flow of funds."

The ED contends that blockchain analytics establish the movement of the tainted assets from wallet to wallet, and that the immutable ledger is self-proving.

In defence it may be argued that on-chain data is powerful intelligence but must still be proved as evidence, and Indian evidence law makes that non-trivial. Electronic records must satisfy the admissibility conditions and the certification requirement now in section 63 of the Bharatiya Sakshya Adhiniyam, 2023 a requirement that fits public-blockchain data awkwardly. Beyond admissibility, blockchain analytics establish movement between *addresses*. Attributing an address to a *person* is an inferential step that exchange KYC support but do not conclusively prove, and is contestable.

(g) Bail and the section 45 twin conditions

Because PMLA offences are treated as cognizable and non-bailable, and because section 45 requires the court to be satisfied that there are reasonable grounds to believe the accused is not guilty and is not likely to offend on bail, custody is a central battleground. The rigour of section 45 has, however, been tempered by a developing Supreme Court jurisprudence that treats prolonged incarceration without trial as itself engaging the liberty guarantee in Article 21 — so that where trial is unlikely to conclude in a reasonable time, the constitutional right to a speedy trial can override the statutory fetter. The delay-based bail argument, coupled with challenges to the *necessity* of arrest under the section 19 standard, should be built into the defence from the outset.[26]

2.7 Blockchain and section 63 BSA conundrum

The shift from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 (in force from 1 July 2024) carried forward, rather than resolved, the core problem of authenticating electronic evidence — and created a genuine puzzle for on-chain records. The old section 65B is now section 63. Electronic and digital records are expressly admissible and are placed on par with documentary evidence, and, under sections 57 and 61, are capable of being treated as primary evidence rather than mere secondary copies.[27]

The friction lies in section 63(4). Admissibility of an electronic record turns on a certificate that identifies the record and the device, addresses the conditions of reliable operation, and — a significant change — is signed both by the person in charge of the device or the management of the relevant activities *and* by an expert, in the mandatory Schedule form (including hash values). The certificate lineage runs through *Anvar P.V. v. P.K. Basheer* (mandatory certificate), the short-lived relaxation in *Shafhi Mohammad*, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, which restored the mandatory rule while recognising an "impossibility exception" where a party genuinely cannot procure the certificate.[28]

2.7.1 Why public-blockchain evidence does not fit

The certificate presupposes a "person in charge" of the device or activity who can attest to the record's creation and the integrity of the system. A public, permissionless blockchain has, by design, **no such person**. There is no operator of Bitcoin or Ethereum to sign a section 63(4) certificate. The structural mismatch produces two unsatisfactory outcomes — either highly reliable ledger evidence is excluded on a technicality, or courts bypass the plain text through the impossibility exception on an ad hoc basis. A principled reform, advanced in

[26]On the interaction of s. 45 with Article 21 and the developing "bail where trial is delayed" line, see the Supreme Court's decisions tempering the twin conditions in cases of prolonged pre-trial detention; on the necessity and recording requirements for arrest, see the Court's decisions refining the s. 19 standard.

[27]Bharatiya Sakshya Adhiniyam, 2023, ss. 2(1)(d), 57, 61 and 63; the Indian Evidence Act, 1872 stands repealed, subject to savings for pending proceedings. Section 63 broadly reproduces the scheme of the former s. 65B while extending it to communication devices and refining the certificate.

[28]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

academic commentary, would differentiate public from private chains and treat public-chain records as capable of **expert self-authentication**. A certificate from a qualified blockchain expert attesting to the hash, the consensus mechanism and the timestamp, and confirming non-tampering would therefore satisfy the *evidentiary objective* of section 63(4) even though it cannot satisfy its literal "person-in-charge" form.[29]

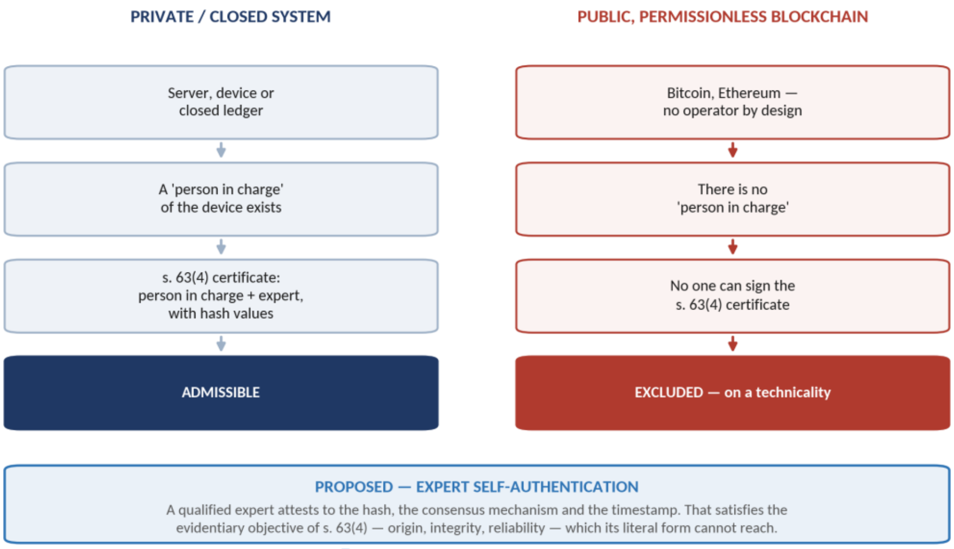

Figure 6 — Why section 63(4) BSA does not fit public-chain evidence.

2.7.2 Capacity, TAR, and AI-generated documents

Three related gaps compound the problem. First, capacity: the dual-certificate model presumes ready access to qualified experts and functioning forensic infrastructure. An assumption that strains against the documented shortage of forensic-science-laboratory personnel and facilities. Second, technology-assisted review and e-discovery: Indian procedure has developed no settled jurisprudence on predictive coding or technology-assisted review to enable proportionate handling of large electronic datasets. As a result, on-chain and exchange-records disputes proceeds without guidance, defaulting to manual review that neither scales nor produces defensible protocols. Third, AI-generated and AI-assisted documents: the authentication framework was built for records produced by deterministic systems, and it has no vocabulary for probabilistic, model-generated outputs whose provenance, integrity and "reliable operation" cannot be certified in the terms section 63 contemplates. As generative systems enter transactional and evidentiary workflows, the

[29]On the incompatibility of s. 63(4) with the decentralised architecture of public blockchains, and the proposal to treat public-chain records as expert-self-authenticating, see academic commentary including the Indian Journal of Law and Technology (NLS) analysis (2025).

certification regime will need a distinct standard for machine-authored material. It may be noted that its absence is a latent risk in any matter where such documents are tendered.

2.8 A reform blueprint

India's problem is not that it has chosen a light-touch model. It is that it has chosen *no* model. Taxing and policing without regulating maximises friction and enforcement risk while minimising legal certainty and consumer protection. The following agenda, drawn from international standard-setting (the FATF, FSB and IMF) and from India's own better instincts (the IFSCA sandbox), would move the country from stasis to a coherent regime.

a) **Enact a dedicated VDA statute with a functional taxonomy.** Legislate a purpose-built framework that classifies tokens by economic function such as payment tokens, utility tokens, security-like tokens and asset-referenced/stablecoin tokens. This is the precondition for everything else.

b) **Designate a regulator (or a coherent multi-regulator allocation), with an SRO in the interim.** Assign clear jurisdiction plausibly SEBI for security-like tokens, the RBI for systemic and payment-token risk, and the FIU-IND retaining AML and, until the statutory architecture is built, empower a self-regulatory organisation to set and enforce market-conduct, custody and proof-of-reserve standards.

c) **Introduce a VASP licensing and conduct regime.** Require licensing or registration of exchanges, custodians, brokers and wallet providers against governance, capital, cybersecurity, audit, client-asset-segregation and disclosure standards replacing the current position, in which the only formal gate is FIU-IND registration designed for AML rather than prudential or conduct purposes.

d) **Rationalise the tax regime.** De-link taxation from de facto criminalisation. Permit set-off and carry-forward of losses on the same footing as other assets, revisit the flat 30% rate, and recalibrate the 1% TDS, whose principal effect has been to drive volume offshore and onto non-compliant platforms which is diametrically opposite of the traceability it was meant to serve.

e) **Resolve the FEMA classification and provide a safe harbour.** The RBI and the Government should settle, by regulation, the status of VDAs under exchange-control law, and provide a clear, compliant channel for legitimate cross-border VDA activity ending the present grey zone in which ordinary commercial flows are exposed to a hawala characterisation and banks decline to process bona fide remittances.

f) **Build proportionality and a compliance safe harbour into PMLA enforcement.** A VASP that has met its KYC, reporting, and record-keeping obligations should enjoy a defined safe harbour against being treated as a co-launderer.

g) **Modernise the evidence framework for on-chain and AI-generated records.** Amend or supplement section 63 BSA to provide an expert-self-authentication route for public-blockchain records, invest in forensic capacity, develop court guidance on technology-assisted review and e-discovery, and create a distinct standard for machine-authored documents.

h) **Fully adopt the UNCITRAL Model Law on Cross-Border Insolvency.** The WazirX experience shows Indian users at the mercy of a foreign restructuring with no coordinated domestic seat at the table. Enacting the long-pending cross-border-insolvency framework would give Indian creditors recognition, cooperation, and standing in exactly the multi-jurisdictional failures this asset class produces.

i) **Mandate investor protection, custody and proof-of-reserves standards, and scale the IFSCA sandbox.** Require segregation and independent custody of client assets, regular proof-of-reserves, and standardised risk disclosures; and extend the risk-calibrated, sandbox-based experimentation already working at GIFT City into a national template for responsible innovation.

India already has the two hardest pieces of a mature regime — a tax hook and an AML hook. What it lacks is the connective statute that turns enforcement into regulation. Supplying that statute, with a functional taxonomy and a designated regulator, would convert a punitive, uncertain and offshore-driving status quo into a framework that is both safer for users and more competitive for the businesses and revenue India is currently exporting to Dubai and Singapore.

3. UNITED ARAB EMIRATES: THE LICENCE-LED, MULTI-REGULATOR MODEL

Where India polices an unregulated market, the UAE regulates an increasingly institutional one. It has become a primary destination for the businesses India exports, and it offers not one regime but several. Arranged in layers are federal, Emirate-level, and financial free zone. The UAE's defining feature is that structuring, not permission-seeking, is the core task. The question is rarely whether one can build in the UAE, but which regulator to build under.

3.1 The architecture : federal, Emirate and free zone

Digital-asset activity in the UAE is governed by a matrix of authorities. At federal level, the Securities and Commodities Authority (SCA) is the financial-services regulator for securities, commodities and virtual-asset service providers across the Emirates (other than in the financial free zones), pursuant to Cabinet Decision No. 111 of 2021 on the regulation of virtual assets. The Central Bank of the UAE (CBUAE) regulates payment tokens (fiat-referenced stablecoins) and stored-value facilities. At Emirate level, Dubai's Virtual Assets Regulatory Authority (VARA) supervises virtual-asset activity in Dubai other than in the DIFC. Within the two financial free zones, the Financial Services Regulatory Authority (FSRA) of the Abu Dhabi Global Market (ADGM) and the Dubai Financial Services Authority (DFSA) of the Dubai International Financial Centre (DIFC) each operate under comprehensive common-law-based regimes. A newer entrant, RAK DAO in Ras Al Khaimah, targets Web3 start-ups and token projects.[30]

[30]Cabinet Decision No. 111 of 2021 on the Regulation of Virtual Assets and their Service Providers (federal SCA regime). VASPs intending to operate in Emirates other than Dubai license directly with the SCA; the DIFC and the ADGM operate independently of the SCA/VARA arrangement under their own frameworks.

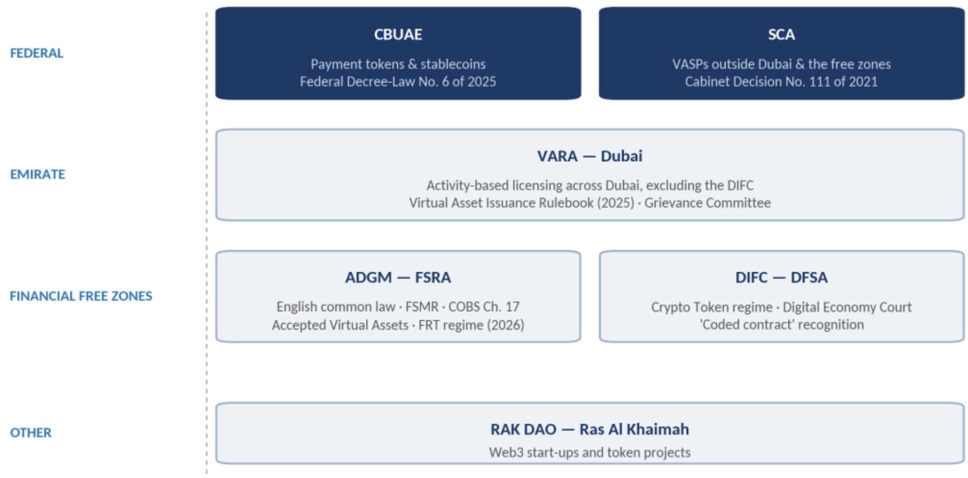

Figure 7 — The UAE's layered regulatory architecture.

3.2 Federal Decree-Law No. 6 of 2025 and the end of the "just code" defence

The most consequential recent development is Federal Decree-Law No. 6 of 2025 (the new Central Bank law), which extends CBUAE licensing to crypto activities carried on through any means, medium or technology, and thereby brings decentralised exchanges, cross-chain bridges, stablecoins and Web3 infrastructure within the Central Bank's direct oversight. In doing so it forecloses the argument that a protocol which is "just code" sits beyond regulation. The regime carries substantial administrative penalties (reported to reach up to AED 1 billion) and criminal sanctions for unlicensed activity, with a transitional runway for existing operators to license, partner with a licensed entity, or cease UAE-facing operations.[31]

3.3 The regulators in detail

3.3.1 VARA (Dubai)

VARA, established in 2022, administers a bespoke, activity-based licensing regime for virtual-asset services in Dubai including advisory, broker-dealer, custody, exchange, lending, and management services under a suite of rulebooks that set governance, technology, market-conduct and AML standards. Its Virtual Asset Issuance Rulebook (effective 19 June 2025) fixed the approval and disclosure mechanics for token issuers and

[31]Federal Decree-Law No. 6 of 2025; Articles 61–62 require CBUAE licensing for crypto activities conducted "through any means, medium, or technology," with a transitional period reported to run to September 2026 and penalties reported to reach AED 1 billion in addition to criminal sanctions for unlicensed activity.

specified the treatment of fiat-referenced and asset-referenced virtual assets as Category 1 issuances, triggering full activity obligations, whitepaper and risk-disclosure duties and, for fiat-referenced tokens, reserve requirements. A Grievance Committee provides a route to challenge VARA enforcement action.[32]

3.3.2 ADGM / FSRA (Abu Dhabi)

The ADGM was the first jurisdiction in the world to introduce a comprehensive, bespoke framework for virtual-asset activity (2018), operating under English-common-law foundations and the Financial Services and Markets Regulations. VASPs are licensed as Authorised Persons and must comply with the product-specific rules for virtual-asset activity in the Conduct of Business Rulebook, alongside a curated list of "Accepted Virtual Assets." The FSRA has continued to refine the regime, expanding its treatment of fiat-referenced tokens (with a broadened framework taking effect on 1 January 2026), and expressly prohibits privacy-enhancing tokens and algorithmic stablecoins. The ADGM's institutional credibility is reflected in the licensing of major global exchanges and stablecoin issuers within its perimeter.[33]

3.3.3 DIFC / DFSA (Dubai)

The DFSA operates a Crypto Token regime within the DIFC's common-law environment, recognising specified tokens for use in financial services following an economic-substance assessment, and has recognised leading fiat-referenced tokens. Two features are of particular interest to transactional counsel. First, the DIFC Courts have established a dedicated Digital Economy Court to hear technology and digital-asset disputes. Second — and directly relevant to smart-contract practice — DIFC contract law has introduced the concept of a "coded contract," giving legal recognition to agreements that exist and execute in software, a rare example of a real-world legal framework built for on-chain automation.[34]

---

[32]VARA rulebooks (2023, updated 2025), including the Virtual Asset Issuance Rulebook effective 19 June 2025; VARA's Grievance Committee (established June 2023) hears appeals against enforcement action. AED-referenced payment tokens are deferred to the CBUAE regime.

[33]ADGM FSRA framework (2018), Financial Services and Markets Regulations; Conduct of Business Rulebook, Chapter 17 (virtual-asset regulated activities); expanded fiat-referenced-token regime effective 1 January 2026; prohibition on privacy tokens and algorithmic stablecoins. Circle (USDC) obtained FSRA money-services permission and a major global exchange secured an ADGM licence.

[34]DFSA Crypto Token regime; recognition of specified crypto tokens (including USDC and EURC, and Ripple's RLUSD) for use within the DIFC; the DIFC Courts' Digital Economy Court; and the "coded contract" concept in DIFC contract law recognising software-executed agreements.

3.4 Stablecoins and payment tokens

Stablecoins have moved from a peripheral crypto instrument to regulated payment infrastructure. The CBUAE's Payment Token Services Regulation centralises the regulation of fiat-referenced payment tokens, licensing dirham-payment-token issuers, custodians/transferors and conversion providers; the transition period has ended, so mainland payment-token services must now be licensed. Fiat-referenced tokens must be fully backed (1:1) and held in segregated reserves, with par-value redemption; and across all UAE regimes, algorithmic stablecoins and privacy tokens are prohibited. The market has responded with regulated AED- and USD-backed tokens issued under CBUAE, ADGM and DIFC oversight.[35]

3.5 Tax

The UAE's tax position is a principal driver of the migration this guide describes. There is no personal income tax and no capital-gains tax on individuals. Corporate tax applies at 9% only on profits exceeding AED 375,000, and the Federal Tax Authority has clarified that transfers of virtual assets are exempt from VAT, with retrospective effect. For a business relocating from India's 30%-plus regime, the contrast is stark and is precisely why the exchange-control and round-tripping analysis in Part 5 matters so much.[36]

[35] CBUAE Payment Token Services Regulation (PTSR): licences for Dirham Payment Token Issuer, Payment Token Custodian and Transferor, and Payment Token Conversion; transition ended in 2025. Approved tokens include AED-backed and USD-backed stablecoins recognised under the CBUAE, ADGM and DIFC frameworks.

[36] UAE: no personal income tax or capital-gains tax on individuals; federal corporate tax of 9% on profits above AED 375,000; Federal Tax Authority clarification (2024) that virtual-asset transfers are VAT-exempt, effective retrospectively from 1 January 2018.

4. SINGAPORE: THE ACTIVITY-BASED REGIME

Singapore is the corridor's most institutionally settled jurisdiction. Its regulator, the Monetary Authority of Singapore (MAS), has for years pursued an explicit policy of an “innovative and responsible” digital-asset ecosystem welcoming activity that submits to supervision while progressively closing the arrangements it cannot supervise. The result is a regime that is more predictable than India's and more consolidated than the UAE's, but no longer the light-touch haven of popular imagination. Further, the year 2025 saw Singapore decisively tighten its perimeter.

4.1 Regulatory philosophy and token taxonomy

MAS regulates by economic function, not by label. It looks past what a token is called to the features it bears and the rights it confers, and sorts tokens into functional categories, each mapped to a statute:

- **Digital payment tokens (DPTs)** — a digital representation of value that is not pegged to any fiat currency (for example, Bitcoin or Ether). DPT services are regulated under the Payment Services Act 2019.
- **E-money** — a token pegged to a fiat currency, which captures most stablecoins; also regulated under the Payment Services Act.
- **Capital-markets tokens** — tokens representing ownership, equity, debt or units in a collective investment scheme, regulated as capital-markets products under the Securities and Futures Act 2001 (with advice on them caught by the Financial Advisers Act 2001).
- **Utility and governance tokens** — tokens used purely for access or governance fall outside the licensing regimes.

Cryptocurrencies are not treated as legal tender or the equivalent of money in Singapore; the regulatory interest is in the *service* provided around tokens, not in conferring monetary status on the tokens themselves.[37]

[37] MAS assesses tokens by their features and the rights of holders rather than their designation; the applicable statute (Payment Services Act 2019, Securities and Futures Act 2001, or Financial Advisers Act 2001) depends on that functional classification.

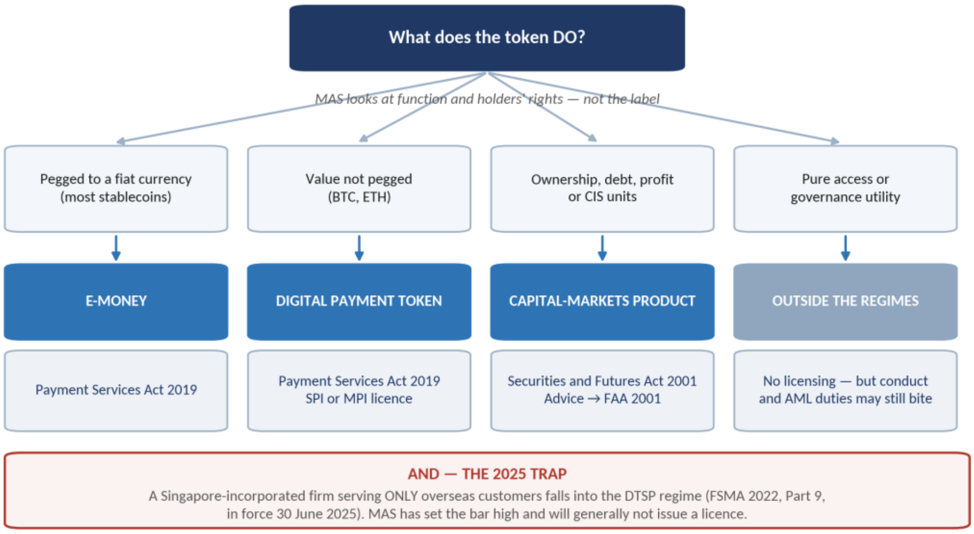

Figure 8 — Singapore — token function determines the statute.

4.2 The Payment Services Act 2019

The Payment Services Act (PSA) is the backbone of DPT regulation. A person carrying on a business of providing a payment service — including a DPT service — must be licensed, in one of two principal tiers: a Standard Payment Institution, subject to lower capital requirements but with caps on transaction volume and float; or a Major Payment Institution, which carries no such caps but attracts higher capital and more demanding prudential and conduct obligations. The Payment Services (Amendment) Act 2021 broadened the scope of regulated DPT activity to align Singapore with the Financial Action Task Force's standards, extending the regime to a wider set of dealing, transfer, custody and facilitation services.[38]

4.3 The DTSP regime under the Financial Services and Markets Act 2022

The most important recent development — and the one most likely to surprise those who still think of Singapore as an easy offshore base — is the digital-token-service-provider (DTSP) regime under Part 9 of the Financial Services and Markets Act 2022, which came into operation on 30 June 2025. The regime targets a specific gap: persons who are incorporated in Singapore, or operate from a place of business in Singapore, but provide digital-token services *solely to customers outside Singapore* — firms that had used a Singapore footprint

[38] Payment Services Act 2019; Payment Services (Amendment) Act 2021 (expanding the scope of DPT services in line with FATF standards). The two licensing tiers are the Standard Payment Institution and the Major Payment Institution.

for reputational benefit while conducting their substantive regulated activity, and generating their money-laundering risk, elsewhere.[39]

MAS's posture is deliberately severe. It has stated that it has “set the bar high” and will “generally not issue a licence,” because it cannot effectively supervise a business whose substantive activity is entirely offshore; there is no transitional period; and existing providers of this kind were required to cease the activity when the regime commenced. Commentators have accordingly read the regime as, in effect, a prohibition on the Singapore-incorporated-but-outbound-only model rather than a conventional licensing gateway. The base-capital floor is S$250,000, and unlicensed provision carries penalties of up to S$250,000 and/or up to three years' imprisonment.[40]

Importantly, the DTSP regime does not create new categories of regulated product; it extends the *territorial* reach of existing regulation. Providers already licensed under the PSA, SFA or FAA for the relevant service, and serving Singapore customers, are generally unaffected for those activities — they may continue to serve overseas customers as well. The regime bites on the narrow but reputationally important class of outbound-only operators.

4.4 Stablecoins and the single-currency framework

MAS finalised the features of its stablecoin regulatory framework in August 2023. The framework applies to single-currency stablecoins pegged to the Singapore dollar or to any G10 currency and issued in Singapore, and imposes requirements on reserve composition and management, capital, and redemption at par value, together with disclosure obligations. Stablecoins meeting the standard may be represented as “MAS-regulated,” a label intended to distinguish genuinely value-stable instruments from the broader field. The framework

[39]Financial Services and Markets Act 2022, Part 9; Financial Services and Markets (Digital Token Service Providers) Regulations 2025 (S 342/2025); MAS Notice FSM-N27 (AML/CFT) and accompanying Guidelines, all in operation from 30 June 2025.

[40]MAS media release and clarification of 30 May and 6 June 2025 (“set the bar high,” “generally not issue a licence,” no transitional arrangement); base capital of S$250,000; penalties up to S$250,000 and/or three years' imprisonment. The DTSP regime chiefly expands the territorial reach of existing regulation rather than creating new regulated product types; existing PSA/SFA/FAA licensees are generally unaffected for the activities already licensed.

sits alongside MAS's broader “Orchid Blueprint” (November 2023) for the infrastructure of digital money.[41]

4.5 Custody and consumer protection

Following the market failures of 2022, MAS introduced pointed retail-protection measures for DPT service providers. Licensed firms must segregate customers' assets from their own and hold them on trust, conduct daily reconciliations, maintain separate blockchain addresses for customer and firm assets, and keep custody functions operationally independent — the very controls whose absence (opacity of ownership, commingling, and the lack of verifiable proof of reserves) turned the WazirX hack into a users' catastrophe. Robust cybersecurity and technology-risk management are ongoing licensing conditions.[42]

[41] MAS stablecoin regulatory framework announced 15 August 2023 (single-currency stablecoins pegged to the Singapore dollar or a G10 currency and issued in Singapore; reserve, capital, and par-value-redemption requirements; the “MAS-regulated stablecoin” label). MAS “Orchid Blueprint,” 16 November 2023.

[42] MAS measures for DPT service providers (in force progressively from 2023–24): segregation of customer assets, holding on trust, daily reconciliation, separate blockchain addresses for customer and firm assets, and operational independence of custody, together with technology-risk-management and cybersecurity obligations.

5. CROSS-BORDER STRUCTURING FOR INDIAN-ORIGIN BUSINESSES

The three preceding Parts describe three very different bargains. Taken together, they explain a single dominant pattern: the migration of Indian crypto talent and capital to Dubai and Singapore. This Part addresses that pattern directly — why it happens, the Indian-law exposure it creates (which is frequently underappreciated), and how to think about venue selection and the failure scenarios that make or break a structure.

5.1 The migration pattern and why it is not a clean exit

The pull factors are obvious: a functioning licensing regime, institutional banking, common-law certainty (in the UAE free zones and Singapore), and — decisively — the absence of India's 30% tax, 1% TDS and loss-set-off bar. The push factors are the enforcement-first climate described in Part 2. But relocation is rarely the clean exit founders assume. Indian users often remain the customer base and the act of moving value and ownership offshore engages the very exchange-control regime the ED has begun to enforce against the sector.

Three Indian-law constraints deserve particular attention:

j) **Overseas investment rules.** Establishing or capitalising a foreign holding company engages the overseas-investment framework under FEMA (the ODI/OPI regime). Structuring a VDA business abroad while resident in India, or contributing Indian-earned value to it, must be mapped against these rules. Informal or undocumented transfers of value offshore are exactly what the ED's FEMA theory targets.[43]

k) **The Liberalised Remittance Scheme.** Individuals remitting funds abroad rely on the LRS, but banks have become markedly conservative about remittances connected to crypto, and using the LRS to acquire VDAs offshore sits at a contested space. The mismatch between what is nominally permitted and what banks will actually process is itself a planning problem.

l) **Round-tripping and the loop back to the ED.** The most dangerous structure is the one that moves value offshore and then routes it back into India — "round-tripping" —

[43]Foreign Exchange Management (Overseas Investment) Rules and Regulations, 2022, and related RBI directions govern outbound investment by Indian residents; VDA-related structures must be assessed against the permissibility, reporting and valuation requirements of that regime.

because it collapses the supposed separation between the offshore entity and the Indian activity, and hands the ED both a FEMA theory (unauthorised cross-border value transfer) and, if any predicate is alleged, a PMLA layering narrative. A structure that cannot withstand the question "where did the value come from, and where did it go?" is not a structure worth having.

5.2 Issuance and licensing

Venue selection turns on the business model. For token issuance, the questions are how the token classifies functionally (payment, utility, security-like or asset-referenced), which regime offers a workable path for that class, and what is prohibited outright — algorithmic stablecoins and privacy tokens are barred across the UAE, and a security-like token will attract securities regulation in each jurisdiction. For a VASP or exchange licence, the trade-off is between the UAE's institutional, common-law free-zone regimes (ADGM, DIFC) or Dubai's activity-based VARA, and Singapore's mature but now-restrictive PSA/DTSP framework.

5.3 The failure scenario

Nothing tests a cross-border structure like its failure, and the unfortunate WazirX collapse (Part 2.5.5) is the corridor's defining lesson. An Indian-facing exchange with a Singapore-domiciled parent suffered a catastrophic hack. The recovery was fought as a scheme of arrangement under Singapore insolvency law and Indian users found that the forum determining their fate was a foreign court applying a foreign statute, while Indian authorities — absent a regulatory framework — could issue notices but not direct an investigation. The restructuring was even reworked to route distribution through an India-registered entity, an implicit acknowledgment that the Indian nexus could not simply be wished away.

Domicile determines the insolvency forum, and therefore which creditors have a coordinated voice. Custody arrangements (independent custodian, segregation, multi-signature discipline, proof of reserves) determine whether user assets survive an operational failure. The *absence* of an Indian cross-border-insolvency framework means Indian creditors cannot readily obtain recognition and cooperation in the foreign proceeding.

5.4 Comparative matrix

The following distils the three regimes across the dimensions that most often drive structuring decisions, including the tax treatment discussed across Parts 2, 3 and 4. It is a starting point for analysis, not a substitute for jurisdiction-specific advice.

Dimension	India	UAE	Singapore
Dedicated VDA statute	None; VDAs defined only in tax law	Yes; federal + Emirate + free-zone regimes	No single statute, but mature activity-based regulation
Primary regulator(s)	No designated regulator; FIU-IND for AML; ED enforces	CBUAE, SCA, VARA, ADGM-FSRA, DIFC-DFSA	MAS (single regulator)
Licensing of VASPs	FIU-IND registration only (AML-focused)	Activity-based licensing across regulators	PSA licensing (SPI/MPI); DTSP regime for outbound-only
Legal status of crypto	Not legal tender; legal to hold/trade	Regulated virtual assets; not legal tender	Not legal tender; regulated by service/function
Stablecoins	No framework; treated as VDAs	CBUAE payment tokens; algorithmic banned	Single-currency stablecoin framework (SGD/G10)
Enforcement climate	Aggressive; PMLA + FEMA fronts	Licence-led; growing enforcement	Firm but predictable; perimeter tightened 2025
Best suited to	Compliance-heavy domestic operations	Institutional and retail builders seeking certainty	Institutional, regionally-facing, licensed models
Tax — gains on transfer	Flat 30% (s. 115BBH), plus surcharge and cess; no deduction other than cost of acquisition	No personal income tax and no capital-gains tax on individuals	No capital-gains tax; trading gains fall to be assessed on general income-tax principles
Tax — withholding at source	1% TDS on the consideration for transfer (s. 194S)	None	None
Tax — loss set-off	Not permitted — losses cannot be set off against any head, nor carried forward	Not applicable	Ordinary principles apply to trading losses
Tax — corporate	Ordinary corporate rates	9% on profits above AED 375,000	Headline corporate rate
Tax — indirect	GST applies to exchange and intermediary services	Virtual-asset transfers exempt from VAT, with retrospective effect from 1 January 2018	Supplies of digital payment tokens are treated as exempt

Dimension	India	UAE	Singapore
Tax — offshore holdings	Reportable in Schedule FA; Black Money Act, 2015 exposure for non-disclosure	—	—

5.5 Penalty exposure at a glance

The exposures below are drawn from the regimes analysed in this guide. Note the structural point that recurs throughout Part 2: India's two principal exposures are of an entirely different character — the PMLA is penal, while FEMA is civil and compoundable.

Regime	What triggers it	Exposure
India — PMLA, 2002	Property derived from a scheduled predicate offence, and any process connected with it	Rigorous imprisonment of 3–7 years (up to 10); provisional attachment (s. 5); reverse burden (s. 24); twin bail conditions (s. 45)
India — FEMA, 1999	Unauthorised cross-border dealing or transfer of value outside the banking channel	Civil: penalty up to three times the sum involved (s. 13) — and compoundable under s. 15
India — PMLA Rules	Reporting-entity failure by a VASP (KYC, STR, records)	Not less than ₹10,000 and up to ₹1,00,000 for each failure
India — tax	Non-reporting of VDA income; undisclosed foreign holdings	Penalty and prosecution; Black Money Act, 2015 for foreign VDAs not disclosed in Schedule FA
UAE — Federal Decree-Law No. 6 of 2025	Crypto activity carried on without a licence, through any means, medium or technology	Administrative penalties reported to reach AED 1 billion, alongside criminal sanctions
UAE — VARA / FSRA / DFSA	Breach of licence conditions or of the applicable rulebook	Regulatory enforcement and licence action; VARA decisions are appealable to its Grievance Committee
Singapore — FSMA 2022, Part 9	Providing digital-token services from Singapore solely to customers outside Singapore	Fine up to S$250,000 and/or up to 3 years' imprisonment; MAS has set the bar high and will generally not licence
Singapore — PSA 2019	Carrying on a DPT service without an SPI or MPI licence	Licensing offence; MAS directions, conditions and enforcement action

6. CONCLUSION AND OUTLOOK

The three jurisdictions surveyed here are converging on a shared recognition — that virtual digital assets are a permanent feature of the financial landscape and must be governed — while diverging sharply on method. The UAE competes for the industry through a licence-led, multi-regulator architecture and a favourable tax base. Singapore hosts it on strict, activity-based terms, welcoming what it can supervise and closing what it cannot. India, alone of the three, has chosen, so far, not to choose. It taxes and polices without regulating, producing a climate in which enforcement, not licensing, is the final say.

That equilibrium is unlikely to hold. Global standard-setting, the pull of a maturing market, the Supreme Court's own prodding and the sheer volume of enforcement activity all press toward a dedicated framework; its likely shape is set out in Part 2.8.

Three propositions are worth carrying away.

1. A tax hook and an anti-money-laundering hook are both in place. What is missing is the law that would turn enforcement into regulation. Almost everything else in the Indian chapter — the punitive rate, the FEMA grey zone, the evidentiary conundrum under section 63, and the steady export of founders to Dubai and Singapore — follows from that single omission.

2. There is no regulator to persuade and no licence to obtain; there is an agency to answer. Four moves recur, and they should be prepared before the first summons rather than improvised after the attachment: attack the predicate, attack identification and control, attack classification, and attack proportionality.

3. Domicile decides the insolvency forum. Custody decides whether user assets survive an operational breach. And the absence of a cross-border-insolvency framework in India decides who is left without a seat at the table. WazirX is not an aberration — it is the template for what a cross-border failure looks like in this corridor.

The law will catch up and it always does. The question this guide has tried to answer is the one that matters in the interval — where, precisely, it has not.

Annexure A — Key Statutes, Instruments and Authorities

A consolidated, non-exhaustive reference to the principal sources relied on in this guide. Citations should be verified against the primary sources as in force on the relevant date.

India

Source	Relevance
Income-tax Act, 1961, s. 2(47A)	Statutory definition of a virtual digital asset (Finance Act 2022; widened 2025)
Income-tax Act, 1961, ss. 115BBH, 194S	30% tax on transfer; 1% TDS; no loss set-off
CBDT Notification No. 75/2022	Carve-out of ownership-transfer NFTs
Black Money Act, 2015	Disclosure of foreign VDA holdings (Schedule FA)
MoF Notification dated 7 March 2023 (PMLA)	VDA service providers as reporting entities; five activities
Prevention of Money-Laundering Act, 2002	ss. 3, 5, 8, 17–19, 24, 45, 50 — the ED's PMLA toolkit
Foreign Exchange Management Act, 1999	ss. 2(h)/(m)/(n), 3, 13, 15, 37 — the FEMA overlay
Bharatiya Sakshya Adhiniyam, 2023, ss. 57, 61, 63	Admissibility and certification of electronic records
IAMAI v. RBI, (2020) 10 SCC 274	Striking down the 2018 banking ban on proportionality grounds
Vijay Madanlal Choudhary v. Union of India (2022)	PMLA scheme; scheduled-offence requirement; civil attachment
Adnan Nisar v. Directorate of Enforcement (Del HC, 2024)	Cross-border predicate; corresponding Indian scheduled offence required
Anvar P.V. (2014); Arjun Panditrao Khotkar (2020)	Mandatory electronic-evidence certificate; impossibility exception

UAE

Source	Relevance
Cabinet Decision No. 111 of 2021	Federal SCA regime for virtual assets and VASPs
Federal Decree-Law No. 6 of 2025	CBUAE oversight of on-chain activity; end of the “just code” defence
CBUAE Payment Token Services Regulation	Licensing of fiat-referenced payment tokens (stablecoins)
VARA rulebooks; Virtual Asset Issuance Rulebook (2025)	Dubai activity-based licensing; issuer disclosure; FRVA/ARVA
ADGM FSRA framework (2018); COBS Ch. 17	Common-law VASP regime; Accepted Virtual Assets; FRT regime (2026)

Source	Relevance
DIFC DFSA Crypto Token regime; "coded contract"	Recognised tokens; Digital Economy Court; smart-contract recognition

Singapore

Source	Relevance
Payment Services Act 2019; PS(A)A 2021	DPT licensing (SPI/MPI); FATF-aligned scope
Securities and Futures Act 2001; Financial Advisers Act 2001	Capital-markets tokens; advice on tokens
Financial Services and Markets Act 2022, Part 9	DTSP regime (30 June 2025) for outbound-only providers
FSM (DTSP) Regulations 2025; MAS Notice FSM-N27	DTSP licensing mechanics; AML/CFT for DTSPs
MAS stablecoin framework (Aug 2023)	Single-currency stablecoins; reserve/capital/redemption
MAS DPT retail-protection measures (2023–24)	Segregation, trust custody, reconciliation, separate addresses

Annexure B: Quick Reference

A litigator's summary of Part 2.6. This is a navigational aid; the reasoning and authorities are in the body.

The ED contends	The answer
The VDAs are proceeds of crime and liable to attachment	No scheduled predicate offence, no PMLA case; the agency must identify the specific tainted property and prove control — pseudonymity makes this a real burden
The exchange is a facilitator knowingly party to laundering	s. 3 requires knowledge/involvement; a compliant VASP that did KYC and filed STRs discharged the AML function — complicity must be proved, not presumed
Provisional attachment is justified to prevent dissipation	Attachment is preventive and civil, hedged by s. 8 safeguards; substitution avoids “civil death”; volatile valuation makes over-attachment contestable
The ED has jurisdiction over foreign frauds	Only with a corresponding Indian scheduled offence (Adnan Nisar); an MLA request to freeze accounts cannot be bootstrapped into a domestic investigation
Cross-border crypto movement violates FEMA (“hawala”)	Crypto is not currency/forex under FEMA; the State cannot tax it as an asset, deny it is currency, and prosecute it as money — and FEMA is civil and compoundable
The on-chain record proves the flow of funds	It must still be proved under s. 63 BSA (certification conundrum); address-to-person attribution is inferential and contestable; chain of custody matters
Custody is warranted; bail should be refused (s. 45)	s. 45's rigour yields to Article 21 where trial is delayed; challenge the necessity of arrest under the s. 19 standard

ABOUT THE AUTHOR

> *"The law is always catching up. The question is whether you are ahead of where the law is going, or behind where it already is."*
>
> — CHANDAN GOSWAMI, PARTNER

Chandan Goswami is a Partner at AT & Partners, where he leads the firm's technology law practice. He has more than a decade of experience advising companies, founders, institutions and private clients on legal matters arising at the intersection of technology and law — from the structuring of businesses and the drafting of AI deployment agreements, to the management of complex commercial disputes across technology, petroleum, FMCG and financial services.

His practice concentrates on the areas where the rate of technological change most consistently outpaces the development of legal frameworks. He has advised on the application of the Prevention of Money Laundering Act to virtual asset service providers, on the structuring of tokens, on hack response and digital-asset recovery, on various legal frameworks, on technology transfer agreements governing IP ownership and liability in semiconductors, and on private participation in India's space sector under the Indian Space Policy 2023 and the norms issued by IN-SPACe.

He writes on artificial intelligence, semiconductor policy, blockchain law and digital regulation, and has contributed to The Hindu, The Telegraph and Mint. He is the author of the AT & Partners Tech Law Guide for Startups, an annual practitioner's reference, available at www.atandpartners.in. Media and conference enquiries may be directed to office@atandpartners.in.