Cryptocurrency Fraud- Legal Challenges in India

Cryptocurrency fraud: what it is, how it works, and how India's experience differs from the global picture

Cryptocurrency fraud is an umbrella term for schemes that exploit the novelty, speed, and borderlessness of digital assets to deceive users and steal value. While the underlying blockchains are typically transparent and tamper-evident, the human touchpoints around them—advertising, chat apps, fake exchanges, high-pressure "investment clubs," and social-engineering pipelines—remain vulnerable. Globally, fraudsters recycle old confidence tricks with a crypto gloss (think Ponzi schemes and boiler rooms), while also inventing crypto-native ploys (rug pulls, "airdrop" bait, phishing that drains self-custody wallets). India's policy stance—cautious acceptance with stringent tax and anti-money-laundering (AML) controls—shapes both receptiveness to crypto and the operational realities of platforms and scammers in ways that are distinct from the U.S., EU, UK, or Singapore.

Below is a crisp tour through (1) what counts as crypto fraud and how it operates, (2) the global regulatory environment that conditions these crimes, and (3) how India's posture makes the Indian experience different in both receptiveness and operations.

1) What "cryptocurrency fraud" actually is

A working definition. Crypto fraud is any deceptive practice that uses cryptoassets or their infrastructure to misappropriate funds or sensitive data. It includes:

- **Investment scams** that promise high, steady returns in "exclusive" coins or trading bots, often dressed up as fake exchanges or MetaTrader screens. The fastest-growing variant worldwide is **"pig-butchering"**—long-con romance/investment scams that groom victims over weeks, then funnel them to bogus "platforms" where deposits are visible but withdrawals fail. Regulators and investigators flag pig-butchering as a major driver of losses today.
- **Rug pulls** and **exit scams**, where token/project insiders drain liquidity or abandon the codebase after hyping a launch. These are endemic in DeFi-flavored launches with anonymous teams.
- **Phishing and wallet-drainers,** which trick users into signing malicious transactions (often via fake airdrop sites or Discord/Twitter DMs) that grant token approvals or sweep assets.
- **Impersonation and giveaway grifts,** leveraging hijacked social media accounts or deepfakes to solicit deposits that can never be reclaimed.
- **Ransomware and sextortion** that demand crypto payments; while not "investment scams," they're intertwined with the same laundering infrastructure and have grown more sophisticated (including AI-aided targeting).

Why crypto is attractive to fraudsters. Three forces recur in casework and data: (i) *instant, final settlement* that is hard to unwind; (ii) *global reach* across chat apps and payment rails; and (iii) a *credibility gap* where novice users struggle to verify platforms or read smart-contract permissions.

Counterintuitively, the **public traceability** of most blockchains has helped analysts measure and disrupt these schemes; annual industry crime reports show both large losses and growing investigative wins as compliance matures.

2) The global rulebook that shapes fraud and enforcement

Because crypto crosses borders by design, the regulatory environment is a patchwork—but several anchors now guide national rules:

- The **FATF "Travel Rule" and R.15** extend AML/CFT standards to **virtual asset service providers (VASPs)** (exchanges, brokers, custodians). Countries are at uneven stages of implementation, and compliance gaps leave seams that scammers exploit.
- The **EU's MiCA** creates a comprehensive licensing regime for crypto-asset service providers across the EEA, phasing in from late-2024 into 2025, with explicit market-abuse, governance, and consumer-protection duties. The premise: tighten conduct rules, harmonize supervision, and reduce space for fly-by-night operators.
- The **UK** is moving toward a bespoke regime by folding crypto asset activities into the perimeter of regulated financial services, with draft legislation published in 2025 and stepped-up enforcement capacity at the FCA.
- **Singapore (MAS)**, a long-standing early mover, couples licensing with **retail guardrails**—including restrictions on lending/staking for retail customers—to limit speculative harm while keeping institutional rails robust.
- At the **G20 level**, the **IMF–FSB Synthesis Paper** (developed under India's 2023 presidency and endorsed by Leaders that September) lays out a global roadmap—push AML/CFT standards, curb regulatory arbitrage, and fortify consumer protection while avoiding outright bans that drive activity underground.

Operationally, tighter licensing and advertising standards in these hubs have forced scammers to **shift tactics**: (a) operate **offshore** or through **unlicensed copycat platforms**, (b) rely more on **OTC brokers, mules, and stablecoins** to move funds, and (c) push users to **self-hosted wallet drainer sites** rather than regulated exchanges. Crime analytics for 2024–25 reflect that scams adapt to compliance chokepoints, with social-engineering lures (pig-butchering) retaining high yield even as classic high-yield investment lures face more friction.

3) India: receptiveness and operations versus the global scenario

India's stance is distinctive: *crypto is not legal tender* and remains outside a dedicated securities law, yet it is **taxed and brought firmly into AML scope**, and advertising is **self-regulated** with strong risk disclaimers. This "cautious containment" approach shapes both **public receptiveness** and **how operations run**—for legitimate firms and fraudsters alike.

3.1 Receptiveness: policy signals and user behavior

- **No blanket ban; judicial guardrails.** In **March 2020**, India's Supreme Court (Internet and Mobile Association of India v. RBI) **struck down** the RBI's 2018 circular that had cut crypto

businesses off from banking, restoring access to payment rails even as policy remained unsettled. This was a turning point: crypto activity resumed, but under watchful eyes.

- **Cautious central-bank stance.** The RBI continues to warn that private crypto poses monetary and financial-stability risks and has, at times, argued for very tight curbs—even a ban—while the government has favored coordinated international regulation. These signals temper mainstream receptiveness even as retail interest persists.
- **Advertising and consumer messaging.** Since **April 2022**, all **VDA** (virtual digital asset) ads must carry **bold risk disclaimers** ("unregulated and highly risky; no regulatory recourse"), avoid certain terms (like "currency"), and hold celebrities to a due-diligence bar—nudging retail sentiment toward caution.

3.2 Operations: the rails crypto must run on in India

- **Tax as a behavioral lever.** From **April 1, 2022**, profits from **VDAs** are taxed at **30%** with **no loss set-off**; from **July 1, 2022**, **1% TDS** applies to most sell trades (Section 194S), which materially impacts liquidity and high-frequency trading behavior on compliant Indian venues. Debate continues on recalibrating TDS to curb offshoring.
- **AML perimeter.** In **March 2023**, India placed VASPs squarely under the **PMLA** and **FIU-IND** reporting regime; guidance followed the same month. Offshore, unregistered exchanges serving Indians have faced **show-cause notices, URL/app blocks**, and—upon seeking re-entry—**fines** and **mandatory FIU registration** (e.g., Binance's FIU registration in 2024 and subsequent penalty). The practical upshot: compliant on-ramps in India must do **KYC, suspicious-transaction reporting, and Travel Rule** work, shrinking easy laundering channels.

How this changes fraud operations in India (vs. globally).

1. **On-ramps/off-ramps get tighter.** Because Indian exchanges carry heavy TDS/AML obligations and strict ad standards, large-scale scammers are more likely to **push victims to offshore or fake platforms** and then route funds through **stablecoins and OTC brokers** rather than domestic orderbooks—especially after FIU's actions against non-compliant offshore apps. In contrast, in parts of the world with unified licensing but lighter tax frictions (say, the EEA under MiCA), fraudsters still prefer **unlicensed** platforms, but the **incentive to avoid local exchanges for every trade** is somewhat lower than in India.
2. **Marketing channels are hemmed in.** India's **ASCI rules** and prominent disclaimers blunt splashy "get-rich-quick" campaigns; scammers adapt by **pivoting to private messaging (WhatsApp/Telegram/Instagram)** and **pig-butchering** scripts—mirroring the global trend, but amplified by India's ad constraints that make open retail solicitation riskier.
3. **Deterrence via enforcement visibility.** FIU penalties and registration headlines (and even App-Store removals for non-compliant exchanges) send visible signals that **unregistered platforms aren't safe**. That visibility isn't universal elsewhere: the EU and UK have strong regimes, but the **public drumbeat** of fines, URL blocks, and onboarding bans in India is unusually salient, and it shapes user perceptions of what "legit" looks like.

4. **Tax-driven market microstructure.** The **1% TDS** can fragment liquidity by discouraging frequent in-and-out trading on domestic platforms; sophisticated users may seek **P2P, OTC, or offshore venues**, which scammers exploit by steering victims to **off-platform "handlers."** Policymakers are actively debating whether tuning TDS could improve compliance without pushing activity abroad.

3.3 India's receptiveness versus "global" receptiveness, in one glance

- **India:** Receptive to **regulated, tax-visible** activity; skeptical of speculative retail manias; **pro-AML** posture; vocal central-bank caution; **ads constrained**; strong **G20 multilateralism** push. Result: mainstream curiosity persists, but retail "virality" is tempered.
- **EU/UK/Singapore (and similar): Licensing-first** frameworks with calibrated retail protections; wide institutional adoption; clearer **passporting** (EU) or permissions (UK/MAS). Result: high adoption among compliant firms, scammers nudged to the **unlicensed fringes**, but retail ads can be broader (subject to conduct rules).
- **Enforcement mood (2024–25):** Rising everywhere—**specialist units** at regulators (e.g., FCA), coherent EU rules, and continuing cross-border AML coordination. India's mix of **tax + AML + ad rules** makes its environment *stricter on the surface* for retail hype, while still leaving social-engineering vectors (romance/WhatsApp cons) that mirror global losses.

4) The mechanics: how crypto frauds typically run (and what changes in India)

Step-by-step playbook (global).

1. **Lure:** Social media DM, dating app, Telegram group, or a celebrity-impersonation post.
2. **Social proof:** Screenshots of "profits," fake testimonials, or **spoofed trading dashboards**.
3. **Initial deposit:** Victim wires fiat to a VASP or sends USDT from a retail exchange to a scam wallet.
4. **Paper gains:** The site shows rising balances; small withdrawals may be honored to deepen trust.
5. **Escalation:** "Limited-time" arbitrage, "VIP tiers," or margin opportunities demand bigger deposits.
6. **Denial/blackmail:** Withdrawals are blocked (KYC "issues," bogus taxes) or the victim is **sextorted** with AI-doctored images.

What's different in India's flow. Because domestic exchanges implement **KYC/TDS** and are under **FIU** oversight, fraudsters more often **steer victims off-platform** early—straight to **imposter websites** or **OTC handlers**—to avoid traceable on-ramps, or they rely on **unregistered offshore apps** (which India has targeted). When victims do start from Indian exchanges, scammers commonly request **stablecoin transfers** to an external address, quickly **chain-hop** across networks to obfuscate, and then cash out via OTC brokers in laxer jurisdictions. India's **ASCI rules** also mean fewer splashy mass-market pitches; the **grooming happens in DMs**, echoing the global pig-butchering profile.

5) What actually works to curb crypto fraud

No single lever eliminates fraud, but the data-backed combination looks like this:

- **Licensing + perimeter clarity** (e.g., **MiCA** in the EU) so users can tell authorized firms from clones.
- **AML harmonization** (FATF R.15/Travel Rule) to reduce jurisdiction shopping.
- **Retail guardrails and truthful advertising** (UK marketing rules, **India's ASCI disclaimers**, MAS limits on retail staking/lending).
- **Visible enforcement** (e.g., FIU fines and URL blocks; FCA crypto enforcement team) to reset user expectations and market norms.
- **Public-private tracing** leveraging blockchain transparency and cross-VASP alerts; yearly industry reports show that while some categories fall (e.g., classic investment "doubles"), others surge (romance/pig-butchering, ransomware), so **tactics must update continually**.

6) Practical red flags and India-specific cautions

- **"Off-app" pressure** to move from a compliant Indian exchange to a **new site** whose URL you've never seen—especially if it promises withdrawal "only after" paying special "taxes." (Real taxes in India apply to gains and TDS at trade time, not as withdrawal ransoms.)
- **"Relationship-first" pitches** from strangers (WhatsApp/Instagram/Telegram) that escalate quickly to investments or "mentorship." This is the hallmark of **pig-butchering** gangs.
- **Celebrity endorsements without the ASCI disclaimer** or with language like "guaranteed returns"/"safe currency." In India, legitimate ads must carry the mandated warning and avoid misleading terms.
- **Unregistered offshore exchanges** courting Indians without **FIU-IND** registration. FIU has blocked or penalized several; registration and penalties are publicly reported.

"Crypto fraud" isn't a flaw in blockchains so much as a **human-system problem**—confidence tricks plugged into fast, global payment rails. The **global trend** is toward clearer licensing, stronger AML, and sharper retail protections (MiCA in the EU; UK's 2025 regime; MAS restrictions; FATF pressure). India's **distinctive mix**—a firm AML perimeter (FIU-IND under PMLA), **30% tax + 1% TDS**, stringent ad disclaimers, and visible enforcement—**reduces the oxygen** for mass-market scam advertising and easy on-ramps, but **shifts fraud** into social-engineering channels and unregistered offshore venues. Knowing these structural differences helps you parse risk: in India, if you're nudged **off** a FIU-registered platform, pressured by an online "friend," or promised "guaranteed" yields without ASCI-compliant messaging—assume you're the target, not the customer.

The legal challenges of addressing **cryptocurrency fraud in India** stem from the tension between a rapidly evolving technology and a legal/regulatory framework that is still adapting. Here are the main challenges:

1. Absence of a Comprehensive Crypto Law

- India does not yet have a dedicated **Cryptocurrency Act** or comprehensive framework for regulating digital assets.
- Current measures rely on **tax law (Income Tax Act, 1961 – Section 115BBH and 194S)**, **anti-money laundering law (PMLA, 2002)**, **FEMA (1999)**, and **advisories by RBI and SEBI**.
- This patchwork creates **ambiguity**: is a crypto asset a security, a commodity, a payment instrument, or something else? Different classifications affect jurisdiction and enforcement.

2. Jurisdictional and Cross-Border Issues

- Many scams originate from **offshore exchanges, websites, or operators**.
- Fraudsters often use **shell companies abroad** or operate from countries with lax enforcement, making **extradition and cooperation** difficult.
- Since transactions cross borders instantly via blockchain, Indian law enforcement struggles with **territorial jurisdiction** under the Code of Criminal Procedure (CrPC).

3. Pseudonymity and Anonymity

- While blockchain transactions are transparent, they are tied to **wallet addresses**, not personal identities.
- Fraudsters can route funds through **mixers, tumblers, and chain-hopping** (moving assets across multiple blockchains), which complicates tracing.
- Without cooperation from global exchanges, identifying the real person behind a wallet is often legally and practically difficult.

4. Gaps in Investigative Tools and Capacity

- Indian investigative agencies (Enforcement Directorate, Cyber Crime Cells, FIU-IND) are still **building expertise** in blockchain forensics.
- Unlike traditional bank frauds, crypto frauds require **specialized tools (Chainalysis, TRM Labs, etc.)**, which not all agencies have access to.
- Gathering **digital evidence** that is admissible in Indian courts under the **Indian Evidence Act, 1872** is another hurdle—especially when servers or data are hosted abroad.

5. Overlap of Regulatory Bodies

- **RBI** opposes private cryptocurrencies on monetary stability grounds.
- **SEBI** would normally regulate securities, but crypto assets don't clearly fit.
- **Ministry of Finance (CBDT, GST Council, FIU-IND)** oversees taxation and AML.
- This fragmented oversight creates **regulatory turf wars** and uncertainty, often slowing enforcement.

6. Consumer Protection Limitations

- Victims of fraud currently have to rely on **general laws** like the **Indian Penal Code (IPC)** (cheating, criminal breach of trust), **IT Act (2000)** (cyber fraud provisions), or **Consumer Protection Act (2019)**.
- These laws were not designed with crypto in mind, so **applicability is stretched**, and punishments may not adequately deter.
- Refund or recovery mechanisms are extremely weak: unlike banks, crypto has **no chargeback system**.

7. Taxation Complications

- The **1% TDS** on transactions and **30% tax on gains** push many users to **offshore or informal channels**, where fraud risk is higher.
- Enforcement is harder when victims themselves may have used **grey channels** to avoid tax, making them reluctant to report crimes.

8. Global Coordination Deficit

- Although India has pushed for a **G20 framework on crypto regulation**, international cooperation on fraud cases remains patchy.
- FATF's Travel Rule is not uniformly enforced across jurisdictions, giving fraudsters safe havens.

9. Legal Recognition of Crypto Assets

- Since crypto is **not legal tender** in India, there is uncertainty about how courts will treat ownership disputes or recovery claims.
- Example: If someone is defrauded of Bitcoin, can it be treated as "property" under the IPC or the Indian Contract Act? Courts have been inconsistent.

10. Speed of Innovation vs. Legal Process

- Fraudsters innovate faster than legal systems can adapt (e.g., **rug pulls, DeFi hacks, AI-powered deepfake scams**).
- Drafting, debating, and passing comprehensive legislation takes years, while scams evolve **month by month**.

India faces legal challenges in tackling crypto fraud because there is **no unified law**, **cross-border enforcement is weak**, **investigative capacity is limited**, and **regulatory overlap causes confusion**. While recent steps—like bringing crypto under the **PMLA** and enforcing **FIU-IND registration** for exchanges—are progress, India still lacks a **clear statutory framework** for defining, classifying, and prosecuting crypto fraud.