# Crypto as a Money Laundering Tool- Explained Pointwise

Cryptocurrency, once seen as a symbol of financial innovation, has increasingly emerged as a tool for global money laundering. Indian agencies now report large-scale frauds and rapid cross-border fund transfers, posing serious regulatory, financial and national-security challenges. Between January 2024 and September 2025, the Indian Cyber Crime Coordination Centre (I4C) flagged 27 crypto exchanges involved in laundering Rs. 623.63 crore from nearly 2,872 victims.

What is Cryptocurrency and What are Crypto Exchanges?

**Cryptocurrencies** are digital assets created and exchanged using blockchain — a secure, decentralised public ledger. Unlike regular money, they are not backed by any government or central bank. Their value depends on market demand, supply and speculation. **Popular examples** include Bitcoin, Ethereum and stablecoins.

**Key features of cryptocurrencies**

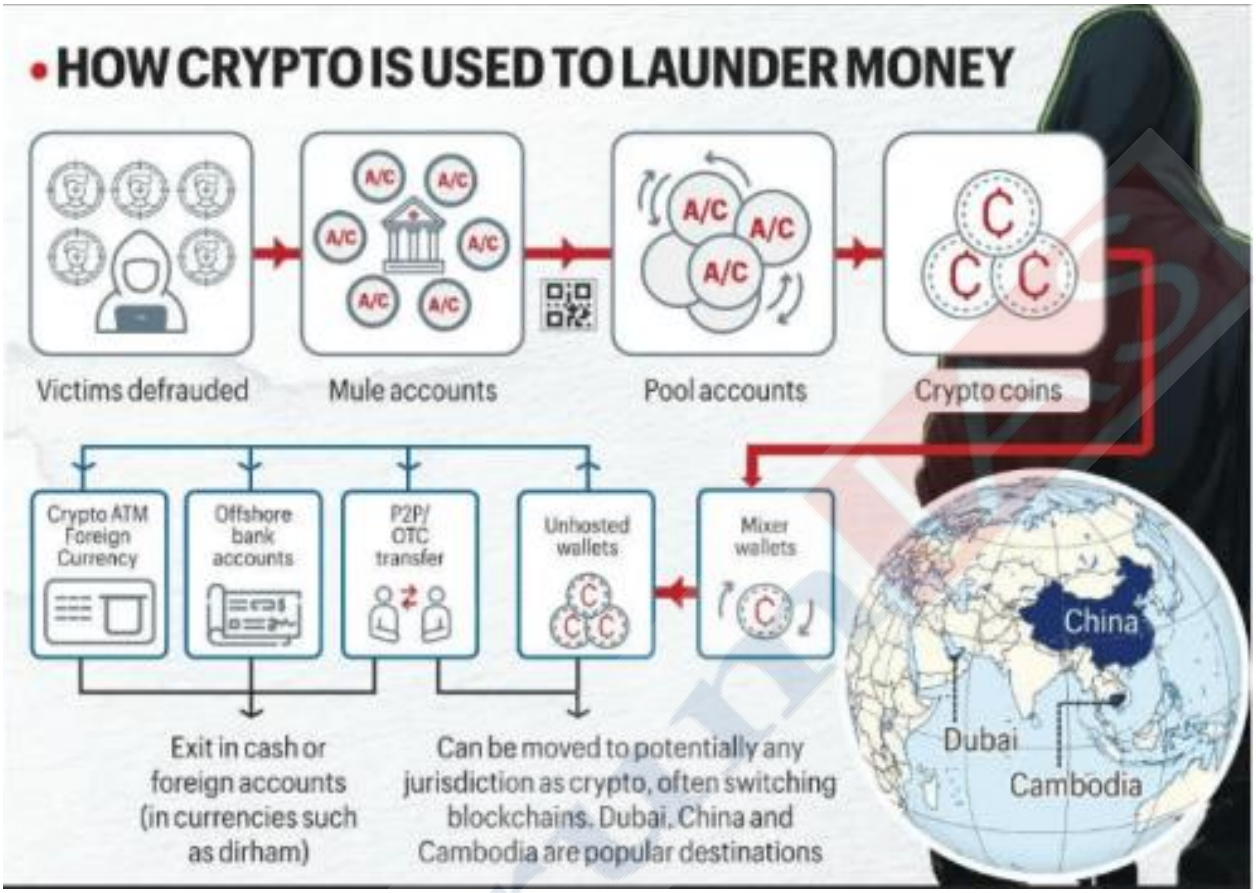
- **Decentralisation:** No central authority controls cryptocurrency, which gives users freedom but also makes it easier for criminals to hide.
- **Pseudo-anonymity:** Transactions use wallet addresses instead of real names, making it difficult to identify people behind them.
- **Borderless transferability:** Crypto can move across countries instantly, avoiding the checks of regular banking systems.
- **Irreversibility:** Once a blockchain transaction is made, it cannot be undone, making recovery of stolen or laundered money very hard.

**Crypto Exchanges**– Crypto exchanges are digital marketplaces where users can buy, sell, trade, or convert cryptocurrencies. They work somewhat like stock exchanges but operate with significantly fewer regulations, making them faster but also more vulnerable to misuse.

**Types of exchanges**:

- **Centralised Exchanges (CEXs):** Platforms such as Binance, Coinbase and WazirX. They typically require KYC verification, though compliance standards vary widely.
- **Decentralised Exchanges (DEXs)**: Peer-to-peer platforms like Uniswap that operate without any central authority. Users trade directly from their wallets, ensuring privacy but offering limited oversight.
- **Hybrid Exchanges:**These platforms combine features of both CEXs and DEXs — offering faster transactions and user-friendly interfaces while trying to maintain greater transparency and security

How do Crypto scams happen?




Source- IE

**1. Fake Exchanges and Websites**– Fraudsters set up websites that look almost identical to genuine crypto platforms. Victims deposit money believing they are trading safely, only for the site to disappear along with their funds.

**2. Pump-and-Dump Schemes**– Scammers artificially boost the price of low-value tokens through coordinated buying and aggressive social-media promotion. When unsuspecting investors join in, the scammers cash out, causing the token price to collapse.

**3. Phishing and Hacking Attacks**– Users are tricked into revealing private keys or seed phrases through fake emails, apps or customer-support messages. Once accessed, wallets are emptied within minutes.

**4. Rug Pulls**– Developers launch a flashy new token or decentralized Finance (DeFi) project, attract investor money, and suddenly shut it down—vanishing with the funds and leaving investors with worthless assets.

**5. Romance and Task-Based Scams (Pig Butchering)**– Criminal networks build emotional connections or offer "high-income tasks" online, slowly convincing victims to invest in fake crypto platforms that show fabricated profits before ultimately wiping out their savings.

Across all these methods, stolen funds are quickly moved through multiple wallets, mixers and loosely regulated exchanges, making the money trail opaque and helping criminals evade traditional anti-money-laundering systems.

What is the size of India's crypto market?

**India's Crypto Market Size**

India today ranks among the world's biggest crypto markets, reflecting both rising digital adoption and growing appetite for alternative assets.

**Key Statistics:**

An estimated 119 million Indians use or hold cryptocurrency — one of the largest user bases globally.

The domestic crypto market was valued at USD 2.6 billion in 2024 (IMARC Group).

By 2035, it is projected to reach USD 15 billion, growing at a 17% CAGR (HDFCTru).

**Who is investing?**

Younger Indians dominate the crypto ecosystem:

**Gen Z (18–25):** 37.6%

**Millennials (26–35):** 37.3%

**Adults (36–45):** 17.8%

**Where is adoption growing?**

Metro cities such as Delhi, Bengaluru and Mumbai continue to lead. But Tier-2 and Tier-3 cities — Jaipur, Lucknow and Patna — are emerging as surprising new hubs of crypto activity.

**What are the key challenges posed by Crypto in India?**

**1. Anonymity and Multi-Layered Laundering**– Crypto transactions use wallet IDs instead of real names, allowing criminals to move money through hundreds of wallets, DEXs and mixers, making tracing extremely difficult.

**2. Cross-Border Movement of Illicit Funds**– Cryptocurrencies enable quick transfers to countries like Dubai, China and Cambodia, where weak regulations and lack of uniform reporting make international coordination very challenging.

**3. Use by Cyber-Criminal and Scam Networks**– Cyber-fraud groups increasingly use crypto for ransomware, extortion and global scam operations because it offers fast, borderless and hard-to-track payments.

**4. Key Role in Online Fraud Schemes**– Crypto is now central to job scams, sextortion, investment frauds and app-loan scams, with victim money quickly converted into crypto and dispersed worldwide, reducing recovery chances.

**5. Regulatory Arbitrage and Exchange Opacity**– Many exchanges operate across multiple jurisdictions with different compliance rules, and some Indian platforms have foreign ownership layers, creating opacity and opportunities for regulatory evasion.

**6. Enforcement and Forensic Difficulties**– Agencies like ED, CBI, and I4C face challenges such as weak KYC standards, complex wallet tracing, lack of protocols for storing seized crypto, jurisdictional limits abroad, and a shortage of trained investigators. These challenges have even led one agency to store seized crypto with a private firm.

**7. Macroeconomic and Financial Stability Risks**– The RBI fears that widespread crypto use could undermine financial stability, weaken monetary-policy control, and disrupt capital-flow management, while high volatility and terror-financing risks deepen concerns. Additionally, high taxes have pushed users offshore, shrinking domestic activity by 97%.

**What is Crypto Governance in India?**

**1. There is no central legislation**, which means crypto has no defined rights, liabilities or consumer protection, and it is not recognised as legal tender.

**2. The Supreme Court–RBI conflict has created regulatory ambiguity**: the RBI banned banking services for crypto in 2018, the Supreme Court overturned it in 2020, and the government later introduced taxes without creating a regulatory framework.

**3. The government remains hesitant to regulate crypto** because doing so may be seen as granting legitimacy, so only a discussion paper is currently being drafted.

4. **There is no investor protection**, as crypto holdings do not have insurance, RBI ombudsman support or SEBI grievance mechanisms, unlike traditional financial products.

**5. Offshore platforms operate outside Indian jurisdiction**, serving Indian users without taxation compliance or regulatory oversight.

**6. Inter-agency coordination is fragmented**, with bodies like the RBI, ED, Income Tax Department, MeitY, state police and FIU-IND following different approaches, creating enforcement gaps.

**What should be the way forward?**

**1. India must enact a comprehensive Crypto Assets and Digital Transactions Act** to define asset classifications, licensing rules, consumer protections, Anti-Money Laundering (AML)/KYC standards and penalties for violations, while clearly distinguishing cryptocurrencies, stablecoins, utility tokens and security tokens.

**2. Exchanges should be brought under a mandatory licensing regime,** similar to the EU's MiCA framework, requiring strict KYC norms, AML checks, travel-rule compliance, long-term data storage and mandatory proof-of-reserves audits.

**3. A regulated system for custody of seized crypto assets is needed**, with national standards for secure storage, recovery procedures and liquidation, supported by a government-approved digital asset custodian.

**4. Blockchain forensics capability must be strengthened**, with specialised labs, AI-based tracing tools, global analytics partnerships and systematic training for agencies like ED, I4C, FIU-IND and state cyber cells.

**5. Cross-border cooperation should be expanded,** using Interpol task forces, FATF networks and bilateral agreements with hubs such as Singapore, the UAE and Europe, given the global movement of illicit funds.

**6. A balanced taxation framework is necessary**, including reducing TDS rates, rationalising capital gains taxes and offering compliance incentives to prevent users from shifting to offshore platforms.

**7. A robust consumer protection architecture must be built**, with a crypto grievance portal, mandatory insurance for exchange-held assets, transparent risk disclosures and compensation systems for fraud victims.

**8. Stablecoins and DeFi need targeted regulation**, including licensing for issuers, reserve audits, transaction reporting and KYC-linked safeguards for high-value DeFi transactions.

**9. Public awareness and digital literacy should be improved**, especially for young investors, through campaigns highlighting common scams, safe wallet practices and the risks of unverified investment schemes.

**Conclusion**

Cryptocurrencies bring useful innovation but also significant risks. In India, rising usage and unclear regulations have increased threats like cyber fraud, financial crime and monetary instability. India now needs a clear, balanced regulatory framework—aligned with global norms—to protect consumers, maintain financial stability and support the safe growth of digital assets.

| |
|---|
| **Read more-** IE |
| **UPSC Syllabus- GS 3**– Issues relating to money laundering, financial frauds, and digital payments |