Mains Analysis: After the US$6.3 billion Binance hack – why India's "tax and watch" approach to virtual digital assets needs a real regulatory framework

Economy · 5 November 2026 · https://www.shanmugamiasacademy.in/upsc-mains-analysis



UPSC Mains Analysis – current affairs of 5 November 2026 (Shanmugam IAS Academy)

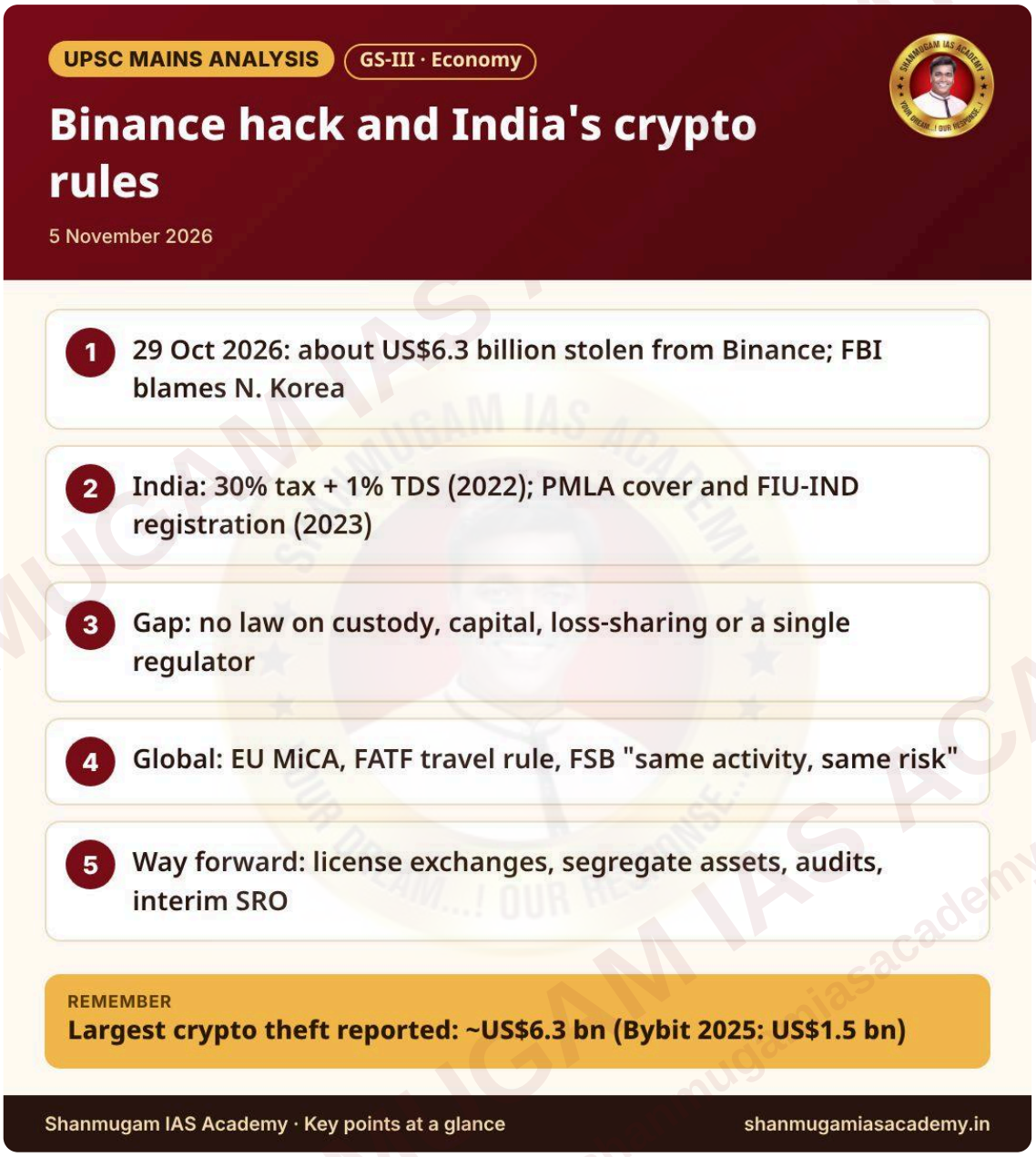
Context

Late on **29 October 2026**, attackers drained about **US$6.3 billion** in crypto-assets from **Binance**, the world's largest crypto exchange – most of it within about 20 minutes. It is reported to be the largest crypto theft on record, far above the US$1.5 billion Bybit hack of February 2025. Binance's early investigation pointed to a **compromised laptop** and malicious software designed to erase evidence; on 31 October the US **FBI** said a North Korean state-backed group known as **TraderTraitor** was responsible. Binance paused deposits and withdrawals, promised that users would not bear the loss, said it had covered about 95% of the stolen assets with company money, and began a phased reopening of withdrawals on **1 November**. About US$3 billion was reportedly frozen with the help of blockchain and stablecoin partners.

For India the hack is not a distant event. Binance serves Indian users and has been registered with India's Financial Intelligence Unit (FIU-IND) since 2024. India taxes crypto heavily and polices it for

money laundering, but it still has **no comprehensive law** on who may run an exchange, how customer assets must be kept, or who pays when an exchange is hacked.

> **GS mapping:** GS-III – Indian economy and mobilisation of resources; investment models; awareness in IT and computers; basics of cyber security; money laundering and its prevention. Also useful for GS-II (regulatory bodies) and Essay (technology and the state).



Background: what India has done so far

Layer	What exists

Taxation (2022)	The Finance Act, 2022 brought a **30% tax** on income from transfer of virtual digital assets (VDAs), with no deduction except cost and no set-off of losses, and a **1% TDS** on transfers from 1 July 2022. These rules were carried into the Income-tax Act, 2025, in force from 1 April 2026.
Anti-money laundering (2023)	A Finance Ministry notification of **7 March 2023** made VDA service providers – those who exchange, transfer, keep in custody or offer financial services on VDAs – "reporting entities" under the **PMLA, 2002**. They must register with FIU-IND, verify customers, keep records and report suspicious transactions.
Enforcement on offshore exchanges	In December 2023 FIU-IND issued show-cause notices to nine offshore exchanges, including Binance, and asked for their websites to be blocked. Binance was fined **₹18.82 crore** in June 2024 and then registered.
Cyber security and KYC (2025–26)	Reports in September 2025 said FIU-IND now requires a cyber-security audit by a **CERT-In empanelled auditor**. Revised FIU-IND guidelines of **8 January 2026** require a live selfie with liveness check, geo-tagging, a "penny-drop" bank check, and bar mixers and anonymity-enhancing tokens.
Central bank view	The RBI's 2018 ban on banks dealing with crypto firms was struck down by the Supreme Court in March 2020. On 2 July 2026 the RBI told Parliament's Standing Committee on Finance that VDAs should not be legalised, citing risks to the financial system.
Policy status	A government discussion paper promised in 2024 has not been published (reported). In September 2025 Reuters reported a government document leaning against a full crypto law. On 23 July 2026 the Standing Committee on Finance suggested an interim regime of recognised **self-regulatory organisations (SROs)** under a designated regulator.

Core analysis: the gap the hack exposes

India's present model can be called **"tax and watch"**: the state collects tax and watches money flows, but nobody supervises the exchange as a business that holds other people's money. The Binance case shows what that leaves uncovered.

Question after a hack	Under Indian law today	Why it matters

Are customer assets kept separate from the exchange's own?	No statutory rule on segregation or custody	If an exchange fails, users may rank as ordinary creditors.
Who bears the loss?	Left to the exchange's choice	Binance absorbed its loss; after the WazirX hack (July 2024, about US$230 million) users waited more than a year for a court-approved restructuring.
Must the exchange hold capital or reserves?	No prudential norms	A smaller exchange could not cover a large theft.
Who inspects wallet and key security?	An audit certificate at registration; no continuing supervisor	Hot-wallet controls and key management are where most hacks start.
Is there a grievance forum?	No dedicated ombudsman	Investors turn to police, consumer courts or foreign courts.

Why it matters for India

- **Investor protection:** Indian users trade on both domestic and offshore exchanges; the 1% TDS and 30% tax do nothing to protect their deposits.
- **Repeated losses at home:** WazirX lost about US$230 million (July 2024) and CoinDCX about US$44 million from an internal account (19 July 2025) – the Binance theft confirms that exchange security is a systemic weakness, not a one-off.
- **National security:** the FBI has linked both the Bybit and the Binance thefts to North Korea; stolen crypto can fund weapons programmes and is laundered across borders within hours.
- **Financial stability and monetary sovereignty:** the RBI fears that legitimising crypto, especially stablecoins, could weaken control over money and capital flows.
- **Tax leakage:** a high tax with no clear licensing regime can push trading to offshore and peer-to-peer platforms that are harder to watch.

Challenges

- **The legitimacy dilemma:** regulating crypto may be read as approving it – the main reason given for avoiding a full law.
- **Borderless platforms:** offshore exchanges, decentralised exchanges and self-held ("unhosted") wallets are hard to reach with national rules.
- **No single regulator:** crypto touches the RBI (payments, stablecoins), SEBI (investment tokens), the tax department and FIU-IND, but none is in charge of exchanges as a whole.
- **Skills and speed:** state-backed hackers move funds in minutes; tracing and freezing need blockchain analytics and quick global cooperation.

- **Policy drift:** the discussion paper has been pending for about two years, leaving investors and firms without a clear direction.

Global approaches

Framework	Key features
EU – Markets in Crypto-Assets Regulation (MiCA), Regulation (EU) 2023/1114	Stablecoin rules from 30 June 2024; fully applicable from 30 December 2024. Crypto-asset service providers need authorisation; custodians must keep client assets legally and operationally segregated and are liable for losses from incidents attributable to them (capped at market value).
FATF standards	Recommendation 15 was amended in October 2018 to bring virtual asset service providers under AML rules; its interpretive note followed in June 2019. The "travel rule" (Recommendation 16) requires sender and receiver details to travel with transfers – reference threshold US$/EUR 1,000. The EU applies it to all crypto transfers from 30 December 2024.
FSB and G20	The FSB framework of July 2023 rests on **"same activity, same risk, same regulation"**. The G20 New Delhi Leaders' Declaration (September 2023), under India's presidency, endorsed the FSB recommendations, welcomed the IMF–FSB Synthesis Paper (with its roadmap) and called for swift implementation of the Crypto-Asset Reporting Framework (CARF) for tax.
Outright ban	China bans crypto trading; the RBI cited China and Qatar before the parliamentary panel. A ban cannot stop peer-to-peer or decentralised trading.

Way forward

1. **Decide the destination:** publish the long-pending discussion paper and set a timeline for a law, so that the "tax and watch" model does not become permanent by default.
2. **Regulate the exchange, not the coin:** licensing of exchanges and custodians with fit-and-proper owners, minimum capital, segregation of client assets and published proof of reserves – without declaring crypto to be money.
3. **Make security a continuing duty:** regular CERT-In audits, limits on hot-wallet balances, multi-party control of keys, incident reporting within hours, and a user-protection fund or insurance for theft.
4. **Interim SRO under a named regulator:** as the Standing Committee suggested, with a grievance-redressal mechanism and investor education.
5. **Work across borders:** full travel-rule implementation, CARF-based tax data sharing, quick freezing protocols with stablecoin issuers, and G20 follow-up on the roadmap India itself pushed in 2023.

Conclusion: The Binance hack shows that the biggest risk to Indian crypto investors today is not price volatility but the safety of the platform that holds their assets. India has built strong tax and anti-money-laundering walls; it now needs the missing floor – clear rules on custody, capital, cyber security and redress – whether or not it ever treats crypto as a legitimate asset class.

Mains practice question

Q. "India taxes virtual digital assets but does not regulate the platforms that hold them." In the light of recent cyber-thefts at crypto exchanges, examine the adequacy of India's current framework and suggest a way forward. *(15 marks, 250 words)*

Answer framework: Introduction – Binance hack (October 2026, about US$6.3 billion) and Indian cases (WazirX 2024, CoinDCX 2025) · Body – (a) present framework: 30% tax + 1% TDS (2022), PMLA notification (March 2023), FIU-IND registration and 2026 KYC rules, CERT-In audit; (b) gaps: custody, capital, loss-sharing, single regulator, grievance redressal; (c) RBI's concerns vs investor-protection needs; (d) global lessons – MiCA, FATF travel rule, FSB/G20 · Way forward – five points above · Conclusion – faculty-view line below.

Prelims pointers

- Virtual digital asset (VDA) – term used in the Income-tax law since the Finance Act, 2022; covers crypto-assets and NFTs.
- VDA service providers became reporting entities under the PMLA, 2002 by notification of 7 March 2023; they register with FIU-IND.
- FIU-IND – Financial Intelligence Unit–India, under the Department of Revenue, Ministry of Finance.
- Hot wallet – connected to the internet for daily transactions; cold wallet – kept offline.
- MiCA – Markets in Crypto-Assets Regulation of the European Union; fully applicable from 30 December 2024.
- FATF travel rule – Recommendation 16; extended to virtual asset service providers in June 2019.

Asked before in UPSC Mains (PYQ)

Official question-paper wording, with how this analysis helps you answer it.

GS-I 2021 15 marks

"What is Cryptocurrency? How does it affect global society? Has it been affecting Indian society also?"

How this helps: The Binance hack, the WazirX and CoinDCX losses and India's tax, PMLA and KYC rules give you fresh global and Indian examples for the "society" part – investor losses, cybercrime and illicit finance.

GS-III 2021 10 marks

"Discuss how emerging technologies and globalisation contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels."

How this helps: Crypto is the clearest case of technology-driven laundering: use the PMLA notification of March 2023, FIU-IND rules (2026) as national measures and the FATF travel rule and FSB/G20 framework as international ones.

GS-III 2021 10 marks

"Keeping in view India's internal security, analyze the impact of cross-border cyber-attacks. Also discuss defensive measures against these sophisticated attacks."

How this helps: A state-linked group attributed by the FBI emptied exchange wallets in minutes – a ready example of cross-border cyber-attacks on financial infrastructure, with CERT-In audits as a defensive measure.

Faculty view – looking ahead (Shanmugam IAS Academy)

The key principle to carry into your answers is **"same activity, same risk, same regulation"**. An exchange that holds customers' assets does what a custodian or broker does, so it should face the same duties – segregation, capital, audits, redress – whatever one thinks of crypto itself. This lets India protect investors without "legalising" crypto as money, which is the RBI's main fear.

- **A shift to note:** the debate is moving from "ban or allow" to "who supervises the platform". Expect questions on regulatory gaps, SROs and investor protection in new-age finance.
- **What to watch next:** (1) Binance's full incident report and how much of the stolen crypto is recovered, (2) the Standing Committee's study "A Study on Virtual Digital Assets (VDAs) and Way Forward", (3) whether the government publishes its discussion paper or names an interim regulator, (4) global follow-up on North Korean crypto theft at the FATF and the UN.
- **Ready-made conclusion line:** "India need not bless crypto to protect the people who hold it – it only has to regulate the vault, not the coin."

Sources: Reuters, The New York Times, TechCrunch, ITV News and others on the Binance hack (29 October – 1 November 2026); Finance Act, 2022; Ministry of Finance PMLA notification of 7 March 2023; FIU-IND orders and guidelines (2023–2026); ANI and Business Today on the Standing Committee on Finance (July 2026); FSB (July 2023); G20 New Delhi Leaders' Declaration (2023); EU MiCA Regulation. Original analysis by Shanmugam IAS Academy.

Shanmugam IAS Academy – your next step

- **Courses:** TNPSC Group 1, 2 / 2A (Prelims + Mains), Group 4, UPSC / IAS – Coimbatore · Madurai · Online – https://www.shanmugamiasacademy.in/fees
- **Books (PDF):** TNPSC PYQ books, UPSC books – https://www.shanmugamiasacademy.in/study-materials
- **Free quiz + daily PDFs:** https://www.shanmugamiasacademy.in/free-pdf-download · All news of this day: https://www.shanmugamiasacademy.in/upsc-mains-analysis

Admissions – call / WhatsApp: 99941 46662 · 99944 27714 · www.shanmugamiasacademy.in