



QUOTE FROM THE QUOTABLE

"The hottest places in Hell are reserved for those who, in times of great moral crisis, maintain their neutrality."

[ Dante Alighieri ]

OUR VIEW |

# Italy's Palestine Protests and the Politics of Recognition

Italy's recent mass protests over Gaza have stirred global attention—not just for their scale, but for their symbolism. Over 100,000 citizens across more than 75 cities blocked ports, railways, and highways in a coordinated 24-hour strike. Their demand: recognition of Palestinian statehood and a halt to arms shipments to Israel. The government's refusal, led by Prime Minister Giorgia Meloni, has sparked a civic reckoning. Meloni's stance is rooted in strategic alignment and ideological clarity. Her government maintains strong ties with Israel and the United States, both of which oppose unilateral recognition of Palestine. She argues that acknowledging a state "that doesn't exist" would be counterproductive—a view shaped by concerns over territorial coherence and institutional viability. Domestically, her coalition includes nationalist factions wary of foreign entanglements, making recognition politically fraught. Yet the protests are not merely reactive. They reflect organized civic intent. Dockworkers halted operations in Genoa, Livorno, and Venice. Students occupied lecture halls and stations. Protesters carried banners reading "Let's Block Everything" and "Against Genocide," framing the movement as a moral stand rather than a geopolitical demand. This uprising reveals a deeper truth: that public outrage often fuses local discontent with global empathy. For many Italians, Gaza became a mirror—reflecting frustrations with democratic erosion, ethical drift, and perceived complicity. Supporting Palestine was not escapism; it was ethical citizenship. Still, symbolic protest must not eclipse domestic accountability. Civic energy must be balanced. Italy's protests show that when citizens act with intent, they can challenge foreign policy while demanding moral clarity at home. What makes this moment striking is its choreography—how unions, students, and civil society converged across geographies and ideologies. It wasn't just a protest; it was a civic performance of conscience, staged in ports and piazzas, demanding that politics respond to humanity, not just strategy. The moment invites reflection. In

# Comment

## Crypto and the Dark Web: India's New Security Frontier

As India embraces digital finance, the unchecked rise of cryptocurrencies has opened dangerous backdoors for terror funding, money laundering, and cross-border crime. This analysis traces how regulatory gaps are being exploited—and why urgent reform is no longer optional.

### Cryptocurrencies as a Tool for Illicit Fundraising

Unregulated digital currencies have become an attractive resource for illicit actors due to their pseudo-anonymity, decentralization, and cross-border abuse potential. Global reports indicate that terrorist groups such as ISKP and Hamas have increasingly utilized stablecoins, privacy coins, and unhosted wallets for fundraising—leveraging mixers and fake credentials to bypass KYC protocols. In India, the Financial Intelligence Unit (FIU-IND) has flagged widespread suspicion that cryptocurrencies are being used in serious criminal activities, ranging from terrorist financing to cybercrime, drug trafficking, and secessionist funding. These concerns, based on suspicious transaction reports (STRs), have prompted action by enforcement bodies including the Enforcement Directorate (ED), Central Bureau of Investigation (CBI), and the Income-Tax Department. FIU has specifically launched investigations targeting Binance and WazirX over suspected crypto flows into Jammu & Kashmir and from Pakistan, suggesting a possible nexus with terror funding. Unregulated private wallets and decentralized transfers via tokens like TRX are emerging as significant threats. The State Investigation Agency (SIA) in Kashmir has conducted coordinated searches across Jammu, Doda, and Handwara to dismantle crypto-linked terror finance networks.

### Cryptocurrencies as a Tool for Illicit Fundraising

Unregulated digital currencies

have become an attractive resource for illicit actors due to their pseudo-anonymity, decentralization, and cross-border abuse potential. Global reports indicate that terrorist groups such as ISKP and Hamas have increasingly utilized stablecoins, privacy coins, and unhosted wallets for fundraising—leveraging mixers and fake credentials to bypass KYC protocols. In India, the Financial Intelligence Unit (FIU-IND) has flagged widespread suspicion that cryptocurrencies are being used in serious criminal activities, ranging from terrorist financing to cybercrime, drug trafficking, and secessionist funding. These concerns, based on suspicious transaction reports (STRs), have prompted action by enforcement bodies including the Enforcement Directorate (ED), Central Bureau of Investigation (CBI), and the Income-Tax Department. FIU has specifically launched investigations targeting Binance and WazirX over suspected crypto flows into Jammu & Kashmir and from Pakistan, suggesting a possible nexus with terror funding. Unregulated private wallets and decentralized transfers via tokens like TRX are emerging as significant threats. The State Investigation Agency (SIA) in Kashmir has conducted coordinated searches across Jammu, Doda, and Handwara to dismantle crypto-linked terror finance networks.

### Money Laundering via Dark Web and Crypto

Crypto's decentralized nature makes it an ideal channel for money laundering. A recent whitepaper highlights how cryptocurrencies enable swift, low-cost cross-border transfers that bypass capital controls, exploiting decentralized exchanges and privacy coins to obscure illicit flows. In India, authorities in Rajasthan arrested individuals who converted over Rs. 1 crore into USDT to funnel funds offshore. The Enforcement Direc-



Prof. Kapil Garg, Operations, Decision Science & IT



Prof. Ruchi Garg, IT, Birla Institute of Management Technology (BIMTECH)

torate has seized both cash and crypto assets worth lakhs in similar operations. Over Rs. 4,000 crore in illicit crypto transactions were unearthed via exchanges in a single year, underscoring the scale of misuse. High-profile cases include arrests in Balrampur for laundering Rs. 50 crore through Chinese loan apps and USDT transfers, and in Ahmedabad, where two brothers were implicated in a Rs. 16 crore crypto scam allegedly controlled by a Chinese cyber syndicate. A Jaipur-based cyber fraud ring used hawala and USDT, facilitated by a Chinese app, for cross-border laundering. In Uttar Pradesh, police dismantled a Telegram-based gang run by Chinese proxies, which transferred Rs. 75-80 lakh over two months via decentralized TRC-20 wallets, bypassing all regulatory oversight. A pan-India scam involving impersonation and conversion of Rs. 47 lakh into USDT was also uncovered, with the accused using dark web data and mule accounts to mask the illicit trail.

### Cross-Border Illicit Transactions and Darknet Commerce

The dark web fosters anonymity, enabling a range of illicit trades. Research summaries link dark web platforms to crypto-enabled drug trafficking in India, with the Home Ministry issuing warnings about national security threats. Dark web forums and trading portals facilitate illegal transactions—from narcotics to forged identities—using cryptocurrency as the preferred medium. The Narcotics Control Bureau is actively monitoring darknet crypto payments to counter drug trafficking. In response to AML non-compliance, the government has blocked Binance and other offshore exchanges, although some were offered restoration upon meeting compliance standards.

### Regulatory, Taxation, and Identity Verification Grey Zones

India currently lacks a comprehensive regulatory framework for virtual digital assets (VDAs). Despite growing threats, cryptocur-

rency remains neither fully legalized nor systematically regulated. Oversight gaps persist in DeFi platforms, decentralized wallets, and coordinated regulation, prompting calls for inter-agency task forces involving RBI, SEBI, ED, and FIU-IND. Both FATF and Indian monitoring agencies emphasize the urgent need for tighter digital regulation, especially given crypto's role in enabling modern terrorism.

The 2022-23 Union Budget introduced a 30% tax on crypto earnings, but concerns remain over reporting clarity and the potential discouragement of legitimate adoption. Identity verification remains a weak link, with crypto systems often plagued by inadequate KYC/AML enforcement—particularly for unhosted wallets and privacy coins. Scammers exploit social engineering, identity theft, and money mule networks to evade detection, as evidenced in numerous cases involving dark web data and false identities.

### Implications and Conclusion

Unregulated digital assets pose a multi-faceted threat to India's internal security—from financing terrorism to facilitating money laundering and drug trafficking. The rapid evolution of these threats has outpaced governance frameworks, creating regulatory grey zones in oversight, taxation, and identity verification. While India's enforcement agencies have demonstrated resolve, structural gaps—particularly in DeFi, cross-border regulation, and KYC compliance—remain critical vulnerabilities. India must act swiftly to craft an integrated regulatory and technological response. Stronger laws, enhanced crypto exchange oversight, international collaboration, and advanced blockchain forensics are essential to safeguard internal security while enabling the legitimate potential of digital finance.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of the newspaper