IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

DEFI PROTOCOLS AND CROSS-BORDER ENFORCEMENT: INDIA'S REGULATORY DILEMMA

Nandini Goyal[1], Dr. Pranay Kumar Aditya[2]

[1]Research Scholar, Raffles University, Neemrana, Rajasthan

[2]Associate Professor, Raffles University, Neemrana, Rajasthan

ABSTRACT

Decentralised Finance operates with dispersed intermediaries, unidentifiable entities and limitless boundaries. It has posed new-age challenges to the current financial regulatory framework. The article analyses the Indian regulatory framework for DeFi protocols under the Prevention of Money Laundering Act, 2002 (PMLA), and the cross-border enforcement challenges it poses when DeFi protocols facilitate illicit financial activities. It is a doctrinal comparative analysis of the USA's actions regarding Tornado Cash and Samourai Wallet, the EU's MiCA framework, and India's fragmented, activity-based approach. Critical gaps identified in the Indian regulations include: (i) Ambiguity in the definition of "sufficient decentralisation"; (ii) Undefined distribution of liability among developers, front-end operators, DAOs, and users; (iii) Absence of cross-border territorial jurisdiction over DeFi matters; (iv) Scarcity of executory regulations against autonomous systems.

Keywords: Decentralised Finance, DeFi, Cross-border enforcement, Cryptocurrency regulation, PMLA, Money laundering, India, Blockchain, Smart contracts, Regulatory technology.

I. INTRODUCTION

The advent of Decentralised Finance has posed enormous challenges to the prevailing financial regulatory framework. As Walch calls out the absence of identifiable intermediaries like banks, exchanges and brokers, the key regulatory contributors in a traditional financial framework and transactions happening through autonomous public blockchains (termed as "accountability gap") as the key reason for troubles[1].

[1] Angela Walch, "Deconstructing 'Decentralisation': Exploring the Core Claim of Crypto Systems," in Crypto Assets: Legal and Monetary Perspectives 39, 42-48 (Oxford University Press 2019).

India's stance on cryptocurrency regulation has shifted from an absolute prohibition to a more conservative approach.[2] In Internet and Mobile Association and Mobile Association of India v. Reserve Bank of India, the Supreme Court struck down the RBI's circular that banned financial institutions from providing services to cryptocurrency businesses, finding it unconstitutional. Later, the Finance Ministry imposed a flat 30% tax on virtual digital asset gains and a 1% TDS on transactions exceeding IND 10,0004[3].

On March 7, 2023, the MoF issued a notification under the PMLA, 2002, classifying entities providing VDA services as "reporting activities".[4] Consequently, bringing the service providers under FIU-IND's direct scrutiny, mandating anti-money laundering and combating the Financing of Terrorism compliance. In conclusion, India's approach is rather "what is" and not "how"[5].

The unique challenges India faces in governing DeFi protocols that attain "sufficient decentralisation"—protocols that operate independently without identifiable controlling parties—are explored in this article. Conventional enforcement mechanisms based on identifying a "responsible entity" fail when a DeFi protocol's smart contracts are unalterable, its governance is dispersed among thousands of pseudonymous token holders, and its front-end interfaces are repeatable. In the absence of a centralised regulatory body, the main research question is: **How can India determine and implement regulatory accountability for DeFi protocols operating across borders?

Due to domestic restrictions, Indian users have over $100 billion locked globally.[6], in DeFi, accessed through offshore platforms. The lack of effective enforcement frameworks has put India at direct risk, including money laundering and capital flight, leading to loss of monetary sovereignty and liquidity risks.

The United States' stance on the prosecution of Roman Storm, the developer of Tornado Cash[7] and Keonne Rodriguez and William Lonergan, founders of Samourai Wallet, provide instructive precedents for holding developers liable in decentralised systems. These highlight the issues. These cases raise important issues, such as whether creating and executing code amounts to running a financial service, whether developers can be held accountable for third-party software misuse, and where to draw the line between criminal facilitation and protected speech (code as First Amendment expression).

There are five sections to this article. The theoretical framework is established in Part II, which defines DeFi and examines the spectrum of decentralisation from completely centralised platforms to truly autonomous protocols. In Part III, the PMLA's current legal framework in India is examined, and significant gaps in applying conventional regulatory concepts to DeFi are identified. In Part IV, enforcement strategies in the US

[2] For a comprehensive overview of India's evolving crypto stance, see Global Legal Insights, "Blockchain & Cryptocurrency Laws & Regulations 2026 | India," October 21, 2025

[3] Finance Act, 2022, Act No. 6 of 2022, inserting Section 194S (1% TDS on VDA transactions) and Section 11 BBH (30% tax rate on VDA income) into Income Tax Act, 1961

[4] Ministry of Finance Notification S.O. 1160(E), dated March 7, 2023, Gazette of India, Extraordinary, Part II, Section 3(i) (March 7, 2023) [hereinafter PMLA VASP Notification]

[5] Id.

[6] DeFiLlama, Total Value Locked in DeFi, https://defillama.com/ (last visited January 2026)

[7] United States v. Roman Storm, Case No. 1:23-cr-00399 (S.D.N.Y. filed Aug. 23, 2023)

and the EU are compared, with lessons that can be applied to India. Recommendations for India's future as a leader in DeFi regulation are included at the end of Part V.

II. THEORETICAL FRAMEWORK: DEFINING DEFI AND THE DECENTRALIZATION SPECTRUM

A. What is Decentralised Finance?

Financial applications built on blockchain networks, mainly Ethereum, that operate via smart contracts rather than centralised intermediaries are referred to as decentralised finance (DeFi).[8]. Fundamentally, DeFi uses autonomous code that carries out preset rules without human intervention to replicate traditional financial services (lending, borrowing, trading, derivatives, insurance)[9].

The defining characteristics of DeFi include:

1. Smart Contract Execution: Blockchain-based self-executing programs that contain financial logic[10]. Once executed, these contracts perform in accordance with their defined rules, handling operations effortlessly when specific criteria are met.

2. Non-Custodial Architecture: Participants remain in authority over private keys; no intermediary holds control of assets[11]. DeFi users engage directly from their wallets, unlike conventional exchanges, where the platform manages user funds.

3. Permissionless Access: DeFi protocols can be used by anybody with a wallet and an internet connection without the need for intermediary gatekeeping, identity verification, or approval procedures[12].

4**. Composability:** DeFi protocols are capable of integrating to create what industry players refer to as "money legos," which are complicated financial products constructed through the combination of several protocol interactions[13].

5. Transparency: unparalleled auditability and verification are made possible by the visibility of every exchange and code for smart contracts on public blockchains[14].

B. The Decentralisation Spectrum

DeFi protocols exist on a continuum from highly centralised to genuinely decentralised. Understanding this spectrum is critical for determining regulatory obligations and the feasibility of enforcement.

1. **Highly Centralized ("CeDeFi")**

   Platforms controlled by legal entities implement KYC verification at multiple checkpoints, and administrators hold admin keys that allow them to modify or suspend smart contracts.

[8] Fabian Schär, "Decentralised Finance: On Blockchain- and Smart Contract-Based Financial Markets," 103 Federal Reserve Bank of St. Louis Review 153-156 (2021)

[9] Campbell R. Harvey, Ashwin Ramachandran & Joey Santoro, DeFi and the Future of Finance 29-54 (Wiley 2021)

[10] Id., at 31-35

[11] Schär, supra note 10, at 157

[12] Harvey et al., supra note 11, at 37-39

[13] Id., at 55-58

[14] Schär, *supra* note 10, at 158

2. **Semi-Decentralised**

   Most of the current platforms fall under this category, and smart contracts and front-end interfaces are controlled by known companies. Example: Uniswap.

3. **Genuinely Decentralised**

   True decentralisation that has a fully open-source code with no proprietary elements, with immutable smart contracts that have no admin keys, and no requirement for KYC protocols. Example: Tornado Cash (pre-sanctions)

Historically, finance has been regulated and monitored by intermediaries, and the level of decentralisation affects the level of regulations that can be imposed.[15] The government needs identifiable entities to hold accountable,[16]

India's activity-based approach under the Prevention of Money Laundering Act (PMLA) focuses on whether a person provides services "for or on behalf of another" rather than examining deeper structural issues. While this approach may work in traditional contexts, it creates significant uncertainties when applied to autonomous blockchain protocols.

The key ambiguities are twofold. First, it is unclear whether simply deploying code that enables financial functions constitutes "providing services" under the PMLA. Second, the framework does not adequately address whether software can be considered to "operate a business" in the absence of ongoing human control or intervention.

These gaps reveal that the PMLA's functional focus, while attempting to capture a broad range of activities, may not be well-suited to decentralised technologies where the traditional relationship between service provider and recipient breaks down.

C. Defining "Sufficient Decentralisation" for India

India needs to define sufficient decentralisation to determine when to deploy traditional or alternative regulatory protocols. Referring to the Bank for International Settlements' Framework and FATF guidelines, we propose the following criteria, all of which should be met:

1. Immutability: When no admin keys exist, and smart contracts cannot be modified post-deployment by any party.
2. No Administrative Control: No individual or entity can pause, censor transactions, blacklist addresses, or exercise discretionary control over protocol functions.
3. Distributed Governance: No individual shall be allowed to hold more than 10% of governance tokens, and the governance outcomes cannot be controlled by a cartel of parties collectively holding less than 33% of governance tokens.
4. Open Source: There shall be no proprietary element in the code, and it shall be publicly available.

[15] Chris Brummer & Yesha Yadav, "Fintech and the Innovation Trilemma," 107 Georgetown Law Journal 235, 265-275 (2019)
[16] Remarks by SEC Chair Gary Gensler at Aspen Security Forum, August 3, 2021

5. Front-End Independence: No single entity shall control the primary method of user access.
6. No Fee Extraction: No one receives any fees, rents, or profits for operations whatsoever.
7. Deployment Finality: Once deployed, it operates autonomously and no support from developers or creators is required.

III. INDIA'S LEGAL FRAMEWORK AND ENFORCEMENT CHALLENGES

A. PMLA Framework for Virtual Digital Assets

To prevent money laundering in India, the Prevention of Money Laundering Act, 2002 (PMLA) was implemented, and by March 7, 2023, the Finance Ministry issued a notification bringing virtual digital assets under its ambit.

1. Scope of VDA Regulation

Activities conducted by or on behalf of a natural or legal person in the course of business that are subject to PMLA obligations include:

(a) Exchange between virtual digital assets and fiat currencies;

(b) Exchange between one or more forms of virtual digital assets;

(c) Transfer of virtual digital assets;

(d) Safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets;

(e) Participation in and provision of financial services related to an issuer's offer and sale of a virtual digital asset.[17]

The definition of "virtual digital asset" follows the one in Income Tax Act, "any information or code or number or token (not being Indian currency or any foreign currency), generated through cryptographic means or otherwise... providing a digital representation of value which is exchanged with or without consideration..."[18] It captures cryptocurrencies, stablecoins, NFTs, and DeFi protocol tokens.

2. Reporting Entity Obligations

VDA service providers shall:

Registration: To operate in India, registration with FIU-IND is a mandatory prerequisite.[19]

KYC/Customer Due Diligence: Verification of customer identity, beneficial ownership, and source of funds[20]

[17] PMLA VASP Notification, supra note 7

[18] Income Tax Act, 1961, S. 2(47A) (as amended by Finance Act, 2022)

[19] Financial Intelligence Unit – India, "Circular for Registration of Virtual Digital Asset Service Providers," July 4, 2023

[20] Prevention of Money Laundering (Maintenance of Records) Rules, 2005, Rule 9

Suspicious Transaction Reporting: When transactions flag suspicious, criminal activities, file Suspicious Transaction Reports with FIU-IND.[21]

Record Maintenance: Maintaining and retaining transaction records, customer identification documents, and account files for a minimum of five years after closing the account.[22]

Travel Rule Compliance: If the transfer is above the specified limits, provide information about the originator and beneficiary to the FATF.[23]

Principal Officer Appointment: An Indian resident to be appointed as Principal Officer responsible for PMLA compliance.[24]

B. Critical Gaps in Applying PMLA to DeFi

While India's actions against centralised exchanges demonstrate resolve, significant falls crop when applying PMLA to decentralised protocols:

1. Absence of definition of "Sufficient Decentralisation." The PMLA's activity-based framework creates uncertainty when applied to decentralised blockchain protocols. The phrase "for or on behalf of another person in the course of business" raises three key questions:

   First, does deploying immutable smart contracts count as "providing services" if developers have no continuing operational role? Second, are users of autonomous protocols considered "customers" when no identifiable entity serves them? Third, does "course of business" require a profit motive and ongoing operations, or can it apply to one-time code deployment?

   These ambiguities create practical problems. Developers cannot determine when PMLA obligations apply to their activities, while the Financial Intelligence Unit-India (FIU-IND) lacks clear standards for deciding which protocols require enforcement action. This legal uncertainty undermines both compliance and consistent regulatory application.

2. Attribution of Liability Problem

   When a decentralised finance (DeFi) protocol facilitates money laundering, determining who should face legal consequences is challenging. Traditional concepts of agency, employment, and corporate structure do not apply easily to decentralised systems. Potential enforcement targets include:

   Developers: Those who wrote and deployed the smart contract code. The key question is whether they can be held liable for third-party misuse of their software. Recent U.S. cases involving Tornado Cash and Samourai Wallet indicate that developers with ongoing operational roles face

[21] Id. Rule 3

[22] Id. Rule 4

[23] Financial Action Task Force (FATF), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," October 2021, 58-64; Bank for International Settlements, "DeFi Risks and the Decentralisation Illusion," BIS Quarterly Review 21, 25-27 (December 2021)

[24] Cyril Amarchand Mangaldas, "FIG Paper (No. 39 – Series 3): Recent Learnings from the Indian Virtual Digital Assets Regulatory Space," September 24, 2024

prosecution risk. However, liability for simply deploying code without continued involvement remains legally uncertain.[25]

Front-End Operators: Entities running websites or applications that provide user access to protocols. These operators can control access through geo-blocking and transaction limits, and often collect fees. This makes them more practical regulatory targets than protocol developers. Recent UK and Singapore regulatory proposals focus on front-end operators as the primary enforcement point.[26]

DAOs and Governance Token Holders: Many DeFi protocols are governed by Decentralised Autonomous Organisations through token holder voting. Whether DAO members should bear liability is unclear, especially since DAOs may have thousands of passive token holders with no operational role. Critically, DAOs lack legal recognition as entities in India, creating a fundamental gap in the regulatory framework.

Liquidity Providers: Users who deposit assets to enable protocol operations and profit from all transactions, including illicit ones. However, this connection appears too remote for direct criminal liability—liquidity providers are passive investors without control over how their capital is used.

Infrastructure Providers: Oracles, validators, RPC nodes, and domain name providers all enable DeFi operations. While these could theoretically be enforcement points, imposing liability on neutral infrastructure providers for end-user conduct raises concerns about chilling effects on internet infrastructure development.

India's PMLA does not provide clear guidance on this attribution hierarchy. The statute assumes identifiable "designated directors" and "principal officers"—roles that may not exist in sufficiently decentralised protocols.

3. Extraterritorial Jurisdiction Ambiguity

India's assertion of jurisdiction over offshore platforms serving Indian users is doctrinally sound under the "effects doctrine"—if conduct produces substantial effects within India, Indian law can apply.[27] However, enforcing these laws against foreign developers and protocols presents practical difficulties:

Jurisdiction to Prescribe: India can claim prescriptive jurisdiction (authority to make laws applicable to foreign conduct) based on effects within its territory. PMLA Section 3 criminalises money laundering "wherever committed," indicating extraterritorial scope.[28]

[25] Press Information Bureau, Government of India, "Financial Intelligence Unit (FIU IND) issues notices for non-compliance to 25 offshore Virtual Digital Assets Service providers," September 10, 2025

[26] See discussion infra Part IV.

[27] Restatement (Fourth) of Foreign Relations Law S. 407 (Am. Law Inst. 2018)

[28] PMLA, S. 3 (criminalizing "whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime")

Jurisdiction to Enforce: India's ability to enforce judgments against foreign parties is limited without extradition treaties, Mutual Legal Assistance Treaties (MLATs), or the defendant's voluntary presence in India. Although India has MLATs with major jurisdictions, the process is slow—often taking years to execute.[29]

Jurisdiction to Adjudicate: Whether Indian courts can assert personal jurisdiction over foreign DeFi developers who have never visited India but whose protocols are accessible to Indian users remains unclear. Traditional jurisdictional analysis requires "minimum contacts" with the forum, which purely online services may lack under conventional doctrines.[30]

The challenge intensifies for protocols deliberately designed to be stateless. When developers are pseudonymous, located across multiple jurisdictions, and the protocol exists as immutable code on a global blockchain, traditional enforcement becomes nearly impossible.

4. Enforcement Mechanism Limitations

Even with clear jurisdictional authority, India faces practical enforcement challenges against decentralised protocols:

Smart Contract Immutability: Once deployed on a blockchain, immutable smart contracts cannot be shut down by any party, including governments. While India can block websites and seize domain names, users can still access protocols directly using blockchain interaction tools.[31]

DNS/IP Blocking Circumvention: VPNs, Tor, and decentralised VPN services enable users to bypass ISP-level blocking. India's attempts to block offshore exchanges have achieved partial success but remain far from comprehensive.[32]

Decentralised Front-Ends: Protocols like IPFS (InterPlanetary File System) allow front-end interfaces to be hosted in a distributed manner, making them resistant to takedowns. [33]

Pseudonymous Transactions: DeFi users transact with pseudonymous wallet addresses rather than identified accounts. While blockchain analysis can trace funds, identifying the individual controlling a wallet requires additional investigation.[34]

Asset Seizure Complexity: Seizing cryptocurrency held in non-custodial wallets is extremely difficult without access to private keys. Unlike bank accounts that can be frozen by court order, self-custody wallets can only be accessed with the private keys.[35]

These limitations do not make enforcement impossible, but they change the cost-benefit calculation. India must invest substantially in blockchain forensics capabilities, international cooperation, and novel legal approaches to effectively regulate DeFi.

[29] For analysis of MLAT delays in crypto cases, see Money Laundering Watch, "The Prosecution of Samourai Wallet Developers: Expanding the Reach of Crypto Enforcement," December 16, 2025

[30] International Shoe Co. v. Washington, 326 U.S. 310 (1945)

[31] Walch, supra note 1, at 45-47

[32] Global Legal Insights, supra note 2

[33] Harvey et al., supra note 11, at 89-92

[34] Chainalysis, "The Chainalysis 2024 Crypto Crime Report" (2024)

[35] Schär, supra note 10, at 164

5. DAO Legal Status Gap

Decentralised Autonomous Organisations (DAOs) govern many major DeFi protocols through tokenised voting mechanisms. A DAO is a governance framework encoded in smart contracts, where token holders vote on protocol parameters, treasury allocation, and development priorities.[36] DAOs present a fundamental challenge: they lack recognition as legal entities under Indian law. Without legal personality, DAOs cannot:

- Register with FIU-IND as a reporting entity
- Enter contracts or own property in their own name
- Appoint designated directors or principal officers
- Be sued or held liable for obligations
- Pay taxes on treasury revenues or protocol fees

This legal vacuum creates accountability gaps. When a DAO governs a protocol used for money laundering, determining who should be prosecuted is unclear. Individual token holders likely lack sufficient control to justify personal liability, yet the DAO as a whole may effectively control protocol operations.

IV. COMPARATIVE ANALYSIS: GLOBAL DEFENCE ENFORCEMENT PRECEDENTS

A. United States: Developer Liability Through Criminal Prosecution

United States v. Roman Storm (Tornado Cash)

Tornado Cash was an Ethereum-based cryptocurrency mixer that used cryptography to obscure transaction histories.[37] Users deposited funds into pooled smart contracts and withdrew to different addresses, breaking the on-chain link between sender and recipient. While serving legitimate privacy purposes, Tornado Cash allegedly processed over $1 billion in illicit proceeds, including $455 million from North Korea's Lazarus Group.[38]

Key Developments:

In August 2022, the U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash smart contract addresses—the first sanctions against autonomous code rather than individuals.[39] However, in November 2024, the Fifth Circuit ruled in Van Loon v. Department of the Treasury that OFAC exceeded its authority by sanctioning immutable smart contracts, as they are not "property" under the International Emergency Economic Powers Act.[40] Following this ruling, OFAC delisted the smart contracts in March 2025, though developer Roman Semenov remained sanctioned.[41]

[36] For detailed analysis of Uniswap's structure, see Dirk A. Zetzsche et al., "Decentralized Finance," 6 Journal of Financial Regulation 172, 185-188 (2020)

[37] U.S. Department of Justice, "Founder of Tornado Cash Crypto Mixing Service Convicted of Knowingly Transmitting Criminal Proceeds," August 6, 2025

[38] Id.

[39] U.S. Treasury Department, Office of Foreign Assets Control, designation of Tornado Cash smart contracts, August 8, 2022

[40] Van Loon v. Department of the Treasury, 103 F.4th 353, 360-365 (5th Cir. 2024)

[41] DeFi Education Fund, "US v. Storm: Background & Timeline," October 15, 2025, https://www.defieducationfund.org/us-v-storm-background-timeline/

In August 2023, the Department of Justice indicted developers Roman Storm and Roman Semenov on conspiracy charges, including money laundering, operating an unlicensed money transmitting business, and violating OFAC sanctions.[42] After a four-week trial in August 2025, a jury convicted Storm of operating an unlicensed money transmitting business but deadlocked on the money laundering and sanctions charges.[43]

Legal Arguments:

The prosecution argued Storm was not merely writing code but actively operating a business. Evidence showed Storm controlled the tornado. cash website (used by 96% of users), updated it approximately 250 times, collected fees from protocol usage, and continued operations despite knowing criminals were using the service extensively.[44]

The defence compared Tornado Cash to privacy tools like encrypted messaging apps and VPNs, arguing that deploying open-source code is protected speech and that developers lacked control over user behaviour once smart contracts were deployed.[45]

Implications:

The split verdict reveals legal uncertainty. The conviction on unlicensed money transmitting suggests that controlling access interfaces and collecting fees constitutes a business operation. However, the deadlock on money laundering indicates hesitation about imputing criminal intent for third-party misuse. This suggests developers who maintain operational roles face liability, while pure code deployment without continued involvement may not constitute facilitation of subsequent crimes.

United States v. Rodriguez and Hill (Samourai Wallet)

Samourai Wallet was a Bitcoin privacy wallet offering "Whirlpool" (a CoinJoin mixing service) and "Ricochet" (transaction hopping to obscure payment origins).[46] Unlike Tornado Cash's immutable smart contracts, Samourai required a centralised coordinator service operated by developers and was actively maintained through regular updates.[47]

In April 2024, the Department of Justice arrested CEO Keonne Rodriguez and CTO William Lonergan Hill, charging them with conspiracy to operate an unlicensed money transmitting business, money laundering, and sanctions violations. Prosecutors alleged Samourai facilitated over $2 billion in transactions, including approximately $237 million in illicit proceeds.[48]

[42] Indictment, United States v. Storm, Case No. 1:23-cr-00399 (S.D.N.Y. filed Aug. 23, 2023)
[43] Money Laundering Watch, "Tornado Cash Jury Deadlocked on Most Serious Charges, but Convicted Founder Roman Storm on Conspiracy to Operate an Unlicensed Money Transmitting Business," August 26, 2025
[44] Government's Post-Trial Brief, United States v. Storm, Case No. 1:23-cr-00399 (S.D.N.Y. filed Nov. 13, 2025)
[45] CoinDesk, "Roman Storm Trial: Is Coding A Crime? The Tornado Cash Court Battle Intensifies," July 25, 2025.
[46] CoinDesk, "Roman Storm Trial: Is Coding A Crime? The Tornado Cash Court Battle Intensifies," July 25, 2025.
[47] Money Laundering Watch, supra note 31
[48] U.S. Department of Justice, supra note 48

In July 2025, both defendants pleaded guilty to conspiracy to operate an unlicensed money transmitting business, with money laundering charges dropped.[49] In November 2025, Rodriguez was sentenced to five years and Hill to four years, with both forfeiting over $6.3 million in fees and paying $250,000 fines each.[50]

Prosecution Evidence:

The case differed from Tornado Cash through direct evidence of criminal intent. Rodriguez explicitly told users on dark web forum Dread that Samourai was ideal for "cleaning dirty BTC" to make funds "untraceable."[51] He publicly encouraged hackers to "feed" stolen funds into Whirlpool and described the mixing process in private messages as "money laundering for bitcoin."[52] Marketing materials explicitly acknowledged "Dark/Grey market participants" as target users.[53]

FinCEN Guidance Contradiction:

The prosecution proceeded despite FinCEN guidance stating that non-custodial wallet providers do not require money transmitter licenses. FinCEN's 2019 guidance indicated that developers providing software without asset custody are not money services businesses.[54] reaffirmed in 2024 when proposed KYC rules for non-custodial wallets were withdrawn.[55] Despite this, prosecutors proceeded after reportedly receiving confirmation from FinCEN that CoinJoin services do not constitute money transmission,[56] creating a situation where defendants faced criminal charges for conduct the regulatory agency deemed unlicensed.

Implications for India:

The Samurai convictions demonstrate several key principles. First, centralised control points create enforcement vulnerabilities—the coordinator service provided clear evidence of operational control. Second, intent evidence is crucial; direct statements showing knowledge and encouragement of criminal use strengthen prosecution dramatically. Third, regulatory clarity is essential; the FinCEN contradiction highlights the need for clear, binding guidance from FIU-IND before pursuing criminal prosecutions. Finally, the plea agreements reflect legal uncertainty about liability for privacy tools subsequently misused by criminals.

[49] U.S. Department of Justice, "Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty," August 6, 2025
[50] U.S. Department of Justice, supra note 48
[51] Id.
[52] Id.
[53] Id.
[54] Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," FIN-2019-G001, May 9, 2019
[55] Money Laundering Watch, supra note 31
[56] Id.

B. European Union: Markets in Crypto-Assets Regulation (MiCA)

MiCA's Scope and DeFi Exemption

The European Union adopted the Markets in Crypto-Assets Regulation, which took effect in phases during 2024-2025.[57] Unlike the U.S. enforcement approach, the EU pursued comprehensive ex-ante regulation through detailed statutory requirements.

MiCA applies to crypto-asset service providers (CASPs) offering services to EU persons, including operating trading platforms, exchanging crypto-assets, providing custody services, providing advice, and placing crypto-assets.[58]

However, MiCA includes a critical exemption: Recital 22 excludes "fully decentralised" services without intermediaries, reasoning that "there is no identifiable person responsible for such service to whom the obligations [can] be imposed."[59] The rationale is that traditional financial regulation assumes identifiable responsible parties; when services operate autonomously without controlling entities, the regulatory model breaks down.

Implementation Challenges

MiCA's decentralisation exemption has proven problematic. The regulation provides no clear definition of "fully decentralised," and regulatory guidance from the European Securities and Markets Authority has been limited. Different member states have adopted varying interpretations, creating regulatory arbitrage opportunities.[60]

Numerous protocols have claimed to be "fully decentralised" to avoid obligations, though most retain centralised elements like foundations, treasuries, or developer teams. Without clarity on what constitutes sufficient decentralisation, enforcement authorities struggle to determine which protocols require compliance and which genuinely fall outside regulatory scope.

Initial discussions of "MiCA II" focused on DeFi losing momentum by late 2025 as policymakers recognised the complexity of regulating truly decentralised systems.[61]

Related EU Frameworks

The Digital Operational Resilience Act (DORA) imposes cybersecurity and operational resilience requirements on financial entities.[62] DeFi protocols relying on third-party infrastructure may face DORA obligations even if exempt from MiCA.

[57] Regulation (EU) 2023/1114 (MiCA)
[58] Id. Art. 3(1)(15)
[59] Id. Recital 22
[60] European Banking Authority, "Report on the Implementation of MiCA," December 2025
[61] Id.
[62] Regulation (EU) 2022/2554 (DORA)

The EU's forthcoming harmonised Anti-Money Laundering Regulation will impose direct obligations on crypto-asset service providers, potentially capturing DeFi components currently outside MiCA's scope.[63]

Lessons for India

The EU experience offers cautionary lessons. Exempting "fully decentralised" protocols incentivises superficial decentralisation—projects claim decentralisation to avoid regulation while retaining practical control. India's activity-based approach focusing on "providing services for or on behalf of another person" may prove more effective than structure-based exemptions. Rather than asking "is this decentralised?" (which can be manipulated), the functional question "is someone providing financial services to users?" is harder to evade. India should establish clear, objective criteria for sufficient decentralisation early in the regulatory process to avoid the EU's definitional ambiguity.

V. CONCLUSION: INDIA'S PATH FORWARD

In contrast to the traditional financial framework, decentralised finance deliberately eliminates recognisable intermediaries that can be held accountable. Hence, the conventional frameworks that were designed for banks and other financial institutions cannot be applied to DeFi.

At the same time, DeFi poses the great threat of becoming the primary channel for money laundering, financial fraud, terrorist funding and all types of criminal activities. Therefore, it cannot be left unregulated.

Under PMLA, India’s activity-based approach doesn’t focus on fully-centralised protocols, which is unlike the EU’s MiCA. India needs protocols that provide comprehensive financial integrity with centralised control points; acknowledge technical limitations while maintaining user liability; cross-border enforcement; all the above, while providing real-time monitoring, but also considering privacy.

[63] Proposed Regulation on the Prevention of the Use of the Financial System for Money Laundering or Terrorist Financing, COM(2021) 420 final