

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Regulatory Ambiguity in Decentralized Finance (DeFi) and Crypto Assets

G.V. KAMALESHWARAN*

ABSTRACT

This paper addresses the conflict between conventional statutory regulation and the decentralized mechanisms of Decentralized Finance (DeFi) and crypto-asset markets. Traditionally, financial regulation has been centralized through banks, brokerages and clearinghouses and has imposed anti-money laundering (AML) requirements, disclosure responsibilities and fiduciary duties. Permissionless blockchain networks can instead use autonomous and self-executing smart contracts, reducing the institutional control structure through which regulators normally intervene. The paper examines the European Union's Markets in Crypto-Assets Regulation (MiCA), the United States' use of existing securities and commodities law and India's tax and compliance-based approach. It argues that inconsistent token classification, unclear legal terminology and uncertainty about the identity of the responsible actor can encourage jurisdictional arbitrage. The major legal issues include token classification, inter-agency jurisdictional conflicts, the absence of an identifiable and regulable person in some decentralized systems, unclear fiduciary duties and consumer protection gaps. The paper finds that an activity- and risk-based approach, in combination with strong global coordination, can create a more complete framework for regulating crypto assets without reliance on technological labels.

Keywords: *Decentralized Finance (DeFi), Crypto Assets, Regulatory Ambiguity, Blockchain Technology, Smart Contracts, Token Classification, Anti-Money Laundering (AML)*

I. INTRODUCTION

Decentralized Finance (DeFi) is a term used to describe blockchain-based applications that replicate the role of traditional financial intermediaries, such as banks and brokerages, in activities like lending and borrowing. DeFi meets current needs in the financial market through smart contracts, which can readily be deployed on a blockchain network. Traditional financial regulation depends on identifiable entities that can be licensed, monitored and held accountable for their compliance with AML and disclosure obligations, consumer protection and fiduciary duties. DeFi challenges this framework because transactions can execute automatically through

* Author is a Student at Shanmugha Arts, Science, Technology and Research Academy (SASTRA Deemed University), Thanjavur, Tamil Nadu, India.

smart contracts, while developers, users, token holders and protocol operators are located in different jurisdictions. This creates numerous legal ambiguities concerning tokens, regulatory duties, jurisdiction, consumer rights and AML/CFT regulation. The absence of a clear intermediary in some DeFi systems makes the enforcement of existing financial legislation more complicated. Regulatory frameworks vary from region to region: the European Union has adopted the Markets in Crypto-Assets Regulation (MiCA), while in the United States crypto-assets are dealt with mainly under pre-existing securities and commodities laws. In India, the focus is primarily on taxation and compliance concerning virtual digital assets, a concentration that may leave regulatory gaps and create opportunities for jurisdictional arbitrage.

There is an urgent need to assess whether the present legal framework is adequate to regulate decentralized financial services. It is equally important to investigate how regulation can safeguard both the financial system and its users while fostering technological advancement. This study analyses the regulatory ambiguities associated with DeFi and crypto-assets and proposes ways to organise effective oversight of these emerging sectors.

A. Research objectives

This paper addresses (a) the meaning and architecture of Decentralized Finance (blockchain networks, smart contracts, permissionless systems); (b) the legal uncertainty surrounding crypto-assets and token classification, and the challenges of AML/CFT, consumer protection, fiduciary duties, liability and jurisdiction; (c) how the regulatory frameworks of the European Union, the United States and India relate to the decentralized and cross-border nature of DeFi; (d) the judicial, regulatory and enforcement developments concerning crypto-assets and decentralized organizations; and (e) the legal and regulatory measures necessary to close regulatory gaps while still enabling technological innovation, on an activity-based and risk-based approach.

B. Scope and methodology

This study employs a doctrinal and comparative approach to investigate the regulatory ambiguities associated with Decentralized Finance (DeFi) and digital assets. It addresses the legal nature and functions of DeFi, token classification, obligations concerning anti-money laundering and counter-terrorism financing (AML/CFT), consumer protection, fiduciary duties, liability, jurisdictional challenges and instances of regulatory arbitrage. The analysis compares the regulatory frameworks that govern crypto-assets and decentralized financial activities in the European Union, the United States and India. The study draws on primary legal materials, including statutes, regulations, judicial rulings and regulatory guidelines, alongside institutional

reports from organizations such as the Financial Stability Board (FSB) and the Financial Action Task Force (FATF). It also draws on secondary sources, including scholarly articles, books, research studies and legal analyses. The methodology compares different regulatory approaches in order to identify legal deficiencies, inconsistencies and obstacles in applying existing financial legislation to decentralized systems.

II. CONCEPTUAL BACKGROUND: DECENTRALIZED FINANCE AND CRYPTO ASSETS

A. Meaning and evolution of DeFi

Decentralized Finance (DeFi) is not a single legal category but an ecosystem of blockchain-based applications that provide financial functions traditionally performed by intermediaries such as banks and brokers. It employs smart contracts, decentralized applications and permissionless blockchain networks to enable lending, borrowing, trading, derivatives, staking and asset management.

DeFi originated in blockchain technology and grew with the development of programmable platforms, including Ethereum, that let users automate financial transactions through smart contracts. According to the Financial Stability Board (FSB), DeFi, despite reducing reliance on traditional intermediaries, does not eliminate financial risk: in attempting to replicate functions of the traditional financial system by different technological means, it inherits, and may amplify, the same vulnerabilities.¹ This is highly relevant to legal risks concerning regulatory responsibility, consumer protection, AML/CFT, liability and jurisdiction.

B. Blockchain, smart contracts and permissionless networks

Blockchain technology functions as a decentralized digital ledger that records transactions across a network without the need for a central authority. Smart contracts are automated programs embedded in a blockchain that execute specified actions when predetermined conditions are fulfilled. Permissionless networks enable users to transact without requiring approval from any central entity. This is a major aspect of Decentralized Finance (DeFi), allowing users to lend, borrow, trade and transfer assets without traditional intermediaries. However, the decentralization characteristic of this technology does not mean that there are no legal responsibilities. Even protocols that use automated smart contracts have identifiable people or organizations that can influence development, governance, software upgrades, treasury management and user experience. To address liability, regulation, consumer protection,

¹ FIN. STABILITY BD., THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE 1 (Feb. 16, 2023), <https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/>.

and compliance with anti-money laundering (AML) and countering the financing of terrorism (CFT) procedures, it is therefore necessary to identify who has control over, or influence on, a DeFi protocol.

C. Major DeFi activities

DeFi systems offer a variety of financial services, including decentralized exchanges, lending and borrowing, derivatives, staking, liquidity provision and asset management. Decentralized exchanges enable users to trade crypto-assets directly through protocols rather than through a centralized exchange. DeFi lending and borrowing platforms allow users to supply digital assets as liquidity and earn returns, or to obtain loans against collateral. Staking and liquidity provision allow users to commit assets to blockchain networks or DeFi protocols and earn rewards. Derivatives and other financial products can offer exposure to the value of crypto-assets through automated protocols. These activities can improve accessibility, transparency and automation, but they also raise legal and regulatory issues relating to market manipulation, consumer protection, loss of funds, smart-contract vulnerabilities, AML/CFT compliance, disclosure and regulatory responsibility. Understanding the nature and risks of each DeFi activity is therefore essential to determining the right legal and regulatory framework.

D. Crypto-asset classification

Crypto-asset classification is a major cause of regulatory uncertainty, because a token may have payment, utility, governance or investment characteristics, which may change over time, so that the same token may attract different legal classifications. Classification matters because it determines the applicable licensing, disclosure, taxation, investor protection and AML/CFT requirements. In the European Union, MiCA distinguishes asset-referenced tokens, e-money tokens and other crypto-assets.² In the United States, classification turns mainly on the characteristics of the asset under general securities and commodities law, while in India the statutory concept of a virtual digital asset is applied mainly for taxation and compliance purposes. Legal definitions of digital assets thus differ widely across jurisdictions. These divergent approaches can lead to legal uncertainty and regulatory arbitrage, which is why a clear, function-based classification is important for effective regulation.

² Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, art. 3(1)(5)–(7), tits. II–IV, 2023 O.J. (L 150) 40 [hereinafter MiCA], <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>.

III. REGULATORY CHALLENGES IN DECENTRALIZED FINANCE

A. Traditional financial regulation and the intermediary model

Traditional financial regulation is based on an intermediary model, in which identifiable institutions such as banks, brokers and exchanges are responsible for licensing, supervision, record-keeping, consumer protection and AML/CFT compliance. DeFi challenges this model because the same financial functions are performed by smart contracts and decentralized protocols without a clearly identifiable intermediary. A DeFi protocol may be developed in one jurisdiction but run by participants in many countries and be accessible to users around the world. This makes it difficult to know who is responsible, which law applies and which regulator has jurisdiction. The consequence is that economically similar activities may be regulated differently merely because of the technology used (for example, smart contracts and decentralized protocols). At the same time, imposing regulatory obligations on every person involved in a decentralized protocol may be unnecessarily burdensome and may suppress technological innovation. The challenge, therefore, is to identify the persons who exercise meaningful control or perform regulated functions and to regulate them according to the actual activity and risk involved. The FSB supports an activity-based and risk-based approach, under which similar activities and risks are regulated alike.³

B. The challenge of decentralization: identifying the regulated entity

A major hurdle in overseeing decentralized finance (DeFi) lies in determining the legally accountable individual or organization. In contrast to conventional financial systems, DeFi involves a diverse array of participants, such as developers, members of decentralized autonomous organizations (DAOs), governance token holders, protocol operators and front-end service providers, which makes accountability difficult to ascertain. Decentralization is a characteristic feature, but it does not absolve individuals of legal responsibility; liability instead turns on each person's role, degree of control and engagement in regulated activities.

The Ooki DAO case illustrates the issue. There, a U.S. federal court held that Ooki DAO was a "person" under the Commodity Exchange Act and could be held liable for violations of that Act.⁴ The ruling underscores that decentralized entities may be subject to existing financial

³ See FIN. STABILITY BD., THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE, *supra* note 1, at 3 (calling for "appropriate regulation of activities giving rise to similar risks"); FIN. STABILITY BD., HIGH-LEVEL RECOMMENDATIONS FOR THE REGULATION, SUPERVISION AND OVERSIGHT OF CRYPTO-ASSET ACTIVITIES AND MARKETS: FINAL REPORT 5 (July 17, 2023), <https://www.fsb.org/uploads/P170723-2.pdf> (Recommendation 2, applying the principle of "same activity, same risk, same regulation").

⁴ *CFTC v. Ooki DAO*, No. 3:22-cv-05416-WHO (N.D. Cal. June 8, 2023) (order granting default judgment); see Press Release No. 8715-23, Commodity Futures Trading Comm'n, Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory (June 9, 2023), <https://www.cftc.gov/Press-Release/2023/06/09/8715-23>.

regulation, and it raises questions about the liability of DAOs, the obligations of developers, governance participation and enforcement strategy. Regulation of DeFi should accordingly focus on actual roles, significant control and the related risks, rather than on decentralization as such.

IV. COMPARATIVE ANALYSIS: EU, US AND INDIA

A. European Union

Before MiCA, the regulation of crypto-assets across the 27 member states of the EU was highly fragmented. The only layer of harmonization came from the Fifth Anti-Money Laundering Directive (AMLD5), which brought providers of exchange services between virtual and fiat currencies and custodian wallet providers under AML/CFT obligations,⁵ but left issuance, trading and consumer protection largely unregulated at Union level. This fragmentation led to supervisory arbitrage, as crypto firms set up in the member states with the lightest licensing regimes and passported services across the bloc. The collapse of major stablecoin and exchange projects in 2022, notably Terra/Luna in May and FTX in November, added urgency to the adoption of a comprehensive framework: MiCA was adopted in 2023 and has applied in full since 30 December 2024, its rules on asset-referenced and e-money tokens having applied from 30 June 2024.⁶ MiCA imposes obligations on issuers of asset-referenced tokens and e-money tokens, establishes an authorization and conduct regime for crypto-asset service providers (custody, exchange, trading platforms and advice) and lays down market abuse rules modelled on the Market Abuse Regulation. Key to the present discussion is Recital 22 of MiCA, which states that crypto-asset services provided in a fully decentralized manner without any intermediary should not fall within the scope of the Regulation,⁷ effectively carving most DeFi protocols, DAOs and automated market makers out of its core obligations. This structural gap is the core of the legal problem of DeFi under EU law. MiCA's obligations attach to identifiable issuers and crypto-asset service providers (CASPs), and in the case of non-custodial protocols running on smart contracts and DAOs there is typically no such entity. The compliance infrastructure of authorization, disclosure and capital requirements therefore does not reach activities such as decentralized lending, automated market-making and the issuance of algorithmic stablecoins. A related problem arises in hybrid structures: many DeFi front ends are

[.gov/PressRoom/PressReleases/8715-23](https://ec.europa.eu/pressroom/pressreleases/8715-23).

⁵ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU, art. 1(1)(c), 2018 O.J. (L 156) 43, <https://eur-lex.europa.eu/eli/dir/2018/843/oj>.

⁶ MiCA, *supra* note 2, art. 149(2)–(3).

⁷ MiCA, *supra* note 2, recital 22.

run by identifiable companies even where the underlying protocol is decentralized, and because “sufficient decentralization” has no legal definition, disputes arise as to whether a given front-end operator should itself be treated as a CASP. The current legal position is provisional by design. On 20 May 2026 the European Commission launched a targeted consultation on the review of MiCA, comprising eighty-six questions and dealing specifically with DeFi, staking, lending and borrowing, and NFTs.⁸ The Commission must report to the European Parliament and the Council by 30 June 2027, accompanied where appropriate by a legislative proposal; commentators already refer to the review as “MiCA 2”.⁹ Finally, even where a DeFi front-end operator can be located, enforcing obligations against protocols with globally dispersed validators, governance token holders and open-source contributors presents real jurisdictional and practical difficulties.

B. United States

U.S. crypto regulation, by contrast, has been shaped almost entirely by the application of existing laws, primarily the Securities Act of 1933, the Securities Exchange Act of 1934 and the Commodity Exchange Act; the principal exception is the GENIUS Act of July 2025, which created a federal regime for payment stablecoins.¹⁰ The central analytical tool has been the *Howey* test for what constitutes an “investment contract”, and therefore a security, first articulated by the Supreme Court in *SEC v. W.J. Howey Co.*¹¹ Treating many tokens and platform activities as unregistered securities offerings, the SEC pursued enforcement through the 2010s and early 2020s, suing Coinbase and Binance in June 2023¹² and scrutinising DeFi-related businesses such as Uniswap Labs; both suits were dismissed by stipulation in 2025.¹³ The enforcement-based approach was widely criticized as “regulation by enforcement”, with inconsistent results and a tendency to push activity offshore to jurisdictions with better-calibrated laws. Following a change in SEC leadership and a shift in the policy environment,

⁸ EUR. COMM’N, Consultation Document: Targeted Consultation on the Review of Regulation on the Markets in Crypto-Assets (MiCA) pt. 4 (May 20, 2026), https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-review-mica-regulation_en; Stuart Davis et al., *MiCA Review: European Commission Launches Consultation on EU Cryptoasset Regulatory Framework*, JD SUPRA (June 2, 2026), <https://www.jdsupra.com/legalnews/mica-review-european-commission-1706716/>.

⁹ MiCA, *supra* note 2, art. 140(1); see CAHILL GORDON & REINDEL LLP, *MiCA, The Sequel: Brussels Reopens the EU’s Crypto Rulebook* (June 18, 2026), <https://www.cahill.com/publications/client-alerts/2026-06-18-mica-the-sequel-brussels-reopens-the-eu-crypto-rulebook> (describing the review as “informally known as ‘MiCA 2’”).

¹⁰ Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Pub. L. No. 119-27, 139 Stat. 419 (2025).

¹¹ *SEC v. W.J. Howey Co.*, 328 U.S. 293, 298–99 (1946).

¹² Complaint, *SEC v. Binance Holdings Ltd.*, No. 1:23-cv-01599 (D.D.C. June 5, 2023); Complaint, *SEC v. Coinbase, Inc.*, No. 1:23-cv-04738 (S.D.N.Y. June 6, 2023).

¹³ Press Release No. 2025-47, Sec. & Exch. Comm’n (Feb. 27, 2025), <https://www.sec.gov/newsroom/press-releases/2025-47> (Coinbase); Litigation Release No. 26316, Sec. & Exch. Comm’n (May 29, 2025), <https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26316> (Binance).

on 17 March 2026 the SEC, joined by the CFTC, issued an interpretive release.¹⁴ The release divides crypto-assets into five categories: digital commodities, digital collectibles, digital tools, stablecoins and digital securities. Under this interpretation the first three categories, and payment stablecoins issued under the GENIUS Act, are not securities, although a non-security crypto-asset may become subject to an investment contract when it is offered with promises of essential managerial efforts. The interpretation also provides that protocol mining, protocol staking and the wrapping of a non-security crypto-asset do not involve the offer and sale of a security, and that certain airdrops involve no “investment of money”.¹⁵ The CFTC, for its part, states that it will administer the Commodity Exchange Act consistently with the interpretation.¹⁶

This interpretation still leaves many questions unanswered. It does not lay down rules, and the line between a “digital commodity” and a “digital security” remains a matter of nuanced factual analysis under the *Howey* test. A crypto-asset may therefore move into and out of an investment contract over its life cycle, with different compliance consequences at each stage. The interpretation is also an agency position rather than a statute: a future Commission may revisit it, and it may be limited or overturned in litigation. Until Congress enacts market-structure legislation, its effect on the market will remain provisional.¹⁷ Another problem is DeFi protocol liability. The interpretation addresses mining and staking, but it does not say who is responsible where an unregistered platform is concerned: the DAO itself, token holders, front-end developers or validators. Enforcement against the developers of Tornado Cash shows the authorities’ willingness to pursue the creators of non-custodial code, and raises difficult constitutional questions about whether code is speech. In August 2025 a jury convicted Tornado Cash co-founder Roman Storm of conspiring to operate an unlicensed money-transmitting business but could not agree on the money-laundering and sanctions counts,¹⁸ while the Fifth Circuit held that Tornado Cash’s immutable smart contracts were not “property” that the Treasury could sanction.¹⁹ State money-transmission licensing rules add a further layer,

¹⁴ Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets, Securities Act Release No. 11412, Exchange Act Release No. 105020, 91 Fed. Reg. 13714 (Mar. 23, 2026); see Press Release No. 2026-30, Sec. & Exch. Comm’n (Mar. 17, 2026), <https://www.sec.gov/newsroom/press-releases/2026-30-sec-clarifies-application-federal-securities-laws-crypto-assets>.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ See Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Cong. (as passed by House, July 17, 2025) (not enacted); see TROUTMAN PEPPER LOCKE, In the Wake of CLARITY Act’s Failure, Agencies Move Forward Without Congressional Action or Certainty (Sept. 25, 2026), <https://www.troutman.com/insights/in-the-wake-of-clarity-acts-failure-agencies-move-forward-without-congressional-action-or-certainty/> (Senate rejected cloture on the motion to proceed, 49–50, on Sept. 15, 2026).

¹⁸ *United States v. Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y. Aug. 6, 2025) (partial jury verdict).

¹⁹ *Van Loon v. Dep’t of the Treasury*, 122 F.4th 549 (5th Cir. 2024).

differing from state to state on top of the federal regime, and their application to non-custodial software that holds no user funds remains uncertain. Consumer protection laws, finally, presuppose a centralized intermediary, a model ill-suited to self-executing smart contracts with no identifiable counterparty against whom redress can be sought.

C. India

India's regulatory journey has been notably turbulent. In April 2018 the Reserve Bank of India issued a circular prohibiting regulated entities from dealing in virtual currencies or providing services to those who did.²⁰ In *Internet and Mobile Association of India v. RBI* (2020), the Supreme Court held that the circular imposed a disproportionate, and therefore unreasonable, restriction on the freedom of trade under Article 19(1)(g) of the Constitution.²¹ India has no crypto-specific statute and has instead adopted a taxation-based approach. The Finance Act, 2022 inserted section 2(47A) into the Income-tax Act, 1961 to define "virtual digital assets" (VDAs), imposed a flat tax of 30% on gains from the transfer of VDAs without set-off of losses (section 115BBH), and required tax deduction at source of 1% on such transfers (section 194S).²² The Income-tax Act, 2025, in force from 1 April 2026, replaced the 1961 Act and carries the same regime forward.²³ In the AML/CFT space, a government notification of 7 March 2023 brought VDA-related activities under the Prevention of Money-Laundering Act, 2002, so that exchanges and other VDA service providers became "reporting entities" required to register with FIU-IND, conduct customer due diligence, maintain records and file suspicious transaction reports.²⁴ FIU-IND,²⁵ the nodal agency under the PMLA, has since substantially revised its AML/CFT guidelines for reporting entities in the VDA sector. The most recent significant update, of 8 January 2026, introduces stronger onboarding authentication, such as live-selfie liveness checks and geolocation capture; multi-layer KYC using the PAN and a secondary identity document; periodic KYC updating according to the client's risk category; enhanced due diligence for clients connected with tax havens or with jurisdictions on the FATF

²⁰ RESERVE BANK OF INDIA, Prohibition on Dealing in Virtual Currencies (VCs), RBI/2017-18/154, DBR.No.BP.BC.104/08.13.102/2017-18 (Apr. 6, 2018), <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243>.

²¹ *Internet & Mobile Ass'n of India v. Reserve Bank of India*, (2020) 10 SCC 274 (India) (W.P. (C) No. 528 of 2018, decided Mar. 4, 2020).

²² The Income-tax Act, 1961, No. 43, Acts of Parliament, 1961, §§ 2(47A), 115BBH, 194S (India), as inserted by the Finance Act, 2022, No. 6, Acts of Parliament, 2022 (India).

²³ The Income-tax Act, 2025, No. 30, Acts of Parliament, 2025, §§ 1(3), 2(111), 194(1) tbl. sl. no. 4, 393(1) tbl. sl. no. 8(vi) (India), <https://egazette.gov.in/WriteReadData/2025/265620.pdf>.

²⁴ MINISTRY OF FINANCE (DEPARTMENT OF REVENUE), Notification S.O. 1072(E) (Mar. 7, 2023), issued under The Prevention of Money-Laundering Act, 2002, No. 15, Acts of Parliament, 2003, § 2(1)(sa)(vi) (India), <https://egazette.gov.in/WriteReadData/2023/244184.pdf>.

²⁵ Yashdeep Agarwal, *FIU-IND New KYC & AML Guidelines for VDASPs: Jan 2026*, SIGNZY (Jan. 27, 2026), <https://www.signzy.com/blogs/FIU-IND-KYC-crypto-guidelines-2026>.

grey and black lists; the discouragement of opaque instruments such as ICOs and ITOs; a bar on facilitating anonymity-enhancing mixers and tumblers; and a five-year record-retention requirement.²⁶ Most importantly, India has not legislated a general legal status for crypto-assets or a licensing regime for exchanges, and has not legislated directly for DeFi, staking or DAOs.

Several legal issues follow. First, VDAs are recognized in India for tax and AML purposes, but no statute settles whether, for the purposes of general civil law, a crypto-asset is property, currency, a commodity or a security. Courts will still have to deal with contract, insolvency and succession questions arising from DeFi positions. Secondly, the PMLA reporting-entity model assumes a central intermediary that can carry out KYC, monitor transactions and report suspicious transactions. That assumption does not hold for non-custodial DeFi protocols such as decentralized exchanges, lending pools and DAO-governed treasuries. Thirdly, although the statutory definition of a VDA is broad, neither the 2023 extension of the PMLA nor the FIU-IND guidelines of January 2026 maps clearly onto truly decentralized activity or DeFi-native tokens. Regulatory authority is also divided among several agencies: the Income Tax Department administers taxation, the Ministry of Finance and FIU-IND administer AML/CFT requirements, and the Reserve Bank of India (RBI) has flagged concerns about payment channels while promoting its own central bank digital currency, the e-rupee. No single regulator oversees crypto markets or exchanges, or the risks specific to DeFi such as smart-contract failure or oracle manipulation. In practice, enforcement has proceeded through show-cause notices and the blocking of access to unregistered offshore VDA service providers.²⁷ That approach is of little use against a wholly protocol-based DeFi arrangement with no corporate entity anywhere. Furthermore, no bill on the comprehensive regulation of crypto-assets or DeFi has been introduced in Parliament, leaving market participants uncertain about the future direction of Indian law.

²⁶ AZB & PARTNERS, Update: AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets, 2026 (Jan. 14, 2026), <https://www.azbpartners.com/wp-content/uploads/2026/01/Client-Update-FIU-Guidelines-2026-AZB-January-14-2026.pdf>; *India Tightens Crypto Noose: Live Selfies, Geo-tagging Now Mandatory for Users*, THE WEEK (Jan. 11, 2026) (PTI), <https://www.theweek.in/wire-updates/business/2026/01/11/india-tightens-crypto-noose-live-selfies-geo-tagging-now-mandatory-for-users.html>.

²⁷ Press Release, Ministry of Finance, Financial Intelligence Unit India (FIU IND) Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers (VDA SPs) (Dec. 28, 2023), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372>.

D. Comparative table: DeFi and crypto-asset regulation in the EU, US and India

	EU (European Union)	US (United States)	India
Approach	One dedicated law (MiCA)	Old securities/commodities laws, reinterpreted	Tax and anti-money-laundering rules only
Main law	MiCA (adopted 2023; fully applicable from 30 December 2024)	Securities Act, Exchange Act, CEA + 2026 SEC-CFTC guidance	Income-tax Act (VDA provisions, 2022); PMLA (VDA notification, 2023)
Who regulates	ESMA, EBA, national regulators	SEC and CFTC (split)	FIU-IND, tax department, RBI; no single body
How DeFi is treated	Left out if truly decentralised	Not mentioned directly	Not mentioned directly
Biggest problem	No issuer to regulate in DeFi	Classification keeps shifting; no clear DAO liability	No law says what a crypto-asset is legally
What's changing now	MiCA review, possibly "MiCA 2" by 2027	New five-category token taxonomy (March 2026)	Stricter KYC/AML rules (January 2026)
Enforcing against DeFi	Hard: no single company to hold responsible	State rules add confusion on top of federal rules	Mostly blocking access to offshore platforms

Table 1: DeFi and crypto-asset regulation in the EU, US and India

V. RECOMMENDATIONS

India's core legal gaps, namely the missing token taxonomy, inter-agency conflict, the absence of a regulable person in decentralized systems and weak consumer protection, all have partial solutions already tested abroad. On token classification, for instance, India's only definition of a VDA comes from tax law, and it does not distinguish a payment token from a governance token or from a security-like token. MiCA's three-category model (asset-referenced tokens, e-money tokens and other crypto-assets) and the US functional five-category taxonomy both point to a viable solution: classify a token by what it does rather than by what it is called, and build this into a dedicated VDA law instead of relying on inference from the income-tax statute. The following recommendations adapt those lessons to India's context.

A. Adopt a functional token taxonomy

India's sole definition of a VDA comes from tax law and does not differentiate between types of token. Both the MiCA categories²⁸ and the US five-part taxonomy are function-based.²⁹ A similar functional taxonomy should be included in a dedicated VDA statute in India.

²⁸ MiCA, *supra* note 2, art. 3(1)(5)–(7).

²⁹ Securities Act Release No. 11412, *supra* note 14.

B. Establish a binding inter-regulatory coordination mechanism

Authority in India is divided among the RBI, SEBI, the tax department and FIU-IND, with no lead regulator. In the United States, the SEC issued its 2026 interpretation jointly with the CFTC, which undertook to administer the Commodity Exchange Act consistently with it. India should establish an equivalent standing inter-regulatory committee with binding authority over classification.

C. Control the nearest identifiable point of centralization

Neither the EU nor the US has fully solved the problem of identifying decentralized actors, but both regulate the nearest identifiable point of centralization: front-end operators, fee-collecting developers and fiat on- and off-ramps. Rather than attempting to regulate the protocol itself, India's PMLA model should follow the same activity-based standard.

D. Embrace fiduciary and consumer protection standards

India has neither MiCA-style custody and fair-dealing rules nor a US-style investor-protection overlay. Extending FIU-IND's existing KYC/AML framework to custody segregation, risk disclosure and grievance redressal would fill this gap with little new architecture.

E. Summary

India need not choose between a MiCA-type statute and a US-type interpretive approach. The practical path is an activity- and risk-based framework that combines MiCA's token categories with the US coordination model, regulates actors by function rather than by the "decentralized" label, and stays aligned internationally through the FATF and IOSCO.

VI. JUDICIAL AND REGULATORY DEVELOPMENTS**A. *SEC v. W.J. Howey Co.***

In *SEC v. W.J. Howey Co.*,³⁰ the Supreme Court considered interests in a citrus-grove arrangement and, in doing so, established the investment-contract test that has since been the benchmark of U.S. securities analysis. Its continuing relevance to crypto-assets lies in the principle that the legal characterization of an instrument depends on the substance of the economic arrangement rather than the label attached to it. Applying the test to DeFi, however, raises questions that *Howey* did not consider: what qualifies as "managerial efforts" when control is spread across token holders; how an expectation of profit is to be assessed when profit derives from an algorithm rather than a central promoter; and whether significant token-holder

³⁰ *Howey*, 328 U.S. at 298–99.

participation in protocol governance displaces the reliance on the efforts of others that the fourth element of *Howey* requires.

B. CFTC v. Ooki DAO

The Ooki DAO litigation concerned a purportedly decentralized trading platform that offered leveraged digital-asset trading without registration under U.S. commodities law.³¹ According to the CFTC, the federal court ruled that the DAO is a “person” that can be held liable under the Commodity Exchange Act. The result was a default judgment imposing a civil monetary penalty of \$643,542 and permanent trading and registration bans.³² The case is significant because it shows that courts can apply established legal definitions of personhood to code-based decentralized entities that lack the traditional corporate infrastructure of officers or boards, and that a DAO without a conventional legal form does not necessarily escape regulatory oversight. The ruling was, however, specific to the statute and to the facts of the case. It does not establish that all DAOs are “persons” for all regulatory purposes.

C. Sarcuni v. bZx DAO

In *Sarcuni v. bZx DAO*,³³ users who lost funds when the bZx protocol was hacked in November 2021 sued, among others, holders of the DAO’s governance tokens in negligence. Ruling on a motion to dismiss, the court held that the plaintiffs had plausibly alleged that the DAO was a general partnership and that defendants holding its governance tokens, which carried the right to propose and vote on governance decisions and to share in the protocol’s profits, were its partners. The case is important because it shows how ordinary rules of partnership law, written long before blockchain existed, can be applied to decentralized decision-making. The practical effect is that token holders who take part in governance could be personally liable for the organization’s debts, like general partners, and cannot shelter behind the claim that the organization is decentralized or autonomous.

D. Internet and Mobile Association of India v. RBI

In 2020 the Supreme Court of India set aside a Reserve Bank of India circular that prohibited regulated entities from providing services to virtual-currency businesses.³⁴ The Court accepted the validity of the regulatory concerns underlying the restriction, such as consumer protection,

³¹ Press Release No. 8590-22, Commodity Futures Trading Comm’n, CFTC Imposes \$250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act (Sept. 22, 2022), <https://www.cftc.gov/PressRoom/PressReleases/8590-22>.

³² *Ooki DAO*, No. 3:22-cv-05416-WHO; CFTC, Press Release No. 8715-23, *supra* note 4.

³³ *Sarcuni v. bZx DAO*, 664 F. Supp. 3d 1100 (S.D. Cal. 2023).

³⁴ *Internet & Mobile Ass’n of India*, (2020) 10 SCC 274.

market integrity and the prevention of money laundering, but found the measure disproportionate to those interests and struck it down. The decision matters for the future regulation of DeFi and crypto-assets in India because it makes clear that, while the state may legitimately pursue AML/CFT and consumer protection objectives in this sector, any regulatory measure must meet the constitutional standard of proportionality: it must be shown to be a reasonably tailored means of achieving a legitimate aim, as opposed to a blanket or disproportionately restrictive prohibition.

Read together, these four judicial and regulatory developments reveal a common theme relevant to the argument of this paper: courts and regulators have repeatedly shown a willingness to reach decentralized and code-based structures by extending existing legal doctrine (the *Howey* investment-contract test, statutory personhood under the Commodity Exchange Act, general partnership law and constitutional proportionality review) rather than treating decentralization as a complete legal exclusion. Each case also reveals the limits of this extension: *Howey* struggles with distributed managerial effort, the finding of personhood in *Ooki DAO* was statute- and fact-specific rather than general, *Sarcuni* exposes governance participants to potentially severe personal liability that they may not have foreseen, and the Indian Supreme Court's proportionality requirement limits how assertively regulators may act even where their underlying concerns are valid. Together, these developments support the paper's larger proposition that an activity- and risk-based regulatory approach, rather than reliance on the technological label of decentralization or on ad hoc judicial analogy, offers a more predictable and legally coherent way forward for the regulation of DeFi and crypto-assets across jurisdictions.

VII. MAIN LEGAL GAPS AND REGULATORY ISSUES

A. Uncertainty of token classification

A challenge common to all three jurisdictions examined in this paper is that the same crypto-asset can be characterized differently depending on the regulatory lens applied, and different characterizations lead to substantially different disclosure, licensing, market conduct, AML/CFT and consumer protection requirements. This is not merely a technical question of labelling, since the obligations that attach to an issuer or intermediary, and indeed whether any obligations attach at all, depend entirely on the category into which a token falls. The challenge is amplified because token attributes are not fixed at issuance but may evolve over the life of the asset. A token that begins as a centrally distributed instrument promoted by a recognizable team may, over time, become truly decentralized as governance passes to a wider community

of holders. Conversely, a token originally sold as a decentralized utility asset may acquire the qualities of a security through later conduct, staking schemes or profit-sharing arrangements. A static classification made at issuance risks becoming outdated as the asset and its ecosystem evolve, leaving regulators, issuers and users uncertain about which rules apply, and allowing assets to fall through regulatory gaps just when their risk profile is changing most.

B. Absence of a recognizable intermediary

The second structural gap arises when a protocol has no single controlling party. A typical regulatory regime assumes an intermediary (for example, an issuer, exchange, custodian or service provider) that can be held responsible for particular obligations and for compliance. A fully decentralized system has no such party. Regulators therefore need to establish whether other identifiable actors (for example, core developers who can change the code, governance administrators who can control or veto changes, and interface operators who control the main points of user access) have control over the system, even if they have no formal role as an intermediary. The *Ooki DAO* and *Sarcuni* cases are two examples of how decentralized structures can still attract liability. In the first, the DAO was held to be a “person” that could be sued under the Commodity Exchange Act; in the second, governance-token holders were plausibly alleged to be members of a general partnership. In both cases the absence of a conventional corporate structure did not shield the decentralized organization from legal liability. Neither approach, however, is complete or predictable, since each depends on the particular statute or on the circumstances of governance participation in the case at hand.

C. Regulatory perimeter and jurisdictional arbitrage

A third significant gap lies in the regulatory perimeter itself, since the same crypto-asset or activity can be classified differently in different jurisdictions: one may treat a token as a security, another as a commodity, and a third may not regulate it at all beyond taxation and AML obligations. This divergence encourages regulatory arbitrage, because DeFi protocols and their users are not confined by jurisdictional boundaries and operate across borders. Projects, developers and even users gravitate towards the jurisdictions with the lightest or most favourable treatment, undermining the intent of more restrictive regimes elsewhere and creating an uneven playing field between jurisdictions. Cross-border cooperation is thus not merely desirable but necessary if the regulatory perimeter of any individual jurisdiction is to have meaning. The FSB’s recommendations expressly call for cooperation, coordination and information sharing among national authorities as a core element of an effective international

response to crypto-asset risks,³⁵ while the joint IMF-FSB synthesis paper makes global coordination, cooperation and information sharing an integral part of its implementation roadmap for crypto-asset policy,³⁶ recognizing that fragmented, jurisdiction-by-jurisdiction regulation is structurally ill-suited to a technology that does not respect national borders.

D. Evidence and cross-border enforcement cooperation

The fourth gap, closely linked to but distinct from the perimeter problem outlined above, concerns the practical mechanics of enforcement once a legal basis for regulatory or judicial action has been established. Even when a regulator classifies a token correctly, or identifies a responsible actor within a decentralized structure, enforcement against that actor is often hampered by the technical architecture of DeFi itself: transactions are recorded pseudonymously on distributed ledgers, protocol code may be deployed by developers located in several jurisdictions, governance votes are cast by token holders whose real-world identities are unknown, and the assets or proceeds of a contravention can be moved across borders and across blockchains within minutes. Collecting admissible evidence in this environment often requires specialized blockchain forensic capabilities that many regulators and enforcement agencies do not yet possess in-house, as well as cooperation from foreign counterparts to identify wallet holders, freeze assets or compel the production of off-chain records held by the centralized on- and off-ramps that interface with an otherwise decentralized protocol. The *Ooki DAO* enforcement action illustrates the challenge: the CFTC settled administrative charges with the founders and their company, bZeroX, but had to pursue the DAO itself in court, where it obtained a default judgment because no one appeared to defend the dispersed, pseudonymous governance community.³⁷ The effectiveness of enforcement in this space therefore depends heavily on the same cross-border cooperation mechanisms advocated at the perimeter-setting stage, including mutual legal assistance arrangements, information-sharing protocols between financial intelligence units (FIU-IND and its foreign counterparts) and the coordinated action recommended by bodies such as the FSB and the FATF. No national regulator acting alone can realistically enforce its rules against a protocol whose developers, validators, governance participants and assets are spread across dozens of jurisdictions at once.

³⁵ FIN. STABILITY BD., HIGH-LEVEL RECOMMENDATIONS FOR THE REGULATION, SUPERVISION AND OVERSIGHT OF CRYPTO-ASSET ACTIVITIES AND MARKETS: FINAL REPORT, *supra* note 3, at 6 (Recommendation 3); *see also* FIN. STABILITY BD., THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE, *supra* note 1, at 3, 38.

³⁶ INT'L MONETARY FUND & FIN. STABILITY BD., IMF-FSB SYNTHESIS PAPER: POLICIES FOR CRYPTO-ASSETS 24 (Sept. 7, 2023), <https://www.fsb.org/uploads/R070923-1.pdf>.

³⁷ CFTC, Press Release No. 8590-22, *supra* note 31; *Ooki DAO*, No. 3:22-cv-05416-WHO, slip op. at 3, 12 (N.D. Cal. June 8, 2023) (order granting default judgment) (finding that the Ooki DAO “intentionally chose to not appear”); CFTC, Press Release No. 8715-23, *supra* note 4.

VIII. CONCLUSION

This paper has examined whether current financial market frameworks, built on identifiable intermediaries, licensed institutions and centralized control points, are adequate for a financial system in which lending, trading, staking and asset management can take place without intermediaries. The findings show that none of the three legal frameworks examined, those of the European Union, the United States and India, fully addresses this issue. Each, however, has developed partial responses that are relevant to DeFi regulation more generally.

The comparative analysis shows that while the European Union's dedicated statutory approach in MiCA provides the greatest legal certainty for centralized crypto-asset issuers and service providers, its design is inherently incompatible with "fully decentralized" systems. The activities of most interest to this paper (non-custodial lending, automated market-making and DAO-controlled protocols) are therefore not covered by MiCA. The gap is well recognized at the highest policy levels but remains open, particularly while the European Commission's review of MiCA is under way, and it is hard to see a principled reason for leaving DeFi outside MiCA's scope. In the United States, the March 2026 SEC-CFTC interpretation has given market participants a taxonomy for distinguishing digital commodities from digital securities. That clarity, however, rests on agency interpretation rather than statute, and it remains unclear who is legally responsible in decentralized protocols (the DAO, the developer or the validator) when problems arise, as the different outcomes of *Ooki DAO* and *Sarcuni* show. India is currently the least advanced of the three, approaching crypto-assets through taxation and anti-money laundering law. Most importantly, there is no general legislative definition of a crypto-asset, and the Supreme Court's proportionality ruling on the RBI circular indicates that regulation must be tailored rather than take the form of a blanket prohibition.

Four legal challenges are common to all three jurisdictions:

1. tokens can change character and classification during an asset's life cycle;
2. there is no regulable intermediary in truly decentralized systems;
3. jurisdictional differences create a risk of regulatory arbitrage; and
4. rules are difficult to enforce in practice against pseudonymous, cross-border, code-based protocols, even once the legal basis has been established.

On this analysis, these four challenges are not separate legal problems but expressions of a single underlying failure, which calls for a change of approach from an entity-centric model to an activity-based one. Financial regulation has always been organised around identifying institutions; DeFi makes it necessary to ask instead what function is being performed at a given

moment, and by whom. Both the Financial Stability Board and the recommendations made here for India call for an activity-based and risk-based approach. There is an emerging global consensus on the appropriate response to decentralization: regulators should neither abandon regulation of decentralized systems nor force them into ill-fitting corporate categories. Instead, they must determine who actually exercises meaningful control at any given time, whether a front-end operator, a fee-collecting developer or an active governance participant, and subject those functions to oversight proportionate to their risk profile.

The judicial trends examined here support this conclusion from another angle. *Howey*, *Ooki DAO* and *Sarcuni*, as well as India's proportionality doctrine, show courts applying existing legal doctrines, such as the investment contract and constitutional reasonableness, to decentralized systems instead of treating decentralization as placing them beyond legal classification. This reasoning is sound but somewhat haphazard, since the outcome often depends on which statute happens to be invoked or which case happens to come before the courts. Case-by-case litigation cannot deliver steady progress, and legislative action is needed. This paper has therefore proposed several recommendations for India: a functional token taxonomy, a binding inter-regulatory coordination mechanism, and an activity-based framework for identifying regulable actors, together with fiduciary and consumer protection responsibilities. The study posits that the ambiguity surrounding DeFi and crypto-assets is not inherent in the technology itself but is the result of regulation that has not evolved. No jurisdiction examined here has a complete solution, but the categorical clarity of the European Union's framework, the functional taxonomy of the United States and the cautious constitutional stance of India together point the way forward: classify assets by function rather than form; regulate those who exercise meaningful control rather than search for non-existent traditional intermediaries; and coordinate rules worldwide through the FSB and the FATF so that one jurisdiction's caution does not become another's gain.

Achieving this will require sustained legislative attention rather than interpretive guidance or piecemeal litigation. Yet the trends in all three jurisdictions show that an activity-focused, risk-oriented international regulatory framework is both necessary and feasible.
