GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation 2026

Eighth Edition

Contributing Editor:
Josias N. Dewey
Holland & Knight LLP

WSBA WALL STREET BLOCKCHAIN ALLIANCE

glg Global Legal Group

TABLE OF CONTENTS

Preface

Josias N. Dewey
Holland & Knight LLP

Glossary

The Contributing Editor shares key concepts and definitions of blockchain

Industry Viewpoint

1 **From headwinds to horizons: the changing U.S. crypto landscape**
Ron Quaranta
Wall Street Blockchain Alliance

Expert Analysis Chapters

7 **Blockchain and intellectual property: a case study**
Ieuan G. Mahony, Brian J. Colandreo & Jacob Schneider
Holland & Knight LLP

23 **Cryptocurrency and other digital asset funds for U.S. investors**
Gregory S. Rowland & Trevor Kiviat
Davis Polk & Wardwell LLP

38 **From paper to protocol: how trust companies became the backbone of RWA tokenization**
Tom Momberg, Angela Angelovska-Wilson & Diana Stern
DLx Law PLLC

68 **Stablecoin use cases and regulations**
Stuart D. Levi, Mark Chorazak, Geoffrey Chan & Sebastian J. Barling
Skadden, Arps, Slate, Meagher & Flom LLP

81 **Stranger things have happened: the evolving regulation of staking**
Richard B. Levin, Bobby Wenner, Jorge Castiblanco & Taylor Hill John
Taft Stettinius & Hollister LLP

99 **CLARITY Act and portfolio margining: lessons and opportunities**
Brandon M. Hammer, Wankun (Charles) Wang & Alec Mitchell
Cleary Gottlieb Steen & Hamilton LLP

109 **Trends in the derivatives market and how recent fintech developments are reshaping this space**
Jonathan Gilmour & Tom Purkiss
Travers Smith LLP

119 **Blockchain taxation in the United States**
David L. Forst & Sean P. McElroy
Fenwick & West LLP

129 **OFAC sanctions and digital assets: regulation, compliance, and recent developments**
Evan T. Abrams, Andrew C. Adams & Sophia Breggia
Steptoe LLP

144 **Dark patterns leading to the dark forest – the next frontier of crypto enforcement?**
Sarah Chen, Gregory Strong & Frank Weigand
Cahill Gordon & Reindel LLP

Jurisdiction Chapters

154 **Australia**
Peter Reeves, Emily Shen & Amiinah Dulull
Gilbert + Tobin

172 **Austria**
Dr. Oliver Völkel & Jara Erhard
CERHA HEMPEL

177 **Bermuda**
Steven Rees Davies, Charissa Ball, Alexandra Fox & Matthew Perriment
Carey Olsen

190 **Brazil**
Rodrigo Caldas de Carvalho Borges & Gabriel Abreu
Carvalho Borges Araújo Advogados

196 **British Virgin Islands**
Chris Duncan & Katrina Lindsay
Carey Olsen

204 **Canada**
Alix d'Anglejan-Chatillon, Ramandeep K. Grewal, Éric Lévesque & Antonin Lapointe
Stikeman Elliott LLP

217 **Cayman Islands**
Richard Munden & Chris Duncan
Carey Olsen

225 **France**
Hubert de Vauplane & Hugo Bordet
Morgan Lewis & Bockius LLP

236 **Germany**
Finn Niklas Nitz & André Schenk
SBS Legal Rechtsanwälte

246 **Gibraltar**
Jay Gomez, Javi Triay, Rupert Moffatt & Johnluis Pitto
Triay Lawyers Limited

254 **Greece**
Dr. Anastasia Mallerou
Bernitsas Law

264 **India**
Reddy Pawan Kumar, Athif Ahmed, Aabha Dixit & Armaan Mistry
Hash Legal

276 **Japan**
Takeshi Nagase, Takato Fukui, Keisuke Hatano & Huan Lee (Henry) Tan
Anderson Mori & Tomotsune

286 **Liechtenstein**
Matthias Niedermüller, Giuseppina Epicoco & Sophie Seliansky
Niedermüller Attorneys at Law

294 **Lithuania**
Vladimiras Kokorevas
Gofaizen & Sherle UAB

303 **Luxembourg**
Harry Lars Ghillemyn, Tristan Husson, Loïck Kabongo & Joffrey Sarmadi
Woud Law

314 **Mexico**
Diego Alonso Ramos Castillo, José Antonio Casas Vessi &
Frida Sofía Rojas Cuéllar
Ramos, Ripoll & Schuster

322 **Norway**
Philip Heyden, Rasmus Jørgensen, Gjert Melsom & Axel Naustdal Cooper
Ernst & Young Advokatfirma AS

333 **Portugal**
Filipe Lowndes Marques, Vera Esteves Cardoso & Ashick Remetula
Morais Leitão, Galvão Teles, Soares da Silva & Associados

348 **Serbia**
Pavle N. Stavretović
STAV | LAW

357 **Singapore**
Kenneth Pereire & Lin YingXin
KGP Legal LLC

367 **Slovakia**
Peter Varga, Roman Baranec & Vladimir Gaduš
Highgate Law & Tax s. r. o.

375 **Spain**
Alfonso López-Ibor Aliño, Olivia López-Ibor Jaume, Victoria Moreno Motilva & Santiago Alsina Gil
López-Ibor Abogados, S.L.P.

385 **Switzerland**
Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock
Homburger

401 **Taiwan**
Robin Chang, Dennis Yu & Eddie Hsiung
Lee and Li, Attorneys-at-Law

408 **Thailand**
Dr. Jason Corbett
Silk Legal Co., Ltd.

420 **Ukraine**
Peter Bilyk & Daniil Voloshcuk
Juscutum

432 **United Kingdom**
Charles Kerrigan & Erica Stanford
CMS LLP

450 **USA**
Josias N. Dewey & Samir Patel
Holland & Knight LLP

India

Reddy Pawan Kumar
Athif Ahmed
Aabha Dixit
Armaan Mistry

Hash Legal

Building for compliance — aligning DeFi with India's regulatory framework

Introduction

The Ministry of Finance (MoF), Government of India, by way of a Notification dated March 7, 2023 (PMLA VASP Notification), marked a transformative moment in India's approach to virtual assets. By classifying entities providing services related to virtual digital assets (VDAs) as "reporting entities" under the Prevention of Money Laundering Act, 2002 (PMLA), the Government effectively ended the regulatory ambiguity that had long surrounded the VDA space. This move was not merely administrative – it heralded a fundamental shift from a stance of observation and inaction to one of active regulation.[1]

The PMLA VASP Notification sought to clarify five specific activities under regulatory purview: exchange of VDAs and fiat currencies; exchange between different forms of VDA; transfer of VDAs; safekeeping or administration of VDAs or instruments enabling control over such assets; and participation in financial services related to VDA offerings.[2] Each of these activities, when conducted "for or on behalf of another person in the course of business", now triggers comprehensive compliance obligations.[3] However, while this framework does not expressly distinguish between centralised entities and decentralised finance (DeFi), gaps and ambiguities remain in its application to DeFi. That said, this does not mean DeFi is outside the purview of the law, as a mere self-claim of being "decentralised" is insufficient; DeFi lies on a spectrum, and only protocols that are demonstrably and sufficiently decentralised may be treated differently. This chapter explores that fine line.

Scope of the chapter

This chapter provides a practical roadmap for DeFi developers and founders navigating India's evolving regulatory landscape, tracing the impact of the PMLA VASP Notification that brought Virtual Digital Asset Service Providers (VASPs) under anti-money laundering (AML) oversight. It examines the compliance obligations faced by DeFi projects within India's regulatory framework, with a particular emphasis on how the activity-based VASP definition applies to various DeFi models.

Importantly, while the law itself does not expressly distinguish between centralised entities and DeFi projects, its application reveals gaps and ambiguities. These gaps do not imply that DeFi projects fall entirely outside the purview of regulation. A DeFi protocol's claim to be "decentralised" is not conclusive. The degree of decentralisation must be demonstrated in practice, given that DeFi exists on a spectrum from heavily centralised models to sufficiently decentralised systems.

Against this backdrop, this chapter examines the practical implementation challenges for different types of DeFi protocols, from fully decentralised systems to hybrid models, as well as analysing critical risk factors such as admin keys, custodial elements and off-chain infrastructure dependencies. Finally, the inherent conflict in applying traditional financial regulations to decentralised systems is examined.

A brief enforcement timeline

India's enforcement trajectory demonstrates a resolute and, at times, bordering regulatory overreach towards both domestic and offshore virtual asset platforms. When the PMLA VASP Notification of March 2023 was first introduced, regulators themselves were grappling with how compliance obligations should apply to VASPs, particularly DeFi. Thus, enforcement initially targeted the "lowest-hanging fruit" – India-based centralised exchanges with obvious points of control.

Once domestic exchanges complied and registered with the Financial Intelligence Unit-India (FIU-IND), enforcement quickly turned outward to offshore exchanges. In December 2023, FIU-IND issued show-cause notices to several major cryptocurrency exchanges – Binance, KuCoin, Huobi, Kraken, Gate.io, Bittrex, Bitstamp, MEXC Global, and Bitfinex – for non-compliance with PMLA provisions. The resultant effects were that non-compliant platforms faced URL blocking and that easy access was cut off to Indian users.[4]

The pressure intensified in June 2024, when FIU-IND passed a detailed order against Binance imposing penalties for operating without registration and failing to meet KYC/AML obligations under the PMLA.[5] Similarly, multiple centralised exchanges have faced proceedings – in January 2025, Bybit Fintech Limited was fined ₹9.27 crore.[6]

In August 2024, India's Directorate General of GST Intelligence (DGGI) issued a formal show-cause notice to Binance, alleging ₹722.43 crore (approx. $85 million) in unpaid goods and services tax on transaction fees collected from Indian users between July 2017 and March 2024,[7] a further indicator of the unrelenting pressure being applied by regulators.

These actions underscore several critical insights. First, the decentralised or offshore nature of a platform does not automatically exempt it from Indian regulatory oversight. Second, enforcement is not merely lip service; authorities have imposed show-cause notices and fines and have even resorted to bank account freezes, website blocking and payment processor disengagement, measures that many in the industry view as regulatory overreach.

FIU-IND has adopted an activity-based approach, focusing on the services provided such as on/off-ramping, custody, and token transfers rather than the label or technical structure of the platform. For DeFi developers, the opaque nature of this enforcement landscape poses a heightened challenge. While public orders (such as the Binance June 2024 order) set out reasoning in detail, many actions against protocols with DeFi-like features have not been publicly disclosed, creating uncertainty about the standards being applied. This fuels concerns that even projects without formal corporate structures or decentralised features operating as protocols could be targeted if they facilitate activities falling within the definition of VASP activity. The PMLA VASP Notification has taken an activity-based approach, focusing on the services provided – such as on/off-ramping, custody, and token transfers rather than the label or technical structure of the platform.

Ultimately, the enforcement history highlights a key lesson: self-identifying as "DeFi" is not sufficient to remain outside the scope of Indian regulation. Regulators will test the degree of decentralisation in

fact, and hybrid or semi-decentralised protocols remain particularly exposed due to identifiable points of control such as admin keys, off-chain infrastructure, or user-facing interfaces. DeFi does not automatically mean an exemption from regulatory oversight.

Understanding the PMLA framework for VASPs

Decoding the VASP definition: beyond traditional exchanges

The PMLA VASP Notification defines VASPs through their activities rather than their corporate structure or, as seen previously, technical implementation. The key phrase "for or on behalf of another person in the course of business" serves as the trigger for regulatory obligations, but its interpretation in the context of decentralised protocols remains a source of ongoing legal uncertainty.

While the PMLA VASP Notification frames obligations around activities carried out "for or on behalf of another person in the course of business", it does not explicitly distinguish between centralised intermediaries and decentralised protocols that facilitate peer-to-peer transactions without intermediaries. Internationally, guidance from the Financial Action Task Force (FATF) has recognised this nuance by emphasising that decentralised platforms or non-custodial service providers are not automatically VASPs unless a person or entity exercises sufficient control over them. However, in the Indian context, this distinction has yet to be clearly articulated. As a result, much remains unsettled, leaving projects uncertain as to how the "for or on behalf of" qualifier will be applied in practice, particularly in the absence of a developed test for analysing the DeFi spectrum.

Ideally, regulators should evaluate certain factors that could be used to determine the amount of control exerted by VASPs more than technical compliance or mere structure. Those factors could be the presence of admin/multisig keys that enable certain parties to alter or override protocol behaviour, upgrade or pause authority, which allows interventions in otherwise autonomous systems, and the ability to set economic parameters, such as interest rates or collateral requirements, which directly shape user outcomes. Each of these elements can operate within the "instruments enabling control" limb of the PMLA VASP Notification.

Custodial elements embedded in design are often reflective of functional administration, even where no individual keyholder exists. For example, smart contract escrows temporarily hold user assets under predefined conditions, liquidity pools aggregate and manage user deposits for trading, staking or delegation services reallocate control to validators, and bridges require assets to be locked before minting representations on another chain. In each case, user assets are being held, managed, or conditioned by the protocol, amounting to a form of "safekeeping or administration".

Yet, more often than not, regulators overlook these indicators of control and instead leap directly to the service-based characterisation in the VASP definition. This approach collapses nuanced distinctions into four broad activity categories:

a. exchange: "exchange between virtual digital assets and fiat currencies" and "exchange between one or more forms of virtual digital assets";

b. transfer: "transfer of virtual digital assets";

c. safekeeping: "safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets"; and

d. financial services: "participation in and provision of financial services related to an issuer's offer and sale of virtual digital assets".

These activity-based characterisations are applied with a broad stroke without first analysing whether the "for or on behalf of" qualifier is truly met in the context of decentralised protocols.

In reality, all projects exist on a spectrum, with varying degrees of decentralisation and therefore varying degrees of control. At one end of the spectrum, one may observe projects in nascent stages of their development, wherein centralised control is a necessity. At the other end of the spectrum, one may observe completely decentralised protocols; no admin keys, no price control, etc., but that does not mean that the aforementioned criteria being met will guarantee the immunity of the entities meeting the criteria from regulatory scrutiny.

How to understand where a project lies on the DeFi spectrum

The PMLA VASP Notification brings VDA activities into scope when conducted "for or on behalf of another person", expressly including safekeeping/administration and "instruments enabling control". This makes control a core operative test for VASP classification rather than corporate-form, claimed decentralisation. Consistent with FATF, assessors ought to look for "control or sufficient influence", which is an indicator that a person is providing or actively facilitating VASP services even if the codebase is labelled "decentralised". Accordingly, on the DeFi spectrum, protocols retaining meaningful levers over user assets or protocol behaviour may be classified as reporting entities under the PMLA, while truly immutable, non-custodial designs may face reduced VASP compliance exposure.

Centralised projects: straightforward

Centralised intermediaries such as centralised exchanges and custodial wallet providers clearly meet the PMLA's VASP test because they exchange fiat for VDA and VDA for VDA, execute transfers and perform "safekeeping or administration of virtual digital assets or instruments enabling control", all "for or on behalf of another person in the course of business". A centralised matching/settlement stack executes fiat to VDA and VDA to VDA conversions and transfers through an internal ledger and routing engine, meeting the "exchange" and "transfer" limbs of the VASP definition. Fiat rails are integrated with banks/payment providers, with client money accounts disclosed at registration, reflecting custodial handling of customer funds. Operator privileges (freeze/lock withdrawals, blacklist/whitelist, change fee parameters, pause flows) are "instruments enabling control", evidencing functional custody and administration, notwithstanding any technical use of multisig. Compliance telemetry (KYC gating, Travel Rule pay loading, suspicious transaction reporting (STR) triggers, records) is embedded into the core stack to meet registration, customer due diligence (CDD) and monitoring. Some examples of centralised governance could be seen by the following: a legal entity appoints a Designated Director and Principal Officer and implements an AML and counter-terrorism financing (CFT) programme with internal controls. Central committees govern listings, market access, fee schedules, leverage/limits and product rollouts. This aligns with the activity-based lens that treats operational discretion as a provision of covered VASP services. Risk management oversees reserves/treasury, wallet key ceremonies, incident response and data retention, anchoring the platform's ability to administer user assets and maintain statutorily required records under PMLA frameworks.

As a result, they must register with FIU-IND as reporting entities and implement full AML/CFT controls, namely: risk-based CDD; transaction monitoring; traction record-keeping; STR; and implementation of the Travel Rule.

Semi-decentralised projects: the grey zone

The majority of DeFi projects operating today are semi-decentralised with elements of decentralised architecture with varying degrees of centralised control. This might include a hybrid governance model that combines elements of traditional centralised control with decentralised autonomous features, which can be characterised by the presence of administrative keys, multisig wallets, and governance tokens alongside automated smart contract functions. Since compliance obligations depend on specific technical

and governance arrangements, these models may face the greatest regulatory uncertainty as they do not fit neatly into either one of the established categories.

Under India's PMLA and FIU-IND regulatory framework, such hybrid structures present compliance challenges because of the existence of centralised control elements, in particular the administrative keys held by identifiable entities, which creates clear regulatory jurisdiction and liability exposure.

This makes these projects potentially subject to "reporting entity" obligations under Section 12 of the PMLA, regardless of their decentralised features. The potentially problematic features include multisig wallets controlled by known parties, governance tokens that concentrate voting power among founders/early investors, and upgrade mechanisms that allow protocol modifications. These features contradict the "truly decentralised" threshold test that might otherwise exempt projects from direct regulatory oversight.

Admin keys with time delays represent a common semi-decentralised pattern. Protocols may implement timelocks that require a waiting period between proposed changes and their execution, allowing community review and potential intervention. Timelocks indicate centralised control mechanisms and could potentially trigger VASP obligations.

Multisig governance structures create additional complexity. When protocol decisions require approval from multiple keyholders, the arrangement may appear decentralised. However, if the multisig participants are affiliated entities or if the threshold for decision-making is low, regulators could view the structures as centralised control. The categorisation turns on whether the multisig represents genuine distributed governance or operational security for a centrally controlled system.

Fully decentralised protocols

For projects that have achieved a level of decentralisation wherein there exists complete user autonomy, the absence of admin keys or other overarching features that meet the control test, there is a very realistic chance of operating outside of the VASP obligations that are imposed on entities having a lesser degree of decentralisation.

However, the notion that fully decentralised protocols operate in a regulatory safe harbour is increasingly being challenged by the reality of recent enforcement actions (in other parts of the world) as seen in the case of Uniswap, Consensys, etc. True decentralisation, which can be characterised by immutable smart contracts, the absence of admin keys and completely autonomous operation, may offer some protection from direct regulatory action but by no means confer any sort of immunity from the aforementioned actions.

Protocols that achieve technical decentralisation could often retain elements that could attract regulatory scrutiny. Front-end interfaces that target Indian users create potential compliance obligations, even if the underlying smart contracts operate autonomously. Token launches and ongoing distributions through supposedly decentralised mechanisms may still constitute "financial services related to VDA offerings" under the PMLA framework. An illustration of the logic captured can be seen in the table below:

Category	Defining Features	Illustrations	Regulatory Exposure under PMLA
Centralised intermediaries	• Full custody of users' assets. • Discretionary control over transactions.	Centralised exchanges, custodial wallets, custodial on/off-ramps, etc.	Clear VASP. Direct registration with FIU-IND and compliance obligations (KYC, STR, Travel Rule).

Category	Defining Features	Illustrations	Regulatory Exposure under PMLA
Semi-decentralised protocols	• Hybrid governance. • Admin/multisig keys. • Smart contracts. • Treasury managed by identifiable actors. • Governance tokens concentrated among insiders.	Many protocols (early-stage).	Possibly high VASP exposure. Regulators view control elements as service "for or on behalf of" users.
Sufficiently decentralised protocols	• Governance widely distributed. • Immutable code. • No admin keys. • Reliant on front-ends.	MakerDAO, Uniswap (with geo-blocked front-end.	Reduced but non-zero exposure. Less likely to be treated as VASPs directly, but interfaces and support structures may be regulated.
Fully decentralised protocols	• Immutable smart contracts. • No human or entity retains control; purely peer-to-peer interaction without central facilitation.	Theoretically, Tornado Cash contracts approached this.	Lowest exposure. However, the U.S. Department of Justice took action against the developer of Tornado Cash.

High-risk elements: what may put you on the PMLA's radar

As per FATF guidance, what matters is not abstract claims of decentralisation but whether there exist identifiable levers of control or sufficient influence. Claims of being "DeFi" or "sufficiently decentralised" are ultimately tested against observable features that either evidence or undermine autonomy. In practice, regulators focus less on abstract architecture and more on the levers of control that shape user outcomes. These levers include admin keys, custodial arrangements, off-chain infrastructure, interface governance, and the trajectory of decentralisation function as the operative criteria in determining whether activity is being undertaken "for or on behalf of" users. While the regulator is still developing a lot of this nuance, it is vital to understand risk factors to map a project's regulatory exposure under the PMLA.

Admin keys and protocol control: the ultimate risk factor

Admin keys represent perhaps the highest-risk element for DeFi protocols and a visible market of centralised control. These cryptographic credentials enable their holders to upgrade the underlying smart contracts, pause operations, adjust parameters, or in some instances access user funds. From a PMLA perspective, such capabilities may constitute "instruments enabling control" and, when exercised "for or on behalf of" users, can trigger classification as a VASP.

The degree of discretion matters. For instance, a narrowly framed pause function for emergency, time-bound and transparently disclosed, may be defensible as a security feature. By contrast, broad powers exist to adjust core economic terms or to unilaterally upgrade contracts, evidence ongoing custody and administration of user assets. The critical insight is that *form is irrelevant*. Whether control is exercised via multisig, timelock or a decentralised autonomous organisation (DAO) wrapper, regulators will test its practical effect.

For compliance, projects should not only disclose who holds such powers, but also publish credible roadmaps to minimise and eventually relinquish them. Progressive decentralisation here is persuasive only if it demonstrably reduces control in practice, not merely in rhetoric.[8]

Custodial elements: when non-custodial is not really non-custodial

The distinction between custodial and non-custodial systems has always been a regulatory hinge point, and DeFi complicates it further. Under traditional financial regulation, custody is straightforward: a bank or exchange physically holds client assets, controls the private keys, and is therefore subject to direct obligations. Centralised exchanges operating in India, or offshore but serving Indian users, fall squarely into this model. They act as custodians in the classic sense holding user assets "for or on behalf of" them, exercising discretion in how those assets are stored, and providing access through internal ledgers. This is why FIU-IND's first wave of enforcement actions post-2023 Notification targeted such exchanges: they are the clearest instantiation of "safekeeping or administration".

DeFi protocols, however, present a subtler picture, often branding themselves "non-custodial", but, globally, regulators have focused on functional custody, i.e. who, in practice, controls the use of assets. Lending pools, automated market makers (AMMs), and vaults decide how deposits are deployed and how liquidations occur. Bridges lock assets on one chain and issue representations on another. Staking arrangements allow validators or pool operators to direct user assets. These arrangements may qualify as "safekeeping or administration" under the PMLA, even if no human custodian exists.

Yet, not "all DeFi is custody". Many protocols minimise custody risks by designing contracts where users can withdraw at any time, limiting discretionary use. The nuance is that custody in DeFi is a spectrum, and careful structuring can reduce exposure. Protocols should therefore recognise that while functional custody triggers obligations, thoughtful design can narrow the scope of what regulators consider "safekeeping".

Off-chain components: oracles, APIs, and infrastructure

Even protocols that achieve on-chain autonomy remain tethered to off-chain infrastructure, which can create hidden points of centralised control. Price oracles, relayers, RPC providers, hosting services, and MEV protection systems all perform critical functions, and their operators may exercise "sufficient influence" over user outcomes.

Price oracles are particularly salient. A single compromised feed can liquidate loans across a lending protocol, wipe out collateral, or distort trading outcomes. In *Commodity Futures Trading Commission vs Ooki DAO* (2022–2023), the CFTC successfully secured a default judgment in 2023, finding that Ooki DAO operating via governance token holders and smart contract infrastructure violated several provisions of the Commodity Exchange Act.[9] The decision held that the DAO is a "person" under the Act as an unincorporated association, and that its members oversaw infrastructure and controls (such as token holder governance, administrative keys, and contract voting) that amounted to significant control over protocol operations.

Yet, the presence of off-chain infrastructure does not mean that DeFi is illusory. Innovative solutions such as multi-source oracle aggregation illustrate that protocols can reduce dependency risks. The legal question is not whether oracles exist, but whether control is sufficiently dispersed such that no single actor can dictate outcomes "for or on behalf of" users.

Projects should therefore map their infrastructure dependencies and disclose how they are mitigated. Redundancy, transparency, and diversity of providers are the strongest safeguards against regulators construing off-chain reliance as centralised control.

User interface and access controls

Front-end interfaces are a critical point of regulatory vulnerability for DeFi protocols, given that they often

provide the primary means for users to interact with decentralised systems. The entities that exercise control over these interfaces may face compliance obligations even if the underlying smart contracts operate autonomously on a decentralised protocol.

The Securities Exchange Commission (SEC) Wells Notice to Uniswap Labs[10] exemplifies this logic: even where smart contracts are immutable, regulatory attention has focused on the fact that a corporate entity maintained the front-end website, curated token listings, and communicated with users. However, as of February 2025, the SEC has dropped its investigation into Uniswap Labs and will not be pursuing enforcement. Similarly, Consensys's MetaMask wallet[11] has faced regulatory scrutiny over whether features such as swaps, or custody, place it within the remit of securities or money transmission laws.

These cases highlight a crucial nuance. The existence of a user interface (UI) does not negate DeFi, but it introduces points of accountability. Some projects, like dYdX, have introduced access controls at the front-end level, for example, by geo-blocking restricted jurisdictions and open-sourcing front-end UI code, so that community members may fork or host their own access points, thereby diffusing control over the interface.

For Indian regulators, the more likely approach is to treat whoever operates or controls the primary user-facing interface as the reporting entity, since the front-end is the most visible point of interaction for Indian users. Enforcement trends elsewhere suggest that interface governance alone can be sufficient to attract regulatory attention, even where the underlying contracts remain autonomous.

Yet, there is a credible counter-argument that projects such as Uniswap have advanced, i.e. that a UI is not a financial service in itself but rather a communication layer enabling interaction with autonomous contracts. On this view, where custody, administration, and governance functions are already credibly decentralised, a UI or user experience (UX) layer may be better understood as a publication or access tool, not as a "safekeeping" or "service provision" within the meaning of the PMLA. This distinction has practical significance: if regulators conflate interfaces with custodial services, they risk extending obligations beyond what the statutory text contemplates.

Accordingly, protocols should tread carefully. Where front-ends are centralised, curated, and operated as commercial gateways, the risk of being treated as a reporting entity is high. But, where they are open-sourced, community-maintained, and demonstrably separate from custody or governance functions, projects can argue with some legitimacy that they are closer to communication channels than service providers. In the Indian context, until regulators clarify their approach, documenting and evidencing these distinctions will be critical.

Progressive decentralisation framework

Progressive decentralisation is a staged governance and technical roadmap, first articulated by a16z[12] and Variant in 2021, through which founding teams relinquish control "by degrees" to achieve "sufficient decentralisation"[13] while the product matures and a community forms. The legal rationale is that the greater the influence over a protocol, the greater the responsibility for its operation. Thus, reducing practical control can mitigate both securities exposure and AML/VASP risk. In India, where the PMLA scopes VASPs by activity "for or on behalf of another person", including "safekeeping or administration" and "instruments enabling control", progressive decentralisation offers a structured way to remove or diffuse those levers of control rather than rely on surface-level appearances. This aligns with FATF's owner/operator test that looks for "control or sufficient influence" over DeFi arrangements and with activity-based expectations on CDD, monitoring, STRs and the Travel Rule where covered services persist. The policy objectives aim to eliminate information asymmetry, reduce reliance on founding-team efforts, and minimise platform and custody-like risks.

In practice, a credible programme proceeds towards decentralisation via a centralised build that openly maps all control levers (admin/upgrade/pause rights, treasury, oracle and UI gates) and meets FIU-IND

registration and AML control requirements whenever in-scope VASP activities reach Indian users. This indicates a governed transition that constrains discretion via timelocks, higher threshold and independent multisigs, parameter changes by on-chain governance, oracle and infra diversification, and open-sourced, forkable interfaces. A "sufficiently decentralised" end-state will have immutable core contracts, burned admin keys and widely dispersed governance such that no actor maintains "sufficient influence". As a result, Indian enforcement targets substance over form. Projects should evidence the transition with on-chain votes, key-burn proof, deprecation of privileged functions and public dependency maps, while accepting that any residual covered services, especially those that are Indian-facing curated front-ends, can still make the relevant operator a reporting entity. There is a strong sense that this reflects a tendency to value substance over the label of a project. If users' assets or outcomes remain shapeable by a person or coordinated group, PMLA VASP exposure will endure regardless of any degree of decentralisation claims.[14]

Roadmap for progressive decentralisation: control tests

Criteria	Regulatory Question (PMLA)	Signals of High Exposure (Centralised/ Semi-DeFi)	Progressive Milestones	Reduced Exposure Outcome
Active facilitation	Does the interface itself route, curate, or batch transactions?	UI undertakes discretionary routing or order-flow shaping.	Open-source the UI; shift to client-side signing; publish clear limits on what the interface does.	UI operates as a neutral communication channel, not a service provider.
Fee flows	Who accrues fees – a protocol operator or a community treasury?	Fees accrue to an identifiable company/ foundation or are split with UI operators.	Route fees transparently on-chain; transfer treasury control to governance.	Fee flows governed by community/DAO, not a private entity.
Control/ sufficient influence	Who can set or change parameters that affect users?	Low-threshold parameter changes by insiders; operator discretion.	Implement timelocks, high quorum thresholds, and broad distribution of governance rights.	Parameters fixed or meaningfully dispersed; no single party can dictate outcomes.
Ongoing business relationship	Is there recurring servicing "for or on behalf of" users?	Managed reward distribution, treasury ops, or curated ongoing services.	Shift to automated smart contracts; eliminate discretionary servicing.	Relationship reframed as self-service code execution, not an ongoing operator user contract.
Governance	Who controls decision-making? How concentrated is voting?	Governance tokens concentrated among founders or insiders; multisig run by affiliates.	Distribute governance power; expand delegate base; publish concentration data.	DAO-driven governance with credible decentralisation, not insider capture.

Criteria	Regulatory Question (PMLA)	Signals of High Exposure (Centralised/ Semi-DeFi)	Progressive Milestones	Reduced Exposure Outcome
Admin keys	Who holds upgrade or pause authority?	Insider-controlled multisigs or unilateral upgrade rights.	Introduce timelocks, multiparty thresholds, and sunset plans to retire keys.	Admin privileges reduced or eliminated; protocol operates without insider overrides.
Solely publishing *vs* operating	Is the team only publishing code, or also running VASP-like services?	Hosting curated front-ends, running custodial bridges, providing off-ramps.	Transition to publishing open-source code; community-hosted interfaces; partnerships with compliant VASPs for fiat rails.	Project role reframed as publisher, not operator, aligning with FATF's "ancillary participant" concept.

This table is intended as a progressive roadmap showing how projects can move from higher exposure to reduced exposure by addressing specific design levers.

Conclusion

For developers and founders, the integration of DeFi protocols into existing regulatory frameworks presents both challenges and opportunities. The PMLA's activity-based VASP definition makes clear that labels are irrelevant; what matters is the degree of control or sufficient influence exercised "for or on behalf of" users. This approach, consistent with FATF guidance, ensures that protocols are assessed on their functional design rather than their aspirational identity.

Understanding regulatory requirements and implementing the framework into the platform is vital. This can only be achieved when builders view regulations as design constraints, as opposed to obstacles. This is the first step towards having an effective compliance programme.

For India, the absence of explicit tests under the PMLA creates uncertainty. Enforcement actions have so far prioritised centralised exchanges and offshore service providers, but without clearer guidance, protocols in the semi-decentralised "grey zone" remain exposed to regulatory interpretation. The critical point is that enforcement actions may be dropped or narrowed, but without top-down policy clarity, similar proceedings may resurface.

However, it is vital to build with an eye on the future. Effective risk mitigation flows by aligning protocol architecture with compliance strategies. Recognising that early-stage projects begin with centralised elements but must trudge a credible pathway towards decentralisation is vital for projects and the regulator. Progressive decentralisation backed by published milestones, control registers, and an observable reduction in insider discretion provides a disciplined framework for moving across the spectrum from high-exposure models to lower-exposure architectures. The end goal is not to sidestep regulations but to drive home the fact the DeFi can co-exist with the existing PMLA compliance framework through careful protocol design, transparent governance and proactive engagement with regulators. By treating control as the decisive test and decentralisation as a progressive journey, builders can reduce exposure, align with regulatory objectives and preserve the functional autonomy that defines DeFi.

Endnotes

1 Available at https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf

2 Financial Intelligence Unit-India, AML & CFT Guidelines For Reporting Entities Providing Services Related To Virtual Digital Assets (March 10, 2023), available at https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf

3 Available at https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/india

4 Available at https://corporate.cyrilamarchandblogs.com/2024/01/fig-paper-no-33-series-2-compulsory-registration-of-off-shore-virtual-digital-asset-service-providers-with-fiu-ind

5 Available at https://fiuindia.gov.in/pdfs/judgements/Binance_Order_10_2024.pdf

6 Available at https://fiuindia.gov.in/pdfs/judgements/Binance_Order_10_2024.pdf

7 Available at https://economictimes.indiatimes.com/news/india/ahmedabad-crypto-exchange-gets-rs-722-croregst-notice-a-first-for-crypto-sector/articleshow/112311656.cms?from=mdr

8 "Decentralised Finance: Use Cases, Challenges and Opportunities", November 2022, available at https://www.iif.com/portals/0/Files/content/DeFi%20Report%2011132022.pdf

9 *Commodity Futures Trading Commission vs Ooki DAO*, available at https://www.cftc.gov/media/8741/enfookidaojudgment060923/download?__cf_chl_tk=ZQBHYI4cBXeYer4SWusOspgiRx5bgWCzUeGI0WwlAKA-1758227769-1.0.1.1-RkR3AW5Ha7iDyFfA7XzjN0sgV1X5tFe.mfpx12_idcc

10 Available at https://blog.uniswap.org/wells-notice-response.pdf

11 Available at https://www.sec.gov/newsroom/press-releases/2024-79

12 Available at https://a16z.com/progressive-decentralization-a-playbook-for-building-crypto-applications

13 Available at https://a16zcrypto.com/posts/article/progressive-decentralization-a-high-level-framework

14 Ministry of Finance (Department of Revenue) Notification (New Delhi, March 7, 2023), S.O. 1072(E), available at https://egazette.gov.in/WriteReadData/2023/244184.pdf

Reddy Pawan Kumar

Tel: +91 963 337 2033 / Email: reddy.pawan@hashlegal.in

Reddy Pawan Kumar is a legal advisor in the tech sector, with a focus on emerging areas of tech such as virtual assets, blockchain, artificial intelligence, gaming and data protection. His in-depth knowledge of Layer 1/Layer 2 blockchain infrastructure projects, token offerings, NFTs, DeFi and CeFi has positioned him as a key advisor of Web 3.0 businesses. With a hands-on approach to navigating regulatory challenges and ensuring compliance, he supports his clients in scaling operations and achieving long-term success in a rapidly evolving industry.

Prior to joining Hash Legal, Reddy built a solid foundation in disputes and commercial law at the Bombay High Court, further strengthening his ability to advise on both litigation and corporate strategy. His combined expertise in tech law, finance, and emerging technologies enables him to provide strategic counsel that aligns legal solutions with business objectives.

Athif Ahmed

Tel: +91 883 872 1433 / Email: athif.ahmed@hashlegal.in

Athif Ahmed leads the emerging tech vertical at Hash Legal, specialising in blockchain, compliance, regulatory, and product development advisory. He has extensive experience assisting clients across all stages of growth, from startups to multinational corporations, helping them set up in India and expertly navigate the unique challenges of operating in the country. With deep expertise in sectors such as gaming, health tech, and fintech, he provides critical guidance through complex regulatory landscapes. In addition to advising companies, he actively works with industry associations on blockchain policy groups.

Athif is a published author on smart contracts and blockchain-related online dispute resolution. His work was featured in the book *Commercial Dispute Resolution: State of Law in India*. A sought-after speaker on emerging technologies, he also serves as an advisor to startups focused on AI and blockchain, shaping the future of tech regulation and innovation in India.

Aabha Dixit

Tel: +91 810 418 3694 / Email: aabhardixit@gmail.com

Aabha Dixit is a dynamic legal professional with significant experience in cross-border M&A, private equity, venture capital transactions, and corporate law. Aabha regularly advises on corporate structuring, regulatory compliance, governance, and general corporate advisory, helping clients align legal obligations with strategic objectives.

Armaan Mistry

Tel: +91 998 788 2662 / Email: armaanmistry7@gmail.com

Armaan Mistry is a technology-focused lawyer with expertise in generative AI and the regulatory challenges of innovation. He brings over two years of sector experience, complemented by a background as in-house counsel for a logistics company. His work combines legal insight with practical understanding of tech-driven enterprise needs.

Hash Legal

Z Square, 2nd Cross Road, Benson Town, Bengaluru, Karnataka – 560046, India
Tel: +91 883 872 1433 / URL: www.hashlegal.in

Global Legal Insights – Blockchain & Cryptocurrency Regulation provides in-depth analysis, insight and intelligence across 11 expert analysis chapters and 29 jurisdictions, covering:

- Government attitude and definition
- Cryptocurrency regulation
- Sales regulation
- Taxation
- Money transmission laws and anti-money laundering requirements
- Promotion and testing
- Ownership and licensing requirements
- Mining
- Border restrictions and declaration
- Reporting requirements
- Estate planning and testamentary succession

globallegalinsights.com