GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation 2025

Seventh Edition

Contributing Editor:
Josias N. Dewey
Holland & Knight LLP

ENTERPRISE ETHEREUM ALLIANCE
WSBA WALL STREET BLOCKCHAIN ALLIANCE
glg Global Legal Group

TABLE OF CONTENTS

Jurisdiction Chapters

India

Reddy Pawan Kumar
Athif Ahmed

Hash Legal

Crypto and blockchain legal compliance in India: Navigating VASP challenges and money laundering regulations

Introduction

'Virtual digital asset' (**VDA**) is a broad term that encompasses assets that leverage blockchain technology for various functions such as creation, storage and transfer of various forms of value or rights, within specific digital environments. For instance, a tangible asset like real estate can be digitally represented as tokens on a blockchain and traded online. VDAs can act as a store of value, similar to traditional property, but instead of existing in the physical world, they exist entirely in the digital environment.

VDAs are more than just digital or physical asset representations; they have a variety of important functions. One key function is serving as a medium of exchange, often referred to as virtual currencies or cryptocurrencies,[1] with Bitcoin and Ethereum being well-known examples. VDAs can also act as investment vehicles, storing value much like traditional assets. Additionally, they play a role as governance tools, often in the form of utility tokens, which help manage decentralised networks. Another type of VDA is the Non-Fungible Token (**NFT**), which holds unique value in areas like digital art, gaming, and intellectual property.

The wide spectrum of use cases for VDAs has led to their increased adoption across multiple sectors, including finance, gaming, and digital media. As more time is spent within virtual environments, the proliferation of VDAs signals a fundamental shift towards a future where digital ownership and digital rights are as significant as real-world ownership and rights over physical assets.

In light of the rapid growth of VDAs, the legal and regulatory framework surrounding them has become an increasingly critical area of focus, especially in jurisdictions like India, which benefits from a large, young, tech-savvy population that has widespread access to smartphones and affordable internet. (India's smartphone user base is projected to reach over 1 billion by 2026, with average mobile data costs amongst the lowest globally.)[2]

However, India's regulatory stance on VDAs remains an evolving issue, and understanding the legal nuances is essential as India constantly navigates this complex space.

Scope of the chapter

This chapter provides a concise overview of the regulatory development of VDAs in India, charting the path from the Reserve Bank of India's (**RBI**) initial ban to the current legal framework established under the Prevention of Money Laundering Act, 2002 (**PMLA**). It critically examines the regulations governing VDAs within India, with a specific focus on how global standards, particularly the Financial Action Task Force (**FATF**) guidelines, have influenced these regulations. Additionally, this chapter delves into the compliance requirements for Virtual Asset Service Providers (**VASPs**) under the PMLA and the guidelines issued by the Financial Intelligence Unit (**FIU**) for VASPs. Importantly, it highlights key gaps and ambiguities in the current Indian regulatory framework, especially regarding the regulation of non-custodial and decentralised VASPs, an area that remains underexplored. Through a comparative analysis, this chapter examines areas where Indian regulations fall short of FATF standards and identifies key regulatory gaps and provides recommendations to address these issues, ensuring that India's legal framework keeps pace with the rapidly changing VDA landscape.

Brief history of the evolution of VDA regulation in India

The evolution of regulations governing VDAs in India has been marked by a series of regulatory shifts, reflecting India's attempts to balance financial innovation with concerns over money laundering and economic stability. This regulatory journey can be traced through several key phases.

Initial concerns (2013–2017)

The RBI first expressed its concerns about VDAs, specifically virtual currencies like Bitcoin, as early as 2013.[3] The RBI highlighted risks posed by unregulated links between virtual and traditional currencies and warned that since VDAs are unregulated, it could lead to potential financial instability, as the issuers of virtual currencies can manage their supply without any oversight. This, coupled with the inherent ease of transfer, particularly across borders, led to the RBI recognising the threat of money laundering and terrorist financing linked to these assets. These early cautionary warnings set the stage for a restrictive approach towards virtual currencies in India. The RBI issued an advisory, cautioning users, investors, and businesses against dealing in virtual currencies due to their speculative nature and lack of government oversight.[4]

During this period, regulatory ambiguity persisted as cryptocurrency exchanges began to emerge in India, operating in a grey area of the law. Although there were no specific legal prohibitions against the trading of virtual currencies, the RBI's cautious stance created an uncertain environment for businesses and investors alike.

RBI ban (2018)

In April 2018, the RBI took a decisive step by issuing a circular that barred financial institutions (like banks) from offering services to businesses involved with virtual currencies. This essentially crippled cryptocurrency exchanges in India by cutting off their access to critical banking services and thereby prevented exchanges from being able to convert cryptocurrencies into fiat (traditional) currency. The ban was driven by concerns over safeguarding the financial system from risk imposed by cryptocurrencies, such as their potential use in illicit activities like money laundering and fraud. The RBI's decision sparked widespread backlash from industry players, who argued that the ban was excessively restrictive and would stifle innovation in the fledgling space.

Supreme Court reversal (2020)

In a landmark judgment in *IMAI v. RBI*,[5] the Supreme Court of India overturned the 2018 RBI circular. The Court ruled that the circular violated the fundamental right to trade under Article 19(1)(g) of the Constitution of India, which guarantees the freedom to carry on any profession, trade, or business.

The Court acknowledged that while the RBI was justified in its concerns about protecting financial institutions, it had failed to satisfy the 'test of proportionality' while imposing an outright ban. The RBI was unsuccessful in demonstrating to the Court that any of the financial institutions regulated by it had suffered any semblance of damage on account of providing services to virtual currency exchanges.

The Court emphasised that any restriction on a fundamental right must be the 'least intrusive measure' available to achieve the intended goal. The RBI had failed to explore less intrusive alternatives and was therefore deemed to have acted disproportionately, thus effectively driving cryptocurrency exchanges out of business.

The decision not only reinstated banking access for cryptocurrency businesses but also marked a turning point in India's regulatory approach, opening the door for dialogue on framing a more effective way forward to regulate VDAs.

Draft VDA bill (2021)

Following the judgment, the Indian government sought to formalise its regulatory approach to VDAs by introducing a draft bill in 2021. The bill proposed to ban private cryptocurrencies while simultaneously laying the groundwork for Central Bank Digital Currency (**CBDC**).[6]

The rationale for banning private cryptocurrencies was grounded in concerns about the volatility, speculative nature, and potential misuse of these assets for unlawful purposes. The draft bill proposed to prohibit activities such as mining, generation, holding, and trading of private cryptocurrencies. However, a final version of the draft bill was not released.

Taxation and regulation (2022)

In 2022, through the annual union budget of the government, India took a significant step towards legitimising VDAs by introducing a flat 30% tax on income derived from the transfer of VDAs[7] and a 1% Tax Deducted at Source (**TDS**) on crypto transactions.[8] This tax is calculated in addition to the income tax payable on all other income of the taxpayer.

This indicated a shift in mindset, signalling a desire to bring the VDA sector under the tax regime. Although the government did not set a clear regulatory framework to bring VDAs within the existing financial ecosystem, the tax provisions of the budget indicated a partial acknowledgment of VDAs as legitimate assets. However, the high level of tax has irked Indian consumers and without clear regulations regarding set-offs and receipt of VDAs for services provided, etc., there remain calls for further changes in the tax regime.

VASP Notification (2023–present)

In March 2023, the Ministry of Finance[9] expanded the definition of a 'Reporting Entity'[10] (**RE**) under the PMLA to explicitly include VASPs as REs (**VASP Notification**). This marked a significant regulatory development.

The VASP Notification includes a wide scope of entities within the ambit of VASPs. Any natural or legal persons who carry out the following activities, for or on behalf of another natural or legal person in the course of business, would be considered a VASP:

'*a. Exchange between virtual digital assets and fiat currencies;*

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

c. Transfer of virtual digital assets;

d. Safekeeping or administration of virtual digital assets or instruments enabling control over digital assets; and

e. Participation in and provision of financial services related to an issuer's offer and sale of a virtual digital.'

The VASP Notification brings VASPs under the same regulatory framework as traditional regulated entities like banks and other financial institutions, requiring them to comply with provisions of the PMLA, as well as the PMLA (Maintenance of Record) Rules, 2005 (**PMLA Rules**).

The introduction of the PMLA framework for VDAs represents the next stage in this regulatory evolution, with the Indian government seeking to align its regulations with FATF standards.

PMLA and implications for VASPs

The PMLA was enacted in 2002 and came into force in 2005 as part of India's commitment to combat money laundering. The primary goal of the PMLA is to prevent money laundering, confiscate property derived from criminal proceeds, and ensure that India's financial system adheres to global Anti-Money Laundering (**AML**) and Counter Financing of Terrorism (**CFT**) standards. With the inclusion of VASPs as REs under the PMLA, it becomes crucial to examine the practical functioning of the PMLA. Analysing the PMLA's mode of operation offers valuable insight, particularly for VASPs, as they undertake steps to comply with the regulations.

Expansive ambit of the PMLA

Since its inception, the PMLA has had a notably expansive ambit. Initially aimed at combatting money laundering activities tied to offences like terrorism and organised crime, its scope has expanded over the years to include a broader range of offences, including corruption and environmental crimes.

Confiscation powers

One of the most striking powers granted by the PMLA to enforcement agencies is the power to confiscate property suspected to be linked to money laundering even when under trial, i.e., before a final verdict. This pre-emptive approach is intended to disrupt the flow of illicit funds by targeting assets before they can be hidden or laundered. However, this provision has not been without controversy, including concerns over potential misuse for political gain.

Burden of proof

The PMLA's approach to the burden of proof departs from conventional judicial norms. The PMLA flips the conventionally accepted burden of proof by placing the burden on the accused, contrary to the widely accepted principle of 'innocent until proven guilty'. The stringent bail conditions under Section 45 of the PMLA have also drawn criticism for making it difficult for accused individuals to secure bail. This has also been subject to controversy and has been severely criticised for its penchant for being used as a tool of suppression of dissent.

Derived from FATF

FATF sets the global standards that underpin India's regulations and AML laws, shaping the provisions of the PMLA. In line with FATF guidelines, financial institutions and intermediaries are required to maintain transaction records and report suspicious activities to the FIU. These obligations are essential for enhancing oversight and ensuring that financial institutions actively contribute to identifying and reporting money laundering to the regulators in line with international standards.

With VASPs now falling under the PMLA regime, it is critical to understand the legal compliances placed upon them. The following section outlines these key legal compliance requirements and their implications for VASPs.

Key compliance measures for VASPs under the PMLA

The VASP Notification has introduced a range of new responsibilities for VASPs. Below is a brief overview of the key obligations and compliances that VASPs must adhere to under the PMLA and PMLA Rules:

1. *Verification of client identity and due diligence*: VASPs are required to conduct Know-Your-Customer (**KYC**) checks on all users. This includes verifying identity through valid documents and identifying whether users are acting on behalf of a beneficial owner, in which case, the beneficial owner's identity must also be verified. KYC measures must be performed at the commencement of an account-based relationship and for all transactions equal to or exceeding INR 50,000 or any international transaction.[11]
2. *Record-keeping requirements*: VASPs must maintain detailed records of customer identities, ultimate beneficial owners (in the case of corporate entities), and transaction details to enable regulators to reconstruct individual transactions. The information to be maintained includes wallet addresses, IP addresses, transaction hashes and any other relevant information.[12] This is critical for ensuring transparency and accountability in VDA transactions, as such data can help trace the origin and destination of VDAs in the event of an illegal activity.
3. *Registration and reporting obligations*: VASPs are now obligated to register with the FIU[13] and must submit electronic copies of users' KYC records to the Central KYC Records Registry within 10 days of the first transaction by a new user.[14] Any suspicious activity that may indicate money laundering or terrorist financing must be promptly reported to the FIU. VASPs are also required to conduct enhanced due diligence when suspecting illegal activity and reassess the business relationship if concerns arise.
4. *Internal compliance mechanisms*: VASPs are mandated to implement robust internal policies, controls, and procedures for conducting due diligence. Senior management must approve these measures, which ensures that a higher degree of accountability exists within the organisation. These internal frameworks are crucial for minimising the risk of financial crime within the VASP sector.
5. *Designated Director and Principal Officer*: VASPs must also appoint a Designated Director and a Principal Officer. The Designated Director, typically a senior management figure, is responsible for overseeing AML compliance, while the Principal Officer is tasked with communicating with the FIU and ensuring the timely submission of reports on suspicious transactions or other prescribed matters.
6. *Enhanced reporting obligations*: VASPs are required to file reports within seven working days in the following instances of increased concern:
    a. There is a reasonable ground of suspicion that the transaction may involve proceeds of an offence (regardless of the value involved).
    b. The transaction appears to be made in circumstances of unusual or unjustified complexity.
    c. The transaction appears to have no economic rationale or *bona fide* purpose and gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.
    d. The transaction involves deposits/withdrawals into an account that may be suspicious.[15]
7. *Specific guidelines for VASPs*: In line with international standards established by FATF, the FIU has issued specific guidelines for VASPs (**FIU Guidelines**).[16] A key compliance element is the 'Travel Rule', which requires VASPs in India to include accurate information about both the originator and beneficiary in all VDA transfers. VASPs of both the originator and beneficiary are obligated to retain and share this information with the relevant authorities upon request. This rule, derived from FATF recommendations, aims to facilitate cross-border cooperation between regulatory authorities across the globe. The implementation of the Travel Rule highlights India's efforts to align its domestic regulations with international norms, thereby promoting greater transparency.

Penalties for non-compliance

Failure to adhere to these obligations can result in serious penalties. The FIU Director has the authority to issue a show-cause notice to non-compliant VASPs and, after inquiry, impose monetary penalties.[17] The severity of these penalties underscores the need for VASPs to implement stringent compliance protocols.

VASP Notification and FATF

FATF is the driving force behind the PMLA regime in India, and the VASP Notification is no exception. The VASP Notification and FIU Guidelines closely mirror the detailed FATF standards on VDAs. For instance, the definition of VDA service providers in the VASP Notification is nearly identical to that in the FATF standards. The FIU Guidelines also heavily draw from these standards. This alignment suggests that the VASP Notification and FIU Guidelines are intended to be interpreted in accordance with FATF standards. This principle has been specifically recognised in the context of the PMLA and FATF standards in the 2022 judgment of *Vijay Madanlal Choudhury v. Union of India*[18] wherein the Supreme Court considered FATF interpretations when construing the PMLA, reinforcing the integration of international standards into domestic regulation.

Under the VASP Notification, any entity that conducts specific activities on behalf of another person as part of its business will be classified as a 'person carrying on designated business or profession', a type of RE under the PMLA. One such category of activities includes the 'safekeeping or administration of VDAs or instruments that provide control over VDAs'.

However, neither the above-mentioned categories nor any of the other categories under the VASP Notification address a very large and integral part of the VDA ecosystem, namely non-custodial and decentralised service providers:

a. *Decentralised platforms*: Decentralised platforms refer to systems that operate on blockchain networks without relying on a central authority or intermediary, enabling direct peer-to-peer interactions. These platforms span a wide range of applications, such as decentralised exchanges (**DEXs**) and decentralised applications (**DApps**).

   DEXs allow users to trade VDAs directly with one another without an intermediary, such as a centralised exchange. Trades on DEXs are typically facilitated by smart contracts (self-executing programs that automatically match buyers and sellers under predefined conditions). DEXs offer greater privacy and control over funds as users retain ownership of their private keys, which reduces counterparty risk.

   DApps are applications that run on a decentralised blockchain network, utilising smart contracts to enable various services or functions. Unlike traditional apps, which rely on centralised servers, DApps distribute their operations across multiple nodes in the network, increasing transparency, security, and resilience against single points of failure. Popular examples of DApps include decentralised finance (**DeFi**) applications for lending, borrowing, and trading, as well as platforms for gaming, social media, and content distribution.

   These decentralised platforms typically operate on public blockchains like Ethereum, Binance Smart Chain, Solana and others, ensuring transparency and security through cryptographic protocols.

b. *Non-custodial wallets*: Non-custodial wallets are digital wallets where users have full control over their private keys. These private keys are cryptographic keys that allow users to access and manage their assets. As a result, users are solely responsible for the security and management of their assets. In contrast, custodial service providers, like centralised exchanges, store users' assets and private keys on their behalf.

Status of decentralised platforms and non-custodial wallets under FATF

Evolution of FATF Guidance on Virtual Assets and VASPs

In June 2019, FATF released its first comprehensive guidance on Virtual Assets and Virtual Asset Service Providers (**2019 Guidance**).[19] This 2019 Guidance recommended that countries apply a risk-based approach to mitigate risks related to VDA activities emphasising the role of central entities responsible for administering and facilitating VDA transactions. FATF's primary focus was on centralised exchanges and custodial services, which mirror the structure of traditional financial institutions where intermediaries maintain control over users' assets.

The 2019 Guidance also recognised that exchange or transfer can occur through decentralised platforms. It further clarified that when such platforms facilitate or conduct the exchange or transfer of value (whether in VDA or fiat), its owner/operator, or both, may fall under the VASP regime. However, this carve-out only applies if the person is engaged in business activities that would qualify them as a VASP.[20]

The 2019 Guidance detailed that countries should not regulate the technology that underlies VASP activities but focus on regulating the natural or legal person behind such technology or software application that uses this technology to facilitate financial transactions. When regulating non-custodial wallets, the 2019 Guidance further stated that countries should not regulate ancillary services or products to a virtual asset service network, such as hardware wallets or non-custodial wallets.

However, the evolving landscape and the increased use of decentralised platforms and non-custodial wallets presented significant regulatory challenges. In response, FATF revisited its guidelines and assessed whether non-custodial wallets and the transactions they facilitate should be subject to AML/CFT regulations, thus releasing an updated guidance in 2021 (**2021 Guidance**).[21]

The challenge of decentralised platforms

Decentralised platforms often integrate non-custodial wallets and smart contracts to enable automated transactions between users without centralised oversight. FATF guidelines acknowledge that the decentralised platforms themselves are not VASPs; however, the guidelines also raised concerns about the potential risk posed by individuals or entities that manage or exercise control over these platforms.

The 2021 Guidance explicitly states that where a person or entity maintains control over key functions of a decentralised platform or influences its activities, they may still be considered a VASP, even if the platform itself is decentralised. FATF suggests that regulators focus on the human or organisational elements behind these platforms to ensure compliance with AML/CFT standards.

Implications for Indian regulators

FATF's stance on non-custodial wallets and decentralised platforms intentionally leaves room for interpretation. Countries are expected to analyse risks based on their specific circumstances and accordingly adopt a risk-based approach when determining how to regulate decentralised platforms and non-custodial wallets. However, FATF has cautioned against overregulation of the technology itself, as this could stifle innovation in the blockchain space.

Countries have addressed these challenges by incorporating FATF recommendations into their regulatory frameworks. However, the diversity of approaches highlights the delicate balance between innovation and regulatory oversight. For instance, some regulators have begun requiring centralised exchanges to impose stricter controls on transactions involving non-custodial wallets, while others are exploring the development of more comprehensive frameworks for monitoring decentralised platforms and non-custodial wallets.

Lacuna in the existing PMLA framework

A careful examination of the VASP Notification and FIU Guidelines under the PMLA reveals significant ambiguities, particularly regarding non-custodial wallets and decentralised platforms. It remains unclear whether entities providing these services are considered VASPs and are thus required to comply with the VASP Notification, register with the FIU, and adhere to the FIU Guidelines.

FATF and its interplay with Indian law

According to FATF's 2019 and 2021 Guidance documents, service providers that merely develop or sell non-custodial wallets do not typically fall under the definition of a VASP. The guidance specifies that unless the provider holds or controls private keys, they are not engaged in activities that would classify them as VASPs.

This distinction is critical for the Indian regulatory framework, which lacks clarity on whether non-custodial wallet and decentralised platform providers are subject to PMLA obligations. Unlike FATF's explicit guidance, Indian regulations fail to distinguish between software developers and custodial service providers, leaving such entities in a legally uncertain position.

Custodial wallet service providers and private keys

Regarding custodial wallet service providers, it is clear that centralised exchanges, which hold users' private keys and control their assets, fall under the scope of the PMLA. These entities must implement robust AML/CFT measures, including KYC procedures, transaction monitoring, and suspicious activity reporting, as per FATF standards.

In the case of multi-signature wallets (where control is distributed across several private keys), FATF guidelines state that if an entity holds even one of the multiple keys required to authorise a transaction, countries may deem that such an entity will exercise control for regulatory purposes. This expands the definition of control in a way that is directly relevant to Indian regulators, as it underscores the need for a more nuanced approach to determine which entities are considered VASPs. Unfortunately, the current Indian framework does not provide guidance on multi-signature wallets, creating potential gaps in enforcement.

Decentralised platforms

Decentralised platforms, such as DEXs and DeFi platforms, also unfortunately find no mention in the VASP Notification.

The FATF Guidance acknowledges that decentralised platforms often do not align well with the traditional VASP framework. Decentralised platforms generally are not classified as VASPs unless a central entity or individual exercises control or influence over the platform's operations. In such cases, the responsible person or entity may be subject to VASP regulations, even if the platform itself remains decentralised. This distinction is essential, as it emphasises that regulators should prioritise oversight of the human or organisational actors behind decentralised platforms, rather than attempting to solely regulate the underlying technology. In contrast, the VASP Notification and FIU Guidelines provide no such clarity on decentralised platforms.

Non-custodial wallets

The misalignment between Indian regulations and FATF guidelines is further exacerbated by the lack of clear guidance on non-custodial wallets. FATF guidelines explicitly state that non-custodial wallets are not considered VASPs unless they engage in business activities that involve control over user assets. This distinction is critical for maintaining a balanced regulatory framework that does not unnecessarily stifle innovation in the blockchain and virtual asset sectors, while maintaining custody over one's funds, which is central to the cryptocurrency and decentralised ethos.

Indian regulations, however, offer no such clarity. The FIU Guidelines and VASP Notification fail to differentiate between custodial and non-custodial services or to account for the unique nature of decentralised platforms that utilise such non-custodial wallets. This lack of differentiation creates confusion for service providers and hinders the ability of the Indian regulatory framework to adequately address the risks associated with virtual assets.

Conclusion

India's regulatory journey has made notable strides, yet key gaps continue to hinder innovation, adoption and growth. While the inclusion of VASPs under the PMLA and taxation of VDAs are strong steps towards formalising the industry, they primarily focus on centralised entities. The core principles of blockchain – decentralisation, transparency, and autonomy – remain largely overlooked. Decentralised platforms and non-custodial wallets are a manifestation of these core principles and are integral to the VDA ecosystem. However, they remain unaccounted for in India's regulatory approach. Though these platforms often operate without central oversight, they represent the very ideals that make blockchain transformative and cannot be overlooked.

Ignoring the decentralised aspects of blockchain could lead to higher risks in AML efforts, while simultaneously leading to the flight of both talent and capital towards more favourable jurisdictions.

To mitigate these risks and support a thriving digital asset ecosystem, India should align its regulations more closely with FATF guidelines. This means focusing on the entities and individuals controlling decentralised platforms, rather than the technology surrounding the platform. By addressing these gaps, India can create a regulatory framework that encourages innovation, reduces financial risks, and positions the country as a leader in the global digital economy. The need of the hour is a nuanced approach, centred on control, taking into account influence over decentralised platforms and identifying specific risks. This would strengthen the PMLA regime and equip regulators to protect consumers while simultaneously fostering innovation and growth, leading to a thriving digital asset ecosystem.

Endnotes

1 Virtual currencies are digital representations of value used as a medium of exchange within specific virtual environments or communities, while cryptocurrencies are a subset of virtual currencies that use cryptography for security and operate on decentralised networks, such as blockchain technology, with examples including Bitcoin and Ethereum. For the sake of this chapter, the terms '*virtual currencies*' and '*cryptocurrencies*' are used interchangeably.

2 Available at https://www2.deloitte.com/in/en/pages/technology-media-and-telecommunications/articles/big-bets-on-smartphones-semiconductors-and-streaming-service.html

3 Reserve Bank of India, *Financial Stability Report No. 7* (Sept. 1, 2024, 4:20 PM), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FSPI260613FL.pdf

4 Reserve Bank of India, *RBI Cautions Users of Virtual Currencies Against Risks* (Sept. 1, 2024, 4:20 PM), https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247

5 *IAMAI v. RBI*, 2020 SCC Online SC 275.

6 The Committee on Payments and Market Infrastructures and the Markets Committee define a Central Bank Digital Currency as a 'digital form of central bank money that is different from balances in traditional reserve or settlement accounts' (Committee on Payments and Market Infrastructures and the Markets Committee, *Central Bank Digital Currencies*, CPMI Papers, No. 174, March 2018).

7 Ministry of Finance, *Department of Revenue Notification 30th June 2022*, S.O. 2959 (E).

8 Ministry of Finance, *Deduction Of Tax At Source Income-Tax Deduction From Salaries Under Section 192 of the Income-Tax Act, 1961 07th December 2022*, Circular No. 24 of 2022.

9 Ministry of Finance, *Department of Revenue Notification 7th March 2023*, S.O. 1072 (E).

10 Section 2(1)(sa)(vi), Prevention of Money Laundering Act, 2002.

11 Rule 9, Prevention of Money Laundering Rules, 2005.

12 Rule 4, Prevention of Money Laundering Rules, 2005 read with Directions under Section 70B(6) of the Information Technology Act, Ministry of Electronics and Information Technology Directions dated 28 April 2022 read with Financial Intelligence Unit Guidelines for Virtual Asset Service Providers, Guideline 6.

13 Ministry of Finance, *Registration of Virtual Digital Asset Service Providers in FIU India as a Reporting Entity*, F. No. 9-8/2023/COMPL/FIU-IND.

14 The Indian government has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (**CERSAI**) to act as, and to perform the functions of, the Central KYC Records Registry *vide* Gazette Notification No. S.O. 3183(E) dated 26 November 2015.

15 Rule 2 read with Rule 3(D) and Rule 8 of the Prevention of Money Laundering Rules, 2005.

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

17 Section 13, Prevention of Money Laundering Act, 2002.

18 *Vijay Madanlal Choudhary v. Union of India*, 2022 SCC Online SC 929.

19 Available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html

20 Paragraph 40, 2019 Guidance.

21 Updated Guidance: A Risk-Based Approach To Virtual Assets And Virtual Asset Service Providers, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

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.

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 analysis, insight and intelligence across 30 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