



Standard Operating Procedures (SOPs) to Regulate Key Concern Areas of Virtual Digital Assets (VDAs)

A REPORT BY CHASE INDIA & **INDUSLAW**

17 MAY 2023

TABLE OF CONTENTS

1. INTRODUCTION AND OVERVIEW	03
2. KEY ASPECTS OF STANDARD OPERATING PROCEDURES (SOPs)	05
3. PRINCIPLE-BASED SOP FRAMEWORK FOR REGULATION OF VDAs	10
4. GLOBAL REGULATORY APPROACH	13
5. ABOUT CHASE	19
6. ABOUT INDUSLAW	20

PREFACE

The crypto assets sector has been on the watch list of both investors and lawmakers in recent years due to the increased adoption across the world. India has an estimated 25 to 30 million crypto investors, and the numbers are likely to significantly increase in the coming years. The sector has a flourishing ecosystem replete with exchanges, wallets, miners, and investors. The sector has massive potential in terms of contribution to the economy and generating employment. According to a report published by CrossTower and US-India Strategic Partnership Forum, embracing and fostering crypto assets in India would grow the country's GDP at a healthy 43.1% CAGR from \$5.1 billion in 2021 to \$261.8 billion over an 11-year period, resulting in a \$1.1 trillion contribution to the GDP. The bulk of this \$1.1 trillion in economic growth for India over these 11 years would be derived from ancillary crypto asset-related businesses that are yet to be materialised.¹

However, despite the large number of players involved in the crypto-asset market, it remains largely unregulated and currently operates in a grey zone, abstruse in its many dimensions. The lacuna stems from the inability of the existing legal framework to deal with policy issues and concerns surrounding crypto assets.

Governments across the world have identified major concerns in the crypto assets sector that revolves around financial stability, investor and consumer protection, money laundering etc. Owing to these risks, the bulk of entities operating in the crypto-asset market in India and across the world currently lack standard operational, governance and risk practices. This has led to market turbulence and uncertainty in operations for the industry players and is gradually eroding consumer trust and confidence in the sector.

Therefore, it is imperative for governments worldwide to develop standard operating procedures for crypto assets. This would help countries globally, across the G20 group and beyond, to have a technology-driven regulatory framework which will promote cooperation across borders and address the major policy concerns. India's ongoing G20 Presidency has been making a strong case for global regulation of crypto assets.

With the objective to create a favourable policy ecosystem for the crypto assets, **Chase India & INDUSLAW** have drafted the report aimed at developing standard operating procedures (SOPs) for the sector. The report has described in detail the four major areas – i) Consumer and Investor Protection, ii) Access for LEAs to Address Fraudulent Activities, iii) Regulatory Arbitrage, and iv) Financial Stability which have been the key cause of concern for the governments and regulators worldwide. As a way forward approach, the report has touched upon the key aspects of these major concern areas and drawn references from the international best practices to identify the SOPs to regulate the sector.



INTRODUCTION AND OVERVIEW

In their short history, Virtual Digital Assets (“VDAs”) have proven their utility in public service, wealth distribution, and economic access worldwide through their utilization of digital ledger technology (“DLT”) or blockchain technology. DLT allows for trust, security, transparency, and the traceability of data, which is especially beneficial to the financial context as it contributes to the reduction of information asymmetry and improves accountability in the provision of financial services. However, the ‘crypto sphere’ can be a potential safe haven for financial transactions by terrorist regimes and white-collar criminals. In addition, large-scale adoption of VDAs without regulatory oversight and control can adversely impact customers or investors who invest in such VDA projects and can have further macroeconomic impacts. On the other hand, globally, inordinate weightage has been placed on these concerns inviting disproportionate restrictions on VDAs by most governments. In doing so, an important economic opportunity is being missed by countries.

In India, regulations relating to VDAs have not been finalized yet, and one can expect some guidance for domestic regulation in India on VDAs emerging from the discussions currently underway within the G20. However, the general regulatory approach towards transactions relating to VDAs has been predominantly cautionary, perhaps for the right reasons. Recently, high taxes on VDA gains in India have been introduced as a means to deter investors/customers from making an investment in VDAs.² This may be done to ensure that the retail investor is discouraged from investing and transacting in crypto, and only large institutional investors with appropriate

risk appetite and financial capability may engage in such investments. In addition, the government has taken note of the problems existing in the sector in relation to money laundering and has brought VDAs under the purview of the extant anti-money laundering framework in India by including VDA Service Providers in the Prevention of Money Laundering Act (PMLA).

Moreover, there are several challenges recognized globally in relation to VDAs. It is necessary to consider such **challenges** in order to formulate an effective framework for SOPs.

Problem of Anonymity

It is pertinent to note here that crypto was built on blockchain ledger technology. The blockchain was lauded for ensuring the authentication of transactions by all users on the blockchain. One of the advantages of the blockchain was not to create a transactional plane where the payer and payee can be faceless and untraceable but to increase consumer ownership of transactions.

This challenge is not the first time that governments have had to deal with a transactional plane that cannot be traced back to the payor or payee. Cash transactions still constitute the bulk of grey market exchange. This does not mean that cash as a medium of exchange and store of value can be banned or derecognized. Credit and debit through bank transfers also occasionally happens over the wire without a need for identity verification or using proxy verification details. In other words, the identity of the source of funds and the fund’s receiver is not critical for a bank transfer to occur as they happen

over the internet. In both the above cases, and in the present case of crypto, regulatory mandates for KYC and a formal customer relationship mechanism between holders/consumers of VDAs and Virtual Asset Service Providers (VASPs) are required.

Transformation of VDAs

Conversion of fiat currency held in traditional bank accounts undergo a complicated 'cleansing' process whereby this money is converted into a virtual digital asset. In this manner, the primary money trail that underlies the asset is obfuscated.³ However, in its current usage, crypto is used as a store value. Thus, the value held in crypto in this manner has to be realizable at some point and be integrated into the fiduciary cash flow of an economy to become usable by the beneficiary. Once again, regulatory efforts should be geared towards recognizing VDA exchanges as regulated entities. It would also behove governments use available softwares which can untangle or 'un-mix' and 'un-layer' crypto which has been converted from fiat to a VDA. This is indeed an opportunity for governments to integrate programs and specialized e-governance frameworks into law enforcement. With the adoption of machine learning based on Bigdata, the regulator will develop an initial database and upgrade or update its existing database to investigate criminals laundering money. As is suggested by international organisations like the FATF, ample budget and personnel need to be set aside for the development of such a database and investigative software.

Central Regulation of a Decentralized Asset Class

VDAs are also the vanguards of decentralized finance. The distributed nature of blockchain ledgers has been put to both virtuous and vicious use. On one hand, blockchain is goal-oriented in that it affords authentic exchange of value over secured networks which are verifiable by anyone who is a part of the transaction. On the other hand, it shuts out centralized law enforcement agencies from knowing the sources of funding. This problem is further exacerbated by the global infrastructure that supports such transactions, with links, in the form of an exchange or a mixer or a custodian, present at every node of the exchange infrastructure.

Global reach, anonymity and speedy transactions between the payer and the payee directly have made VDAs conduits for money laundering, terror financing and other illegal activities. To combat such activities, SOPs (in line with requirements under the PMLA) could help LEAs in quick and timely intervention. We suggest a model of regulatory agility and enforcement tools that can enable governments to confidently allow VDAs and benefit from their success.

Policymakers and stakeholders across the world have been closely monitoring the developments in India amid the ongoing G20 Presidency, which is expected to build a global consensus to regulate the crypto asset sector in India. The country's Finance Minister Nirmala Sitharaman on multiple occasions reiterated that ***"crypto has been a very important part of the discussion under India's G20 Presidency, given so many collapses and shocks. We seek to develop a common framework for all countries to deal with this matter"***. The stage has already been set and it's just a matter of time before the crypto asset sector will be regulated by a set of comprehensive laws.





KEY ASPECTS OF STANDARD OPERATING PROCEDURES (SOPs)

India has begun engaging in dialogues on crypto regulation through platforms such as G20 where discussions shall be conducted on policy approaches towards this sector. Further, distinguished institutions such as the IMF are developing papers focused on “monetary policy and policy approach to crypto assets” through multi-stakeholder consultations. The government has time and again acknowledged the need for prioritizing crypto regulation and the need for developing SOPs.

Setting Minimum Standards

To achieve the overarching goal of promoting global regulations for Web3, it is essential to establish minimum policy and technology standards that countries around the world must adopt. These standards can be classified into different categories based on the nature of the regulatory measures a country wishes to adopt, ranging from conservative to liberal. The minimum standards cover a wide range of issues, including common definitions and classification, consumer protection norms, minimum data collection guidelines, transaction monitoring infrastructure, standardised due diligence, disclosure requirements, compliance measures including licensing for virtual asset service providers, technical standards for cybersecurity, standards to mitigate the adverse impact on the climate, and standardised audit requirements.

Data Sharing

Given the capacity of Web3 to facilitate the peer-to-peer transfer of value via crypto-assets, there is a potential for it to be exploited for unlawful activities, such as money laundering, terrorism financing, and tax evasion. It is, therefore, crucial to establish channels for nations to share information on crypto-asset transactions. Such a mechanism will serve as a crucial tool in promoting transparency in cross-border financial investments and combating offshore tax evasion, and other illicit activities. Thus, it is essential to incorporate a framework for the collection and automatic exchange of information on crypto-asset transactions in global efforts to regulate the Web3 space. The compliance mandate should aim to strike a balance between safeguarding investors and preventing illicit activities while simultaneously promoting innovation and competition.

Capacity Building

Capacity building is critical for the development and growth of the Web3 ecosystem. As industry evolves and new technologies emerge, it is essential to ensure that there is a skilled workforce equipped with the necessary knowledge and expertise to navigate the space effectively. These initiatives can take various forms, such as training programs, workshops, hackathons, mentorship, and education initiatives. These efforts can help create a pool of talented developers, entrepreneurs, and innovators who can drive the growth of the Web3 industry and

contribute to the creation of new products and services. Additionally, by investing in capacity building, these organizations can help develop a talent pipeline that can meet the demands of the rapidly evolving industry.

Against this backdrop, we have identified four priority areas where there is a need to develop SOPs in order to effectively regulate the VDA sector in India (and globally).



Consumer and Investor Protection

- Lack of Effective Consumer Protection Standards:** In the international scenario, consumer protection in relation to VDAs are driven predominantly from a disclosure-based approach, similar to India. Certain countries have proposed regulation as a conscious decision of dissociation from the unregulated nature of crypto trading. In contrast, jurisdictions that are still pondering regulation and consequent legislation have advocated for cautionary standards to be included while showcasing VDAs to the public, including advertisement conditions and trading prohibitions. However, there is no singular plan of action in relation to effective consumer protection standards that have been adopted prominently by the international community as a whole, which appears to be the need of the hour.
- Advertising Guidelines:** The Advertising Standards Council of India ("ASCI"), the independent body regulating advertising content in India and has issued specific guidelines for advertising and promotion of virtual digital assets and services, including cryptos on March 8, 2022 titled 'Guidelines for Advertisements of Virtual and Digital Assets and Services' ("ASCI Guidelines").⁴ The purpose of these guidelines is to provide advertisers and advertising agencies with

clear and comprehensive rules for advertising and promoting virtual and digital assets and services in a manner that is truthful, honest, and not misleading.

The ASCI Guidelines cover various aspects of advertising, including the use of endorsements and testimonials, the depiction of risk and safety, and the clarity and adequacy of disclosures, specifically by celebrities and prominent personalities. The ASCI Guidelines also require a categorical disclaimer to be made to the general public regarding the risky nature of VDAs and the potential unrecoverable loss of funds which may result from investments being made in VDAs.⁵ Additionally, advertisements are prohibited from portraying VDA products as being regulated in India or being compared to regulated asset classes.

- Caution to Investors due to the Unregulated Nature of Crypto:** Sectoral regulators have also cautioned investors in relation to investments made in VDAs. The RBI had also issued circulars in relation to the unregulated nature of crypto assets in India, clarifying to users, holders, and traders of VDAs the immense risk associated with an investment in an unregulated asset class.⁶ The Union Ministry of Corporate Affairs has also amended the Companies Act, 2013, requiring companies to disclose any transactions in relation to VDAs in their balance sheets.⁷ SEBI, in its

responses to the Parliament Standing Committee on Finance has also suggested the applicability of existing laws like the Foreign Exchange Management Act, 1999, Banning of Unregulated Deposit Schemes Act, 2019 and the Consumer Protection Act, 2019 to endorsements of VDAs made in violation of such laws.

Accordingly, from a regulatory perspective, there is a need to ensure that exposure to virtual assets is carried out through verified channels, after proper due diligence, in order to prevent larger macroeconomic impacts from any untoward incidents in the virtual asset industry. Issuance of SOPs may be helpful in this regard, to appraise entities involved in the banking and financial sector of the prevailing regulatory stance regarding virtual assets, requisite risk assessment practices, and guidance on broader impacts and avoidance of the same by such entities.

Access to Law Enforcement Agencies (LEAs) to Address Fraudulent Activities (AML/CFT)

- **Issue of Jurisdiction:** The primary issue with VDAs is that VDA transactions seem to exist in a parallel space where international boundaries and jurisdiction are in abeyance. Most of the commentary around VDAs and the jurisdictional issues faced by law enforcement agencies in clamping down on crypto-fueled financial crime sees jurisdiction as a primary challenge.⁸ The silver lining is that the lack of centrality and domicile seems to be every regulator's problem and can be tackled if agencies act in lockstep. Jurisdictional issues are a matter of procedure and need to be dealt with at the international level. Appropriate Conflict of Laws rules can be formulated to deal with the post-investigation adjudication stage.
- **Issue of Inquiry and Investigation:** At the investigation stage, a robust system of inter-agency networks needs to be put together for information sharing and cooperation. India can take the lead in inter-agency information sharing and making its financial systems available for investigation by other agencies. A standard operating protocol, in line with international best practice, as reflected in FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs) must be adopted.⁹ India has taken a robust step in

this direction by including VDA Service providers in the PMLA and can leverage its G20 presidency in heralding multilateral cooperation in enabling VDA transactions with regulatory oversight.

- **VDAs under India's Money Laundering Framework:** As stated in the above point, India has made notable advances in preventing the use of VDAs under money laundering regulations. Reiterating India's commitment to the Vienna Convention on combating money laundering, drug trafficking, and countering the financing of terror (CFT), all crypto transactions have been brought under the ambit of the Prevention of Money Laundering Act, 2002 from March 7, 2023.¹⁰ Reporting requirements inscribed into the existing AML framework under the Prevention of Money Laundering Act, 2002 now apply to virtual asset providers equally. Further, transaction-related information has also been mandated for reporting if it falls under the category of "suspicious transactions".
- **CERT-In Mandate for Cyber Incidents:** Recently, the Indian Computer Emergency Response Team (CERT-In) issued new guidelines for cyber incidents.¹¹ These rules have introduced record-keeping and KYC mandates for VASPs and custodian wallet service providers. The mandate is exhaustive enough to reconstruct the transaction in case of a cyber incident involving VDA transactions. These rules have been formulated based on the experience of CERT-In and the difficulties it has faced while investigating cyber fraud. In this manner, they ensure a timebound process to clamp down on the malicious use of VDAs.

Regulatory Arbitrage

- **Absence of Uniform Regulation:** Crypto assets are functioning amidst varying jurisdictional oversight owing to the absence of global governance or international standards. Given its architecture, it may be excluded from the definition of conventional securities. It thus operates outside any established regulatory frameworks, thereby being vulnerable to regulatory arbitrage. Lack of market transparency, clarity about client asset custody, etc. can further lead to asymmetries that can cause voids, loopholes, redundancies, and contradictions.

- **Existence of Non-Integrated Crypto Exchanges:** Multiple non-integrated and non-compliant crypto exchanges have popped up within the crypto ecosystem, which are independently owned and exist in parallel across countries. On an individual basis, the majority of these exchanges function like traditional equity markets where traders submit, buy and sell orders, and the exchange clears trades based on a centralized order book. However, in contrast to traditional, regulated equity markets, the crypto asset market lacks any provisions to ensure that investors receive the best price while executing businesses.
- **Deviations in Crypto Asset Prices:** It has also been observed that there exist deviations in crypto asset prices across different exchanges, which are likely to persist for several days and weeks. Studies have suggested that this arbitrage is larger for exchanges across different countries than within the same country. The absence of regulatory mechanisms increases the role of arbitrageurs who can trade across different markets heterogeneously and any constraints to the arbitrage capital flow may result in market segmentation.¹²
- **Co-opetition Approach for Crypto Regulations:** The regulatory framework for crypto assets should follow a 'Co-opetition Approach', a term coined by renowned academicians Adam M. Brandenburger and Barry J. Nalebuff in 1996, where the principles of competition and cooperation are paid weightage while taking public policy decisions. This approach focuses on minimizing the chances of regulatory nationalism by attempting to balance domestic, political, and economic interests with international expectations. The recommendation aligns with the views of senior IMF counsel, Marianne Bechara, who believes that crypto regulatory frameworks need to be coordinated internationally but tweaked to meet local differences.

Financial Stability

- **Regulatory Concerns in India:** The RBI has been vocal about the risks that virtual digital assets may pose to traditional banking and financial institutions and to India's financial stability. In 2018, the RBI issued a circular banning any regulated entities, including banks, from dealing in crypto. However, this ban was challenged and struck down by the Supreme Court of
- **Reducing Sovereign Control over Monetary and Fiscal Landscape:** Considering that most virtual currencies and virtual digital assets are controlled solely by corporate enterprises, utilisation of such currencies for transactions will reduce the impact of government control on monetary policy and impair financial and macroeconomic stability of the country.

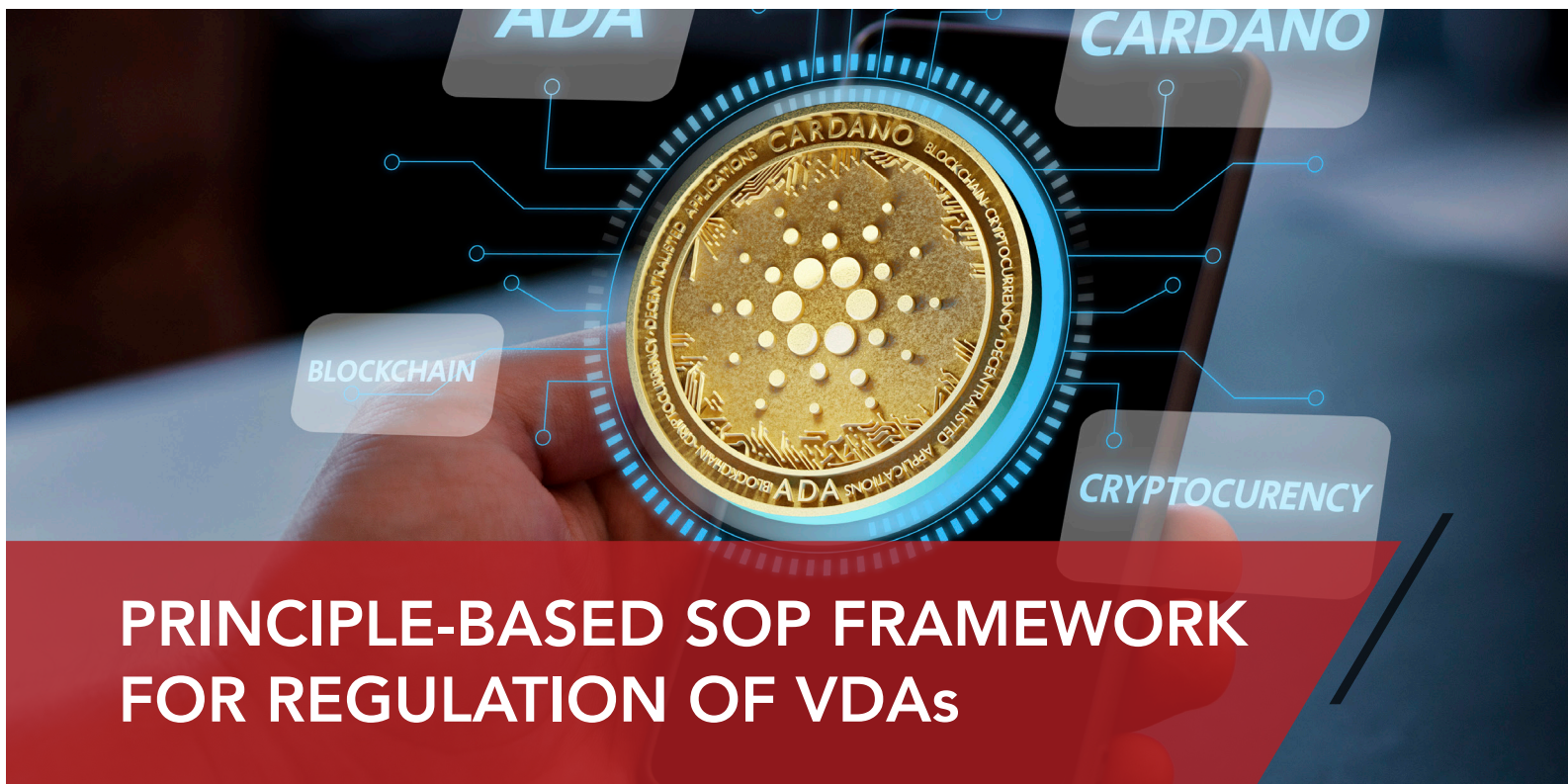
India ("Supreme Court") in the Internet and Mobile Association of India v. Reserve Bank of India case.¹³ Even as the Supreme Court struck down the ban under the circular, it had noted that - *"Irrespective of what VCs actually do or do not do, it is an accepted fact that they are capable of performing some of the functions of real currencies. Therefore, if RBI takes steps to prevent the gullible public from having an illusion as though VCs may constitute a valid legal tender, the steps so taken, are actually taken in good faith."*

- **Dollarisation of the Indian Economy:** While the RBI has generally recognized the benefits that cryptography and DLT may provide to the financial sector, it has identified that there exist broader financial and macroeconomic risks that are associated with private virtual digital assets (like private cryptos, and more broadly, for all private currencies). The use of private currency, including virtual digital assets and crypto, results in the "dollarisation" of the Indian economy - which refers to the use of parallel currency in financial transactions. At times, the use of crypto leads to literal dollarisation, if stablecoins linked to the dollar start being increasingly utilised in financial transactions. Acceptance of Cryptos as legal or acceptable tender would adversely affect the integrity of the capital account regime, as policy control on capital flows would be eroded. The consequence of this on foreign exchange reserve accretion and exchange rate management raises serious macroeconomic stability issues.
- **Diminishing Credit Creation and Mobilisation:** Crypto priced in convertible currencies like the Euro and Dollar may diminish the Indian banking system's ability to mobilise deposits in Rupees. Additionally, utilisation and adoption of such crypto would also reduce the banking system's ability to create credit and would further reduce the impact of the government's monetary policies on credit creation in relation to the foregoing convertible currencies.

Accordingly, the RBI has clarified that private virtual digital assets and crypto do not qualify as legal tender in India. Importantly, the RBI has introduced the central bank digital currency ("CBDC") of India called Digital Rupee or e₹, which incorporates the unique advantages of central bank money, namely, trust, safety, liquidity, settlement finality and integrity. Through the CBDC, the RBI aims at providing the public with benefits that virtual currencies or blockchain based currencies offer. Further, through the CBDC, the RBI intends to route investors in virtual digital assets to adopt the e₹ for conducting

transactions in place of private virtual digital assets. This enables sovereign control over Indian currency, while providing tangible benefits of DLT to entities engaged in financial transactions, within the legal and regulatory framework of India. But it must be noted here that CBDCs and VDAs are two independent technologies, aimed at solving different things, and hence can coexist. While one is a legal tender, the other is the representation of blockchain which incentivises truly decentralized ledgers. Assuming that CBDCs could solve for what VDAs offer, and vice versa would not be entirely accurate.





PRINCIPLE-BASED SOP FRAMEWORK FOR REGULATION OF VDAs

Any attempt to regulate the VDA sector must align with the avowed goals of the financial sector formulated by the Government of India. In this regard, reference is made to the report of the Financial Sector Legislative Reforms Commission.¹⁴ According to the Report, the objectives of financial regulation to ensure consumer protection are:

1. Protecting and furthering the interests of consumer financial products and services; and
1. Promoting public awareness in financial matters.

Applying these goals to the regulation of VDAs, we can surmise that regulation of VDAs should promote information dissemination and relevant disclosures about VDAs. Further, regulation should not suffocate the VDA industry. The benefits of VDAs should be maximized even as their misuse is being controlled.

Regulatory Bodies for VDAs and VASPs

- The Ministry of Electronics and Information Technology (MeitY) could be tasked with having oversight over the development and opportunities related to blockchain technology, VDAs, Web3 and other related emerging technologies.
- The Department of Revenue (DoR) and the Financial Intelligence Unit of the DoR can have the authority and jurisdiction over existing and emerging risks such as VDA-related fraud, money laundering etc. In doing so, the DoR and FIU-IND may co-opt other Ministries, Departments and agencies on a need basis.

- A Self-Regulatory Body / Organisation (SRO) shall be empowered and granted statutory status as an independent self-regulatory body for regulating the VDA sector in India. Such an SRO shall work closely with the Government of India in formulating and ensuring the application of standards and self-governing codes which shall be adhered to by the members of the SRO.
- Given that VDAs as an asset class overlap in some of their properties with other existing asset classes, and given also the financial aspects related to VDAs, the existing monetary and financial markets regulators i.e., RBI and SEBI respectively, may be empowered to formulate guidelines in relation to such aspects of the VDA sector that overlap with their existing mandate / jurisdiction.
- Formation of a high-level coordination committee / task force that may issue periodical advisories for regulatory requirements to be adhered to by VASPs, and coordinate and collaborate with the various arms of the government in developing further regulation in light of evolving sectoral challenges.

Framework for VDA Regulation

- Different existing laws and regulations may be amended to accommodate VDAs as a use case.
- A Code of Ethics shall be developed under the aegis of the SRO for the issuance, exchange, trade, and usage of VDAs.

- Obligation to act honestly and fairly in the best interest of customers.
- VASP shall support their customers with clear information, in particular, in marketing communications. They shall not, deliberately or negligently, mislead a customer in relation to the real or perceived advantages of any VDA.
- The VASP shall ensure that the platform does not engage in bait or surrogate advertising, endorsements by celebrities or free claims advertisements, or any activity prohibited under the Consumer Protection Act, 2019. It shall be the duty of the VASP to comply with all provisions of the 'Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, issued by the Central Consumer Protection Authority.
- Given their nuances and properties, VDAs may be categorized as a separate asset class. [Such a discussion is currently underway within the G20, and it is expected that India may work on a domestic classification and categorisation of VDAs post the G20 discourse. Hence it will be premature at this stage to classify and categorize exactly what VDAs are].
- Considering the macroeconomic and financial risk perceived by VDAs and DLT related financial services, VASPs shall be mandated to apply for and obtain approvals for their business operations by the SRO. [A regulatory sandbox approach may also be considered where VASPs shall demonstrate the efficacy and safety of their products / services to the SRO and / or any designated regulatory bodies and shall be allowed to function after receiving approval from the sandbox].

Prudential Framework for VASPs

- Adherence to prudential norms shall be ensured, bearing in mind the specifics and nuances of the VDA sector (and its differences from other existing asset classes).
- VASPs shall provide users / investors with specific

information about VDAs being issued, their platforms, projects, functions and other relevant information that may be essential to the user or investor engaging with the VDA, in the spirit of risk related disclosures and investor education.

- VASPs shall adhere to any risk-assessment procedures mandated by the SRO, for instance, related to complying with any minimum capital requirements.
- VASPs shall adhere to cyber-risk related assessment and timebound reporting of incidents, in line with the prescribed CERT-In directions of 28 April 2022 (and any others from time to time) for cyber fraud and data losses.¹⁵
- Auditing requirements prescribed by the SRO for VASPs and other VDA services providers such as issuers, custody wallets service providers etc.
- VASPs shall establish and maintain an effective and transparent grievance redressal mechanism for handling of complaints received from customers. The grievances must be addressed in a time-bound manner. They must appoint a Grievance Officer and display their name and contact details on the platform or website.

Fraud and AML Standards

- Procedure for reporting suspicious transactions by VASPs and other VDA service providers to the FIU, for transactions exceeding specific threshold amounts or brackets, should be devised and implemented. [These requirements, and related concerns, have been adequately addressed in the recent PMLA Notification of 7 March 2023].
- An inter-agency data sharing and collaborating protocol to be formulated by the Central Government in cases where Indian law enforcement agencies need to collaborate with foreign law enforcement agencies for a malfeasance identified in India, or malfeasance identified outside India that has an impact in India, also with the aim of encouraging reciprocal cooperation.

Regulations for Business Conduct of VASPs

- VASPs and other VDA service providers may be required to apply for a license to operate, which would be granted by the SRO (or any designated regulator at a later stage) upon fulfilment of certain conditions. The SRO shall make publicly available an updated list of all licensed VASPs, trading platforms, other VDA service providers etc., in the overall interest of users/consumers and other stakeholders.
- While the SRO considers licenses applications by VASPs etc., VASPs etc. may be allowed to enter into a pre-registration undertaking (PRU) with the SRO, which allows unregistered VASPS etc. to continue to operate while the SRO pursues their applications for a license / registration.





GLOBAL REGULATORY APPROACH

Whereas outright bans or prohibitions on the use of crypto assets / VDAs have largely been avoided and are generally not recommended, regulatory frameworks for crypto assets / VDAs have utilized an approach that prioritizes disclosures regarding VDAs. For instance, the Monetary Authority of Singapore (MAS) has provided comprehensive guidance on disclosure requirements applicable to service providers of digital payment token services to the public.¹⁶ These guidelines require clear and conspicuous disclosures including the licensing status of the service provider, risk disclosures regarding volatility and the possibility of a loss of funds, and the nature of services provided to the public by the service providers. Further, the Prudential Regulation Authority ("PRA") in the United Kingdom ("UK") also recommended disclosures of such nature to be made. Specifically, reporting such operational risks becomes imperative in cautioning investors about the nature of the asset being invested in, considering the higher risk of fraud and cyber-attacks with virtual digital assets.

Therefore, taking into consideration the role that legislative commonalities play in addressing globally identified problems posed to international and domestic financial and monetary systems by virtual digital assets, it is imperative that a standardized approach be adopted with respect to the regulatory handling of virtual digital assets. This includes the development of accurate and detailed disclosure frameworks for firms that provide virtual digital asset services as well as financial entities that have exposure to crypto assets. Further, creating mechanisms of valuation for virtual digital assets and development of categorizations and assessment frameworks for legitimate virtual digital assets may be considered as a preventive measure against investment into detrimentally volatile assets. Implementation of these measures should be considered in addition to the implementation of CBDCs by individual nations. This step shall be significant in the development of a consistent practice and a principled approach globally towards financial assets like virtual assets that are utilized on an international scale.

Jurisdiction	Regulation	Regulator	Consumer Protection Standards
Canada	<p>VDAs which may be considered securities are regulated under provincial securities law, covering investment activities of crypto traders dealing in VDAs.¹⁷</p> <p>Provincial laws are harmonized by the Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada ("CSA").¹⁸</p>	CSA	<ul style="list-style-type: none"> VDA traders dealing with VDAs that are under the provincial securities law need to register with provincial regulators. In Feb 2023, the CSA issued guidance for mandatory pre-registration commitments from crypto exchanges to abide by additional investor protection commitments like holding assets in a designated trust or acceptable third-party custodian. For advertising, marketing and social media, the CSA- IIROC have released guidelines on rules applicable to crypto-trading platforms ("CTPs").²⁰ These guidelines focus on : <ul style="list-style-type: none"> false or misleading ads, especially on registration status, endorsement by the securities regulator, suitability of investments, and reasonable material needed for decisions; gaming-like contests and promotions, including the duty to treat clients fairly, honestly, in good faith; compliance and supervisory challenges, dealing with the adoption of policies and procedures governing social media marketing especially with respect to record-keeping systems and ensuring appropriate supervision to prevent false or misleading content. The Financial Consumer Agency ("FCA") in Canada has issued statements to regulated entities dealing in crypto assets to submit pre-registration undertakings ("PRUs"). These PRUs ask the firm to agree to adhere to requisite regulations as well as ensure that risks from crypto-asset activities are addressed properly. In March 2023, the FCA introduced additional requirements in the PRU.²¹ This includes- <ul style="list-style-type: none"> additional commitments on custody and segregation of crypto assets held by Canadians, provision of evidence of meaningful compliance systems, prohibition of unregistered platforms from offering any client leverage, and prohibition of trading on proprietary tokens without CSA's written consent. The Canadian Anti-Fraud Center has issued various handouts and guidelines on how crypto-related scams work.²²

Jurisdiction	Regulation	Regulator	Consumer Protection Standards
Singapore	<p>Crypto is an intangible property regulated as 'digital payment tokens' under the Payment Services Act 2019 ("PSA").</p> <p>Licensing and regulation of Digital Payment Token ("DPT") service providers is overseen by the Financial Services and Markets Act, 2022 ("FSA").</p> <p>Crypto assets with features similar to the capital market products or securities might fall under Singapore's Securities and Futures Act 2001 ("SFA").</p>	Monetary Authority of Singapore (" MAS ")	<ul style="list-style-type: none"> There is no regulation specifically regulating VDAs in Singapore. If a VDA is regulated as a 'digital payment token' or 'e-money' under the PSA, the issuer of such VDA would need a license to provide VDA services.²³ Documentation like token sale terms and conditions, privacy policy, AML/CFT compliance manual, private placement memorandum, or prospectus may be required. If regulated under the PSA, a prospectus is usually required. There is no prohibition on banks dealing in crypto, only a stipulation they must decide whether to accept clients dealing in crypto after customer due diligence and consideration of the risk.²⁴ The MAS has instituted a ban on any public advertisements by DPT service providers in the country.²⁵ MAS guidelines and notices say that advertisements to professional investors by DPT service providers are permitted. For instance, advertising on their websites or social media accounts is allowed. On the other hand, ads in public places like public transport, shopping malls, social media (including third-party social media influencers) or other platforms that could target retail customers are prohibited. The Consumer Protection (Fair Trading) Act, 2003 ("CPFTA") generally prohibits unfair practices that make false claims or might reasonably deceive or mislead consumers. The Second Schedule of the CPFTA provides a list of these unfair practices.²⁶ In October 2022, MAS published consultation papers for measures to reduce consumer harm from crypto and support stablecoins.²⁷ Broadly, it covers the following: <ul style="list-style-type: none"> a. consumer access to information, b. Business conduct for DPT providers for mitigating conflict of interests and handle complaints, and c. security of their systems. MAS has proposed to regulate the issuance of stablecoins, wherein issuers are mandated to: <ul style="list-style-type: none"> i. hold cash reserves for stability ii. pegged to G10 or Singapore dollar, iii. Disclosure requirements and iv. base capital requirements for issuers.²⁸

Jurisdiction	Regulation	Regulator	Consumer Protection Standards
Switzerland	<p>The Distributed Ledger Technology (DLT) Act 2021 and DLT Ordinance (collectively "DLT Framework") regulates all companies, organizations, and individuals dealing in DLT tokenization, investments, and capital markets.</p> <p>Swiss Financial Market Supervisory Authority's ("FINMA") 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings' provide a specific classification system for tokens.</p> <p>The Federal Financial Institutions Act ("FinIA") applies to tokens qualifying as securities.</p>	FINMA	<ul style="list-style-type: none"> The DLT Framework allows for the creation of blockchain digital assets. It describes how private entities should operate and what requirements they must meet to use DLT technology.²⁹ The framework requires all companies within Switzerland to disclose their activities in relation to any DLT assets to ensure transparency. Additionally, it adds a condition to companies to segregate crypto assets from other assets in case of a custodian's default. Utility tokens, asset tokens and stablecoins may be classified as 'securities' and may trigger prospectus and licensing requirements under the FinIA, unless specifically exempted from it.³⁰ Any crypto based assets under the Federal Ordinance on Banks and Saving Institutions ("FBO") have to obtain a FinTech license that disallows investing or bearing any interest, unless exempted.
Germany	<p>Crypto assets have been defined under the German Banking Act (Kreditwesengesetz, or "KWG").</p> <ol style="list-style-type: none"> Digital payments regarded as financial instruments will be regulated under the KWG. Utility tokens are not considered securities under the German Securities Prospectus Act ("WpPG") or investments under the German Capital Investment Act Vermögensanlagegesetz, "VermAnlG"). Security tokens classified as securities or financial instruments and regulated under WpPG and KWG respectively 	Federal Financial Supervisory Authority (" BaFin ")	<ul style="list-style-type: none"> VDAs like digital payment tokens require prior written authorization from the BaFin under the KWG.³¹ The BaFin has also published a list of guidelines on crypto custody businesses including requirements for authorization and AML requirements.³² Prospectus requirements under the WpPG apply to VDAs that are considered securities. This entails that securities offered to the public require a prospectus to be drawn up unless exempted.³³ The prospectus must present sufficient information to enable the investor to be able to decide on the purchase and subscription of the VDA. The German Capital Investment Code ("KAGB") sets out a framework for management and safekeeping including transparency requirements for investment funds. These may apply to VDAs.³⁴ Asset investments that are not covered by the KAGB are regulated under the German Asset Investment Act ("VermAnlG"), which prescribes for publication of a sales prospectus and investment information sheet approved by the BaFin. In the case of e-money involving processing fiat currency, additional technical compliances are required for trading under the Payment Services Supervision Act ("ZAG").³⁵

Jurisdiction	Regulation	Regulator	Consumer Protection Standards
			<ul style="list-style-type: none"> General consumer protection laws in Germany like the German Act against Unfair Competition ("UWG") state that false advertising and misleading information is prohibited.³⁶ On the question of the applicability of EU consumer protection and e-commerce regulations, the European Central Bank has said that these are not applicable to crypto token transactions.³⁷ However, the EU's Data Protection Rules i.e., the GDPR is applicable to protect consumer data. German regulators have left the crypto space largely unregulated. The BaFin issued a warning that the acquisition of tokens as ICO may lead to substantial investment risks as it is a highly speculative instrument that is largely unregulated, leading to fraud.³⁸
UK	<p>General Regulatory Framework-</p> <ol style="list-style-type: none"> Exchange tokens (or crypto assets) for which there are no specific regulations, security tokens amounting to 'specified investment' are regulated under the Financial Services and Markets Act (2000) (Regulated Activities) Order ("FSMA Framework"), Utility tokens for access to a specific product do not have any specific regulation, and e-money is regulated under Electronic Money Regulations 2011 ("EMR"). The Financial Conduct Authority ("FCA") Guidance note 1.10 sets out which category is regulated by which organization. 	<p>FCA, His Majesty's Treasury ("HMT"), and the Bank of England ("BoE").</p>	<ul style="list-style-type: none"> The FCA banned the sale, marketing and distribution of 'unregulated transferable crypto assets' except security tokens to retail customers.³⁹ Crypto assets involving 'controlled activity' or 'controlled investment' are covered by the FSMA Framework. Chapter 4 of the Conduct of Business Sourcebook requires these promotions or ads to be clear and fair, not misleading. Section 21 of this order says that promotions by unauthorized firms' promotions must be approved by an authorized firm.⁴⁰ The FSA regulates and prescribes authorization, registration, and capital requirements for e-money under the EMR.⁴¹ VDAs that are out of the scope of the FSMA framework need to comply with Advertising Standards Authority ("ASA") guidelines.⁴² It stipulates that ads should show that these VDAs are not regulated by the FCA, include all material information, and specify whether the value can go up or down. Most VDCs fall in this category. The Consumer Rights Act 2015 and Consumer Protection from Unfair Trading Regulations 2008 give consumers rights and remedies against suppliers of goods, services and digital content generally.⁴³ Additional rights against entities providing goods and services digitally are covered by the Electronic Commerce Regulations 2022.⁴⁴ In early 2023, Britain proposed a set of rules to regulate crypto. The rules include licensing, minimum capital and liquidity requirements along with showing their ability to comply with AML measures.⁴⁵

Jurisdiction	Regulation	Regulator	Consumer Protection Standards
Japan	<p>Crypto and utility tokens are regulated as "Crypto Assets" under the Payment Services Act (PSA).</p> <p>Business operators who engage in the business of buying, selling or exchanging crypto assets are required to undergo registration as a Crypto Asset Exchange Service Providers (CAESP).</p> <p>The so-called security tokens are regulated under the Financial Instruments and Exchange Act (FIEA).</p>	<p>Payment Services Act (PSA) and Financial Instruments and Exchange Act (FIEA)</p>	<ul style="list-style-type: none"> Japan's Payment Services Act offers a Virtual Currency Exchange license that is enforced by the Japanese Financial Services Agency. The license covers various crypto-related activities, including the operation of crypto exchange and initial coin offerings.⁴⁶ Crypto has been divided into utility tokens, security tokens, stablecoins and non-fungible tokens. The Financial Instruments and Exchange Act in Japan has laid down penalties for any party involved in market manipulation, fraudulent practices, intimidation, or any other wrong practice.⁴⁷ Crypto Asset Exchange Service Providers (CAESP) in Japan are mandated to create an internal control system to resolve disputes. Under the Act on Prevention of Transfer of Criminal Proceeds, service providers are obligated to verify consumer data, prepare and maintain financial records and report suspicious transactions to relevant authorities. Crypto service providers in Japan are bound by regulations for advertisements and solicitations. False and misleading representations as well as representations promoting crypto trading for profits are prohibited. Japan Virtual and Crypto Assets Exchange Association (JVCEA) introduced self-regulatory rules to guide the SROs.⁴⁸
Dubai	<p>Dubai Virtual Assets Regulatory Authority has been mandated to regulate, supervise and oversee the expansive global virtual assets industry in the Emirate of Dubai.</p> <p>VARA works with all the VASPs to regulate crypto.</p>	<p>Dubai Virtual Assets Regulatory Authority ("VARA")</p>	<ul style="list-style-type: none"> The licensing process consists of separate options for three different categories of applicants: current minimum viable product ("MVP") applicants, existing legacy virtual asset service providers ("VASPs") and new applicants. VARA, in collaboration with the concerned entities, is required to develop a process for the assessment and monitoring of VASPs; and the procedures and measures that must be taken in respect of suspicious transactions conducted in violation of Federal Law.⁴⁹ Crypto assets have been divided into investment assets, crypto tokens, utility tokens and prohibited tokens. Virtual Assets Marketing and Advertising Guidelines in Dubai mention that crypto advertisements and marketing should ensure factual accuracy, should not explicitly demonstrate any promotional intent, and in no way mislead on the guaranteed nature of their returns. The guidelines further mention that the users get all the information before making decisions.⁵⁰ The Dubai Multi Commodities Centre (DMCC) Free Zone Authority approves crypto licenses in Dubai free zone based on stringent regulatory constraint.⁵¹ The Grievance Committee has been created with Director General as the head to resolve disputes.

ABOUT CHASE INDIA

Founded in 2011, Chase India is a leading public policy research and advisory firm with growing practices in Technology & FinTech, Transport & Infrastructure, Healthcare & Life Sciences, Development and Sustainability. Chase provides consultancy services to organizations for mitigating business risks through insight-based policy advocacy. Over the years, Chase India has collaboratively worked with multiple stakeholders such as government, parliamentarians, civil society organizations, academia, and corporates on several policy issues of critical importance. Chase India is committed to using its knowledge, high ethical standards, and result-oriented approach to drive positive action for its partners. Chase India has pan India presence with offices in New Delhi, Mumbai, Pune, Hyderabad, Chennai, and Bengaluru and is a part of the WE Communications Group worldwide. For more information, please visit www.chase-india.com





ABOUT INDUSLAW

INDUSLAW is a top tier full-service Indian law firm, with over 65 partners. The firm provides advice and assistance on all legal aspects, including general corporate, mergers and acquisitions, fund investment, employment law, TMT, fin-tech, start-up, banking & finance, capital markets, tax, energy & projects, infrastructure, aviation, intellectual property, real estate, competition, white collar crime as well as dispute resolution/litigation. INDUSLAW has presence in 5 major cities of India.

For more information, please visit www.induslaw.com

1. [Indias-1-Trillion-Digital-Asset-Opportunity.pdf\(crosstower.com\)](#)
2. Sections 115BBH, Section 194S and Section 56 of the Income Tax Act, 1961 (as amended by Finance Act 2022).
3. News report available [here](#).
4. ASCI guidelines can be accessed [here](#)
5. The guidelines require the following disclaimer to be made - *"Crypto products and NFTs are unregulated and can be highly risky. There may be no regulatory recourse for any loss from such transactions."*
6. RBI's public notices dated December 24, 2013, February 01, 2017 available [here](#) and December 05, 2017 available [here](#). These were later challenged in the *Internet and Mobile Association of India v. Reserve Bank of India* case (2020 SCC OnLine SC 275).
7. Corporate Affairs (MCA) notification dated 24.03.2021 available [here](#)
8. Columbia Journal of Transnational Law publication "Crypto exchange's jurisdiction-shopping: a regulatory problem that requires a global response" dated 23 February, 2023, Kaal, W.A. and Calcaterra, C., 2017. Crypto transaction dispute resolution. *The Business Lawyer*, 73(1), pp.109-152., Salmon, J. and Myers, G., 2019. Blockchain and associated legal issues for emerging markets.
9. Financial Action Task Force, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', (2021). This can be accessed [here](#).
10. Notification No. [S.O. 1072\(E\)](#), Dated 07.03.2023, available [here](#)
11. CERT-In, "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet" No. 20(3)/2022-CERT-In dated 28 April, 2022 available [here](#).
12. Volume 135 of the "Journal of Financial Economics" dated February 2020 available [here](#)
13. 2020 SCC OnLine SC 275.
14. Volume I of the "Report of the Financial Sector Legislative Reforms Commission" dated 27 March 2013 available [here](#).
15. CERT-In, "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet" No. 20(3)/2022-CERT-In dated 28 April, 2022 available [here](#).
16. MAS "Guidelines on the Provision of Digital Payment Services to the Public" PS-G02 dated 17 January 2022 available [here](#).
17. News update on the MCA's website titled "Canadian securities regulators expect commitments from crypto trading platforms pursuing registration " available [here](#).
18. Ibid.
19. CSA Staff Notice 21-332, 'Crypto Asset Trading Platforms: Pre-Registration Undertakings – Changes to Enhance Canadian Investor Protection', available [here](#).
20. CSA Staff Notice 21-330 - Guidance for Crypto-Trading Platforms; Requirements relating to Advertising, Marketing and Social Media Use.
21. CSA Staff Notice 21-332 – Crypto Asset Trading Platforms: Pre-Registration Undertakings — Changes to Enhance Canadian Investor Protection (SN 21-332). SN 21-332.
22. Canadian Anti-Fraud Centre's handout titled "Protect yourself from crypto scams" may be accessed [here](#).
23. Section 5 of the PSA, 2019.
24. News report available [here](#) and Reply to Parliamentary Question on prudential treatment of Singapore banks' crypto asset exposure dated 28 November 2022 (question 2448) available [here](#).
25. MAS Guidelines on Provision of Digital Payment Token Services to the Public [PS-G02].
26. Section 5 and Schedule II of the CPFTA.
27. MAS media release titled "MAS proposes measures to reduce risks to consumers from cryptocurrency trading and enhance standards of stablecoin-related activities" dated 26 October 2022 available [here](#).
28. MAS Consultation Paper on Proposed Regulatory Measures for Digital Payment Token Services dated 26 October 2022 available [here](#).
29. DLT Framework.
30. Clause 12 of the FinIA.
31. BaFin guidance available [here](#).
32. BaFin guidance note and guidelines titled "crypto custody business" available [here](#).
33. BaFin guidance titled "prospectus requirement" available [here](#).
34. KAGB.
35. BaFin Guidance Notice "Information on the Payment Services Supervision Act" dated 29 November 2017.
36. Section 5 of the ZAG.
37. European Central Bank publication "Virtual Currency Schemes" dated October 2012 available [here](#).
38. BaFin guidance titled "Bitcoin, ether et al.: the risks of investing in crypto assets" available [here](#).
39. FCA's Press Release title "FCA bans the sale of crypto-derivatives to retail consumers" available [here](#).
40. Para 4.4.3 of FCA's conduct of business sourcebook available [here](#).
41. FCA guidance on electronic money and payment institutions available [here](#).
42. ASA's guidance "Financial Products and services: Cryptoassets" available [here](#).
43. UK government's guide to consumer rights available [here](#).
44. Section 20 of the Electronic Commerce (EC Directive) Regulations 2002.
45. HM Treasury's press release titled "UK sets out plans to regulate crypto and protect consumers" dated 1 February 2023 available [here](#).
46. Japan's Payment Services Act is available [here](#)
47. Financial Instruments and Exchange Act is available [here](#)
48. Japan Virtual and Crypto Assets Exchange Association (JVCEA) is available [here](#)
49. Regulating Virtual Assets in the Emirate of Dubai is available [here](#)
50. Regulation of Marketing, Advertising and Promotions related to Virtual Assets are available [here](#)
51. Regulatory framework for businesses offering, issuing, listing, and trading crypto assets in Dubai Multi Commodities Centre (DMCC) is available [here](#)

Authors

Avimukt Dar

Founding Partner

INDUSLAW

avimukt.dar@induslaw.com

Avnika Nagar

Senior Associate

Chase India

avnikan@chase-india.com

Shreya Suri

Partner

INDUSLAW

shreya.suri@induslaw.com

Spriha Pandey

Senior Associate

Chase India

sprihap@chase-india.com

Surabhi Chaturvedi

Associate

INDUSLAW

surabhi.chaturvedi@induslaw.com

Gaurav Chaudhary

Account Director

Chase India

gaurav@chase-india.com

Kaushal Mahan

Vice President

Chase India

kaushal@chase-India.com

INDUSLAW OFFICES

BENGALURU

101, 1st Floor, "Embassy Classic" # 11
Vittal Mallya Road
Bengaluru 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

HYDERABAD

204, Ashoka Capitol, Road No. 2
Banjarahills
Hyderabad 500 034
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

CHENNAI

#11, Venkatraman Street, T Nagar,
Chennai - 600017 India
T: +91 44 4354 6600
F: +91 44 4354 6600
E: chennai@induslaw.com

DELHI & NCR

2nd Floor, Block D
The MIRA, Mathura Road, Ishwar
Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

9th Floor, Block-B
DLF Cyber Park
Udyog Vihar Phase - 3
Sector - 20
Gurugram 122 008
T: +91 12 4673 1000
E: gurugram@induslaw.com

MUMBAI

1502B, 15th Floor
Tower – 1C, One Indiabulls Centre
Senapati Bapat Marg, Lower Parel
Mumbai – 400013
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

#81-83, 8th Floor
A Wing, Mittal Court
Jamnalal Bajaj Marg
Nariman Point
Mumbai – 400021
T: +91 22 4007 4400
E: mumbai@induslaw.com

CHASE INDIA OFFICE

NEW DELHI

74, Link Road
Lajpat Nagar - III
New Delhi - 110 024
India
T: + 91 11 4662 5614
F: + 91 11 4662 5625
E: info@chase-india.com

DISCLAIMER

This newsletter is for information purposes only and is not an advisory of a medical or legal nature. Nothing contained herein is, purports to be, or is intended as legal/medical advice or a legal/medical opinion, and you should seek advice before you act on any information or view expressed herein. We make no representation or warranty, express or implied, in any manner whatsoever in connection with the contents of this alert. No recipient of this alert should construe this alert as an attempt to solicit business in any manner whatsoever.