PRIMUS PARTNERS®
Solutions for Tomorrow

Unlocking India's Trillion Dollar Web3 Potential

The Time for Regulation Is Now

FOREWORD

Rohit Kumar Singh

Member NCDRC and
Former Secretary - Ministry of Consumer Affairs,
Government of India

We are witnessing a transformative era in technology with the rapid emergence of Web3, an evolution that is fundamentally reshaping how the internet functions. This decentralized version of the web, built on blockchain and distributed ledger technologies, is poised to redefine industries, financial systems, and the very structure of digital interactions. From decentralized finance (DeFi) and virtual digital assets (VDAs) to smart contracts and decentralized autonomous organizations (DAOs), the possibilities presented by Web3 are immense and far-reaching.

Yet, alongside the excitement and opportunities, Web3 presents a unique set of challenges—particularly from a regulatory standpoint. As governments and policymakers around the world grapple with understanding this new paradigm, it becomes increasingly important to create a regulatory framework that encourages innovation while safeguarding consumer interests and maintaining market integrity. India, with its growing tech ecosystem and digital economy, has the potential to be a global leader in shaping a balanced and forward-thinking regulatory environment for Web3.

The challenge is twofold: first, to ensure that regulation does not stifle the incredible potential of Web3, and second, to provide the necessary safeguards for consumer protection. With decentralized technologies offering new models of digital ownership and financial interaction, users may face risks such as fraud, market manipulation, and data breaches. Therefore, regulation must strike the right balance—protecting consumers without dampening innovation. Robust consumer protection mechanisms, including clear legal recourse and dispute resolution systems, are essential to build trust in the ecosystem. This requires close collaboration between regulators, innovators, industry leaders, and legal experts to craft policies that are adaptable and comprehensive. A clear and consistent regulatory framework will not only foster innovation but also provide confidence to investors, businesses, and consumers, enabling the Web3 sector to thrive responsibly.

This thought leadership delves into the complexities of regulating the Web3 sector, providing a detailed analysis of current regulatory approaches, both in India and internationally. It highlights the challenges that arise from regulating decentralized technologies, the need for clear definitions and classifications, and how we can adopt global best practices while addressing local needs. Importantly, it also highlights the importance of consumer protection measures and the role they play in sustaining a healthy, secure, and inclusive Web3 ecosystem. It is my hope that this work will serve as a valuable resource for policymakers and stakeholders as they navigate this fast-evolving landscape.

As we stand at the threshold of the next digital revolution, it is crucial that India takes a proactive and progressive approach to regulation. By doing so, we can ensure that Web3 becomes a force for inclusive growth, consumer empowerment, economic empowerment, and technological leadership on the global stage.

TABLE OF CONTENTS

PREFACE 5

EXECUTIVE SUMMARY 6

1. Enabling India's Path to Global Web3 Prominence 11

1.1. Quantifying India's Web3 Presence 12

1.2. Potential through Applications 13

2. Case for Comprehensive Regulations 17

2.1. Key Developments in India's Regulatory Approach 18

2.2. Current Gaps in Regulatory Oversight 20

3. Cybersecurity for the Web3 sector 24

4. The 'SECURE' Framework for Web3 Regulations in India 27

4.1. Standardised 29

4.2. Equitable 29

4.3. Consumer focused 30

4.4. Unified 31

4.5. Risk based 31

4.6. Economy-centred 32

5. Contours of Web3 Regulation for India 33

5.1. Enacting a Separate Legislation 35

5.2. Amending Existing Laws 41

5.3. Empowering Self-Regulatory Organizations 43

6. Anticipated Benefits of Web3 Regulations 50

7. India's Path to Web3 Leadership: Recommendations and Way Forward 55

7.1. For the Government 56

7.2. For the Industry 57

ANNEXURE 1: Global Examples of Taxonomy for Virtual Digital Assets 59

ANNEXURE 2: Categorization of VDA Service Providers Globally 64

PREFACE

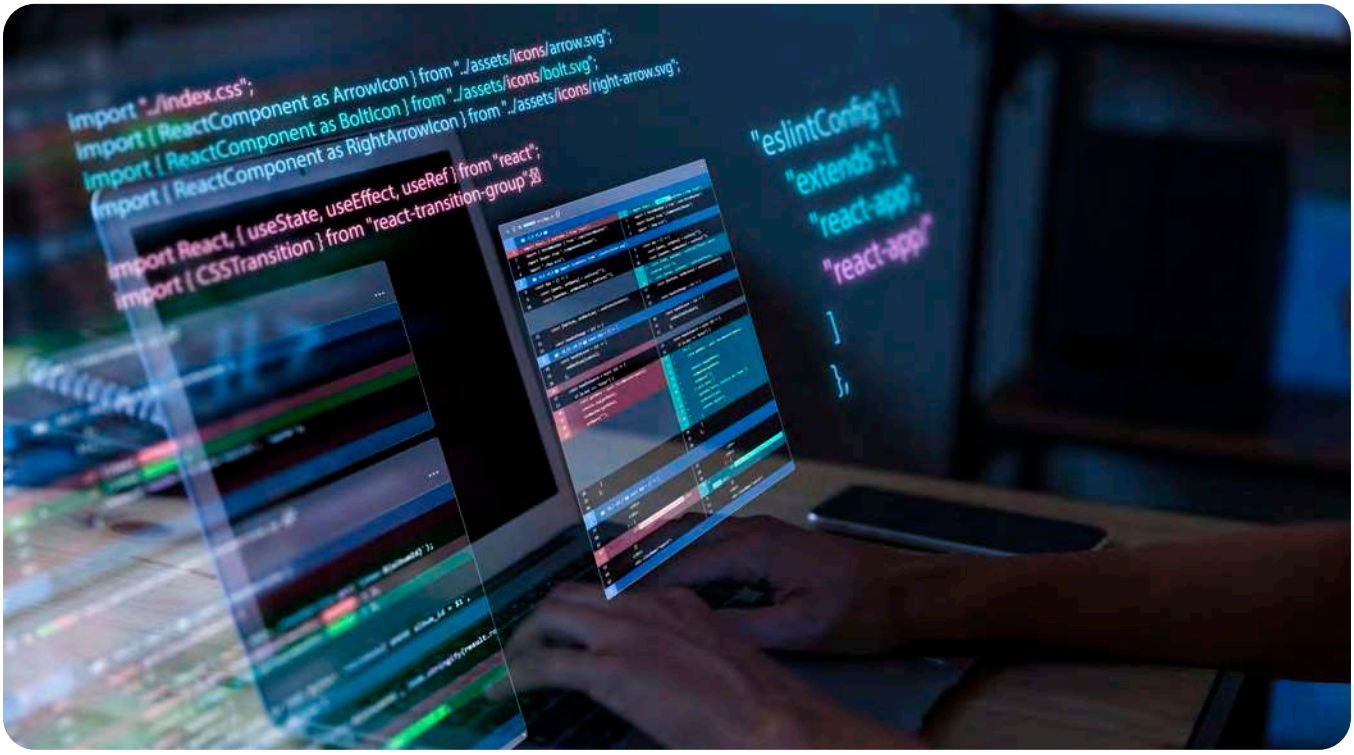
Shravan Shetty
Managing Director
Primus Partners

India stands at a critical juncture in its digital transformation journey, and the emergence of Web3 offers an unparalleled opportunity to reshape industries and bolster economic growth. Web3's decentralized technologies have the power to unlock new efficiencies, transparency, and innovation across sectors. With its rapidly growing talent pool and vibrant startup ecosystem, India is uniquely positioned to harness the full potential of this technology, contributing an estimated 27% to our incremental GDP by the year 2032[1]. However, realizing this vision requires more than technological advancement—it demands a comprehensive regulatory framework that fosters innovation while protecting users.

In the absence of clear regulations, we risk losing not only our competitive edge but also a significant portion of the incremental economic growth projected over the next decade. The current regulatory gaps have already driven many promising Web3 startups to relocate, depriving India of talent and foreign direct investment. A cohesive and forward-looking regulatory strategy is imperative if we are to safeguard the future of this sector and secure India's place as a global Web3 leader.

This document outlines a multi-faceted approach to crafting a robust regulatory framework for India's Web3 ecosystem. By adopting the SECURE Framework and addressing the regulatory gaps through dedicated legislation, amendments to existing laws, and empowering self-regulatory organizations (SROs), we can ensure that India remains at the forefront of this technological revolution.

EXECUTIVE SUMMARY



Web3 has the potential to revolutionize industries through greater efficiency, transparency, tokenization and digitization

By virtue of its decentralised nature and processes, Web3 has the potential to redefine commerce, investment, and industry processes in a way that fosters transparency, efficiency, and innovation through:

1. **Increased Efficiency:** Web3, powered by blockchain, enhances efficiency by enabling faster and more secure transactions. It reduces intermediaries, cuts costs, and improves productivity across various industries.
2. **Improved Traceability and Transparency:** Blockchain ensures permanent records of all transactions, providing an immutable audit trail. This is crucial in sectors like healthcare for tracking pharmaceuticals.
3. **Digitization of the Physical World:** Web3 integrates with technologies like Internet of Things (IoT) and smart contracts to create digital twins—virtual representations of physical assets. This can transform industries such as real estate, manufacturing, and e-commerce, offering new opportunities for innovation and commerce.
4. **Tokenization of Assets:** Web3 introduces new asset classes, such as Non-Fungible Token (NFTs), that merge transactions with experiential value. NFTs tied to experiences or royalties democratize investments, expanding opportunities in areas like cultural assets. This shift may require new strategies for managing and valuing these emerging asset classes.

India is uniquely positioned to become a leader in Web3 innovation

India is a critical player in the global Web3 ecosystem, with the third-largest Web3 talent pool globally. In 2023 alone, the country added 3.5 million developers to the sector.

With over 1,000 Web3 startups and five unicorns, the country's potential is immense, offering transformative applications across industries such as education, healthcare, logistics, and supply chain management. Web3 could contribute significantly to India's economic growth, with the potential to add $1.1 trillion to the Gross Domestic Product (GDP) by 2032 and create over 8 million jobs.

However, despite advancements, India's regulatory framework remains fragmented

There have been significant advancements in the regulatory landscape for Web3, notably the inclusion of Virtual Digital Asset Service Providers (VDA SPs) as 'Reporting Entities' under the Prevention of Money Laundering Act (PMLA). Despite these advancements, India's regulatory framework for Web3 remains fragmented.

- **Lack of Licensing Regime:** No established licensing protocols for Web3 service providers exist, making accountability difficult and hindering consumer trust.
- **No Defined Taxonomy:** Without a clear classification system for Virtual Digital Assets (VDAs), there is regulatory ambiguity in how regulations can be tailored to address the specific risks and benefits associated with each type of asset.
- **Smart Contract Legality:** Smart contracts currently lack a legal definition in India, posing challenges in recognizing them as enforceable agreements.
- **Lack of Cybersecurity Guidelines:** There are no formal cybersecurity protocols for Web3, leaving users vulnerable to attacks like 51% attacks, DDoS attacks, and smart contract vulnerabilities.

Regulatory uncertainty can curtail India's ability to fully capitalize on Web3

The absence of a comprehensive regulatory framework in India presents significant risks that could hinder the country's potential to lead in this emerging sector.

- **Flight of Startups:** Over 270 Web3 startups have already moved to more favourable jurisdictions due to regulatory uncertainty, reducing potential contributions to India's GDP and the job market.
- **Economic Loss:** Without an enabling ecosystem in India, India risks losing an estimated $1.1 trillion in potential GDP contributions by 2032. The government also stands to lose tax revenue due to volumes shifting to offshore platforms.
- **Employment Impact:** This will also limit employment opportunities, especially for the tech talent representing 12% of India's workforce, slowing domestic innovation.
- **Decline in Foreign Direct Investment (FDI):** Regulatory uncertainty discourages foreign investors from entering India's Web3 space, potentially reducing FDI in blockchain sectors.
- **Consumer Protection Risk:** Without a regulatory framework, consumers are more vulnerable to fraud and financial loss with little recourse for protection.
- **Loss of Global Competitiveness:** India risks falling behind other nations with more progressive Web3 regulations, limiting its influence on shaping global Web3 policy.

Therefore, India must create a regulatory framework by leveraging the 'SECURE' principles that balances risk and innovation

The report suggests a multi-faceted approach to address the existing challenges and capitalize on India's Web3 potential through the following framework:

- **Standardised:** Introduce clear taxonomy for Virtual Digital Assets (VDAs) to provide regulatory clarity. Adopting global best practices ensures smoother integration and adoption of Web3 services.
- **Equitable:** Adapt regulations to account for decentralized systems while protecting users, ensuring that emerging technologies find representation in India's Web3 landscape.
- **Consumer-Focused:** Mandate transparency with clear disclosures from service providers and prioritize consumer protection.
- **Unified:** Encourage international cooperation to align India's regulations with global standards, minimizing risks like regulatory arbitrage and facilitating cross-border transactions.
- **Risk-Based:** Tailor compliance requirements based on the size and risk profile of entities, ensuring stricter oversight for larger players while allowing flexibility for smaller startups.
- **Economy-Centered:** Foster innovation by creating a conducive environment for Web3 startups, potentially adding over $1 trillion to India's economy by 2032.

India can operationalize the Regulatory Framework through 3 broad contours

i. **Enacting Separate Legislation:** A dedicated legal framework for VDAs and Web3 should be established, drawing on global best practices. This would include:

   a. Defining taxonomy of VDAs to bring clarity around regulations

   b. Identifying the Regulatory Authority

   c. Identifying VDA SPs that will be covered in the legislation along with licensing and other requirements

ii. **Amending Existing Laws:** Modify existing legislation, such as the Income Tax Act and Indian Contracts Act, to include provisions for VDAs and recognize smart contracts as legally binding.

iii. **Empowering Self-Regulatory Organizations (SROs):** Establish SROs to set industry standards, promote compliance, and address consumer grievances. These organizations would play a vital role in maintaining a secure, transparent, and innovative ecosystem.

This will enable India to fully unlock the potential of its digital economy

i. **Economic Growth:** Implementing these recommendations could see Web3 technologies contribute $1.1 trillion to India's GDP by 2032, while also creating over 8 million jobs.

ii. **Fostering Innovation:** A conducive regulatory environment will attract global investment, prevent the outflow of talent, and boost the startup ecosystem, positioning India as a leader in the digital economy.

iii. **Consumer Protection and Security:** Clear guidelines and cybersecurity protocols will protect consumers from fraud, cyber-attacks, and financial loss, thus enhancing trust in the system.

iv. **International Influence:** By aligning domestic policies with international frameworks, India could play a leading role in shaping **global Web3 regulations.** This would also reduce the likelihood of market manipulation and fraud.

v. **Enhanced Tax Compliance:** Clear regulations around VDAs will help the government capture tax revenues from the booming Web3 sector while improving transparency in digital transactions.

vi. **Fair Competition:** By enforcing consistent standards, the proposed framework will ensure fair competition, and fostering diversity in the Web3 ecosystem.

Going forward, it is essential for all stakeholders to take a collaborative approach to craft balanced regulations

Both the government and industry stakeholders must collaborate to unlock the full potential of Web3 in India:

- **Role of Government:** The government should lead with consultations, international coordination, and the introduction of regulatory sandboxes to foster innovation while maintaining oversight.
- **Role of Industry:** The industry must work with the government to implement self-regulation, enhance consumer education, and demonstrate the tangible use cases of Web3 across sectors.

PRIMUS PARTNERS®
Solutions for Tomorrow

01

Enabling India's Path to Global Web3 Prominence

Web3 has witnessed tremendous progress, with the global Web3 sector poised to contribute 8% of global GDP by 20302. This progress has been visible through emerging use cases for the technology as well as favourable legislation around the world fostering its potential.

- The NFT market is projected to grow at a 34% CAGR, reaching $212 billion by 2030. Tokenized assets could be valued between $5 trillion and $16 trillion globally, potentially making up 10% of global GDP by 2030.[3]
- Metaverse projects like Decentraland were valued at $1.2 billion in 2022, with major brands like Samsung and Adidas investing in digital properties.[4]
- Venture capital funding in blockchain and crypto hit $28.5 billion in 2022, a 15x increase since 2015.[5]
- By June 2023, over 21,000 developers were actively working monthly, reflecting a 92% increase since 2020.[6]
- Global spending on blockchain solutions is projected to reach $19 billion by 2024, a 46.4% increase from 2021.[7]

1.1. Quantifying India's Web3 Presence

3rd biggest talent pool in the world; added 3.5 million developers in 2023

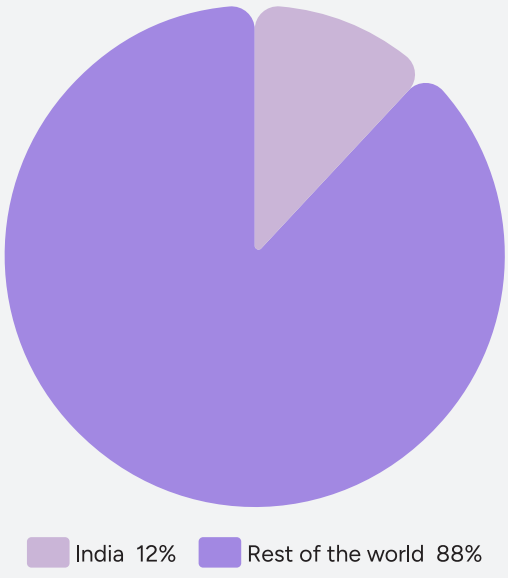
Contribution to Economy

$1.1tn	$200	8
contribution to India's GDP by 2032	billion market opportunity	million jobs to be unlocked

Web3 Startups & Investments

1000	$270
Web3 Startups; 5 Unicorns	million funding for Web3 startups

Global Web3 Developer Pool



While considerable progress has been made in India's Web3 landscape, to fully realise the potential in the country, there must be a proportionately conducive ecosystem for innovation, while ensuring the highest degree of consumer protection.

"India retained its #1 position in crypto adoption as per Chainalysis' Global Crypto Adoption Index 2024 propelled by the world's second-largest blockchain developer base and strong retail investor interest. The Indian web3 landscape is bustling with activity with founders building globally competitive products across a diverse range of sectors with real-world use cases and user traction. Key themes for this year include middleware infrastructure, blockchain gaming, DePIN, stablecoins and AI x Crypto."

- Tak Lee, CEO and Managing Partner, Hashed Emergent

1.2. Potential through Applications

The potential of Web3 to transform sectors like finance, healthcare, supply chain, and governance is immense. By embracing Web3, India can not only drive economic growth but also address social challenges and improve the quality of life for its citizens.

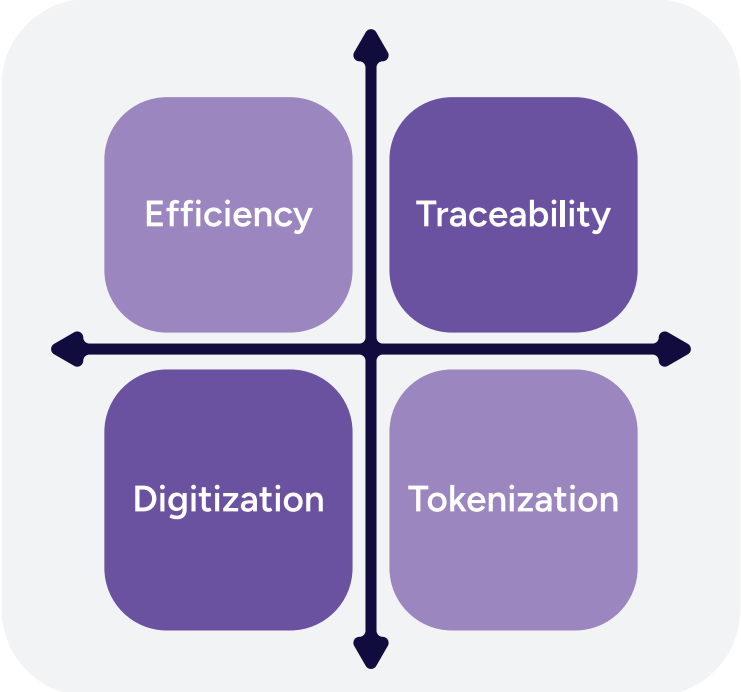


Figure 1: Benefits of Web3

> *"We at Ava Labs see a lot of potential in the web3 space in the South Asia region, especially as regulators begin to work with web3 companies to understand and embrace the space. We're excited to see the use cases coming out of the regulatory sandboxes and look forward to being a part of this explosive growth"*
>
> - Devika Mittal, Regional Head, Ava Labs

1.2.1. Increase in Efficiency

One of the most significant advantages of Web3 lies in its ability to enhance efficiency across various sectors. By leveraging blockchain technology, Web3 enables faster, more secure transactions, reducing the need for intermediaries and cutting down costs. It also eliminates inefficiencies and friction in transactions, thereby driving significant productivity gains across the economy.

For instance, in the education sector, Web3 can revolutionize credential management. Blockchain technology enables the creation of digital records of academic achievements, allowing students to manage and share their credentials securely while reducing administrative overhead for educational institutions. This can eliminate the inefficiencies associated with traditional paper-based systems, thus driving productivity gains in the education sector.

The Maharashtra State Board of Skill Development (MSBSD) has introduced a blockchain-based diploma certificate issuance and verification system in partnership with Zupple, a web3 startup specializing in credentials and applications on blockchain. In the past, MSBSD issued diplomas in hard copy, a laborious process that usually required the participation of over 1,000 staff members across its chain of training institutes and departments, taking over a month. Students are now able to get their diploma verified within seconds, which would otherwise take over 30 days.

Data on these blockchains are open and easily auditable by nature, providing a transparent mechanism for instantaneous verification of data. Zupple's LegitDoc technology makes use of Ethereum blockchain combined with modern cryptography to issue digital diplomas that are tamper-proof, hack-proof, instantaneously verifiable and privacy-centric.

1.2.2. Improvement in Traceability and Transparency

Web3 offers unprecedented levels of traceability and transparency, which are crucial for building trust in the digital ecosystem. Blockchain's immutable ledger ensures that all transactions are recorded permanently, providing a verifiable audit trail. This is particularly beneficial in industries such as healthcare, where ensuring traceability of pharmaceuticals is critical.

Similarly, in supply chain management, Web3 provides end-to-end visibility by tracking goods in real-time, from raw materials to the end consumer. This transparency reduces risks of fraud and counterfeiting, ensuring a more reliable and efficient supply chain. By giving all stakeholders access to the same unalterable data, Web3 fosters greater trust, accountability, and efficiency in the marketplace.

Whrrl blockchain platform in the production stage has a presence in 1400 warehouses in 5 states of India and has facilitated over Rs. 175 crores in digital loans and generated tokenized warehouse receipts worth more than Rs. 6,500 crores. The platform's blockchain integration ensures that receipt generation, lending processes, and trade operations are all conducted on-chain, providing an immutable and fraud-resistant financial environment.

1.2.3. Digitization of the Physical World

Web3 transcends the realm of digital transactions by seamlessly integrating with the physical world through technologies like the Internet of Things (IoT), smart contracts, and the metaverse. This convergence empowers the creation of digital twins—virtual representations of physical assets that can be tracked, managed, and traded in real time.

The impact of this paradigm shift is transformative, particularly for industries like real estate, manufacturing and e-commerce. Furthermore, the metaverse emerges as a captivating space where users can engage with these digital assets in an immersive virtual environment. This opens up new avenues for commerce and innovation, fostering novel business models and enhancing customer experiences.

Flipkart Labs is focused on leveraging emerging technologies to create immersive customer experiences and differentiation for the Flipkart Group. At Flipkart Labs, the technologies that are being worked on currently include 3D, AR, Metaverse, Web-3/ Blockchain and Generative AI. Flipverse is a metaverse space where Flipkart customers can shop in a photorealistic virtual destination via the Flipkart app.

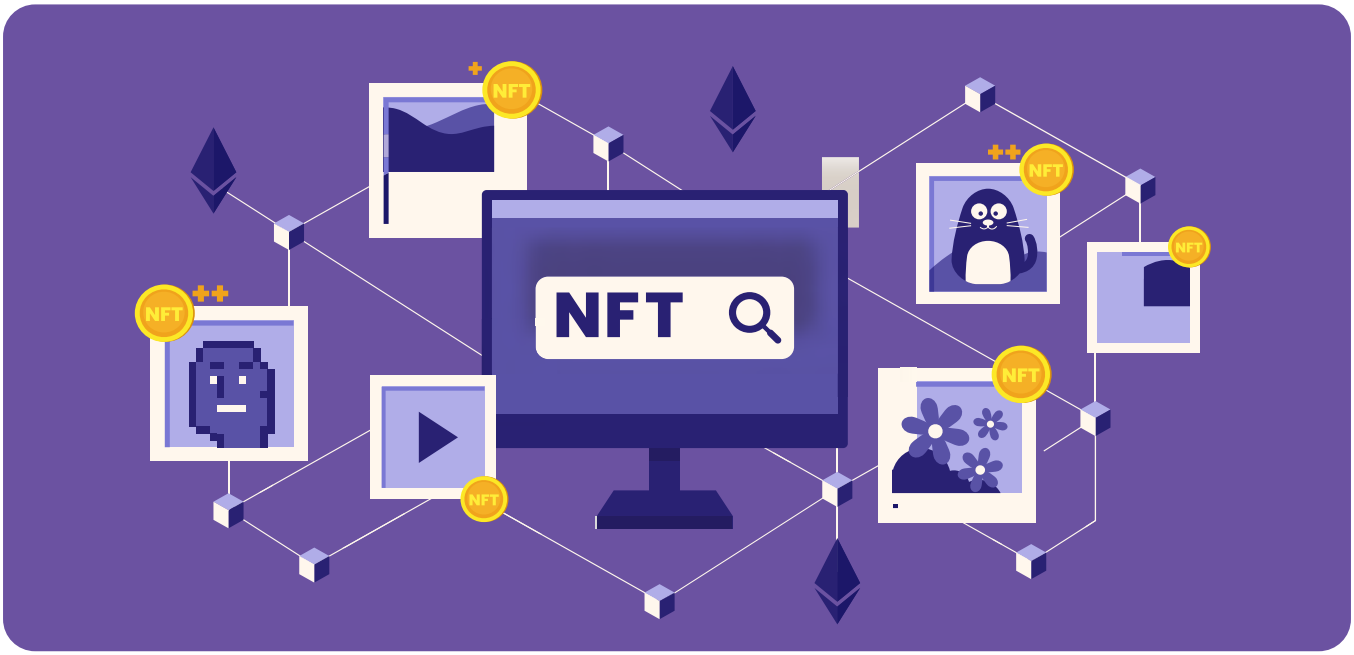
Terazo is an asset tokenization platform that facilitates the issuance, management, and trading of tokenized securities on blockchain. As India's first private market investment platform offering a complete solution for issuing and trading security tokens, Terazo operates under a regulated and transparent framework. It enables fractionalized investments in real estate, venture capital funds, and unlisted companies. Notably, Terazo has launched India's first tokenized security offering, regulated by IFSCA under the regulatory sandbox framework, with a corpus of $7 million.

1.2.4. Tokenization of Assets

Web3 is revolutionizing commerce and investment by merging transactions with experiential value, creating new asset classes. Unlike traditional transactions, where the value is often limited to the product or service exchanged, Web3's smart contracts embedded in tokens introduce multi-dimensional investments.

For instance, NFTs now offer not just ownership but access to exclusive experiences and communities, enhancing their value. The recent example of NFTs tied to music royalties illustrates this shift, democratizing access to investments previously reserved for institutional players. These innovations not only lower barriers but also expand investment opportunities into areas like cultural assets, where emotional and experiential returns play a crucial role. This blending of commerce and investment through Web3 could redefine portfolio construction, requiring new valuation models and management strategies to optimize these emerging assets.

The potential benefits of Web3 are substantial but unlocking Web3's potential in India requires a comprehensive regulatory framework that fosters innovation while ensuring user protection. Without this, India risks losing significant economic opportunities as Web3 startups and talent may shift to more favourable jurisdictions. **A well-designed regulatory environment could prevent this outflow, stimulate the startup ecosystem, attract investment, and boost GDP, positioning India as a global leader in digital innovation.**



PRIMUS PARTNERS®
Solutions for Tomorrow

02

Case for Comprehensive Regulations

Owing to the borderless nature of Web3 and its core characteristics, comprehensive regulation is essential for its governance worldwide. The regulatory frameworks must remain consistent across jurisdictions as the technology continues to grow and evolve in its decentralized form. Therefore, there is a pressing need for a unified regulatory approach on a global scale. As a leading force in Web3 innovation, India must take the initiative by establishing a robust domestic regulatory framework. This framework can serve as a foundation for shaping global regulations in the future.

2.1. Key Developments in India's Regulatory Approach

India's Web3 and VDA regulatory landscape has evolved considerably over the past few years. A brief timeline of events is depicted below:

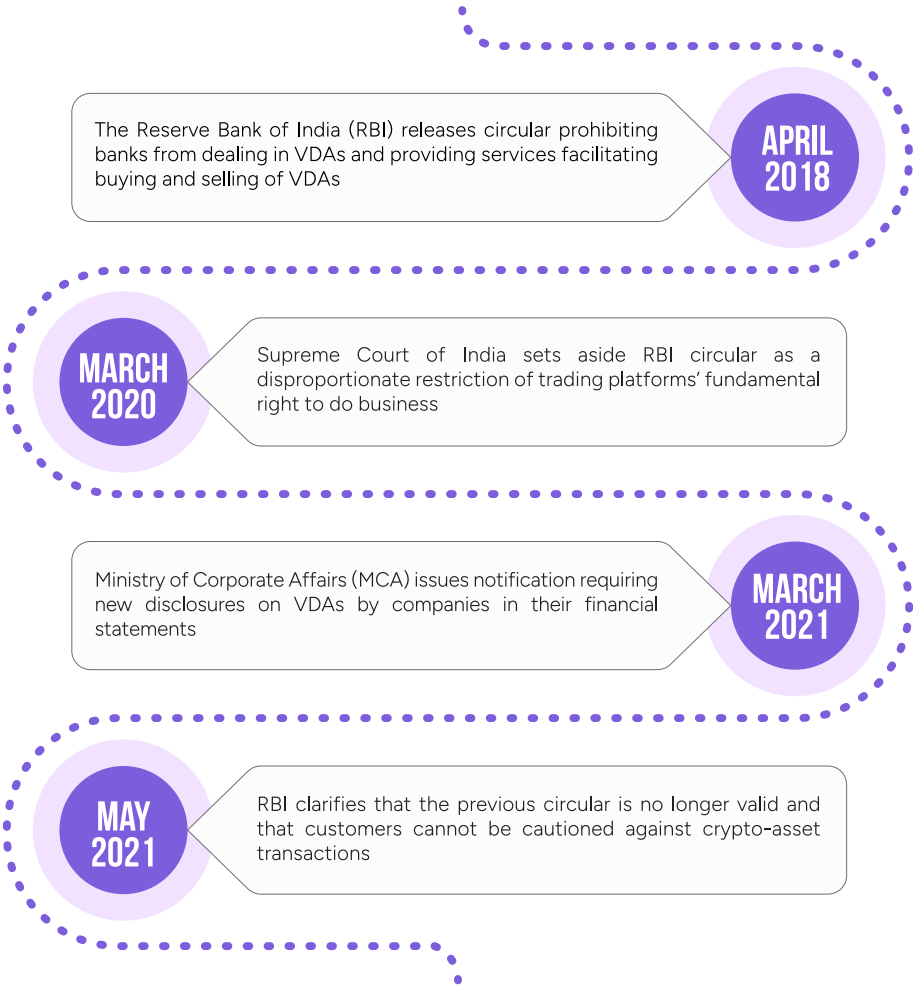


Figure 2: Timeline of India's Regulatory Developments

A key milestone of India's G20 presidency was the release of the synthesis paper on crypto by the IMF and FSB in September 2023. This paper includes a roadmap for creating a coordinated global policy and regulatory framework, with policy guidelines to help authorities address the risks associated with VDA activities. It also represents the first step toward cross-border regulatory coordination. This momentum has continued into Brazil's G20 presidency as well; the country's central bank has said it will introduce a concise set of Web3 guidelines by the end of the year.[9]

As global consensus on Web3 regulation gains momentum, India must now align its domestic policies with these international efforts. Building on a year of focused discussions, the time is ripe for India to demonstrate its leadership by introducing progressive domestic legislation tailored to its unique requirements.

2.2. Current Gaps in Regulatory Oversight

While these developments signal a positive outlook towards the Web3 sector, they lack material and comprehensive oversight, such as:

2.2.1. Need for Cybersecurity Guidelines

In the Web3 space, particularly in VDAs, stolen assets lead to immediate financial loss, strongly motivating companies to prioritize cybersecurity. This is especially true for companies that self-custody assets, where financial alignment with security needs is almost perfect. However, companies holding assets on behalf of others may not have the same incentives, potentially leaving users vulnerable in the event of a hack, highlighting the need for regulatory oversight. The stakes in Web3 are exceptionally high because security breaches involve the loss of real, non-reversible financial assets, making robust cybersecurity essential. Startups in this space must prioritize security from the outset, as delaying measures could lead to significant losses.

Despite these needs, there is currently no cybersecurity guideline for Web3 in India, creating a regulatory gap that leaves companies and users exposed. Given these dynamics, while financial incentives drive companies to take security seriously, a tailored regulatory approach, including the establishment of clear guidelines in India, is necessary to ensure comprehensive protection.

2.2.2. Lack of Licensing Regimes for Service Providers

There is a lack of clear licensing regimes for Web3 service providers outlining the necessary qualifications, financial requirements, and operational standards that businesses must meet before they can offer their services. This helps in creating accountability, enhancing consumer protection, and fostering trust within the ecosystem.

Web3 participants, including developers, token issuers, custodians, exchanges, and DeFi platforms, do not have specific regulatory requirements based on their roles and responsibilities within the ecosystem. These requirements could include Know Your Customer/

Anti-Money Laundering (KYC/AML) obligations, cybersecurity protocols, risk management strategies, and consumer protection measures. As these service providers handle a host of assets and important user details, it is vital to clarify the regulatory responsibilities for each of these service providers.

2.2.3. No Defined Taxonomy

Currently, there is no defined taxonomy for VDAs; taxonomy is essential for regulatory clarity and consistency. This would involve categorizing VDAs based on their unique characteristics and intended uses, such as utility tokens, security tokens, stablecoins, and non-fungible tokens (NFTs), which would allow for tailored regulations that address the specific risks and benefits associated with each type of asset.

2.2.4. Defining Legality of Smart Contracts

Currently, smart contracts lack a legal definition; these smart contracts operate autonomously and execute automatically without requiring direct human involvement once coded. Regulation may need to acknowledge smart contracts as legitimate and enforceable agreements, despite being executed digitally and without manual intervention.

2.2.5. Regulation of Digital Spaces

With the development of new spaces that are entirely digital in nature (for example, metaverse spaces), there needs to be comprehensive regulatory frameworks for these new digital spaces, to ensure that users are protected in these areas as well.

2.3. Potential Implications of an Unregulated Web3 Ecosystem

A lack of regulatory framework for Web3 in India could lead to missed economic opportunities, talent migration, and diminished global competitiveness.

Impact on Economy

- Flight of Web3 Startups
- Loss of GDP
- Loss of Emp loyment Opportunities
- Decline in FDI

Impact on Users and Society

- Lack of Consumer Protection
- Legal and Financial Uncertainty
- Stunted Innovation

Impact on Government

- Loss in Tax Revenue
- Growth of Grey Markets
- Loss of Influence in Global Markets

Figure 3: Counterfactual Scenario

"India retained its #1 position in crypto adoption as per Chainalysis' Global Crypto Adoption Index 2024 propelled by the world's second-largest blockchain developer base and strong retail investor interest. The Indian web3 landscape is bustling with activity with founders building globally competitive products across a diverse range of sectors with real-world use cases and user traction. Key themes for this year include middleware infrastructure, blockchain gaming, DePIN, stablecoins and AI x Crypto."

- Tak Lee, CEO and Managing Partner, Hashed Emergent

2.3.1. Impact on Economy

- **Flight of Web3 Startups:** Industry estimates suggest that 270+ operators/startups have moved outside India due to regulatory frictions / uncertainty since April 2022.[10] The unfavourable policies have left the Indian Web3 ecosystem uncompetitive in foreign markets.
- **Loss of GDP:** According to estimates, Web3 technologies have the potential to contribute USD 1.1 trillion to India's GDP by 2032.[11] Without a policy in place, India risks losing this massive economic contribution.
- **Loss of Employment Opportunities:** The developer community, representing 12% of India's total tech talent pool[12], will see a decline in job opportunities. Rather than fostering product development in India, India may continue to be an exporter of talent, with limited growth in native Web3 solutions.
- **Decline in FDI:** Foreign Direct Investment (FDI) in the blockchain sector is likely to decrease due to regulatory uncertainty, impacting the nation's overall investment ecosystem.

2.3.2. Impact on Users and Society

- **Lack of Consumer Protection:** The absence of robust policies increases the risk of fraudulent activity in the Web3 market, leaving consumers vulnerable and with little recourse for protection.
- **Legal and Financial Uncertainty:** Users are left in limbo without clear guidelines, contributing to hesitation in adopting new financial technologies.
- **Stunted Innovation:** The lack of a clear regulatory environment will discourage entrepreneurs and innovators from developing new solutions, hampering technological advancements and growth in the blockchain space.

2.3.3. Impact on Government

Loss in Tax Revenue: As startups and talent leave the country and transactions remain opaque, the government stands to lose substantial tax revenue from this booming sector. The Indian exchequer may have potentially lost ~INR 2,489 crores in tax revenue between February 2022 and January 2024 from VDA trades undertaken on the top 6 Indian Exchanges and may further lose around INR 5,894 crores in the next 3 years if the current TDS policy continues. [13]

- **Growth in Grey Market:** Without regulation, the VDA market could shift further into the unregulated territory, leading to a rise in unrestricted activities within a grey market.
- **Loss of Influence in Global Markets:** As India lags behind other nations with more progressive Web3 regulations, its role and influence in the global Web3 ecosystem could diminish significantly, limiting its ability to shape international policies.

Due to the cross-jurisdictional nature of Web3, a blanket ban on such assets can never be a viable deterrent measure to regulate VDAs and curtail cyber-crime. Reference can be given to China, who is within the top 20 on the Global Crypto Adoption Index 2024[14] despite imposing significant restrictions and declaring all VDA transactions as illegal.

PRIMUS PARTNERS®
Solutions for Tomorrow

03

Cybersecurity for the Web3 sector

As the Web3 ecosystem rapidly expands, it introduces new cybersecurity challenges, particularly as machine agents become integral to this data-driven, decentralized web, presenting both opportunities and risks for organizations to address.

Anonymity and Traceability: Blockchain systems are built on transparency, but transactions remain anonymous unless identity information is linked to services (e.g., email, phone number). Public keys are traceable, but they don't always connect to external identities depending on the service's centralization. Solutions like Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols can help link transactions to identities. Privacy-focused blockchain systems like zero-knowledge proofs allow for balance between transparency and user privacy.

Exploitation of Anonymity: Anonymity is a double-edged sword, offering privacy but also enabling fraudulent activities and making it difficult to trace malicious actors. Enhanced surveillance mechanisms like transaction monitoring tools, combined with decentralized identity (DID) systems, can track malicious actors without compromising user privacy. Law enforcement can collaborate with blockchain and smart contract auditing firms to trace suspect transactions.

51% Attacks: A critical cybersecurity concern where attackers control over 51% of a network's mining power. This allows them to manipulate the network, double-spend coins, and prevent new transactions. This is more common in smaller networks but a concern for all blockchain ecosystems. To mitigate the risk, networks can increase decentralization by involving more participants in consensus mechanisms, such as proof-of-stake (PoS) over proof-of-work (PoW). Regular audits and collaborative partnerships with miners also reduce vulnerabilities.

DDoS Attacks and Phishing: Distributed Denial-of-Service (DDoS) attack is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

DDoS attacks disrupt blockchain networks by overwhelming them with excessive requests. Phishing attacks deceive participants into revealing sensitive information like private keys, compromising wallets and assets.

Decentralized networks inherently reduce the impact of DDoS attacks by distributing infrastructure. Implementing secure wallet designs, two-factor authentication (2FA), and educating users about phishing techniques are critical steps to prevent attacks.

Smart Contract Vulnerabilities: Smart contracts, essential for automating transactions, can be vulnerable due to coding errors or design flaws. This emphasizes the need for rigorous security audits before deployment. Comprehensive security audits, formal verification, and bug bounty programs can detect and address vulnerabilities. Additionally, modular contract designs allow for easier upgrades and patches, reducing risks of exploitation.

"Security testing and auditing in the Web3 sector isn't just about finding vulnerabilities—it's about building trust in a decentralized future. As the foundation of digital value shifts, ensuring the integrity and resilience of smart contracts and protocols is not a luxury, but a necessity. Only through rigorous security practices can we empower innovation without compromise."

- Preetam Rao, Co-founder and CEO, QuillAudits

Web3 has the potential to drive the internet industry to unprecedented success and growth, opening up opportunities that were previously out of reach for the business world. However, this latest iteration of the web must ensure the cybersecurity of its operational mechanisms and functions. The growth of Web3 could be threatened by data breaches and leaks, making it crucial for the industry to offer reliable solutions to reassure potential customers.

PRIMUS PARTNERS®
Solutions for Tomorrow

04

Cybersecurity for the Web3 sector

The Indian Web3 sector has thrived, despite regulatory uncertainty that have persisted since the inception of the sector in India. In the absence of rationale based and proportionate regulation, this fledgling, but high potential sector will not be able to capitalize and fulfill its true potential. Without proper regulation, India's ability to enforce capital controls, taxes, and guardrails will erode, stifling growth and compromising national interests.

Given this, there is a need for a balanced, principle based regulatory approach that will provide the flexibility to keep pace with changing technology and ensure consumer interests are protected.

This report recommends the SECURE framework—Standardised, Equitable, Consumer-focused, Unified, Risk-based, and Economy-centric—for Web3 regulation in India. Each pillar represents an essential aspect of Web3 regulations, ensuring that all stakeholders are safeguarded through appropriate regulatory measures.

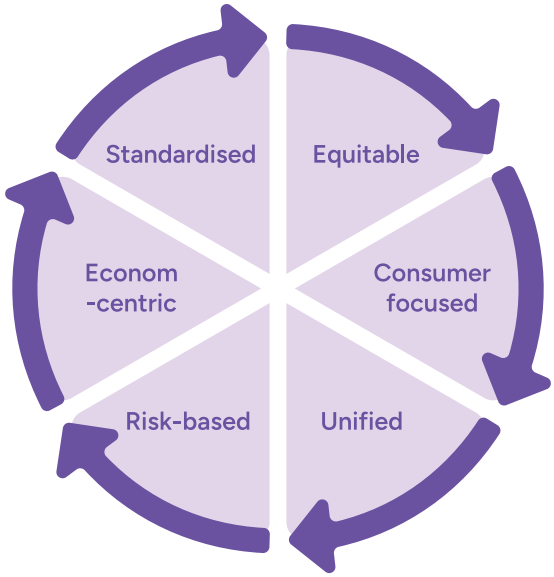


Figure 4: Primus Partners' SECURE Framework for Web3 Regulation

Web3 represents more than just technological advancement, it's a powerful force for empowerment, inclusion, and meaningful global impact. I firmly believe that establishing a robust policy framework is essential for nurturing this innovation. The report outlines a forward-thinking approach that prioritizes not only economic growth but also the safety, privacy, and rights of consumers. With the right policies in place, India can set a global benchmark for Web3 regulation, creating an environment where startups can thrive, talent can flourish, and digital assets can be used responsibly and securely.

This is our moment, and we have the opportunity to shape the future. We are proud to support this vision, by collaborating closely with the policymakers, innovators, and the broader ecosystem ensuring that India fully seizes the opportunity presented by Web3 . The path to an inclusive digital economy is filled with promise and we are committed to being at the forefront of this journey, driving sustainable innovation that benefits everyone.

- Sumit Gupta, CEO & Co-founder, CoinDCX

4.1. Standardised

- **Taxonomy-based Classification for VDAs:** VDAs should be classified by their nature and use cases, such as utility tokens, security tokens, or closed-loop tokens, using a taxonomy-based approach. This helps tailor regulations and compliance requirements to specific asset characteristics and risks.

  It is also important to differentiate VDAs from digital legal tender like e-rupee. International models, such as Dubai's VARA and the EU's MiCA regulation, can serve as references for such classifications.

- **Tech Neutrality:** Where individuals or entities in the Web3 world perform the same roles as, or provide services similar to traditional intermediaries, they may be subject to similar laws, adjusted as needed to accommodate benefits and address respective risks.

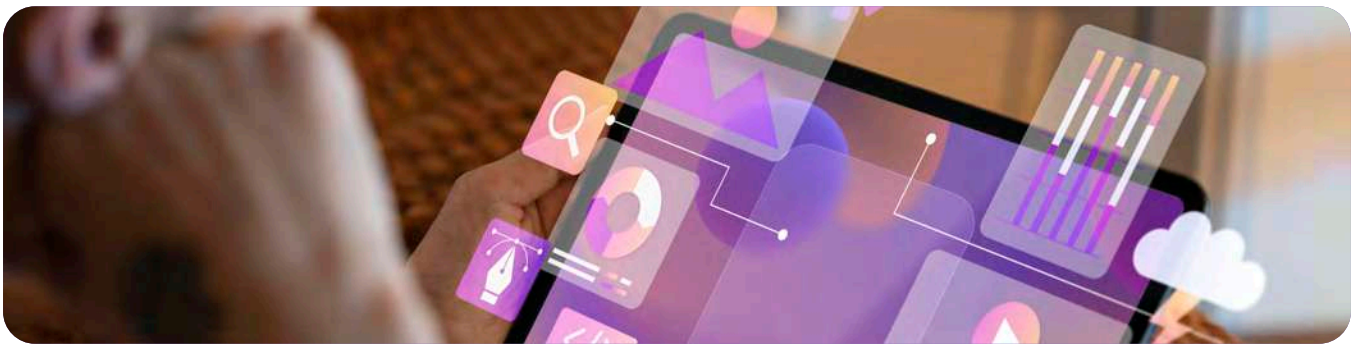
  However, where technology replaces functions typically performed by persons in traditional systems, lawmakers should not force the existence of intermediaries to which to apply traditional regulation. Regulation should remain unbiased against technology, and laws should respect that blockchain-based software can allow individuals to be stewards of their own personal data. Any laws that address activities rather than technology alone can then grow with the technology.

4.2. Equitable

Promote Equitable Decentralisation: Decentralized blockchain systems differ fundamentally from centralized ones, as they lack intermediaries. Regulations should be adapted to accommodate the unique risks posed by decentralized systems, like code vulnerabilities, while ensuring user protection and market integrity. The "same activity, same risk, same regulation" principle must be adjusted for decentralized networks. Regulations should support decentralized technology, which offers opportunities for financial inclusion and self-ownership. A policy framework must be equitable and innovative, addressing regulatory needs in decentralized systems while preserving the benefits of decentralisation, including greater access and user empowerment.

> *"Web3 holds immense promise for India's digital transformation, offering unparalleled opportunities for economic growth, financial inclusion, and global leadership in technology. To harness this potential, it's crucial that we adopt balanced regulations—protecting consumers and ensuring market stability without hampering innovation. Learning from industries like fintech and telecom, where measured regulatory approaches have spurred growth, we must focus on key areas: implementing KYC and AML protocols to prevent illicit activities, establishing smart contract security standards, and clarifying taxation policies for digital assets. By regulating critical aspects like consumer protection and data privacy while allowing creative freedom elsewhere, we can foster a thriving Web3 ecosystem that empowers our citizens and positions India at the forefront of the digital future."*
>
> - Ashish Khandelwal, Founder and CEO, ANQ

4.3. Consumer focused



- **Transparency in policies:** Transparency is key in regulation, involving two main aspects: (i) Clear, jargon-free disclosures by developers and stakeholders to help users easily access and understand blockchain information, ensuring protection and accountability; (ii) Open-source code, which adds security by allowing anyone to audit it, ensuring safety and decentralization. These transparency principles align with blockchain innovations like zk-proofs, which let users control their own data while still benefiting from security and openness. This will ultimately drive greater adoption and growth of the Web3 ecosystem.

- **Controlling Illicit Activities and Enhancing User Protection:** A balanced regulatory framework will help control illicit activities and focus on user protection, education, and addressing concerns. Unlike Web 2.0, Web3's decentralized nature requires consumer protection guidelines tailored to its unique risk profile. Blockchain technology offers secure, censorship-resistant systems without relying on centralized intermediaries. Ensuring the security of decentralized networks is key to protecting users and upholding the integrity of the system.

4.4. Unified

- **Global Coordination:** Policies in the Web3 space must promote fair competition, especially given its borderless nature, and require global cooperation to be effective. Unilateral policies often fall short, making international coordination essential. Web3, like any disruptive technology, brings both immense potential and inherent risks. However, the transformative power of Web3 outweighs these risks, and a global coordinated approach will help address them proactively.

  Global collaboration could involve streamlined registration for cross-border service providers, allowing fewer requirements if they are already licensed in jurisdictions with strong frameworks. Mutual recognition agreements could further reduce regulatory burdens. Authorities could review foreign licenses, asking for additional documents specific to India only when necessary, ensuring compliance while improving access to services. An example of this approach is the EU's MiCA regulation, which allows service providers licensed in one EU country to operate across the entire bloc.

4.5. Risk based

- **Compliance Requirements based on Risk Assessment, Scale and Nature of Business:** Compliance regulations should be scaled to a company's operations and systemic risk. Thresholds based on revenue or user numbers could determine when stricter requirements apply. Smaller businesses would only need to meet essential compliance standards, while larger entities would face more rigorous policies, reducing the burden on startups while holding major players accountable.

- This approach mirrors India's IT Rules 2021, which impose additional requirements on significant social media intermediaries based on user base. Adhering to the 'Segregation of Duties' principle, similar to traditional financial markets, would distribute risks across specialized market intermediaries. Custodial service providers, for example, should be subject to regulations based on the risks they pose and the services they offer, ensuring only high-risk custodians are subject to strict requirements like maintaining liquidity and reserves.

4.6. Economy-centred

- **Foster Innovation:** Given Web3's potential to shape our digital future, policies must foster innovation. Regulating software development directly risks stifling innovation, as writing and publishing code should not subject developers to the same regulations as service providers. As Web3 continues to evolve, policies must remain flexible, promoting innovation while addressing emerging risks.

- **Macroeconomic and Financial Stability:** Macroeconomic and financial stability is important to maintain with respect to VDAs, and strong monetary policies as well as ensuring a stable economic environment is crucial. Effective monetary policies that account for the presence of VDAs will prevent VDAs from undermining financial systems, safeguarding economic stability.

  Policies that account for capital flow issues, such as VDA trading volumes being significantly higher in countries with stricter capital controls, as well as strong monetary measures which recognise the presence of VDAs while simultaneously ensuring that traditional institutional monetary measures are solidified is ideal.

PRIMUS PARTNERS®
Solutions for Tomorrow

05

Contours of Web3 Regulation for India

To operationalize the SECURE framework into a comprehensive regulatory framework, three key areas will be considered:

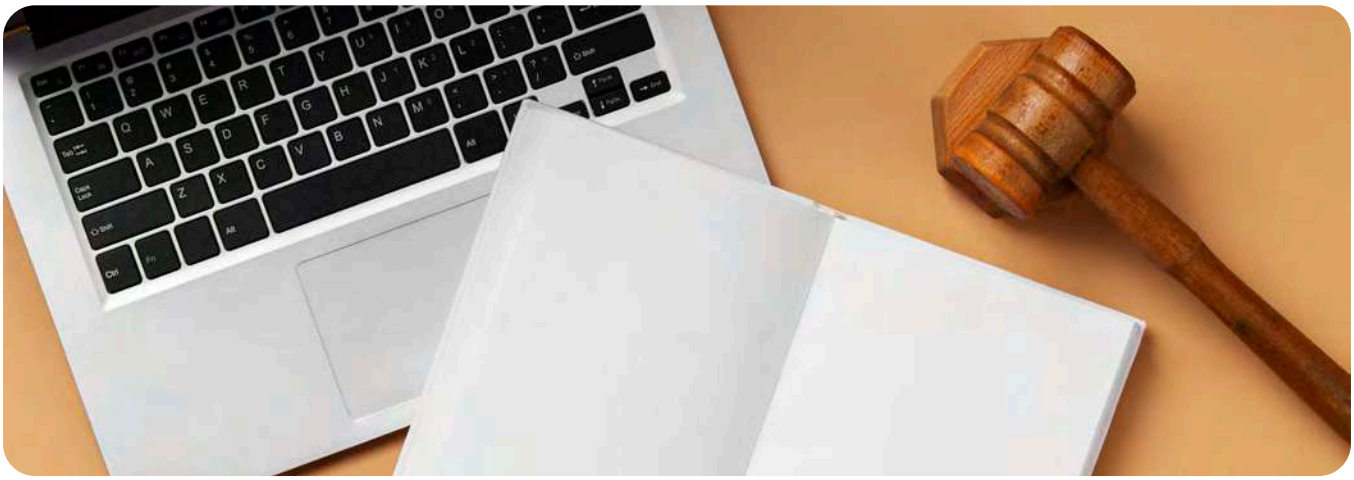
- Enacting a separate legislation
- Amending existing laws to incorporate Web3 components
- Establishing self-regulatory organizations to keep pace with emerging technologies.

Each of these pillars will bring benefits to India's economic landscape and foster the growth of the Web3 sector within the country.

Framework Parameter	Web3 Regulation Contours			Impact
	Enacting Separate legislation	Amending existing laws	SROs	
Standardisation	VDA Taxonomy	Inclusion of features such as smart contracts in existing laws	Standardized processes through Guidelines (e.g. settlement)	Regulatory clarity and improved risk management
Equity	Service providers to be subjected to regulation and not Hardware and Software Developers.		Diverse representation of industry	Increased innovation and accelerated growth of the ecosystem
Consumer-focused	Licensing requirements for VDA SPs Compliance measures such as KYC requirements Insurance requirements Creation of consumer protection fund Proof of Reserve		Ombudsman's Office Proof of Reserve Cybersecurity Guidelines	Increased trust, fraud prevention, and accountability leading to growth of users within the regulatory ambit
Unified	Aligning to international standards set by SSBs (FATF, IOSCO, IMF, FSB etc.)		Aligning guidelines to international standards set by SSBs (FATF, IOSCO, IMF, FSB etc.)	Reduction in cross-jurisdictional arbitrage
Risk based	Licensing and compliance requirements based on scale			Protection against market volatility and black swan events, maturity of markets with secondary market participation Boost to startup ecosystem

Framework Parameter	Web3 Regulation Contours			Impact
	Enacting Separate legislation	Amending existing laws	SROs	
Economy Centric	Addressing macroeconomic and financial stability risks		Ensuring growth and innovation while balancing risks	Increased contribution to GDP, global competitiveness and enhanced economic resilience

5.1. Enacting a Separate Legislation



While many countries have subsumed laws for VDAs within existing legislation, Indian juridical infrastructure lacks the institutional capabilities to ensure that all aspects of VDAs and Web3 are effectively regulated. Therefore, the Indian landscape will require creation of new legislation to successfully regulate Web3 in the country.

5.1.1. Defining Taxonomy

A taxonomy-based approach to classifying virtual digital assets (VDAs) according to their nature and use cases would enable more effective regulation by identifying the specific characteristics and risks associated with each category. Accordingly, specific compliance requirements for each category can be crafted. Careful distinction should be maintained between VDAs and e-money, such as the e-rupee or digital rupee, which will be treated as legal tender and issued exclusively by the RBI.

Updating the VDA definition to eliminate ambiguities and identifying the correct regulatory bodies for each asset type are also critical steps in ensuring clarity and effective regulation in the evolving landscape of VDAs.

International Best Practices

VDAs currently lack globally consistent definitions, classifications, or taxonomy. Various organizations, including the World Bank, Financial Stability Board (FSB), and Financial Action Task Force (FATF), have proposed their own definitions.

Dubai's Virtual Assets Regulatory Authority (VARA) excluding closed-loop and non-transferable tokens from its licensing process, and the European Union's Markets in VDAs (MiCA) regulation, which classifies digital assets into asset-referenced tokens, electronic money tokens, and utility tokens, illustrate the benefits of such an approach. Although India currently lacks a specific definition for taxonomy in this context, drawing on definitions from other jurisdictions could help establish a robust framework. This would ensure that the classification of VDAs in India is clear, comprehensive, and standardised with global best practices as per the above-described framework.

A detailed overview of global definitions can be found in Annexure 1.

Proposed Taxonomy

The proposed regulation may use the following taxonomy:

i. **Utility Tokens:** VDAs that provide users with access to a product or service within a specific blockchain platform or ecosystem.

ii. **Security Tokens:** VDAs representing ownership in an external asset, such as stocks or real estate, and subject to securities regulations.

iii. **Stablecoins:** VDAs that are pegged to stable assets like fiat currency to reduce price volatility.

iv. **Unbacked or Native Tokens:** VDAs that do not have external backing but derive value from their own network, like Bitcoin or Ethereum.

v. Governance Tokens: VDAs that grant holders voting power or influence over the decisions and direction of a decentralized project or protocol.

vi. **Non-fungible Tokens (NFTs):** Unique digital assets representing ownership of specific items, like art, music, or virtual real estate, stored on the blockchain.

vii. **Hybrid Tokens:** VDAs that combine the characteristics of multiple types of tokens, such as having both utility and security features.

Regulatory Requirements

i. Requirements for issuers related to issuing whitepaper, notifications to the authority, marketing activities, legal entity status etc.

ii. Compliance with relevant legislation related to Anti-money Laundering & Counter-terrorism Financing (AML & CTF), cybersecurity etc.

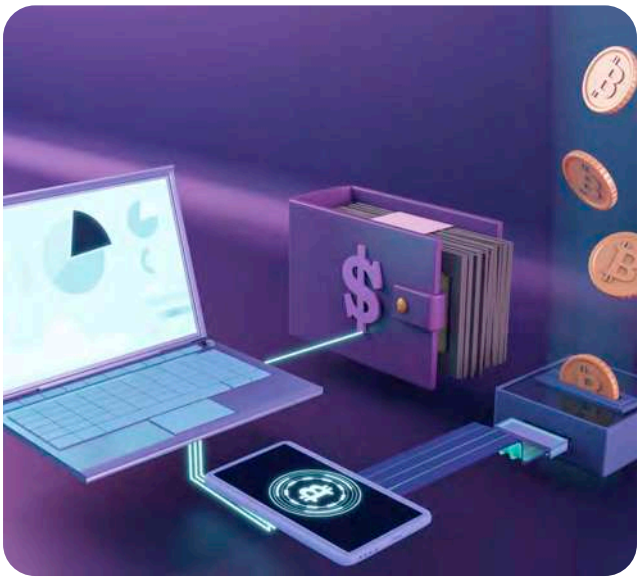
iii. Specific requirements for stablecoins such as reserve holdings

iv. Exclusions such as security tokens that can be covered under existing laws

v. Market abuse safeguards

5.1.2. Identifying Virtual Digital Asset Service Providers

Establishing a regulatory framework in India that categorizes various Virtual Digital Asset service providers (VDA SPs) and specifies requirements for each category is essential to ensure market integrity, protect consumers, and mitigate risks such as money laundering and fraud. Such categorization enables tailored regulations that address the unique risks and operational models of different service providers, fostering a safer and more transparent VDA ecosystem in the country.



International Best Practices

Various jurisdictions, such as the European Union, Canada, the United States of America, and Singapore, have introduced distinct definitions and compliance requirements for entities involved in the custody, trading, and management of VDAs. In each case, the regulatory frameworks aim to mitigate risks while fostering innovation within the Web3 space. Understanding these diverse regulatory approaches is crucial for VDA SPs seeking to operate in global markets, as they must navigate complex compliance obligations and ensure their operations meet local legal standards.

A detailed overview of global VDA SP categorisation can be found below in Annexure 2.

Based on the findings, the following conclusions can be made:

- **Regulation over Prohibition:** It is more effective to regulate rather than outright prohibit certain activities owing to the cross-jurisdictional nature of Web3.
- **Regulation of Intermediaries:** In most jurisdictions, entities that serve as intermediaries between users and VDAs are subject to regulation. These intermediaries provide services to users professionally, without directly acting on their behalf. This includes safekeeping, administration, or offering instruments that enable control over VDAs.
- **Decentralized Services:** For services provided in a decentralized manner, a "wait and watch" approach is recommended.
- **Regulation of Service Providers:** While hardware and software providers themselves are not regulated, the service providers utilizing these products are subject to regulation.

Proposed Categorization

It is proposed that future regulations should define VDA SPs as those providing one or more of the following services:

i. Providing custody and administration of VDAs on behalf of clients;

ii. Operation of a trading platform for VDAs;

iii. Exchange of VDAs for funds (fiat currency);

iv. Exchange of VDAs for other VDAs;

v. Execution of orders for VDAs on behalf of clients;

vi. Reception and transmission of orders for VDAs on behalf of clients;

vii. Placing VDAs in the market, possibly as part of an issuance or sale;

viii. Providing advice on VDAs;

ix. Providing portfolio management for VDAs;

x. Providing transfer services for VDAs on behalf of clients;

xi. Participation in, and provision of, financial services related to an issuer's offer and sale of a VDAs;

xii. Safekeeping and administration of VDAs or instruments enabling control over VDAs; and

xiii. Any other activities related to VDA that the Regulatory Authority may include from time to time.

Regulatory Requirements

i. Licensing

ii. Data collection and reporting requirements

iii. Cybersecurity measures

iv. Transaction reporting

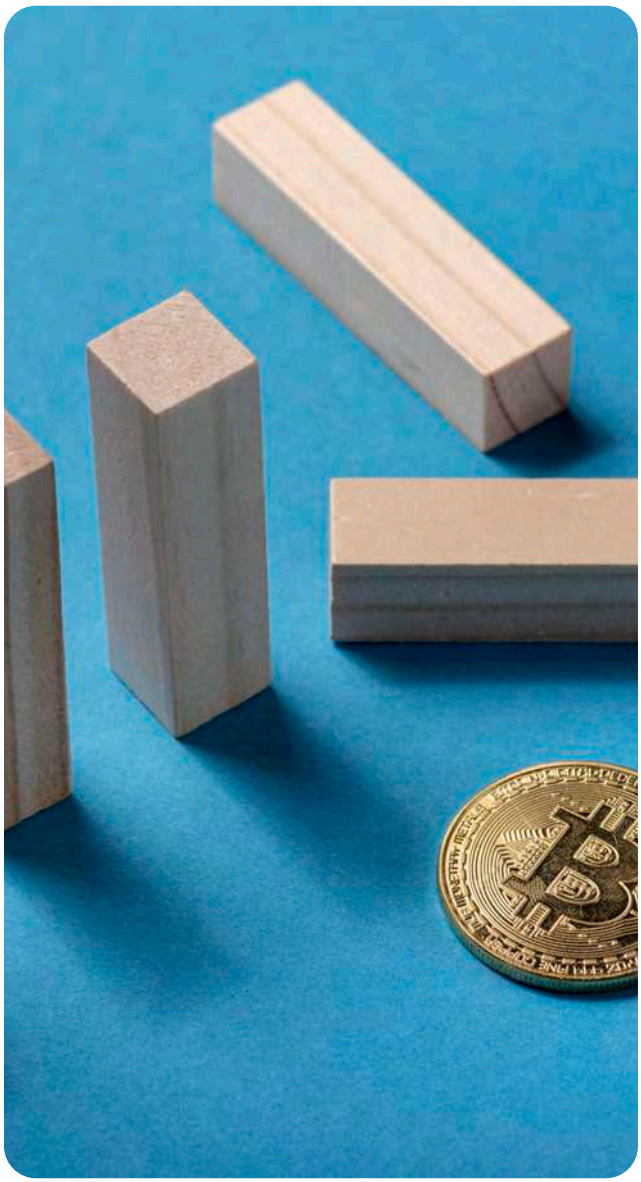
v. Disclosures to users

vi. Compliance requirements

vii. Penalties, adjudication and suspension

viii. Standards and directions

ix. Protection of consumer funds with respect to maintaining liquid assets, insurance, etc.



5.1.3. Identifying the Regulatory Authority

Regulating the Web3 sector effectively will need expertise across domains, i.e., finance, technology, markets regulation, economics, and law. At present, no single existing regulatory framework is structured to address all the aspects of virtual digital asset activity that may need to be addressed.

In order to address the diverse nature and scope of the Web3 sector, it is imperative to form a separate and independent Regulatory Authority. An inter-ministerial committee can be formed to deliberate upon the specific composition and powers of the Authority. Similar approach has been followed in the UAE for instance, Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai establishes the Virtual Assets Regulatory Authority (VARA) (VARA Act) to authorise and regulate virtual asset service providers.

Composition of the Authority

- Financial sector regulatory experts from the RBI, Securities and Exchange Board of India (SEBI), Ministry of Home Affairs and Ministry of Finance and experts in digital technology, cybersecurity, and international law
- Serving or retired Supreme Court or High Court Judge
- Persons selected by a selection committee who have expertise in Web3
- The Authority can also be empowered to form specialized committees or panels to address emerging issues in the Web3 space, such as DeFi or cross-border transactions.

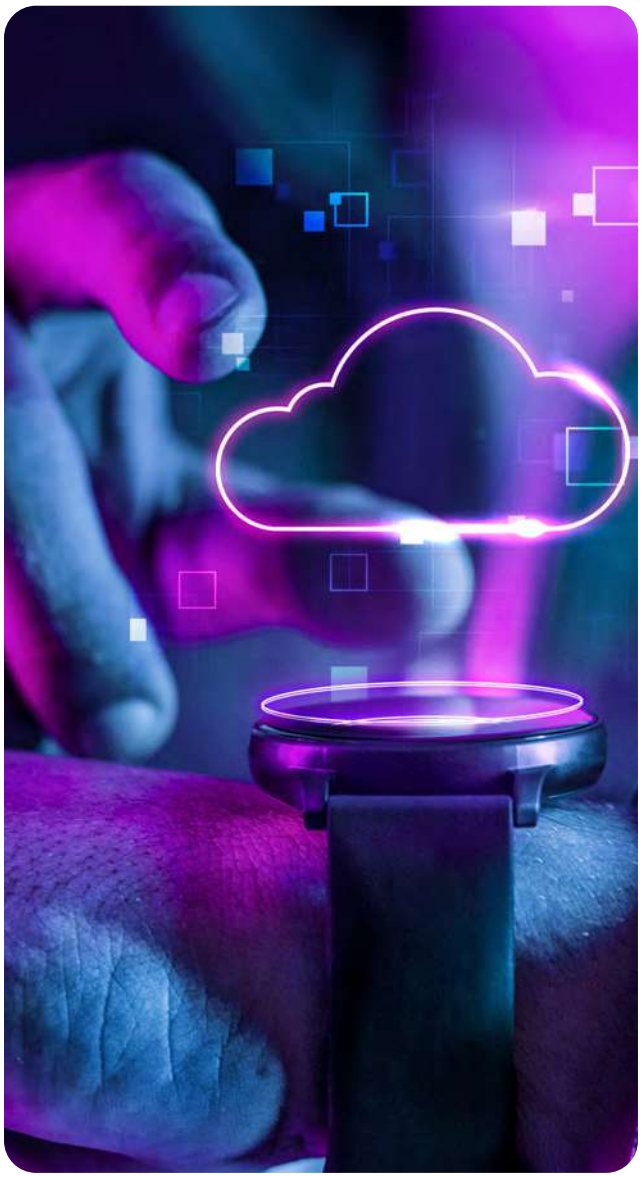
Diversification of the Authority ensures that the regulations issued will be equitable by having adequate representation from different stakeholders and sectors.

Functions and Powers of the Regulatory Authority

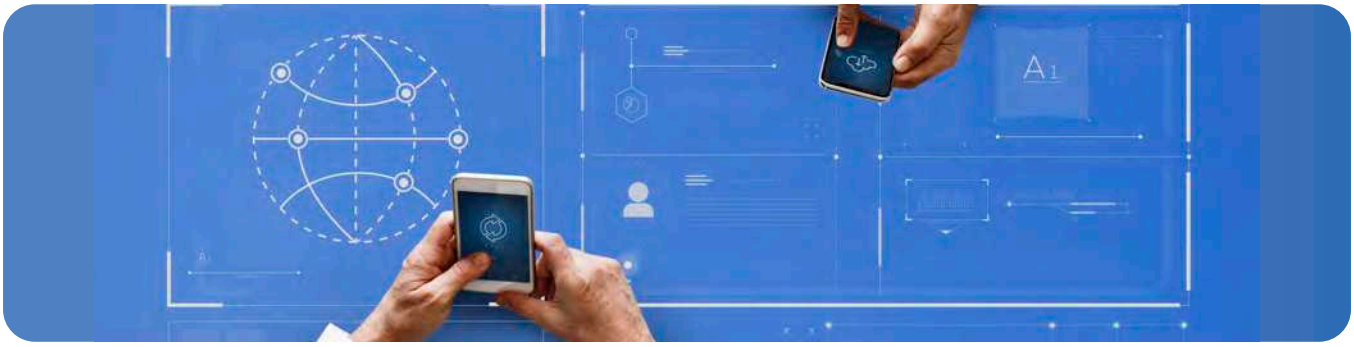
The Authority can be responsible for regulating all aspects of the VDA market which shall include but not be limited to:

- **Licensing and Regulation:** Authorizing the business of VDA SPs including licensing entities involved in VDAs and ensuring they comply with regulatory standards.
- **Supervision and Enforcement:** Enforce regulatory compliance, and impose fines, penalties, or suspend the operations of non-compliant entities, monitor market activity to prevent fraudulent practices, market manipulation, and other illicit activities.
- **Consumer Protection:** Ensure that consumers are protected from fraudulent activities and market manipulation within the VDA space, fostering and maintaining fairness, transparency, and efficiency in the sector.
- **Policy Development:** Provide inputs to future policies, aligning with global standards and fostering market integrity.
- **AML and CTF Oversight:** Collaborate with the Financial Intelligence Unit of India (FIU-IND) and other agencies to enforce AML and CTF laws concerning VDAs and ensure compliance with suspicious transactions reporting and adherence to due diligence standards.

- **International Cooperation:** Cooperate with international bodies and regulatory authorities in other jurisdictions to ensure effective cross-border regulation and enforcement.
- **Market Integrity:** Ensure the integrity of Web3 markets through monitoring and controlling market practices, including prohibiting fraudulent and unfair trade practices.
- **Dispute Resolution:** Resolve disputes between VDA SPs and consumers, ensuring a fair and transparent process.
- **Self-Regulatory Organizations:** Empower Self-Regulatory Organizations (SROs) to help maintain industry standards and enforce compliance.
- **Regulatory Sandbox:** Establish regulatory sandboxes to provide a controlled environment for emerging Web3 activities related to that do not fit within existing VDA SP definitions.
- **Research and Education:** Conduct research and promote education and training programs to advance knowledge and understanding in the Web3 sector.
- **Information Sharing:** Call for information from, or furnish information to, other authorities, including private and public stakeholders, in accordance with the law of the land, unless prohibited otherwise.



5.2. Amending Existing Laws



To bring VDAs and Web3 under a comprehensive regulatory framework in India, several existing laws may need to be amended or clarified. The key areas where amendments could be required include but not limited to:

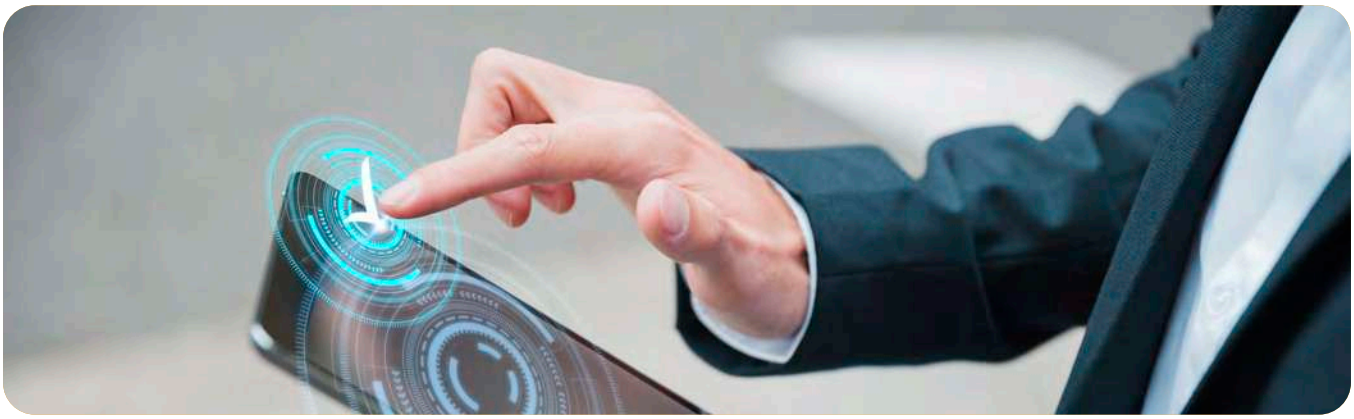
Act	Current Status	Required Amendments
Finance Act and Income Tax Act, 1961	The income Tax Act currently only defines Virtual Digital Assets.	Along with defining VDAs, a rationalisation of tax rates basis the taxonomy should be considered to ensure fairness, promote compliance, and encourage the growth of the VDA ecosystem in India.
Companies Act, 2013	The Companies Act governs corporate behaviour and compliance in India. VDAs are not explicitly mentioned in the Act.	Modifications may be necessary to define how VDAs are treated in financial statements, capital raising, disclosures, and asset valuation. For example, how companies report VDA holdings and transactions in their financial accounts may need to be specified.
Securities Contracts (Regulation) Act (SCRA), 1956	This Act regulates securities and stock exchanges in India. VDAs do not fall under the current definition of "securities.	If certain VDAs are classified as securities, amendments to the SCRA may be necessary to regulate exchanges dealing with VDAs. This would bring these VDAs under the regulatory purview of the Securities and Exchange Board of India (SEBI).
Information Technology Act, 2000	The IT Act governs cybersecurity, digital signatures, and electronic records. VDAs and blockchain technology are not explicitly covered.	Amendments may be required to address the security of VDA transactions, privacy, data protection, and cybersecurity aspects of blockchain and digital ledger technologies.

Act	Current Status	Required Amendments
Consumer Protection Act, 2019	The act protects consumer rights but does not specifically cover VDA transactions.	Amendments may be needed to extend consumer protection rights to transactions involving VDAs, including mechanisms for grievance redressal and dispute resolution for users of VDA platforms.
Indian Contract Act, 1872	The Indian Contract Act governs traditional contracts based on offer, acceptance, consideration, and lawful objects. The Act assumes contracts are executed and enforced by human parties.	Smart contracts are self-executing and may not involve explicit human intervention once programmed. The Act may need to recognize smart contracts as valid, enforceable agreements, even though they are executed digitally without manual input.

DeFi and DAOs both have a common attribute in that they are decentralised and autonomous which leads to a unique situation where no juristic entity or person exists against whom liability may be attached. Given recent precedents internationally, it may be useful to introduce some guidance on whether a deeming fiction will apply to these entities to give them the character of a legal person (a simple partnership or association of persons). It would also be useful to give recognition to the acceptance of or even mandating incorporating 'legal wrappers' to give a juristic presence to decentralised autonomous organisations.

- Pranay Agrawala, Partner, Panda Law

5.3. Empowering Self-Regulatory Organizations



For a sector such as Web3, where the technology is continuously evolving, establishing a Self-Regulatory Organization (SRO) could be advantageous. Striking a balance between fostering Web3's potential and mitigating the risks it may pose to broader systems is vital. An SRO, being closely aligned with ongoing developments, can swiftly adapt to the sector's dynamic changes.

By adopting a self-governance model, Web3 entities can establish and adhere to industry standards and best practices, showing a proactive commitment to responsible innovation. Sector-wide collaboration can address challenges, encourage innovation, and uphold ethical standards.

"As the Web3 ecosystem expands, the need for a balanced regulatory framework that fosters innovation while ensuring compliance has never been more critical. The Bharat Web3 Association (BWA) has taken a leadership role, guiding the industry toward responsible practices through collaboration and self-regulation.

BWA has taken proactive steps in issuing guidelines that prioritize consumer protection. Our collaboration with FIU-IND highlights our commitment to strengthening compliance for VDA SPs. With diverse representation from over 45 Web3 players, BWA promotes self-regulation in both letter and spirit, fostering accountability and innovation.

While a strong regulatory framework is crucial, in a fast-evolving sector like Web3, SROs provide unique value. With on-ground experience and industry insights, SROs can effectively complement regulatory authorities, ensuring practical and forward-looking governance."

- Dilip Chenoy, Chairperson, Bharat Web3 Association

5.3.1. Web3 SROs around the World

The global focus on SROs underscores their importance, validating the need for such an approach in the Web3 sector. By studying international SRO models, India can draw relevant lessons and adapt them to our local context, ensuring a tailored approach to governance.

a. Taiwan

Authority for Self-regulation	*Taiwan Virtual Asset Service Provider Association*
Regulator	*Financial Supervisory Commission (FSC)*
Composition of SRO	*24 crypto firms compliant with FSC's AML regulations*
Powers	*Develops self-supervisory rules, enhances regulatory oversight, implements consumer protection measures*
Role in Industry	*Fosters collaboration between stakeholders and government; promotes innovation*

Taiwan has taken a major step towards regulating its Web3 sector by establishing the Taiwan Virtual Asset Service Provider Association, guided by the Financial Supervisory Commission (FSC)[15]. The primary goal of the association is to create self-regulatory guidelines that ensure VDA SPs adhere to industry practices that meet government expectations while safeguarding consumer rights[16]. This initiative aims to balance industry interests with the need for stringent regulation[17].

The government has shown strong support for this initiative. The FSC has tasked the association with drafting self-regulatory guidelines that meet both industry needs and regulatory standards, reflecting a proactive stance on industry oversight[18].

b. Japan

Authority for Self-regulation	*Japan Virtual and Crypto Assets Exchange Association (JVCEA)*
Regulator	*Financial Services Agency (FSA)*
Composition of SRO	*Diverse members, Board of Directors, various committees, member exchanges, advisors, collaborative partners*
Powers	*Sets standards, issues license, conducts market surveillance, manages risks, enforces compliance*
Role in Industry	*Enhances operational standards, rebuilds trust, addresses regulatory concerns, adapts to new challenges*

The Japan Virtual and Crypto Assets Exchange Association (JVCEA) has set a proactive regulatory framework for Japan's Web3 sector, enhancing operational standards[19] and consumer protection. As an SRO, it updates guidelines, monitors compliance, evaluates licenses, conducts market surveillance, and engages in international regulatory dialogues to shape global standards and advocate for favourable industry conditions[20].

Japan's experiment with self-regulation in its digital asset sector, led by JVCEA, is evolving amid ongoing discussions with the country's financial regulator.[21] The FSA has highlighted areas for improvement, such as the timely implementation of anti-money laundering (AML) regulations and enhancing transparency in decision-making processes. Given the regulatory challenges & fluctuations in market conditions in Japan, JVCEA continues to address the challenges and paves the way through increased transparency and efficiency in the processes.

5.3.2. SROs in India

India is increasingly embracing SROs to enhance governance and compliance in various sectors. In recent developments, the Reserve Bank of India (RBI), recognizing the importance of self-regulation, has issued a framework to enhance industry standards through SROs for the Fintech sector and Non-Banking Financial Companies (NBFC). [22]These SROs leverage technical expertise to aid in regulatory policy formulation, fostering innovation, transparency, fair competition, and consumer protection. The table below outlines the eligibility and purpose and functions of SROs in both sectors.

Aspect	Fintech SRO[23]	NBFC SRO
Regulator	RBI	RBI
Eligibility	• **Balanced mix** of NBFC-ICCs, HFCs, and NBFC-Factors as members (At least 10% of smaller NBFCs from the Base Layer within 2 years) • **Net worth** of > Rs. 2 Cr • Max. **2 recognised SROs** for the NBFCs • **Separate categories** to serve different kinds of NBFCs	• **Not-for-Profit:** Must be registered under Section 8 of the Companies Act, 2013. • **Diversified Shareholding:** No entity should hold 10% or more of the share capital. • **Primary Objective:** MoA must state the primary purpose as an SRO for fintech. • **Net Worth:** Minimum net worth of ₹2 crore within one year of recognition. • **Infrastructure:** Must have the necessary IT and operational systems. • **User Harm Management:** Systems to handle fraud, mis-selling, and misconduct. • **Domiciled in India:** Must be registered in India, but can have overseas members. • **Voluntary Membership:** Must represent fintech entities of various sizes and activities.
Functions & Responsibilities	• Act as a unified voice • Addresses sectoral concerns, • Aids in policymaking, • Gathers and shares information • Align activities with regulatory frameworks • Support FinTech innovation under RBI supervision • Ensures robust oversight and regulatory adherence	• Standard-Setting • Oversight and Enforcement • Developmental Role • Grievance Redressal • Responsible Innovation • Data Management • Communication with RBI

The RBI's move to establish SROs in the fintech and NBFC sectors represents a strategic shift towards more nuanced regulation. These SROs can leverage technical expertise to aid in policy formulation and promote collaboration between the industry and regulator, enhancing innovation, transparency, competition, and consumer protection. By uniting the industry in addressing sectoral concerns and engaging with the RBI, SROs can help shape policies that align with industry needs, contributing to adaptive and effective regulation in India's evolving financial landscape.

ASCI Guidelines for VDA Service Providers

The Advertising Standards Council of India (ASCI), established in 1985, serves as a model Self-Regulatory Organization (SRO) by overseeing the advertising sector to ensure content honesty, truthfulness, decency, safety, and fairness. Comprising representatives from businesses, advertising agencies, media, and related professions, ASCI sets and enforces standards, swiftly addressing non-compliant ads through corrective actions. As a voluntary, not-for-profit entity, ASCI operates independently of the government but is supported by major industry players committed to ethical advertising practices.

ASCI has also introduced specific guidelines for advertising Virtual Digital Assets (VDAs) in India. These guidelines are designed to enhance consumer protection and transparency by mandating clear risk disclaimers, prohibiting misleading terms like "currency" or "securities". Although not legally binding, these guidelines have been widely adopted by industry players, contributing to a more trustworthy advertising environment and reinforcing consumer confidence in the Web3 sector.

5.3.3. Insights and Lessons for Web3

SROs usually exist in industries and sectors with some common elements:

Emerging technology sectors: Industries that utilise new and emerging technologies with dynamic and fast paced environments usually form SROs to ensure that these new technologies are represented; while ensuring they follow existing regulations.

Robust consumer protection frameworks: SROs are usually present in industries where they are regularly in contact with private consumer details, including and especially consumer funds. In these cases, it is important for SROs to implement certain guidelines to ensure consumers are safeguarded successfully.

Balancing innovation with compliance: Industries in sectors with new and innovative products and services need to balance these with the necessary compliance measures, where SROs could help in ensuring the same.

SROs successfully exist in industries such as fintech and NBFCs and are important for representation as well as assurance of compliance. However, there are certain factors that are needed to ensure that these SROs are successful in their representation:

SROs need to have diverse representation from across the industry they serve, ensuring a balanced mix of stakeholders, such as members from the industry, academia, and think tanks. This diversity helps ensure that all voices within the sector are equally represented.

SROs need to possess the necessary capacity to adequately perform important functions of representation and regulation both within their membership as well as with the government. They need to ensure that they have enough technical prowess, manpower and practical know-how for smooth functioning.

SROs need to have strong governance structures with defined processes that it will use for gathering input regarding how rules are created. This ensures independent functioning of the SRO and effective governance models.

Lastly, SROs need to work closely with regulators and government bodies to ensure constant communication and successful compliance, as well as provide updates on the functioning of firms in the industry.

5.3.4. SRO for the Web3 Sector in India

Establishing an SRO for the Web3 sector in India is crucial to ensure industry-driven standards, promote responsible innovation, and foster compliance within the rapidly evolving decentralized ecosystem. An SRO will play a pivotal role in bridging the gap between regulatory authorities and industry participants, ensuring that the Web3 landscape grows in a secure and transparent manner.

Eligibility Criteria

i. Encompassing entities across all verticals within the Web3 sector

ii. Aiming for broad representation, reflecting different stages of development and sizes within the Web3 ecosystem

iii. Domiciled and registered in India, with the capacity for global membership

iv. Structured as a not-for-profit entity under Section 8 of the Companies Act, 2013, ensuring transparency and clarity

v. Working towards achieving and maintaining a high minimum net worth, aligned with RBI guidelines for fintech and NBFC SROs

vi. Establishing different verticals or divisions to address various aspects and complexities of the Web3 ecosystem as needed

These requirements ensure that important players in the Web3 sector are part of the SRO, ensuring diverse yet concise representation.

5.3.5. Functions and Responsibilities of SRO

SROs also need to have certain responsibilities and requirements to ensure that their members maintain the necessary compliance principles:

Standard Setting and Enforcement: Develop and enforce industry standards for blockchain protocols, smart contracts, and operational practices to ensure consistency and reliability across the Web3 ecosystem. Regular audits should be mandated to ensure compliance with established standards, with the power to impose penalties for non-compliance.

Certification: Implement certification programs for developers and companies to ensure adherence to best practices and ethical guidelines.

Market Surveillance and Risk Management: Conduct market surveillance to detect and prevent illicit activities, such as fraud and money laundering, within the Web3 space. Develop and enforce risk management frameworks to address cybersecurity threats and other operational risks.

Dispute Resolution and Grievance Redressal: Establish mechanisms for resolving disputes between consumers and Web3 entities, ensuring fair and transparent resolution processes. Create a system for addressing consumer grievances, providing timely and effective solutions to user complaints.

Consumer Protection and Education: Develop ethical guidelines and best practices to protect users from scams, misinformation, and technical vulnerabilities. Launch educational programs to inform users about their rights and responsibilities within the Web3 landscape, promoting safe and informed participation.

Regulatory Sandbox Initiatives: Create regulatory sandboxes to allow innovators to test new technologies and business models under a regulated yet flexible environment, promoting innovation while ensuring compliance.

Collaboration with Regulatory Bodies: Act as a unified voice for the Web3 sector in engagements with regulatory bodies such as the RBI and MeitY, facilitating the development of comprehensive and practical regulatory frameworks.

By establishing a well-structured and inclusive SRO, India can ensure a robust, transparent, and self-regulated Web3 ecosystem that fosters innovation while maintaining high standards of compliance and accountability.

PRIMUS PARTNERS®
Solutions for Tomorrow

06

Anticipated Benefits of Web3 Regulations

Implementing Web3 regulations is crucial for fostering innovation, ensuring consumer protection, and promoting market stability. A well-defined regulatory framework can position India as a global leader in the digital economy while mitigating risks associated with emerging technologies.

Increased Security

A robust regulatory framework can significantly enhance the security of digital transactions and VDAs, mitigating risks associated with fraud and cyber-attacks.

In India, a regulatory framework could mandate stringent security protocols for virtual asset exchanges and service providers. This would include requirements for regular security audits, encryption standards, and robust anti-fraud measures. For instance, similar to VARA's emphasis on cybersecurity in Dubai, regulations could require adherence to high security standards akin to those set by the National Payments Corporation of India (NPCI) for secure transactions, thereby reducing incidents of financial fraud and cyber-attacks.

VARA in Dubai mandates rigorous cybersecurity measures for virtual asset businesses, which includes anti-fraud protocols and regular security assessments. MiCA, on the other hand, requires stablecoin issuers to maintain adequate reserves and transparency, enhancing the overall security and reliability of VDAs.

Consumer Protection

Clear regulations can ensure that consumers are protected from misleading practices and scams, providing them with accurate information about their investments.

In India, consumer protection regulations could require virtual asset platforms to provide transparent information about investment risks and ensure that users are well-informed. For example, regulations could mandate that all crypto exchanges display clear risk warnings and detailed operational information, similar to disclosure requirements enforced by the Securities and Exchange Board of India (SEBI) for traditional financial instruments.

VARA's regulations include strict guidelines for transparency and accurate information disclosure. MiCA enhances consumer protection by requiring detailed white papers and regular updates from crypto-asset issuers, ensuring that investors understand the nature and risks of their investments.

Market Stability

Regulations contribute to market stability by creating a structured environment that reduces the likelihood of market manipulation and speculative bubbles.

In India, a regulatory framework could introduce measures to stabilize the virtual asset market, such as guidelines for fair trading practices and reserve requirements for stablecoins. For example, similar to MiCA's rules for stablecoin reserves, the Reserve Bank of India (RBI) could implement regulations ensuring that issuers maintain sufficient reserves to stabilize their tokens and prevent market volatility.

VARA's licensing regime helps stabilize the market by ensuring that only compliant entities operate, reducing risks of manipulation. MiCA sets rules for issuance and trading of various VDAs, including stablecoins, to promote market stability and reduce speculative risks.

Legal Clarity

Providing legal clarity through regulations helps businesses and developers navigate the legal landscape more effectively, reducing uncertainty and potential legal disputes.

In India, a clear regulatory framework would offer legal certainty for virtual asset businesses and developers. This could involve defining the legal status of digital assets and providing guidelines for compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) laws. For instance, regulations similar to VARA's licensing regime could clarify the legal obligations for crypto exchanges and wallet providers, simplifying their operational compliance.

VARA provides legal clarity by setting out clear regulations for virtual asset activities in Dubai. MiCA harmonizes crypto-asset regulations across the EU, providing consistent rules and reducing legal uncertainties for businesses operating in multiple jurisdictions.

Interoperability

Regulations can promote interoperability by setting standards that ensure different systems and platforms work seamlessly together.

In India, regulations could encourage interoperability by establishing standards for digital asset transactions and reporting. This might involve creating frameworks that allow seamless integration between Indian platforms and international exchanges, similar to the unified approach seen in MiCA within the EU.

VARA's alignment with international standards facilitates global interoperability. MiCA promotes interoperability within the EU by providing a consistent regulatory framework, ensuring seamless operation of digital assets across member states.

Innovation Encouragement

A well-defined regulatory environment can foster innovation by providing a clear framework that supports new technologies while ensuring compliance with safety standards.

In India, a regulatory framework could create a supportive environment for innovation in the Web3 space. For example, regulations could include sandbox provisions allowing startups to test new technologies under regulatory supervision. This approach, similar to other countries' fintech sandboxes, would help Indian startups develop and scale their technologies while ensuring regulatory compliance.

VARA's regulatory framework supports innovation by providing a clear set of rules while ensuring compliance. MiCA's comprehensive framework encourages the development of new crypto products by offering a stable and predictable regulatory environment.

Fair Competition

Regulations help ensure fair competition by enforcing consistent standards and practices across the industry, preventing monopolistic behaviors.

In India, regulations could prevent unfair practices and promote healthy competition in the virtual asset sector. By implementing rules that apply equally to all market participants, such as disclosure requirements and operational standards, the regulatory framework would prevent dominant players from exploiting their position and encourage a more diverse and competitive market.

VARA promotes fair competition by enforcing uniform standards for all virtual asset businesses. MiCA aims to create a level playing field across the EU by applying consistent requirements to all crypto-asset issuers and service providers.

Tax Compliance

Clear regulations facilitate tax compliance by ensuring that transactions and activities are well-documented and transparent.

In India, a regulatory framework could enhance tax compliance by establishing clear guidelines for reporting and documenting virtual asset transactions. This would help the Indian government track and manage tax obligations related to digital assets more effectively. For example, regulations could require exchanges to provide transaction reports to tax authorities, similar to reporting obligations in traditional financial markets.

VARA's emphasis on transparency supports tax compliance by requiring accurate reporting from virtual asset businesses. MiCA's framework includes provisions for clear documentation of transactions, aiding tax authorities in managing crypto-related tax obligations.

Regulatory Integration

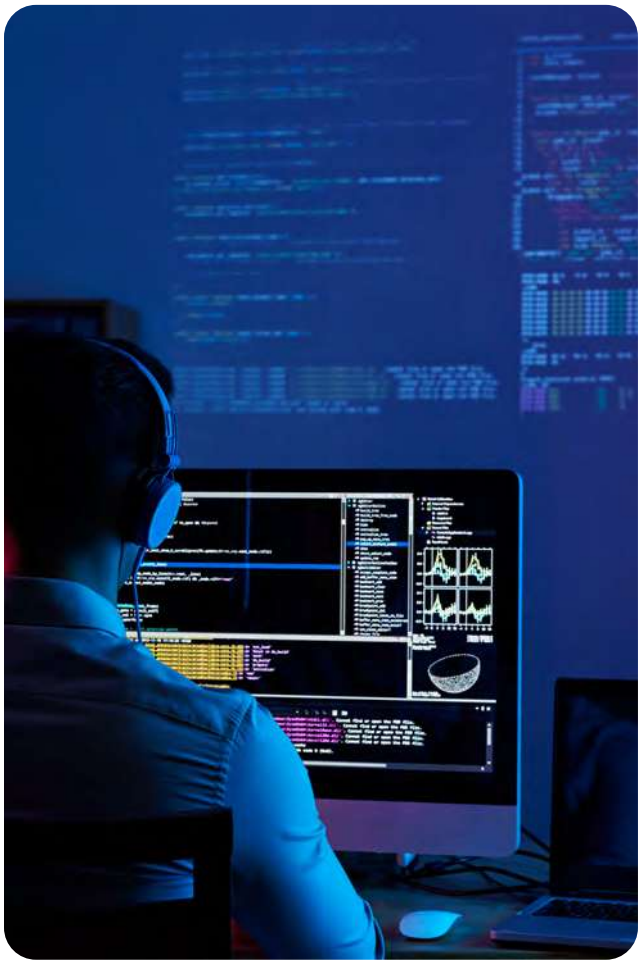
Effective regulations integrate new technologies with existing financial and legal systems, promoting broader adoption and smoother interactions.

In India, regulatory integration could help align virtual asset activities with existing financial regulations. For example, regulations could ensure that digital assets are compatible with India's financial infrastructure, such as integrating with the existing banking system and payment networks. This integration would facilitate smoother interactions between traditional and digital financial systems.

VARA's approach aligns with international standards, facilitating integration with global systems. MiCA integrates VDAs into the broader EU regulatory framework, promoting seamless interactions between digital and traditional financial systems.

Ethical Standards

Introduction: Regulations establish ethical standards that ensure industry practices align with societal values and expectations, fostering public trust.



India Context: In India, a regulatory framework could set ethical guidelines for the virtual asset industry, addressing issues such as responsible marketing and fair treatment of consumers. By enforcing standards that align with societal values and consumer protection principles, the regulations would help build public trust in digital assets and ensure that industry practices are transparent and ethical.

VARA promotes ethical standards by requiring fairness, transparency, and integrity from virtual asset businesses. MiCA sets ethical guidelines for VDAs, including responsible marketing and accurate representation, helping maintain public trust and align practices with societal norms.

In summary, a comprehensive regulatory framework for Web3 technologies in India could significantly enhance security, consumer protection, market stability, and innovation, among other benefits. By drawing on successful models like VARA and MiCA, India can create a robust regulatory environment that supports the growth and development of the virtual asset sector while ensuring a safe and fair market for all participants.

"Web3 holds immense potential to transform India, emerging as a key pillar in advancing good governance and improving the quality of life for all citizens. By harnessing blockchain technology, it can streamline complex processes, enhance transparency, and rebuild trust in public institutions. From facilitating seamless payments to revolutionizing citizen services, healthcare, taxation, and beyond, Web3 promises a more efficient, reliable, and secure digital ecosystem. This shift will not only reduce administrative burdens but also empower individuals to participate more meaningfully in governance, fostering a more equitable and prosperous India.

One of the most transformative aspects of Web3 is the development of secure, portable digital identities. Coupled with zero-knowledge proof-based verifications, these identities will safeguard citizens' personal data, offering robust privacy protection. By enabling real-world asset tokenization, Web3 identities will provide indisputable proof of ownership for both physical and digital assets—such as land parcels, health records, and financial bonds and securities—significantly increasing trust and transparency while eliminating data leaks and fraud.

However, the uncharted nature of Web3 technology requires the development of a comprehensive regulatory framework. Such a framework must foster innovation while ensuring consumer protection and ethical development. It is crucial that these regulations strike a balance: they must be straightforward yet robust, enabling blockchain technology to be both democratic and secure, ensuring its widespread adoption in a safe and inclusive manner. With a flexible regulatory framework, Web3 will usher in a new era of trust, transparency, and sustainability."

- Alok Gupta, Co-founder and CEO, ChainCode Consulting LLP

PRIMUS PARTNERS®
Solutions for Tomorrow

07

India's Path to Web3 Leadership: Recommendations and Way Forward

Web3 presents India with a chance to lead globally, transitioning from a talent source to a product powerhouse. The first two phases of the internet, namely Web1 and Web2 were primarily Western phenomena. However, to seize this opportunity in Web3, now is the time to act. We therefore recommend for the following:

7.1. For the Government

Consultation with the Industry through a Discussion Paper: Issuing a formal consultation paper that seeks input from key stakeholders in the Web3 industry would foster an open dialogue between the government and the industry. Such consultation can help create a more inclusive and effective regulatory framework that takes into account the insights and on-the-ground experiences of industry players and Web3 experts.

Minimum Standards for Adoption to Avoid Regulatory Arbitrage: To mitigate the risk of regulatory arbitrage, the regulatory framework should include minimum standards that G20 nations should adopt. Adopting these global benchmarks will level the playing field for businesses and provide equitable protections for consumers.

International Best Practices and Learning for the Indian Context: The government can study international regulatory frameworks for Web3, such as the EU's MiCA regulations and Dubai's VARA framework. A customized approach that integrates global best practices with domestic needs will create a balanced regulatory environment conducive to growth and innovation.

Innovation and Sandbox Initiatives: The government may introduce regulatory sandboxes to allow startups and innovators to test Web3 solutions in a controlled environment. This approach would help the government gather data on the risks and benefits of various Web3 applications while allowing businesses to innovate with fewer restrictions.

Consumer Awareness and Education: Public awareness and education initiatives would educate consumers about the benefits, risks, and use cases of Web3, empowering them to participate in the digital economy responsibly. Consumer trust and understanding are key to the sustainable growth of the Web3 ecosystem.

7.2. For the Industry

Collaborate with the Government: The industry should proactively collaborate with the government by offering model legislation and frameworks for Web3 regulation. By providing detailed insights into how regulatory measures can be structured, the industry can help ensure that the government's policies are both practical and conducive to innovation. This collaboration can also include joint initiatives to address shared challenges in areas like compliance, cybersecurity, and data protection.

Provide Use Cases and Demonstrate the Benefits of Web3: Industry players should actively present real-world use cases that demonstrate how Web3 and blockchain technologies can solve critical issues in areas such as supply chain management, financial inclusion, and data security. By showcasing the tangible benefits of Web3, the industry can help the government and the public understand the transformative potential of these technologies, encouraging broader adoption and regulatory support.

Implement Self-Regulation: Until a formal government regulatory framework is in place, the industry should take the lead in implementing self-regulation. By establishing internal guidelines and best practices for compliance, security, and consumer protection, Web3 companies can demonstrate accountability and build trust with regulators.

Enhance Consumer Education: The Web3 industry must invest in educating consumers about the practical applications, benefits, and risks of Web3. Consumer awareness is critical for informed participation in the Web3 ecosystem, and the industry should take the lead in providing resources, workshops, and educational content to users at all levels.

Foster Collaboration Across the Ecosystem: The industry should encourage collaboration between startups, established companies, and regulators to foster a cohesive Web3 ecosystem. Sharing knowledge, promoting innovation, and working together on compliance and best practices will help the ecosystem grow responsibly. This collaboration will ensure that new entrants to the market are supported and that the industry moves forward collectively, rather than in isolated silos.

By taking these steps, both the government and the Web3 industry can ensure that India capitalizes on the immense potential of Web3, fostering innovation, protecting consumers, and positioning the country as a global leader in the digital economy.

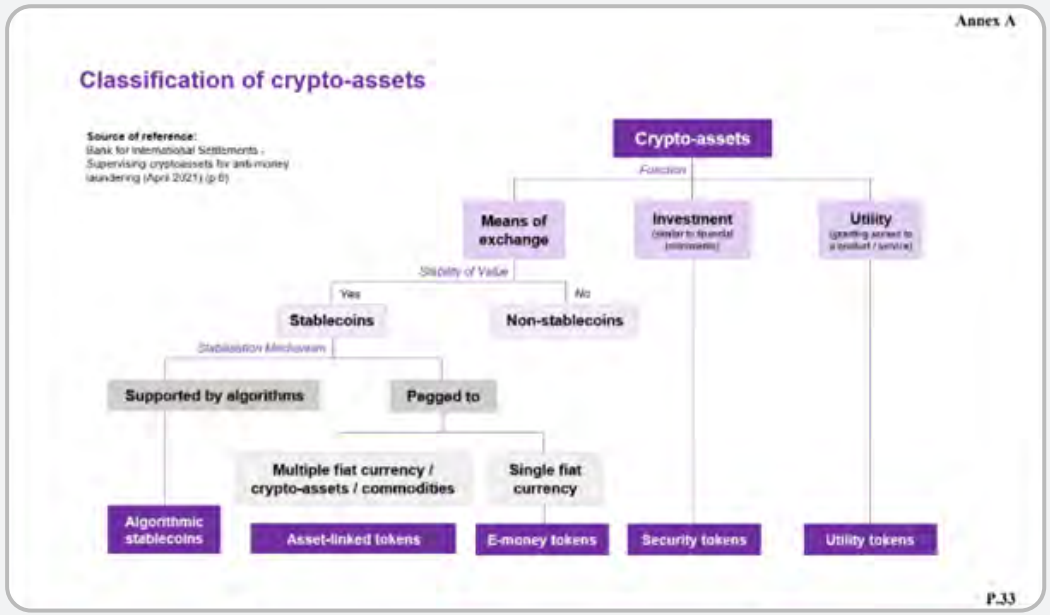
ANNEXURE 1: Global Examples of Taxonomy for Virtual Digital Assets

S.No	Organisation	Definition
1	**World Bank**	Crypto-assets can be broadly defined as private digital representations of value that can be used for payment or investment purposes or to access a good or service and rely on a distributed ledger or similar technology... More specifically, crypto-assets typically operate on open, decentralized computer networks which aim to maintain an immutable distributed ledger that enables users to store, transfer, and receive funds 24/7 with global reach and relatively fast settlement in a purely peer-to-peer fashion without the need for intermediaries (i.e., "permissionless") or the potential of third-party interference (i.e., "censorship resistance"). The open-source software protocols enforced by these decentralized networks allow for consensus formation about the "state of the world" in low-trust environments without requiring a trusted third party and seek to imbue crypto-assets with certain characteristics such as scarcity, verifiability, and, more broadly, programmability.[24]
2	**Financial Stability Board (FSB)**	Crypto-assets are a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology. The different segments of crypto-asset markets – including unbacked crypto-assets (such as Bitcoin), so-called "stablecoins", and decentralised finance (DeFi) – are closely interrelated in a complex and constantly evolving ecosystem and need to be considered holistically when assessing related financial stability risks. [25]
3	**Financial Action Task Force (FATF)**	Virtual assets (crypto assets) refer to any digital representation of value that can be digitally traded, transferred or used for payment. It does not include digital representation of fiat currencies.[26]
4	**The Commonwealth Model Law on Virtual Assets**	Virtual Assets mean a digital representation of value that may be digitally traded or transferred, and may be used for payment or investment purposes, but do not include a digital representation of Fiat Currencies, securities and other financial assets to the extent that they are regulated by other laws of [the Jurisdiction]

S.No	Jurisdiction & Regulatory Framework	Regulatory Framework	Definition
1	**Europe**	MiCA(Market in Crypto Assets)	**Crypto Asset:**A digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology. **Asset-referenced Stablecoin:** A type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies **Fiat Stablecoin:** A type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency. **Utility Token:** A type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer. **Small local exchange token:** A type of crypto-asset that is only used in exchange for goods and services in a limited network of merchants with contractual arrangements with the offeror, whereas the total yearly consideration of the offer to the public does not exceed 1 million EUR. Non-Fungible Token Crypto-assets that are unique and not fungible with other crypto-assets. **Security Tokens:** Transferable securities; money-market instruments; units in collective investment undertakings; options, futures, swaps, and other derivatives linked to securities, currencies, interest rates, emission allowances, or financial indices; derivative contracts linked to commodities, whether settled physically or in cash; derivative contracts tied to commodities traded on regulated markets, MTFs, or OTFs; financial contracts for differences; derivative instruments for transferring credit risk; derivative contracts involving climatic variables, freight rates, or inflation rates; and emission allowances conforming to the requirements of Directive 2003/87/EC.

S.No	Jurisdiction & Regulatory Framework	Regulatory Framework	Definition
2	Canada		Stablecoins include • **Fiat Stablecoins:** Value-Referenced Crypto Assets (Need CSA written consent, CSA SN 21-332) Fiat-backed Crypto Asset (single currency) (e.g. E-money) • **Asset-Referenced Stablecoins:** Value-Referenced Crypto Assets (Need CSA written consent, CSA SN 21-332) (Backed by gold, other crypto-assets, basket of assets) • **Algorithmic Stablecoins:** (Algorithm) - algorithmically linked to value through buy/sell or some other mechanism (CSA indicated unlikely to give consent, CSA SN 21-332) **Coin Token:** Cryptocurrency / Virtual Currency / Digital Currency (e.g. BTC, ETH etc) • Crypto contracts • Crypto instruments **Non-Fungible Tokens:** Not currently regulated in Canada • Non-Fungible Token (art, music, real-world assets) ° Fractionalized (case-by-case determination needed) ° Non-Fractionalized • Token used for games **Security Tokens/ Crypto Contracts:** Securities include Security Tokens and instruments or contracts involving crypto assets. Securities laws apply unless a CASP obtains the necessary exemptions **Crypto Asset Fund:** Public funds investing in crypto assets are subject to the same regulatory framework as other publicly distributed investment funds in Canada
3	United Kingdom	U.K. Financial Services and Markets Act (2000)	**Fiat Stablecoin:** "Fiat-backed" Crypto Asset used for payment **Stablecoin:** "Unbacked" Crypto Assets (Algorithmic Stablecoin) **Other Token Types:** "Unbacked" Crypto Assets (e.g. BTC / ETH) **Non-Fungible Token ("NFT"):** Non-Fungible Token **Governance Token:** No specific mention **Security Tokens:**

S.No	Jurisdiction & Regulatory Framework	Regulatory Framework	Definition
4	Singapore	Monetary Authority of Singapore ("MAS")	**Fiat Stablecoin:** Single-currency pegged stablecoins Label MAS Regulated Circulation of S$5.0mm Non-Fungible Token ("NFT"): Non-Fungible Tokens; Gaming Credits
5	United States	Financial Crimes Enforcement Network (FinCEN), Securities and Exchange Commission (SEC), Commodity F...	**Fiat Stablecoin:** Payment Stablecoin[27] Other Token Types (including Governance Tokens): Digital Asset:[28] Digital Commodity[29] Non-Fungible Digital Assets[30]: Gaming Credits
6	Dubai	VARA	**Virtual Asset[31]:** A digital representation of value that may be digitally traded, transferred, or used as an exchange or payment tool, or for investment purposes. This includes Virtual Tokens, and any digital representation of any other value as determined by VARA. **Virtual Tokens:** A digital representation of a set of rights that can be digitally offered and traded through a Virtual Asset Platform. **Fiat-Referenced Virtual Asset[32]:** means a type of Virtual Asset that purports to maintain a stable value in relation to the value of one or more fiat currencies, can be digitally traded and functions as— [a] a medium of exchange; [b] a unit of account; and/or6 [c] a store of value, but does not have legal tender status in any jurisdiction. A Fiat-Referenced Virtual Asset is neither issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the Fiat-Referenced Virtual Asset.

S.No	Jurisdiction & Regulatory Framework	Regulatory Framework	Definition
7	Hong Kong	Hong Kong Monetary Authority	**Crypto Assets[33]:** Also referred to by some market players or overseas jurisdictions as "crypto-currencies". Given that such assets are actually not currency per se, this paper uses the term "crypto-assets" unless the situation requires otherwise, e.g. the government of another jurisdiction uses the term "crypto-currency". **Stablecoins[34]:**  [35]Crypto assets whose values are linked or referenced to an underlying asset, e.g. securities or fiat currencies, are commonly referred to as stablecoins. According to the FSB and the BIS, stablecoins are defined as "a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets" and "cryptocurrencies with values tied to fiat currencies or other assets" respectively.

ANNEXURE 2: Categorization of VDA Service Providers Globally

S.No	Jurisdiction & Regulatory Framework	Definition of VDA Service Providers	Regulation
1	**European Union:** MiCA	**'crypto-asset service'** means any of the following services and activities relating to any crypto-asset: a. providing custody and administration of crypto-assets on behalf of clients; b. operation of a trading platform c. exchange of crypto-assets for funds; d. exchange of crypto-assets for other crypto-assets; e. execution of orders for crypto-assets on behalf of clients; f. placing of crypto-assets; g. reception and transmission of orders for crypto-assets on behalf of clients; h. providing advice on crypto-assets; i. providing portfolio management on crypto-assets; j. providing transfer services for crypto-assets on behalf of clients;	• MiCA requires CASPs to obtain authorization from their respective national competent authorities (NCAs). This applies to services such as custody, exchange, and trading of crypto-assets. • The regulation includes stringent consumer protection measures, including transparency obligations, requirements for whitepapers, and rules to prevent market abuse. • MiCA also addresses risks related to the use of stablecoins, introducing specific provisions for issuers of these assets.
2	**Canada:** CSA[36], CIRO, NI and Federal (Bank of Canada)[37] Canadian Securities Administrators (CSA), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	**Crypto Asset Trading Platforms (CTPs):** Platforms facilitating the buying, selling, and trading of crypto assets. CTPs are divided into two categories - CTP marketplace and CTP dealer platform A CTP is brought into the regulatory perimeter in Canada if it facilitates trading in crypto assets and there exists a contractual right to delayed delivery of a custodied cryptocurrency. A CTP could perform a marketplace function, or a broker/dealer function. • A **CTP marketplace** brings together the orders of multiple buyers/sellers of securities; and in some jurisdictions, parties to certain types of derivatives, using established, nondiscretionary methods through which buyers/sellers agree to the terms of a trade.	• **VASPs:** Must register as MSBs with FINTRAC and comply with AML/CTF regulations, conduct CDD, and report suspicious transactions. • **CTPs:** Regulated by provincial securities regulators; must comply with CSA guidance if crypto assets are considered securities. • **Custodians:** Must segregate client assets and meet operational standards; subject to AML/CTF regulations.

		→ CTP dealer platform trades security tokens or crypto contracts → Facilitates Primary Distribution (Listings) → Acts as a Counterparty to each trade → Acts as an Agent → On-boards clients → Offers custody of assets (directly/3rd party) **Custodians:** Entities that hold and manage crypto assets on behalf of clients. **Central Clearing Houses:** Entities that clear and settle trades, managing counterparty risk.	• **Central Clearing Houses:** Recognized or exempted by provincial regulators; must adhere to high standards for risk management and operational resilience. • The **CSA** provides guidance on when crypto-assets may qualify as securities, subjecting them to the relevant securities laws, including requirements for registration, disclosure, and investor protection. • Provincial regulators may impose additional requirements, with specific oversight over certain activities like ICOs or trading platforms. • Lending is not specifically allowed in 4/5 provinces in Canada until such time as entities are registered with the CSA and subject to terms and conditions on lending activities; the remaining provinces are silent.

S.No	Jurisdiction & Regulatory Framework	Definition of VDA Service Providers	Regulation
3	**USA**[38]: Financial Crimes Enforcement Network (FinCEN), Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC)	**Virtual Asset Service Providers (VASPs):** Not specifically defined in the US however, entities are regulated under different terms and frameworks.	• **FinCEN:** VASPs must register as Money Services Businesses (MSBs) and comply with the Bank Secrecy Act (BSA), including AML/CTF obligations. • **SEC:** Regulates crypto-assets that qualify as securities. • **CFTC:** Oversees crypto-assets considered commodities and regulates derivatives markets. • **State Regulations:** Some states have their own regulations and definitions for entities involved in digital assets. For example, New York has a BitLicense framework for businesses engaged in virtual currency activities.
4	**UK:** Financial Conduct Authority (FCA)	**crypto-assets:** Digital representations of value or contractual rights that can be stored and transferred electronically. **'Crypto asset businesses'** under FCA: Entities providing services related to crypto-assets, such as exchanges and custodian	• **Fifth Anti-Money Laundering Directive (5AMLD):** Under 5AMLD, which was transposed into UK law, businesses involved in crypto-asset activities, including exchanges and wallet providers, are required to register with the FCA. They must comply with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations. • VASPs must register with the FCA as 'crypto-asset businesses' and comply with AML/CTF requirements under the Money Laundering Regulations. The FCA also oversees consumer protection and market integrity measures.
5	Dubai, UAE Virtual Assets	**Virtual Assets (VAs):** Digital representations of value that can be digitally traded, transferred, or used as a means of exchange,	• VARA mandates that all VASPs in Dubai obtain a license and comply with

	Virtual Assets Regulatory Authority (VARA)	payment, or investment. **Virtual Asset Service Providers (VASPs):** VARA defines VASPs as entities that provide one or more of the following services related to crypto-assets: Exchange Services, Wallet Services, Issuance Services, Custody Services, Advisory Services and Brokerage Services.	strict Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations, aligning with global standards like FATF. • VARA requires VASPs to maintain high standards of security and operational practices to protect virtual assets and ensure the integrity of their services. • VARA imposes rules to protect consumers, ensuring transparency in operations and safeguarding client assets

S.No	Jurisdiction & Regulatory Framework	Definition of VDA Service Providers	Regulation
6	Singapore Monetary Authority of Singapore (MAS)	**Digital Payment Tokens (DPTs):** Any cryptographically secured digital representation of value that is used or intended to be used as a medium of exchange **"Digital payment token service"** means any of the following services: (a) any service of dealing in digital payment tokens (other than any such service that the Authority may prescribe) (b) any service of facilitating the exchange of digital payment tokens (other than any such service that the Authority may prescribe)	MAS has established a licensing framework under the Payment Services Act (PSA) to regulate VASPs • Regulated Activities include: • Performing Issuance activities (in Singapore) • Facilitating the exchange of digital payment tokens ("Payment activities") • Dealing in digital payment tokens • Match orders, central limit order book (market operator) • Route orders to liquidity providers and other trading venues (broker) • Be the counterparty to the trade (dealer) Regulation: • VASPs must be licensed under the Payment Services Act (PSA) and comply with AML/CTF requirements, including customer due diligence, transaction monitoring, and suspicious activity reporting. Prohibited activities include: • Lending arrangements with retail clients • Staking arrangements with retail clients

7	Japan Financial Services Agency (FSA)	**Crypto-assets:** Property value that can be electronically transferred and used as a means of payment or investment under Japan's Payment Services Act (PSA). **'Virtual Currency Exchange Service':** Fall under the Payment services Act and carry out the following activities: → Purchase and sale of a Virtual Currency or exchange with another Virtual Currency → Intermediary, brokerage or agency services for the act set forth in the preceding item → Management of users' money or Virtual Currency, carried out by persons in connection with their acts set forth in the preceding two items	• VASPs in Japan must register with the FSA and comply with the PSA and Financial Instruments and Exchange Act (FIEA). • Japan imposes strict AML/CTF regulations, including requirements for user identity verification, transaction monitoring, and reporting. • The FSA also mandates that VASPs segregate customer funds from their operational funds, implement robust security measures, and provide regular financial audits.
8	Indonesia Commodity Futures Trading Regulatory Agency (BAPPEBTI)	Crypto Asset Service Providers (CASPs): Not specifically defined.	• CASPs must register with BAPPEBTI, trade only approved assets and comply with strict AML/CTF regulations. Indonesia has issued various regulations and guidelines concerning digital assets, including requirements for registration, reporting, and compliance for businesses engaged in crypto-asset activities.

REFERENCES

1. Primus Partners Research
2. Arthur D Little: Web3 & Metaverse — The rise of the new Internet & the India opportunity
3. Skyquest report titled "Global Non-Fungible Tokens Market" (Apr 2023)
4. Kotaku article titled "$1.2 Billion Metaverse Company Boasts It Has A Whopping 8,000 Daily Users" (Oct 2022)
5. CoinTelegraph article titled "VC blockchain and crypto funding drops off in Q4 2022: Report (Feb 2023)
6. Electric Capital report titled "Developer Report 2023 Mid-Year Update" (Jul 2023)
7. The Web3 Landscape in India, Bharat Web3 Association
8. India's Web3 Landscape Report, Hashed Emergent 2023
9. Brazil central bank plans year-end proposal for crypto regulation, May 21, 2024, Reuters
10. NASSCOM, The India Web3 Startup Landscape
11. NASSCOM, The India Web3 Startup Landscape
12. India's Web3 Landscape Report, Hashed Emergent 2023
13. TDS on Virtual Digital Assets, 2024, NALSAR
14. The 2024 Global Adoption Index by Chainalysis
15. https://coingape.com/taiwan-forms-official-crypto-association-to-regulate-crypto-sector/
16. https://www.theblock.co/post/299888/taiwan-forms-crypto-industry-association-as-major-step-toward-self-regulation
17. https://www.chiphi.in/taiwan-launches-crypto-association-to-enhance-industry-self-regulation/
18. https://cointelegraph.com/news/taiwan-major-crypto-exchanges-form-association
19. https://www.marketswiki.com/wiki/Japan_Virtual_Currency_Exchange_Association_(JVCEA)
20. https://www.regulationasia.com/japan-allows-self-regulation-among-cryptocurrency-exchanges/
21. https://www.regulationasia.com/japan-fsa-dissatisfied-with-crypto-industry-self-regulation-report/
22. https://www.livemint.com/money/personal-finance/rbis-framework-for-sros-from-minimum-net-worth-to-mix-of-members-key-regulations-explained-nbfcs-11724150072162.html
23. https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=58123
24. https://openknowledge.worldbank.org/server/api/core/bitstreams/18b85478-630f-5f12-b5e3-a3d06acfdf51/content
25. https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/
26. https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20

27. PAYMENT STABLECOIN.—The term 'payment stablecoin'— "(A) means a digital asset— '(i) that is or is designed to be used as a means of payment or settlement; and "(ii) the issuer of which— "(I) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value; and "(II) represents will maintain or creates the reasonable expectation that it will maintain a stable value relative to the value of a fixed amount of monetary value; and "(B) that is not— "(i) a national currency; or "(ii) a security issued by an investment company registered under section
28. 26) DIGITAL ASSET.— 18 "(A) IN GENERAL.—The term 'digital 19 asset' means any fungible digital representation of value that can be exclusively possessed and transferred, person to person, without necessary reliance on an intermediary, and is recorded on a cryptographically secured public distributed ledger.
29. " DIGITAL COMMODITY.—The term 'digital commodity' has the meaning given that term under section 1a of the Commodity Exchange Act (7 18 U.S.C. 1a). "(52) DIGITAL COMMODITY.— 16 "(A) IN GENERAL.—The term 'digital commodity' means— "(i) a digital asset that was issued to any person, other than a digital asset issuer, a related person, or an affiliated person, through an end-user distribution; "(ii) a digital asset that is held by any person, other than a digital asset issuer, a
30. (The definition of a Digital Asset excludes non-fungible digital representation of value)
31. https://rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_338_VER1.pdf
32. https://rulebooks.vara.ae/rulebook/schedule-1-definitions-3
33. https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2022/20220112e3a1.pdf
34. https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2022/20220112e3a1.pdf
35. https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2022/20220112e3a1.pdf
36. "The joint guidance noted that the securities regulator would assert jurisdiction over the trading of cryptocurrencies that were securities (on their own), and would also assert regulatory jurisdiction over the trading of cryptocurrencies that were commodities (like Bitcoin), and not securities on their own, if the CTP took custody of the commodity cryptocurrency and then provided the user with a "contractual right" to the delayed, rather than immediate, delivery of the cryptocurrency. Cryptocurrency: Challenges to Conventional Governance of Financial Transactions (Dr. Ryan Clements) on Pg 15 Link Here
37. Payment and Clearing Settlement Act Link Here
38. The U.S. House Committee on Financial Services and House Committee on Agriculture have jointly prepared a Digital Asset Market Structure Discussion Draft that aims to provide a regulatory framework (June 2, 2023) for crypto assets Link Here It is proposed that crypto assets issuance i.e., a capital raise, would be deemed a "private offering of securities" and once they become decentralized (criteria to be determined) would be designated as commodities).

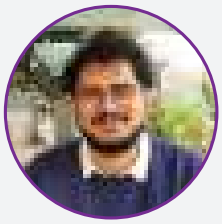
CONTRIBUTORS

Shravan Shetty
Managing Director

Shristi Singh
Vice President

Suman Kasana
Manager

Yash Saksena
Manager



Srinjit Venkatesh
Sr. Consultant

Parth Sabharwal
Consultant

DISCLAIMER

The report is prepared using information of a general nature and is not intended to address the circumstances of any particular individual or entity. The report has been prepared from various public sources and the information receives from these sources is believed to be reliable. The information available in the report is selective and subject to updation, revision and amendment. While the information provided herein is believed to be accurate and reliable, Primus Partners Private Limited does not make any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and data available in the public domain. While due care has been taken while preparing the report, Primus Partners Private Limited does not accept any liability whatsoever, for any direct of consequential loss arising from this document or its contents.

We do not claim ownership over the images used in this document.

PRIMUS

PASSION
for providing solutions to help clients achieve goals

RESPECT
for all and alternate viewpoints

INTEGRITY
of thoughts and actions

MASTERY
of our chosen subject to drive innovative and insightful solutions

US
representing the Primus collective, where each individual matters

STEWARDSHIP
for building a better tomorrow

SOLUTIONS FOR TOMORROW

PRIMUS PARTNERS

Primus Partners India
@partners_primus
www.primuspartners.in

BENGALURU
91 Springboard, Business Hub 175, 176 Bannerghatta Rd, Dollars Colony, Bengaluru - 560076

CHANDIGARH
2nd Floor, Netsmartz, Plot No. 10, Rajiv Gandhi Chandigarh Technology Park, Chandigarh - 160019

DELHI
15, Tolstoy Road, Atul Grove Rd, Janpath, Connaught Place, New Delhi - 110003

KOLKATA
4th Floor, Siddhartha Apartments,188/2, Block J, New Alipore, Kolkata 700053

MUMBAI
601, 6th Floor, Raheja Centre, Nariman Point, Mumbai 400021