ESYA centre

WHY INDIA NEEDS AN INTERMEDIARY LIABILITY FRAMEWORK FOR WEB3 AND WHAT IT SHOULD LOOK LIKE

AUGUST 2023 | ISSUE NO. 034

Why India Needs an Intermediary Liability Framework for Web3 and What it Should Look Like

Attribution: Meghna Bal and Mohit Chawdhry, *Why India Needs an Intermediary Liability Framework for Web3 and What it Should Look Like*, August 2023, Esya Cen 2023, Esya Centretre

Esya Centre
B-40 First Floor
Soami Nagar South,
New Delhi - 110017, India

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at www.esyacentre.org

About the Authors: Meghna Bal is Head of Research and Fellow at the Esya Centre, New Delhi. Mohit Chawdhry is a Fellow at the Esya Centre, New Delhi.

CONTENTS

I. INTRODUCTION

The intermediary liability provision or "safe harbour" is the cornerstone of Web2. Without these protections, which exempt online intermediaries from liab[1]ility for content generated by users, the largest platforms in the world would not exist. However, as online intermediaries have evolved, so have the harms associated with them. The size of many of these platfroms allows online malfeasance to be carried out at scale, raising socio-political and economic concerns. Consequently, nations are reworking their intermediary liability provisions to place additional responsibilities on these platforms, to protect consumers. Chief among them is European Union's Digital Service Act which requires online intermediaries to comply with stringent transparency reporting, know your business, and audit requirements. Notably, India has also widened the scope of intermediary liability by introducing delegated legislation for social media, e-commerce, and online gaming intermediaries.

The World Economic Forum defines Web3 as a growing segment of decentralised technologies that help "establish provenance, veracity, and value of data."[1] Web3 technologies, which include cryptography, distributed ledger systems, smart contracts and fungible and non-fungible digital assets, aim to redress the centralisation of data, with large Web2 internet companies, by returning ownership and control to users.[2] Interest in Web3 technologies has grown exponentially, as evidenced by the 20x increase in search queries on Google between April 2020 and April 2023.[3] The growing interest in and consumer exposure to Web3 has also increased greater regulatory scrutiny of underlying technologies, particularly digital assets.

However, decision-makers tend to be concerned about the financial aspects of Web3 regulation. For instance, the RBI's statements on Web3 have focused on financial stability. The Finance Minister too has requested the Financial Stability Board and the International Monetary Fund to develop principles for digital asset governance in the country.[4] These considerations are undoubtedly important. However, it is also necessary to regulate aspects of the exclusively digital component of Web3, which has implications for privacy, security, content moderation, and platform governance.

The scope of the recommendations in this paper is limited to centralised Web3 or Web2.5 businesses. These entities play an important role in bridging the gap between Web2 and Web3, and helping users access the latter. In addition, as centralised players, they are also integral to enforcement efforts pertaining to illegal and infringing content and the institution of accountability and governance in Web3.

In this context, this paper argues that the digital product aspect of Web3 should be regulated under a specialised intermediary liability framework targeting centralised Web3 or Web2.5 entities. Such a framework would ensure Web3 digital product risk redressal, while still enabling entrepreneurs to innovate. India has developed a practice of introducing intermediary liability frameworks targeting different digital sectors such as social media and online real money gaming. Thus, the paper contends that a Web3 intermediary liability framework is best implemented under the Information Technology Act, 2000 or the Digital India Act when it is enacted.

II. WHY SHOULD WEB3 BE REGULATED UNDER THE INTERMEDIARY LIABILITY FRAMEWORK?

II.a. Most Web3 Platforms Are Intermediaries

Although Web3 centres around decentralization, there is a centralization of key activities within the space due to its nascent and evolving nature. Some of the largest players in the ecosystem are traditional entities that offer their consumers Web3 experiences using Web2 elements (information management, payment systems etc.). Entities that bridge the divide between Web2 and Web3 constructs are often labelled "Web 2.5".[5] These entiries are necessary because they:

a) **Facilitate user onboarding –** Centralised entities lower entry barriers for users who don't possess the necessary technical know-how. For instance, centralised exchanges allow users to purchase, transfer, and store their digital assets without necessarily interacting with a Web3 wallet or managing their private keys.[6] An international survey of 32,000 users suggests that centralised entities, particularly exchanges, serve as key entry points to Web3 for first-time users.[7]

b) **Reduce transaction costs –** Web3 transactions conducted through blockchain systems can involve high transaction or "gas" fees. These levies are charged to remunerate validators who help secure the network. Centralised entities lower "gas" fees by using their own blockchain infrastructure for transactions and, hence, facilitate the democratisation of Web3 technology.[8]

c) **Create legal and safe ways to access Web3 technologies –** Web2.5 entities are set up as traditional corporations with identifiable management and shareholders. Resultantly, these entities can be subject to laws and regulations that ensure accountability, transparency, and consumer welfare. Users can interact with Web3 technologies safely, knowing that they will have legal recourse against potential violations of their privacy, security, and trust.

The centralisation afforded by large Web2 platforms is leveraged by intermediary liability frameworks to regulate the activity of their users. Conditions for content moderation, privacy, security, and trust and safety translate into community guidelines or terms of service on Web2 platforms. Users who violate these terms of service will either have their harmful or unlawful content taken down or profiles blocked, based on the severity of their violations. Such a model can be deployed for centralised Web2.5 intermediaries such as:

II.a.i Web3 Exchanges

Web3 exchanges are services where users can buy and sell digital assets. These exchanges allow Web3 businesses to offer their tokens for sale on the former's platforms, giving the latter access to a global pool of capital. At the same time, however, there are risks that emerge from such business models. For instance, exchanges may not thoroughly vet tokens sold via initial coin offerings before being listed on their platforms. This can lead to the sale of fraudulent or poorly designed coins ones. Exchange regulation can tackle some of these risks, such as blacklisting digital assets that give rise to security, economic, and user welfare risks. For instance, France and South Korea banned exchanges from offering privacy coins, such as Monero, which completely obfuscate the identity of parties to a transaction due to money laundering concerns.[9] However, due to the immediacy of risk, and the fact that any regulation for digital assets is not imminent, it may make sense to address such issues through an intermediary liability framework.

The current IT rules, both draft and proposed, may not be adequate to address the platform governance requirements for Web3 exchanges, particularly in the context of token vetting. It is advisable, then, to introduce a specialised due diligence framework for Web3 exchanges.

II.a.ii Web3 Gaming

Web3 gaming services leverage digital assets to offer rewards to players and allow them ownership over different aspects of a game. The open-source nature of Web3 gaming also gives players the freedom to modify games. There are already unicorns, companies valued at USD 1 billion or more, in the Web3 gaming sector. One example is Forte, a gaming infrastructure tool that enables gaming publishers to integrate Web3 technologies with their platforms.[10]

Players can also earn money for playing Web3 games. Illustratively, the game Axie Infinity requires them to contribute a certain amount up front to play, but are given an in-game token that is built on the Ethereum blockchain.[11] A majority of players hail from the Philippines, and several of them report that earnings from the game constitute their primary source of income.[12] Such a model presents a high degree of risk as well. To ensure a steady stream of income, players are dependent on more affluent gamers to continue making in-game purchases.[13] Moreover, the more ubiquitous a pay-to-play-to-earn model becomes, the greater the likelihood of more scammers setting up fronts of such games to siphon away funds from unsuspecting individuals.

Web3 games could technically be brought under the proposed online real money gaming rules which require their parent companies to carry out KYC for user account establishment, and setup a grievance redressal mechanism. Under the rules, self-regulatory bodies must be established to facilitate the governance of online gaming companies with a real money component.[14] Real money gaming companies must register with a recognised self-regulatory body (SRB) to qualify for the intermediary liability framework and adhere to its code of conduct. The framework is flexible enough to create an SRB for Web3 gaming with a unique code of conduct. However, there may be some shortfalls particularly in the context of gaming ventures run by decentralised autonomous organisations (DAOs). These are "*entities existing solely on computer code and within a given blockchain, having relatively autonomous and self-sufficient corporate governance mechanisms, and whose core members - the tokenholders - exercise a great degree of control.*" DAOs are not recognised legal persons in India and it is not known how liability will be imputed to platforms run by them. There are, however, ways around such legal ambiguity. For instance, liability can be imputed on the core administrators within the DAO by the SRB. Further, a condition may be introduced that DAOs can only be established if their underlying smart contracts can be modified or updated by the core administrators or through voting by members.[15] This is similar to a measure that has been introduced in Wyoming, which requires DAOs seeking legal registration to ensure that the underlying smart contracts can be modified or upgraded.[16] However, the Ministry of Corporate Affairs may have to introduce such a measure.

ii.a.iii Web3 Social Media Platforms

Web3 social media is not a widespread phenomenon but an emerging trend. Like their Web2 counterparts, Web3 social media platforms also qualify as intermediaries because they facilitate communications between different user groups. Abbing, Diehm and Warret 2023 present different decentralised architectures for social media that raise concerns about the enforcement of content moderation requirements. The issues their models raise provide insight on how Web3 social media platforms can be managed in the event of their popularity:[17]

a) **Federated**: Federated social media services such as Mastodon and PeerTube decentralise social media through hosting providers and rely on open web standards and open source systems. However, such platforms do rely on a centralised administrative structure for privacy and security – which proffers the prospect of enforcement despite a decentralised server structure. Illustratively, while Telegram hosts data across a distributed cloud network it can still take channels or groups down.[18]

b) **Peer to Peer:** P2P social media such as Secure Scuttlebutt enables users to host their own content. It uses elements of Web3, like cryptography to keep user content and identity secure. Encrypted content is hosted locally by users, signed by their public key, which can then be decrypted by a friend's key. In such systems, users have to take individual calls to block unpleasant or unlawful content. Bevensee (2020) notes that it is difficult to pinpoint the identity and quantum of users in P2P social media systems. In the past, radical elements have used Secure Scuttlebutt to coordinate and organise attacks on the public.[19]

c) **Blockchain-based or Web3**: Web3 social media projects like Minds and Steemit deploy virtual digital assets to enable micropayments for content creators and platform governance. Abbing, Diehm and Warret contend that content takedowns on Web3 social media may present enforcement challenges as the content is placed on a distributed and decentralised network structure.[20] Specifically, they suggest that the persistent and immutable nature of blockchains may mean it will be difficult to remove unlawful content.

II.b. Web3 May Offer Technological Advantages Over Web2 platforms such as Trust and Safety by Design

Web1, the first generation of the internet, was devised by Tim-Berners Lee. Its functionality was limited to enabling several users to read information generated by a few creators.[21]There was no capability for two-way interaction on this information, a hallmark of digital technologies today. It was inefficient and poorly designed.[22]

Web2 allowed users to both read and write information, enabling interaction and the creation of legitimate networks engaged in information exchange. However, it lacked the key elements of trust and accountability – users could upload false or malicious information and there were limited avenues for authentication or authorisation.[23] Thus, Web2 created a way to index and share data, without giving users any control or line of sight over what is being done with it.

According to Sheridan et. al, Web3 is a proposed new version of the internet, centred on "decentralisation, blockchain technology, and token-based" incentive systems.[24] Web3 could create an online environment where data is not only created and shared, but owned and monetised by the individuals that generate it.

Thus, Web3 presents some distinct advantages over Web2, such as:[25]

1 **Data Transparency and Ownership**: Where Web3 leverages blockchain technology, transactions are logged in an immutable ledger, enabling the understanding of where data is going and how it is being used. These transactions are marked by a unique identifier, typically known as a wallet address, that enables proof of ownership as well.

2 **Transactional Traceability and Accountability :** To access Web3 applications, users must sign in to wallet application such as Metamask. Each wallet has a unique address that can be tagged to the identity of a natural or legal person, making it possible to authenticate and trace online activity.

3 **Decentralisation of Innovation**: Web3 typifies open innovation. Permissionless blockchains lower barriers to entry in different digital markets because anyone can build applications on them. While Web3 technologies and applications are still prone to network effects, the open innovation ecosystem ensures that larger entities are forced to continuously innovate – otherwise newer ventures will unseat them. Illustratively, though the Bitcoin network was established well before Ethereum or other blockchain networks. However, due to technical shortcomings like slow transactions and limited functionality, networks like Ethereum are much larger hubs of Web3 activity. Ethereum has about a million transactions per day, whereas Bitcoin only has 258,413. In 2021, the total number of transactions on Ethereum surpassed those carried out on Bitcoin.[26]

4 **Token-based Trust:** Web3 relies on an incentive mechanism to verify transactions. For instance, nodes on the Bitcoin blockchain compete to verify blocks consisting of multiple transactions and are rewarded

with Bitcoin if they succeed. However, this token-based reward system can be leveraged to generate value for a wider set of stakeholders as well. Illustratively, Gitcoin is a Web3 version of Github where developers are paid to work on open-source software.

5 **Privacy-by-Design:** On Web3, identities are cryptographically secured**,** protecting user privacy from the start. These measures, however, do not preclude the identifiability of a user if KYC mandates are in place.

The technological advantages of Web3 can be used to enable better governance, making a strong case for the creation of an intermediary liability framework for such entities.

II.c. Risks Prevalent in Web3 Are Largely Well Known Creating Scope for Comprehensive Due Diligence Requirements

Web1, the first generation of the internet, was devised by Tim-Berners Lee. Its functionality was limited to enabling several users to read information generated by a few creators. There was no capability for two-way interaction on this information, a hallmark of digital technologies today. It was inefficient and poorly designed.

Web2 allowed users to both read and write information, enabling interaction and the creation of legitimate networks engaged in information exchange. However, it lacked the key elements of trust and accountability – users could upload false or malicious information and there were limited avenues for authentication or authorisation. Thus, Web2 created a way to index and share data, without giving users any control or line of sight over what is being done with it.

According to Sheridan et. al, Web3 is a proposed new version of the internet, centred on “decentralisation, blockchain technology, and token-based” incentive systems. Web3 could create an online environment where data is not only created and shared, but owned and monetised by the individuals that generate it.

Thus, Web3 presents some distinct advantages over Web2, such as:

II.c.i Trust

Trust-based risks are those that erode consumer confidence. In Web3, these can be financial or technological. Cong et. al (2023) have prepared a taxonomy of financial risks emanating from Web3:[27]

1 **Investment Scams**: Users are typically told about an investment opportunity with very high returns, which they can avail off by sending digital assets from their wallets. They may receive updates about their investments but are usually unable to “cash-out”. Cong et. al (2023) note that many “cloud mining companies” which offer investment opportunities in mining activities, are investment scams.

2 **Ponzi Scheme:** These dole out fake dividends to investors by siphoning money from other their deposits. The facade of returns on investment prompts customers to put more money in and recruit others.

3 **ICO Scams**: These have been discussed above. Typically, an entity creates and lists a sham token and seeks public investments. Once investments have been made, the entity disappears, taking with all the profits from the ICO.

4 **Rug Pulls**: Similar to ICOs, rug pulls involve developers setting up Web3 projects backed by tokens. Once the project has attracted a certain level of investment, the developers abdandaon the project and withdraw user funds.

5 **Phishing**: Scammers impersonate digital assets exchanges or other platforms in order to get sensitive information related to their wallets to access it and steal funds.

6 **Giveaway Scam**: These are also known as trust trading scams in which the scammer pretends to giveaway digital assets to users in exchange for some digital assets. The scammer tells the users that he will send back double the amount of digital assets sent by the user – but this never happens.

Importantly, these risks are not unique to Web3. Many of these practices have arisen in traditional financial markets.

Trust also encompasses several technology-based risks. These include systemic security vulnerabilities in smart contracts which permit devious elements to siphon away user funds.[28] However, it is important to note that analysis tools, testing, security audits and bounty programs can resolve and mitigate most of these deficiencies.[29]

II.c.ii Safety

Safety-based risks are those that may cause physical or mental harm to consumers. Trust-based and safety-based risks are not mutually exclusive because they both have similar concerns and concepts. Web3 will present many of the same issues as Web2 such as online harassment, violence against women and children, hate speech and other illegal activities. However, there may be differences in the way harm is perpetuated. These differences stem from the increased privacy and anonymity that Web3 provides, which lends an additional layer of protection to dubious online elements.

1 **Illegal Content:** Social media platforms, which use different elements and technical concepts from Web3, can present takedown challenges due to federated governance structures where a community of individuals takes decisions to make changes, rather than a centralised entity. Some platforms such as Minds are also taking steps to form their own content moderation policies, possibly as a pushback against de-platformisation on major social media platforms.[30] Illustratively, Minds indicates that it allows extreme content to “de-radicalise” users, and has been promoted by both Al Qaeda and ISIS.

The encryption and decentralisation that Web3 offers also plays a part in concealing illegal content while still making it available to those who seek it out. Encrypted chat platforms proffer similar “safe havens” for such actors (Rogers 2020).[31] These applications “reconcile dual desires of protection and publicity by offering private messaging and broadcasting”.

However, Rogers also notes that the more “public-facing” personalities are, the more they are easily discoverable.[32] Indeed, distributed, decentralised, and encrypted social media networks may not be as efficient at creating vast networks as their open Web2 counterparts. Web3 has technical limitations that make it less attractive for the distribution of multimedia user-generated content. According to Bodo and Trauthig, the increased privacy and security comes at the cost of “usability and discoverability”.[33] Indeed, the current Web2 ecosystem “has clear advantages [over Web3] when it comes to usability, convenience, and speed”.[34]Thus, the protection afforded by privacy and security on these platforms necessarily reduces the possibility for publicity – something radical elements desire to propagate their views.

Further, in a balkanised information delivery system, bad actors would be confined to sharing information within limited networks. The extent of discoverability in such channels, however, would be limited.

It is also likely that the analytics and forensics of such systems will improve over time, particularly if there is a legal exigency. As such, bad actors will have to gauge the extent to which are they willing to compromise privacy and protection to broadcast their content.

2 **Buyer Beware:** A common problem with Web3 marketplaces is that consumers are responsible for verifying the legitimacy of a digital product. Illustratively, buyers on most NFT marketplaces must assess whether the seller is dubious or not, or whether the NFT infringes the right of an IP owner. These are hard things to discern, particularly when consumers are dealing with digital products.

In the past, marketplaces such as OpenSea have attempted to introduce measures to enhance consumer protection. One example was an approval process for seller onboarding, but OpenSea rolled back the requirements after it experienced a sharp increase in trading activity.[35] In such contexts, there is a necessity for government intervention to nudge platforms to act more responsibly.

3 **IP and Counterfeiting:** Web3 raises numerous IP concerns. NFT markets are riddled with IP theft. Illustratively, OpenSea, a prominent NFT marketplace, once admitted that 80 percent of its NFTs were "plagiarized works, fake collections, and spam".[36]

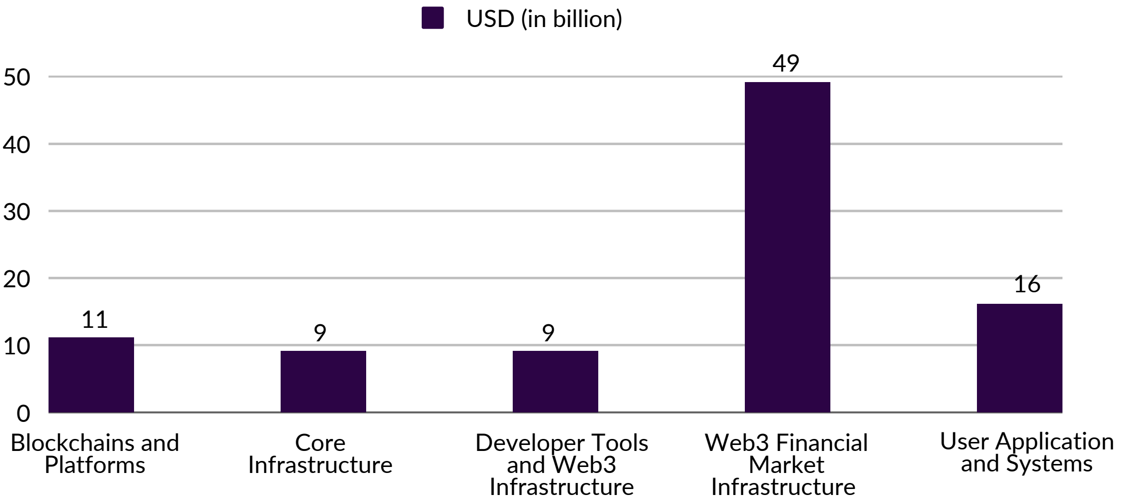
The issues related to IP, illegal content, and consumer risk exist in Web2 too. However, the absence of regulation heightens the prevalence of these risks in Web3. Illustratively, OpenSea had introduced verification programs but was forced to roll them back because of user-pressure.[37] A clear cut regulatory requirement could mitigate against such actions.

II.d An intermediary liability framework will help realise Web3's economic potential

India's deep talent pool and growing domestic market position it well to emerge as a leading nation for Web3 development. A NASSCOM survey estimates that there are currently more than 450 Indian Web3 start-ups which employ more than 75,000 developers.[38]Another 25,000 jobs are expected to be added by 2025.[39]

Indians' Web3 start-ups have also pulled in more than $1.2 billion in funding over the last two years, highlighting the role they can play in attracting capital flows.[40] Web3 technologies are expected to contribute $1.1 billion to the Indian economy by 2032.[41]

Establishing an intermediary liability framework for centralised Web3 companies is a crucial step in realising the sector's economic potential. Investment trends suggest that centralised entities, such as exchanges, custodians, and user applications, attract the maximum capital within the Web3 ecosystem.[42]



Source- Crunchbase; The Block, Bain Crypto Database

An intermediary liability framework will clarify the obligations that Web3 companies are subject to and provide the certainty required to encourage investment in the sector.

A 2023 report found that 80 percent of Indian Web3 start-ups deem the absence of regulatory clarity as a key impediment in operating in the Indian market.[43] Therefore, the introduction of an intermediary liability framework will also help stymie the tide of Indian talent opting for more Web3-friendly jurisdictions, such as Dubai and Singapore.[44] Illustratively, close to 60 percent of Indian Web3 start-ups are registered outside the country even though their employees are based in India.[45]

III. WHAT ARE THE PRINCIPLES AND MECHANICS OF AN INTERMEDIARY LIABILITY FRAMEWORK FOR WEB3

Intermediary guidelines for Web3 under the IT Act would require a form of specialized due diligence, beyond what is provided for Web2 intermediaries. Such compliance for Web3 must reflect a principles-based approach that accommodates the technology's rapid development. It will foster certainty without hampering innovation in the ecosystem.[46] The following section identifies principles that should underpin such a framework, based on reports and recommendations on Web3 and digital asset regulation by international organisations.[47]

1 **Technology Neutrality** – Technological neutrality forms the basis of the IT Act, which aims to accommodate the rapid pace of innovation by refraining from recognising only certain technological constructs. Illustratively, the IT Act was amended in 2008 to accommodate all forms of electronic signatures, rather than just digital signatures.[48] Any framework that addresses Web3 should imbibe the principle of technological neutrality as it is a nascent and fast-moving space.

2 **Risk-based Application** – The intermediary liability framework should be tailored to address different degrees of risk within the Web3 ecosystem and not adopt blanket provisions for all stakeholders.

3 **Cooperation and Coordination** – The cross-cutting nature of Web3 requires collaboration between the public and private sectors, and civil society to ensure effective regulation and oversight. Therefore, the due diligence framework should encourage the participation of industry and academia, especially in standard setting.

4 **Agility** – The framework should adopt agile construct to allow for responsive and iterative regulation of Web3 technologies.

III.a. Specialised Due Diligence

The following section provides a blueprint for a specialised Web3 due diligence framework based on the identified principles. It was created with centralised Web3 entities, or Web2.5 companies, in mind. As mentioned previously, these entities have identifiable centralized elements that can be held accountable under the proposed framework. Moreover, most users interact with Web3 technologies through them. Therefore, bringing these centralised intermediaries under the ambit of the framework will be a significant step in safeguarding consumer welfare in Web3.

This is not to suggest that entities based on P2P or decentralised models should be left unregulated. Indeed, they also have elements of centralization that can be subject to regulation. However, identifying and enforcing obligations against them is not a straightforward process. Moreover, ascertaining the jurisdiction and laws applicable to Web3 entities is also complex. While some international best practices are emerging, it may be prudent for Indian policymakers to wait and watch before creating a regulatory framework for decentralised entities. In the interim, the Government should commission technical reports on the operation of decentralised Web3 entities and identify how they may be regulated in future.

III.a.i. Blueprint for Specialized Due Diligence

Before issuing an IL framework for centralised Web3 companies, the Ministry of Electronics and Information Technology must issue a clarification indicating that the term intermediary includes centralised Web3 companies within its scope. Broadly, an IL framework for centralised Web3 companies should encompass the following:

1 **Prior Authorisation and Self-Regulatory Bodies**: the Draft Online Gaming Rules under the IT Act require for the creation of self-regulatory bodies that online real money gaming companies must register with. These SRBs are expected to establish codes of conducts for their members that address financial fraud, and other user harms related to gambling addiction. The Ministry can adopt a similar framework under the IT Act for Web3 companies, albeit with the following modifications:

   a **Recognition of Expert Groups and Standard Setting Organisations**: Article 44 of the EU Digital Service Act states that the European Commission shall support and promote the development of voluntary standards in key areas related to online trust and safety on Web2 platforms.[49] These include standards for the targeted protection of minors and other areas surround consumer trust and safety. Voluntary standard setting is becoming an increasingly popular trend, particularly in the context of emerging technologies. European and international standardisation bodies are tasked with developing such standards. Typically these bodies comprise of range of stakeholders that are experts in areas of policy, as well as relevant thematic sectors such as technology, psychology etc. A specialised due diligence framework for Web3 may recognise the work being done by standard setting bodies in this area, both in India and abroad. The framework should also prescribe the adoption of such standards by industry as a pre-condition to authorisation to operate. Such standard setting bodies could ensure that Web3 intermediaries verify the technical legitimacy of digital products being made available through their platforms. This could include a whitepaper and audit requirement before a product is listed for sale on the platform, which could help mitigate the scams highlighted in this paper and counter technical vulnerabilities that dubious elements can exploit.

   b **Voluntary Codes of Conduct**: Rule 5 of the Consumer Protection (E-Commerce) Rules, 2020, requires e-commerce marketplaces to take undertakings from sellers about the veracity of claims regarding the goods they are selling. They must also display seller details such as customer care number, geographic address etc. Web3 e-commerce intermediaries should be required to verify sellers making products available on their platforms. However, since this can place constraints on marketplaces, such verification requirements can be made mandatory to refrain from burdening start-ups with compliance costs. A voluntary code of conduct also gives companies a a way to compete on consumer trust by signaling a commitment to greater transparency on their platforms. Certain global Web3 intermediaries are already doing so. NFT marketplaces such as Nifty and SuperRare require verification of both assets being sold as well as sellers.[50]

2 **Content Moderation**: Article 19(2) of the Indian Constitution frames the permissible grounds for restricting speech. Content moderation is a requirement for Web2 intermediaries. However, the same exercise for Web3 may require some modification of policies meant for Web2. Higher levels of encryption and anonymity featured by Web3 platforms lead to their growing utilisation by radical elements. Another concern is that many social media platforms which utilise elements of Web3 have their own content moderation policies and permit the publication of extreme content.

   Dealing with these challenges requires a combination of content takedowns and community-based moderation that is better suited to the federated nature of Web3 social media platforms. Centralised Web3 platforms can be mandated to block accounts of individuals and organisations present on sanctions lists created by the Union and State Governments. Web2.5 platforms such as OpenSea and Metamask, have previously banned accounts based in sanctioned countries, like Russia and Venezuela, demonstrating their ability to comply with blocking and takedown orders. Additionally, file transfer size limitations and a reliance on hashing techniques to detect illegal content are other solutions that could prove to be useful for content moderation on web3 platforms.

   Platform level-interventions, such as prescribing codes of conduct that regulate user behaviour, have worked well for decentralised platforms. Illustratively, Mastodon does not list servers that are not "committed to active moderation against racism, sexism and transphobia". The self-regulatory bodies mentioned above can create codes of conduct which govern how Web3 platforms will deal with issues of content moderation.

The experience of platforms like Secure Scuttlebutt reveal that the introduction of abuse audits may also help mitigate some of these problems. Additionally, while members have to take a call to block an abusive actor individually, the bans constitute a form of signalling, causing other users to block them as well.[51]

3 **Consumer Protection**: Web3 e-commerce platforms include high risks of fraudulent transactions and counterfeiting. Transparency and disclosure requirements for digital products under IT law restrict themselves to the terms of service and privacy policies of the platform. The problem with such mechanisms is that they are unfriendly to users. According to one study, it would take a user 200 hours to read the privacy policies of each website he or she uses. Moreover, another report found that users needed a college degree to make sense of privacy policies and terms of service. More importantly, Indians may be more vulnerable to the risks presented by online commerce, particularly on Web3. The 2023 Multiple Indicator Survey of the National Sample Survey Office found that a majority of respondents lacked the ability to do basic computer tasks.[52] Only 26.7 percent of the 11 lakh respondents surveyed knew how to send emails with attached files.

However, given the financial risk presented by Web3 it is necessary that platforms are subject to requirements pertaining to:

a **Transparency and Disclosure**: Platforms may be encouraged to rely on labelling programs that use icons and images along with minimal and relevant explanatory text that gives consumers information up front about transactional risks and uncertainties. The introduction of such measures ensures that disclaimers are understandable to a wide range of audiences and prevents consumers from being inconvenienced by having to read through reams of legal text that is difficult to comprehend. Labels can be introduced on Web3 platforms, especially NFT marketplaces, to indicate whether a seller or a digital asset is verified, whether the IP claim it is making (if any) is valid etc.

b **Consumer Grievance Redressal**: A prevalent problem on Web3 platforms is the absence of adequate consumer grievance redressal mechanisms. Just like their Web2 counterparts, Web3 platforms should be required to provide contact information and put in place SOPs for grievance redressal. An important consideration is a situation where an approved seller acts in bad faith and defrauds a consumer. In such cases, the platform should first investigate the incident, verify its genuineness and, if a fraud is committed, it should, notify the appropriate authorities in a timely manner and cooperate with them.

4 **Supervisory and Regulatory Technologies:**[52] Several technologies can enhance regulatory supervision, as per a paper by the Bank of International Settlements . These technologies, known as supervisory tech, or suptech, already exist in the fields of data collection and analytics. For collection, emerging applications of suptech include reporting, data management, and virtual assistance. In the area of analytics, they are "market surveillance, misconduct analysis, microprudential supervision and macroprudential supervision". The paper notes that these forms of suptech can help unearth wrongdoing such as suspicious trading, market manipulation, AML/CFT infringements etc. Supervisory tech can leverage the different elements of Web3 technologies such as privacy, safety, and transparency by design to enhance the capabilities of authorities overseeing the sector.

5. **Harmonisation with other delegated legislation to avoid duplication**: Several business models on Web3 will be similar to Web2. The way to harmonise frameworks is to ensure that the Web3 safe harbour rules are restricted to tackling Web3-specific product concerns.

IV. CONCLUSION

Platform governance enables the regulation of highly decentralised spaces by focussing on centralised sources of activity. On Web3, there are several types of intermediaries which play such a role. A number of policy challenges that pertain to technical aspects of products and business models are presented by Web3 and must be addressed by information technology law.. As such, it is recommended that a comprehensive due diligence framework under the intermediary liability provision of the IT Act, 2000, and further on, the Digital India Act, when enacted, should govern such businesses. Such a model of governance will enable the development of emerging technology in Web3 while accounting for the risks it presents. To be clear, such a framework should operate in addition to and conjunction with others to govern the working for Web3 technologies in the country.

ENDNOTES

1 World Economic Forum, *Interoperability in the Metaverse*, Briefing Paper- World Economic Forum, January 2023, https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf.

2 Gaurish Korpal & Drew Scott, *Decentralisation and Web3 technologies*, University of Arizona, https://attachment.victorlampcdn.com/article/content/20220824/drewscott_gkorpal_web3.pdf.

3 *Google search volumes for the term "web3"*, Google Trends, July 21, 2023, https://www.theblock.co/data/alternative-crypto-metrics/web-traffic/google-search-volume-web3.

4 *G20 meet: India proposes joint technical paper by IMF, FSB on crypto assets*, The Indian Express, February 26, 2023, https://indianexpress.com/article/cities/bangalore/g20-meet-india-proposes-joint-technical-paper-by-imf-fsb-on-crypto-assets-8466467/.

5 Hanna Gawel, *Web 2.5 as a safe shift from Web 2.0 to Web 3.0: A definition of Web 2.5 in informatological approach*, 2022, https://www.cambridge.org/engage/api-gateway/coe/assets/orp/resource/item/638df3bd14d92d5c41a1b27d/original/web-2-5-as-a-safe-shift-from-web-2-0-to-web-3-0-a-definition-of-web-2-5-in-informatological-approach.pdf.

6 *International Survey of Web3 Adoption*, Coinbase Institute, 2022, https://downloads.ctfassets.net/c5bd0wqjc7v0/1ltW7EcyoCKpliiD1Slb23/a23a7657b9700fa06ac47a4fe04d48e0/Coinbase_IntlSurvey-Web3Adoption.pdf.

7 *Ibid*

8 Zhixuan Zhou & Bohui Shen, *Toward Understanding the Use of Centralized Exchanges for Decentralized Cryptocurrency*, https://arxiv.org/pdf/2204.08664.pdf.

9 Josh Adams & Ryan James, *Privacy Coins Take Another Beating, It Won't Be the Last Time*, February 09, 2023, https://beincrypto.com/privacy-coins-take-another-beating/.

10 Sam Gilbert, *Crypto, web3 and the Metaverse*, Bennett Institute for Public Policy Cambridge, March 2022, https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/03/Policy-brief-Crypto-web3-and-the-metaverse.pdf.

11 *Ibid*

12 *Ibid*

13 *Ibid*

14 online real money game' means an online game where a user makes a deposit in cash or kind with the expectation of earning winnings on that deposit

15 Wyoming Decentralized Autonomous Organization Supplement. ¶ 17-31-115. (66th Leg.) Gen. Sess. (2021)

16 Wyoming Decentralized Autonomous Organization Supplement. ¶ 17-31-115. (66th Leg.) Gen. Sess. (2021)

17 Roel Roscam Abbing, Cade Diehm & Shahed Warreth, *Decentralised social media*, Internet Policy Review, February 20, 2023, https://policyreview.info/glossary/decentralised-social-media.

18 *Introducing Telegram Passport*, Telegram, https://telegram.org/blog/passport?setln=de ; Ezra Cheung, *Telegram shuts down 2 channels created under same name as account blocked for alleged doxxing after Hong Kong privacy watchdog report*, myNEWS, June 03, 2022, https://www.scmp.com/news/hong-kong/law-and-crime/article/3180366/telegram-shuts-down-2-channels-created-under-same-name.

19 Emmi Bevensee & Rebellious Data LLC, *The Decentralised Web of Hate: White Supremacists are starting to use peer-to-peer technology. Are we prepared?*, Rebellious Data, September 2020, https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf.

20 Roel Roscam Abbing, Cade Diehm and Shahed Warreth, *Decentralised social media*, Internet Policy Review, February 20, 2023, https://policyreview.info/glossary/decentralised-social-media.

21 Keshab Nath, Sourish Dhar & Subhash Basishtha, *Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges*, *Conference Paper: 2014 International Conference on Optimization, Reliabilty, and Information Technology (ICROIT)*, February 2014, https://attachment.victorlampcdn.com/article/content/20220809/WEB_1.0-3.0.pdf.

[22] *Ibid*

[23] *Ibid*

[24] Dan Sherridan, James Harris, Et al., *Web3 Challenges and Opportunities for the Market*, September 06, 2022 https://arxiv.org/pdf/2209.02446.pdf.

[25] Adapted from Forrest Bai, *How the privacy and data storage features of Web3 can empower society*, VentureBeat, June 05, 2022, https://venturebeat.com/datadecisionmakers/how-the-privacy-and-data-storage-features-of-web3-can-empower-societies/.

[26] *10 most popular blockchain networks*, Kriptomat, https://kriptomat.io/blockchain/most-popular-blockchain-networks/

[27] Summarised from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4358572

[28] Sandeep Joshi et. al., *Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract*, IEEE Access, 2022, https://ieeexplore.ieee.org/abstract/document/9667515

[29] Daniel Perez & Benjamin Livshits, *Smart Contract Vulnerabilities: Does Anyone Care?*, May 17, 2019, https://allquantor.at/blockchainbib/pdf/perez2019smart.pdf.

[30] Roel Roscam Abbing, Cade Diehm and Shahed Warreth, *Decentralised social media*, Internet Policy Review, February 20, 2023, https://policyreview.info/glossary/decentralised-social-media.

[31] Rogers R, *Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media*, European Journal of Communication, 2020, https://journals.sagepub.com/doi/10.1177/0267323120922066

[32] *Ibid*

[33] Lorand Bodo and Kristina Tauthig, *Emergent Technologies and Extremists: The DWeb as a New Internet Reality?*, Global Network on Extremism and Technology, 2022, https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf

[34] *Ibid*

[35] Justin Scheck, *OpenSea's NFT Free-for-All*, The Wall Street Journal, February 12, 2022, https://www.wsj.com/articles/openseas-nft-free-for-all-11644642042.

[36] Kristen E. Busch, *Non-Fungible Tokens (NFTs), Congressional Research Service Report*, July 20, 2022, https://crsreports.congress.gov/product/pdf/R/R47189.

[37] *Ibid*

[38] Sohini Mitter, *11% of world's crypto, Web3 talent is in India: NASSCOM*, Business Today, October 20, 2022, https://www.businesstoday.in/crypto/story/11-of-the-worlds-crypto-and-web3-talent-is-in-india-nasscom-350353-2022-10-20.

[39] Sumit Gupta, *India's $5-trillion-GDP dream has an untapped potential in Web3*, The Economic Times, Dec 30, 2022, https://economictimes.indiatimes.com/markets/cryptocurrency/indias-5-trillion-gdp-dream-has-an-untapped-potential-in-web3/articleshow/96628677.cms.

[40] Naandika Tripathi, *India can lead the Web3 revolution, but lack of regulations can be a business-killer*, Forbes India, May 18, 2023, https://www.forbesindia.com/article/take-one-big-story-of-the-day/india-can-lead-the-web3-revolution-but-lack-of-regulations-can-be-a-businesskiller/84997/1#:~:text=There%20are%20over%20450%20Web3,founded%20between%202021%20and%202022.

[41] *Indian Web3 industry growing at 57% CAGR, to reach $1.1 bn by 2032: Report*, Business Standard, March 14, 2023, https://www.business-standard.com/article/technology/indian-web3-industry-growing-at-57-cagr-to-reach-1-1-bn-by-2032-report-123031400748_1.html.

[42] Thomas Olsen, Et al., *Web3 Remains Highly Relevant for Private Equity*, Bain & Company, Feb 27, 2023, https://www.bain.com/insights/web3-remains-highly-relevant-global-private-equity-report-2023/#:~:text=Bain%20%26%20Company's%20web3%20and%20digital,over%20the%20past%20three%20years.

[43] Naandika Tripathi, *India can lead the Web3 revolution, but lack of regulations can be a business-killer*, Forbes India, May 18, 2023, https://www.forbesindia.com/article/take-one-big-story-of-the-day/india-can-lead-the-web3-revolution-but-lack-of-regulations-can-be-a-businesskiller/84997/1#:~:text=There%20are%20over%20450%20Web3,founded%20between%202021%20and%202022.

44 Sanghamitra Kar, *The new brain drain: Indian Web3 startups flock to Dubai amid regulatory uncertainty, stiff taxes*, Moneycontrol, April 19, 2022, https://www.moneycontrol.com/news/business/cryptocurrency/the-new-brain-drain-indian-web3-startups-flock-to-dubai-amid-regulatory-uncertainty-stiff-taxes-8378361.html.

45 *ibid.*

46 World Economic Forum, *Pathways to the Regulation of Crypto- Assets: A Global Approach*, White Paper, World Economic Forum, May 2023, https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf.

47 The following reports were relied on for these principles:
IMF Executive Board Discusses Elements of Effective Policies for Crypto Assets, Press Release No. 23/51, International Monetary Fund, Feb 23, 2023, https://www.imf.org/en/News/Articles/2023/02/23/pr2351-imf-executive-board-discusses-elements-of-effective-policies-for-crypto-assets.
Parma Bains, *Et al.*, *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets*, Fintech Notes, International Monetary Fund, Sept 26, 2022, https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715.
The Financial Stability Risks of Decentralised Finance, Financial Stability Board, Feb 16, 2023, https://www.fsb.org/wp-content/uploads/P160223.pdf.
Policy Recommendations for Crypto and Digital Asset Markets, Consultation Report, The Board Of The International Organization Of Securities Commissions, May 2023, https://www.iosco.org/library/pubdocs/pdf/ioscopd734.pdf.

48 The Information Technology (Amendment) Act, 2008, Act No.10 of 2009, Acts of Parliament, Feb 5, 2009 (India), https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=.

49 REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), October 27, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

50 Emmi Bevensee & Rebellious Data LLC, *The Decentralised Web of Hate: White Supremacists are starting to use peer-to-peer technology. Are we prepared?*, Rebellious Data, September 2020, https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf.

51 *Multiple Indicator Survey in India*, Ministry of Statistics & Programme Implementation, National Sample Survey Office (Government of India), March 2023, https://mospi.gov.in/sites/default/files/publication_reports/MultipleIndicatorSurveyinIndiaf_0.pdf.

52 Summarized from Dirk Broeders & Jermy Prenio, Innovative technology in financial supervision (suptech) – the experience of early users, Financial Stability Institute, Bank for International Settlements, July 2018, https://www.bis.org/fsi/publ/insights9.pdf.

ESYA centre

www.esyacentre.org