NATIONAL LAW SCHOOL
OF INDIA UNIVERSITY

BENGALURU

धर्मो रक्षति रक्षितः

WEB3: A TECH AND POLICY BRIEF FOR INDIA

CON-TENTS

1. INTRODUCTION 4

2. CORE CONCEPTS 6
A. WEB3 6
B. WHAT DOES WEB3 HAVE TO DO WITH BLOCKCHAIN? 8
BLOCKCHAIN DEFINED 8
SMART CONTRACTS 9
C. WEB3 EXAMPLES 10
CRYPTOCURRENCY 10
NATIVE COINS AND TOKENS 11
NON-FUNGIBLE TOKENS 12
THE METAVERSE 13
DAPPS 14
DAOS 15
DEFI 15
SELF-SOVEREIGN IDENTITY 16

3. KEY POLICY QUESTIONS 17
A. DIGITAL OWNERSHIP AND INTELLECTUAL PROPERTY LAWS 18
B. COMMUNITY GOVERNANCE 19
C. PRIVACY AND DATA PROTECTION 19
D. CONSUMER PROTECTION 20
E. FINANCIAL FLOWS AND TAXATION 20
F. ONLINE GAMING 23

INTRO-DUCTION

During the second week of November 2022, many tech enthusiasts found themselves bewildered at the rapidly unfolding events surrounding cryptocurrency exchange FTX and its now infamous founder, Sam Bankman-Fried. There are multiple reports of poor oversight of the company, improper usage of customer funds for a sister trading firm, ill-advised investments and exploitation of regulatory gaps. Whatever the effect of this public collapse of a leading player on the crypto industry might be, it has definitely captured the attention of the world and turned the spotlight towards the wider ambit of Web3. FTX declared bankruptcy on November 11, leaving many of its investors devasted over the possible evaporation of their funds. Hence, this episode certainly shatters the idea that the developments in the Web3 operate in a separate technological plane and do not affect regular consumers and the 'real' economy. This downfall emphasises the need to understand Web3 technologies and the implications of the changes ushered in by their arrival.

Although the set of technologies together known as Web3 has seen a lot of attention in media and policy making circles in the last few years, the terms used and approaches adopted have varied widely. India has been characterised as the third largest market for Web3 in the world with over 450 Web3 related start-ups; regulatory activity has also been high, with the Reserve Bank of India making progress on launching the Centralised Digital Bank Currency (CBDC) and the Finance Bill, 2022 proposing a tax on the transfer of Virtual Digital Assets (VDAs), that include the growing Non-Fungible Tokens (NFTs), crypto-assets and other digital assets.

DISCUSSIONS ON LAW AND POLICY IN THIS SPACE HAVE BEEN BROADLY USHERED TOGETHER UNDER THE UMBRELLA SCOPE OF TECH WITHOUT ACKNOWLEDGING THE NUANCE AND DIFFERENCES THAT THE UNDERLYING TECHNOLOGIES THAT TOGETHER FORM THE WEB3.

Discussions on law and policy in this space have been broadly ushered together under the umbrella scope of tech without acknowledging the nuance and differences of the underlying technologies that together form the Web3. This primer is an attempt to connect technology and policy developments in the Web3 space for India. It, first, gives a brief overview of Web3 and its components. Then, it looks at defining some key examples of technologies in the paradigm. Finally, we will look at some of the key policy questions facing Indian regulators with respect to Web3.

CORE CONCEPTS

A. Web3

Web3 is a set of emerging technologies comprising blockchain, cryptographic protocols, digital assets, decentralised finance, NFTs, etc. The term is also used in the sense of a new Internet era – following on from Web2 which was characterised by centralised platforms and proprietary protocols, leading to so-called 'walled gardens'. The umbrella term is best understood as a reference to new paradigms in the online world, that transitions from one set of core technologies to another gradually.

THE KEY PRINCIPLE THAT WEB3 IS BUILT UPON IS DECENTRALISATION, BEST UNDERSTOOD AS ANY ACT OR PROCESS OF MOVING CONTROL FROM ONE SINGLE PLACE TO SEVERAL SMALL ONES.

The key principle that Web3 is built upon is decentralisation, best understood as any act or process of moving control from one single place to several small ones. In the context of the online world, it could mean many things. It could mean distributing the power of centralised platforms (like Amazon and Facebook) to smaller platforms. It could also mean moving from storing our data in a single place to storing data across several smaller spaces. It also could mean enabling user-to-user transactions without the aid of central institutions like banks.

Web3 ushers in an era of decentralisation in many ways. It introduces underlying mechanisms that encourage user-to-user interactions, user control over their data and content monetisation, and restructuring the relationship between buyers and sellers.

A SECOND KEY PRINCIPLE THAT IS OFTEN DISCUSSED IN CONNECTION WITH WEB3 IS THE NATURE OF OWNERSHIP.

A second key principle that is often discussed in connection with Web3 is the nature of ownership. With Web3, ownership of assets, ownership of one's own data, and ownership and responsibility in organisations have the potential to majorly shift towards empowering users. However, as with any emerging technology, it is easy to lose ourselves in the utopian prospects they pose. The hype surrounding the nature of ownership in Web3 could be pre-emptive. But observing the differences from its predecessor - Web2, there are many indicators that ownership within Web3 is very different and can decentralise concentrated structures of hierarchy like banks and corporations.

How is this operationalised? The primary driver for innovation in Web2 was the ability to persist data and solve the problem of statelessness. Web2 introduced mechanisms to store, analyse and interpret users' data through cookies, local Storage objects, session Storage objects and similar mechanisms. This data is usually stored in a server. The process of storing and using users' data also led to the emergence of social media and revenue potential for businesses. Aggregation of data and provision of services through platform ecosystems (such as Amazon, Flipkart) depict the centralised nature of Web2. This centralisation often results in inequitable relationships between the platforms and their users due to the aggregation of data within the platforms.

Hence, the emphasis on decentralisation in Web3 is a leap from the ethos of Web2. The technologies that Web3 is built upon allow for storage of data on a network of computers instead of a single server. Data is maintained through consensus mechanisms, thus also reducing the reliance on a central authority for maintenance, facilitation and moderation. Web3, thus, persists data and also has high potential to solve the problem of inequitable relationships generated due to centralisation in Web2.

One of the ways that Web3 changes the Web2 paradigm is the way its protocols are built. A protocol is a set of rules and processes that govern the communication between different computers that are in a network. There exist different kinds of devices with different hardware and software running on them. When they exist on a network (such as the Internet) and need to exchange information with each other, they need standard processes to carry out these communications. In the networking realm, a protocol acts as a language - the lingua franca - between computers and other devices that are operating on different hardware and software[1].

Web1 operated on open protocols such as Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) and Transmission Control Protocol (TCP). The technical standards for the protocols were set through consolidated efforts of government agencies, non-profit organisations, academicians and private organisations. In the era of Web2, companies built closed protocols over these open protocols. Microsoft built the proprietary Outlook over the open SMTP protocol, which is why the user must pay to be able to use this email application. This contributed to the centralisation of many products because companies held unilateral power over network access, features, user data, etc.

Web3 uses open protocols for most of its functions like storage, computation, and value exchange. With the principle of decentralisation at its core, development of Web3 protocols has been open and transparent. Much akin to Web1, Web3 protocols would benefit heavily from consolidated efforts of government agencies, academicians, non-profit organisations and others.

B. What does Web3 have to do with Blockchain?

Blockchain Defined

A typical blockchain is a sequence of blocks that holds a list of transactions like a conventional public ledger. The blockchain is extended every time a new block is added to it after being validated by certain mechanisms. In addition to holding the transaction details, the block also holds the address to its previous block and a unique hash function. Each node is validated by other nodes and transactions would be checked. Hence, it is nearly impossible to tamper with data stored on the blockchain.

The full range of impact of blockchain technology is still unclear, at this stage. But it

[1] Communication between two nodes in a network occurs on various levels such as physical layer, data link layer, network layer, etc,. (depending on the model that is chosen to understand the networking). In the context of this document, we are looking at application layer protocols such as HTTP, FTP, SMTP, etc.

is worth noting that blockchain has immense potential to alter institutional structures and economic activities. Considering the aspects that uphold market capitalism itself - property rights, exchange mediums, native money and law - blockchain is positioned to create massive impact.

Smart Contracts

Smart contract is a key building block of Web3, but is not a well-understood term, possibly due to the use of the term 'contract'. Nick Szabo introduced the idea of smart contracts before blockchain emerged in 2008. He intended that smart contracts utilise protocols and user interfaces to facilitate all steps of the contracting process. For example, consider the case of a person using their car to secure credit from a bank. The terms of the smart contract can be such that the said person can possess the ownership of the car as long as they make payments to the bank. Once they fail to make their payment, the smart contract is breached - which will initiate a protocol that transfers the ownership of the car to the bank. A smart contract reduces the transactional costs - such as principals, lawyers, third parties, etc. - that are incurred in a traditional contract.

Many applications of blockchain adopted the mechanism of smart contract. Smart contracts - within blockchain - are automated programs that transfer digital assets when a set of conditions are met. Ethereum is an example of one such blockchain application that uses smart contracts. The use of smart contracts alters the relationship between consumers. No longer are intermediaries required to establish trust between parties involved in a transaction. Consumers can use pre-programmed contracts with conditions written into the code to act as purchasing agents.

WEB3 IS BUILT ON THE PRINCIPLE OF DECENTRALISATION AND THIS PRINCIPLE IS ACHIEVED BY BUILDING UPON BLOCKCHAIN TECHNOLOGY. IN THE FOLLOWING SECTIONS, WE WILL SEE HOW DIFFERENT APPLICATIONS AND USES OF BLOCKCHAIN INTERACT WITH CURRENT PARADIGMS TO FORM THE CORE TECHNOLOGIES OF WEB3.

C. Web3 Examples

For Web3 to operate, the core technologies described above have to serve certain common digital needs of markets and individuals in new decentralised ways – the need to transact financially, to assert identities in secure ways, to communicate and interact with each other online, and the like. This is where the following set of applications come in.

Cryptocurrency

Before we understand what cryptocurrency is, it is helpful to understand the term 'crypto-asset'. A crypto-asset is a form of digital asset that uses cryptography, peer-to-peer networks, algorithms and a distributed ledger technology (such as blockchain) to create, verify, record and settle transactions. They operate independent of a central authority or a third-party for validation - which makes them trustless.

OXFORD DICTIONARY DEFINES IT AS "A DIGITAL CURRENCY IN WHICH ENCRYPTION TECHNIQUES ARE USED TO REGULATE THE GENERATION OF UNITS OF CURRENCY AND VERIFY THE TRANSFER OF FUNDS, OPERATING INDEPENDENTLY OF A CENTRAL BANK".

A cryptocurrency is a type of crypto-asset. Oxford dictionary defines it as "a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank". When digital currency was envisioned in its earlier days, the issue of double-spending arose. In the current scenario, if one spent a note of Rs. 10 to buy a cup of tea, that same person would not be able to spend that same note of Rs. 10 again. In the realm of digital currency, it had been difficult to ensure that a person did not reacquire the digital currency that they had just spent. This was where cryptocurrency rose as a solution to this problem.

To solve the issue of double-spending, there are processes put in place on a cryptocurrency to verify and confirm transactions involving cryptocurrencies. Once these transactions are verified and confirmed, they are recorded on the blockchain and they become irreversible. If a person has one unit of a cryptocurrency and they attempt to send it to two wallet addresses, both the transactions will first go into a pool of unconfirmed transactions. When the first transaction is confirmed and verified, it is recorded onto the blockchain. After this, when the second transaction undergoes the process of confirmation, it will turn out to be invalid because the considered unit of cryptocurrency has already been a part of a confirmed transaction.

Therefore, cryptocurrency is envisioned as a replacement for fiat money, with the verification of transfers happening without the participation of any State agency. It is a medium of exchange and has no inherent value of its own. Bitcoin is one of the foremost examples of a cryptocurrency. Other examples of cryptocurrency are Ether, DogeCoin, Tether.

Native Coins and Tokens

Crypto assets are widely divided into two categories: native coins and crypto tokens. Native coins are a completely new class of electronic money that are operational on universally accessible peer-to-peer payment networks. For example, Ether is the native coin that exists on the blockchain called Ethereum. Currently, every native coin operates on its own blockchain network without any way to interact with other blockchain networks. Ether cannot interact with the Bitcoin network. This lack of interoperability is a major hurdle to the uptake of blockchain technology as payment systems.

NATIVE COINS ARE A COMPLETELY NEW CLASS OF ELECTRONIC MONEY THAT ARE OPERATIONAL ON UNIVERSALLY ACCESSIBLE PEER-TO-PEER PAYMENT NETWORKS.
CRYPTO TOKENS ACT AS DIGITAL VOUCHERS THAT CAN BE USED TO REALISE ANY TYPE OF ASSET OR SERVICE.

The second category of crypto assets is the crypto token. Crypto tokens act as digital vouchers that can be used to realise any type of asset or service. These tokens are built on top of native coins and hence, do not have a blockchain network of their own. These tokens are often programmed by a smart contract to carry out transactions after satisfying a set of conditions. They are therefore used for many purposes such as fundraising, investments, payments, shares in companies, and voting stakes in the decision-making process of a company. There are several standards defining the types of crypto tokens in existence. The following are some broad categories of tokens that are popular:

i. Security tokens: A security token is an asset - such as a debt or an equity claim on the issuer. Therefore, they are analogous to traditional investments such as stocks, bonds, equities or derivatives. Blockchain Capital is one of the leading pioneers of security tokens. Their BCAP token is the first security token in the market.

ii. Utility tokens: A utility token provides a definable benefit - like access - to an application or a service. They serve as digital vouchers. After a utility token is issued to a user, the user can redeem this as a coupon at some time in the future. Examples of the benefits offered by utility tokens are voting rights, rewards, or staking governance. One of the most popular examples of a utility token is the Basic Attention Token (BAT) which is used in tandem with the Brave browser. Brave blocks ads and tracking and hence, users are rewarded with BAT if they choose to view non-targeted ads.

Non-Fungible Tokens

Non-Fungible Token (NFT) is a digital asset based on the blockchain technology that is used to prove the authenticity of a purchase of a digital or a physical asset. The concept of each asset being unique and non-*fungible*[2] differentiates the NFTs from other cryptocurrencies – one Bitcoin is like another but every NFT is unique. NFTs operate on smart contracts - which are pieces of code that are set into action if certain conditions are met. Hence, when these predetermined conditions are satisfied, an automated workflow creates the NFTs.

NFTS DO NOT CONTAIN THE ACTUAL ASSET THAT THE BUYER IS PURCHASING. THEY CONTAIN THE METADATA OF THE ASSET AND THE WALLET ID OF THE BUYER - HENCE ACTING AS PROOF THAT THE INDIVIDUAL OWNS THAT PARTICULAR ASSET.

NFTs do not contain the actual asset that the buyer is purchasing. They contain the metadata of the asset and the wallet ID of the buyer - hence acting as proof that the individual owns that particular asset. There is broad diversity in the application of NFTs. NFTs are used to sell art, fashion, assets in gaming and metaverse, real estate, etc. In 2021, a bundle of artwork called the Bored Ape Yacht Club (BAYC) by Yuga Labs sold for $24.4 million. This NFT bundle is a bunch of semi-randomly generated but unique cartoon-like images of apes which provides the owners of each NFT with exclusive benefits like merchandise drops, bonus NFTs, etc. The uniqueness of each ape within the bundle is what lends the artwork its non-fungible aspect. Therefore, NFTs conveniently pave a secure way to transfer the ownership of a possessions such as paintings, music and memes. It is important to note that NFTs do not transfer the copyrights of the artwork in consideration.

[2] A fungible asset is an asset that is easy to exchange or trade for something else of the same type and value. Following that, a non-fungible asset is an asset that is unique and cannot be interchanged with another asset of similar type or value.

NFTs, in the fashion industry, have a broad range of applications. NFTs are used to sell both physical and digital objects, transferring ownership – much like how other forms of artwork, like paintings, are sold. A more diverse application arises out of the interaction of fashion with augmented and virtual reality. Accessories and clothing are designed to be used in the virtual world. Nike and RTFKT released the Nike Dunk Genesis CRYPTOKICKS NFTs that are designed to be worn in the metaverse – another important technology of Web3.

NFTs in real estate introduce a new subtype called the Fractionalised-NFTs (F-NFTs) which allow buyers to buy a part of the NFT and share the ownership with other buyers. Therefore, F-NFTs are fungible. They are used to buy high-cost assets (such as a house) and democratise investment. Multiple buyers can buy a property and split the rent obtained from the rent on that property. Fractal Property is one such platform that enables fractionalised real estate. Therefore, we see that NFTs have a wide array of applications that need vastly different treatment in terms of regulation.

The Metaverse

The metaverse is a shared virtual world where people can interact with each other like they do in the real world using Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR) or Extended Reality (XR). The key concept behind metaverse is creating an immersive experience for people instead of just viewing in 2D on their (flat) computer or smartphone screen. The metaverse is not an example or an application of blockchain, but a technology that is enabled by blockchain technology.

THE KEY CONCEPT BEHIND METAVERSE IS CREATING AN IMMERSIVE EXPERIENCE FOR PEOPLE INSTEAD OF JUST VIEWING IN 2D ON THEIR (FLAT) COMPUTER OR SMARTPHONE SCREEN.

In some form, the concept of people interacting and engaging with one another in real time on virtual platforms has existed in video games like Roblox, Minecraft, Second Life, Fortnite, Animal Crossing, Pokémon Go, etc. These prototypes of metaverse are called Massive Multiplayer Online (MMO) video games. Second Life is a virtual world where you can interact with other users and also use its currency - called the Linden Dollar - which can be exchanged with real-world fiat money. Similarly, Minecraft is a sandbox game with User Generated Content (UGC). Users play within a modifiable 3D environment by building architectures and huge structures using metre-sized blocks. Metaverse differs from these prototypes by providing the user with an immersive experience. Therefore, the user is living in the virtual world instead of looking at it on a flat screen on their phones, tablets or computer screens.

The metaverse is enabled by a mix of emerging technologies such as blockchain, 5G, Artificial Intelligence (AI), XR, digital twins[3], etc. Blockchain introduces decentralised social systems into the metaverse. It provides a safe, secure, transparent and efficient way for transactions to transpire and goods be exchanged. Transactions can be traced in the metaverse, if built on blockchain. With the use of NFTs and Decentralised Finance (based on smart contracts and Fungible Tokens such as crypto assets), economic activity in the metaverse becomes decentralised. The tokens provide liquidity using existing Decentralised Exchange (DEX) solutions like Uniswap and Sushiswap. In these open peer-to-peer marketplaces, users can exchange their tokens without the presence of a centralised authority.

Apart from providing a viable economic model to the metaverse, blockchain also enables safe storage of the voluminous data that is generated in the metaverse. Massive amounts of data are generated in creating profiles for users and recording their interactions and transactions with each other. Storing this data in a central storage system leads to high risk of data loss, tampering and corruption. Given the nature of highly sensitive and personal data that could be collected in the metaverse (biometric data, vocal data, vital signs, etc,.), the metaverse requires a secure way to store data. The decentralised and transparent nature of blockchain will reduce the time taken to label and cleanse data through collaboration among data scientists. It will also provide a reliable and safe way to store the voluminous data generated in the metaverse.

DApps

Decentralised Applications are popularly stylised as DApps. DApps are trustless peer-to-peer applications that do not operate through a centralised model, i.e, there is no single entity running the application, which also means that it doesn't run as a traditional client-server application.

There are several ways in which DApps embrace decentralisation in their working. First, while storing data, DApps can store it on the blockchain. This ensures transparency in the transactions because this transaction cannot be altered, deleted or withdrawn. An example of this decentralisation would be Cryptokitties. Users can collect, breed and

[3] Digital twin establishes a virtual twin of an object existing in the real world. Ubiquitous sensing technologies can be used to maintain the same state of the object as that of their corresponding twin.

trade virtual cats. These data of the cats and the ownership details are stored on the blockchain. Second, decentralisation can occur by providing decentralised ownership or authority in the application to users. These kinds of applications are called Decentralised Autonomous Organisations (DAOs). Let us examine this kind of DApp in the following section.

DECENTRALISED APPLICATIONS ARE POPULARLY STYLISED AS DAPPS. DECENTRALISED AUTONOMOUS ORGANISATIONS (DAOS) ARE DECENTRALISED, COLLECTIVELY-OWNED AND BUILT ON THE BLOCKCHAIN NETWORK.

DAOs

Decentralised Autonomous Organisations (DAOs) are decentralised, collectively-owned and built on the blockchain network. They are supported primarily by smart contracts - which are pieces of code only triggered after certain conditions are met with. These smart contracts hold the rules of the organisation. They are transparent and public on the Internet. Thus, people can make the decision to fund the DAO solely on the strength of its smart contract. This process eliminates the inconvenience of forming business relationships with strangers. On the reception of funding, members are issued tradeable tokens that give them voting rights.

Therefore, the members become stakeholders in the organisation and will have a say in the dealings of the organisation through whatever voting mechanism is written in the smart contract. The rules governed by the smart contract cannot be changed unless decided by a vote by its users. This means that there is no CEO or a CFO of the organisation who is making big decisions about the organisation. The community of the DAO guides the decision-making process of the organisation. There are several examples of DAOs in different categories of media, philanthropy, investment, etc. Some of the leading examples are Gitcoin, Decrypt and BitDAO.

DEFI ENVISIONS FINANCIAL SERVICES WITHOUT THE INVOLVEMENT OF CENTRALISED FINANCIAL ENTITIES LIKE BANKS. THESE CENTRALISED INSTITUTIONS ARE REPLACED BY DEFI THROUGH WEB3 APPLICATIONS SUCH AS THE DAPPS.

DeFi

Decentralised Finance (DeFi) is a range of peer-to-peer financial applications that use the distributed ledger technology, such as blockchain and smart contracts. DeFi envisions financial services without the involvement of centralised financial entities like banks. These centralised institutions are replaced by DeFi through Web3 applications such as the DApps. The functioning of the DApps is transparent and trustless because they are built on smart contracts that are open-source and public.

DeFi is set to revolutionise the way financial services are disseminated throughout the world. Traditional financial services face many challenges such as high eligibility criteria for setting up of bank accounts, lack of transparency in the operations of the financial institutions, involvement of intermediaries, risk of breach of personal data, etc. There are considerably less barriers while accessing DeFi services because anyone with a crypto wallet and adequate funds can participate in the system. Transactions between users are not governed by any central authority and users are allowed to carry out transactions directly between each other. Aave is a DeFi platform built on the Ethereum network where incentives are provided to users for lending and borrowing assets in a decentralised manner.

Self-Sovereign Identity

In the current online world, an Internet user has many identities for the many different applications that they interact with. It is difficult to manage many of these jumbled identities. This system also provides little control to users over the data of their identities. The concept of Self-Sovereignty Identity (SSI) emerged in this context to provide users with control over their identity data. The many features of a SSI would be portability across multiple locations, user autonomy, user-controlled attribute disclosure based on user's consent, not reliant on third parties and ability to make claims about your own identity.

THE CONCEPT OF SELF-SOVEREIGNTY IDENTITY (SSI) EMERGED IN THIS CONTEXT TO PROVIDE USERS WITH CONTROL OVER THEIR IDENTITY DATA.

Blockchain technology has the properties required to realise this vision of self-sovereignty. It enables decentralisation and the elimination of a centralised single entity that controls the identities. Users can have power over their identity data and who can access it. Therefore, blockchain provides a good foundation for SSI to be developed on. Some examples of blockchain-based applications that attempt to provide self-sovereignty in identity are uPort, Jolocom, Sovrin and Blockcerts.

KEY POLICY QUESTIONS

While these technologies are evolving rapidly, and descriptions of the same may look very different in as little as a year, regulatory bodies around the world are struggling to keep up with the ever-changing landscape. Web3 technologies are set to potentially blur nation-state borders, redefine existing organisational structures, alter transactions between any two individuals and reimagine the privacy of the user. These fundamental shifts often do not sit well within the current regulatory landscape that are based on certain existing assumptions and structures. In the following sections, we will delve into some particular and important instances of policy issues arising due to Web3.

A. Digital Ownership and Intellectual Property Laws

Blockchain technology enables the possibility of digital timestamping the creation of any intellectual property - thus making it possible to trace the ownership of the work being sold. This process is called Blockchain-based Timestamping. For example, when an artist creates an original digital painting and records it on the blockchain, the timestamp of when that work has been created will be stored in the blockchain. Once this data has been recorded on the immutable blockchain, even the owner of the work - who is the artist, in this case - cannot change this timestamp. Therefore, Blockchain-enabled Timestamping provides irrefutable evidence for when the original work has been created.

This can also be coupled with smart contracts to trigger some compensation to the initial owner whenever ownership of the work changes. Hence, blockchain technology has the potential to reduce the reliance on notaries or intermediaries to verify ownership of intellectual property. It can be used to address the complex issues of intellectual property ownership such as patents, copyrights, trademarks, etc. At the same time, as the use of intelligent tools to create assets increases, new questions of ownership arise – who owns the AI generated art-work based on millions of physical artworks turned into an NFT by a third party? With the sale of an NFT, the owner of the asset does not transfer the copyrights to the buyer. Hence, this buyer could infringe upon the Intellectual Property Rights (IPR) of the original artist by trying to resell the NFT and the original artist would not even know!

IPR becomes more complicated in the context of metaverse where there are constant efforts in the industry to blur the lines between the real and the virtual world. Users of the metaverse will create content, objects and other assets in the metaverse. Therefore, it also becomes important to protect the intellectual property of these users. Wider debates are also emerging about the use of patents in the virtual world. Is someone infringing upon the inventor's patent rights if they recreate the same technology in the virtual world? Would the same laws as that of the real world apply in this scenario or do we have to reimagine how we regulate and govern IPR in the metaverse?

B. Community Governance

In the era of Web2, users generated content on centralised platforms (such as Twitter and Instagram) and the responsibility of moderating that content fell to the centralised platform. The decentralised nature of Web3 allows users to own the content that they generate. This, hence, poses difficulties over the question of community moderation and compliance with legal standards around defamation, hate speech etc. For example, Steemit is a blockchain-based social media where users can act as content creators and content moderators. The website is built on the principle of community building. Hence, it shares its profits, not just with its financial contributors, but with its users who create the content. Users are rewarded with cryptocurrency payments. Users can upvote and downvote the content that they see on the website. The weight of a user's vote depends on the reputation of their content (measured by the votes they get on their content) or financial contributions to the website. While this voting mechanism decentralises the process of content moderation, it also creates inequality between the users who have different powers behind their votes. Additionally, since there is no single authority who is responsible for removing malicious content, the problem of the same can get exacerbated by decentralised content moderation.

C. Privacy and Data Protection

The boundaries of privacy have expanded beyond the confines of personal data, the family, the body and the home. People communicate and interact on the Internet - more so, now over emerging technologies such as Internet of Things and smart devices. Violations of privacy no longer just occur bodily and spatially, but also through intrusions in various spheres of life that were previously not considered private. Therefore, the fundamental definition of privacy has been altered in the past few years, making it imperative to redefine the confines of privacy legally.

In the purview of Web3, blockchain technology is touted to be secure, and many decentralised privacy-first applications are emerging in the Web3 spectrum. Self-sovereign identity allows users to assert multiple portable identities in different contexts, so that centralised verification of identity is not a pre-condition to transacting and interacting online. On the other hand, public blockchains are open for anyone to read and write. Transactional details on the blockchain can be monitored to trace the ownership of that transaction to the owner - thus making it possible to identify the owner. Private blockchains, meanwhile, restrict the viewing and writing to an authorised set of participants. While private blockchains are secure, they are also less transparent than their public counterparts.

Outside of the blockchain ecosystem, Web3 is still accessible through existing Internet infrastructure such as programming languages, communication protocols and storage. If a user wants to access a Web3 application or service, they need to access it through a centralised platform - say, a website or a mobile application. Web-side access exposes the users to traditional privacy vulnerabilities faced by front-end access like design pitfalls, malicious attacks, and tracking of addresses of users accessing the platform. Thus, the existing privacy concerns still persist in Web3.

D. Consumer Protection

While the entry barrier for consumers to invest in crypto-assets is low, the level of technical knowledge and education required to understand the technologies behind crypto-assets is high. The most recent CoinEgg scam reportedly defrauded as much as Rs. 1000 crores from Indian users. Standard mechanisms for consumer grievance redressal have not yet developed across the range of decentralised offerings outlined above, particularly where exchanges or platforms themselves actively defraud thousands of users.

E. Financial Flows and Taxation

The many emerging technologies in Web3 pose serious concerns over tax treatment and tax jurisdictions. The metaverse is a sprawling virtual world where users can interact with each other from any part of the world. DAOs enable the existence of collective ownership through governing and voting rights in organisations through tokens. The transactions involving crypto assets are peer-to-peer, not monitored by a centralised financial institution. Therefore, there are changes in the way assets are viewed in the Web3 paradigm.

The transactions on the metaverse raise the question of which jurisdiction can tax the digital assets acquired in this virtual world. Additionally, the tax treatment of crypto assets is a complex and evolving process that needs to adapt to the speed of adoption of the technologies of Web3.

Additionally, economic activity around Web3 offerings like DApps, DAOs and NFTs easily lends itself to fraudulent and money-laundering activities. The metaverse is bustling with economic activity through crypto assets like wearables, art, collectibles, etc. In general, regulation for technologies in Web3 has not progressed enough to prevent fraud and crime.

An example is wash trading, or the act of selling an asset to yourself or to a collaborating actor to drive up the prices in the market or make the asset look more voluminous than it is. In this scheme, the seller is on both sides of the transaction. This serves the purpose of misguiding the buyers about the real value and the liquidity of the crypto assets that they are buying. Wash trading is prevalent in the crypto markets. According to an Elliptic report, around 2% of all NFTs sold in the global market are wash-traded.

Due to the limited knowledge surrounding buyers in the crypto market, the grounds of Web3 are also ripe for scams. Several types of scams include marketing for fake non-existing metaverses, phishing attacks through which NFTs and cryptocurrencies have already been stolen from Coinbase and OpenSea, creating bad smart contracts on purpose, posing as technical customer support and obtaining private keys of users' wallets, delivering a subpar project after inviting early minting investment in a metaverse.

Apart from wash-trading and scams, the metaverse also presents a good front for money laundering. Purchasing of 'plots' in the metaverse has been reported as being a front for laundering money obtained through illegal means. Shops in the metaverse could be selling perfectly legal items on the outside and could redirect customers to real-world illegal transactions, thus leading to laundering. New kinds of financial crimes in the Web3 world are likely to emerge due to the dynamic and novel nature of the technologies.

It is not always clear whether existing regulations designed to curb these kinds of activities are applicable to Web3. For example, anti-Money Laundering (AML) processes include all regulations or policies that ensure that institutions are not laundering illegal money or financing terrorism. Know-Your-Customer (KYC) is a set of practices used by financial institutions to verify customer identity to prevent fraud, money laundering and terrorist financing - intentionally or unintentionally. KYC is a part of AML to ensure that financial institutions and customers are safe from frauds. KYC compliance responsibility rests with the banks. In Web3, the possibility of fraudulent transactions and money laundering is high, especially in the absence of centralised entities responsible for compliance like banks. Due to the lack of clarity on the consumer protection regulation surrounding the technologies in Web3, it is difficult to determine where, under the current circumstances, these technologies fall with respect to KYC and AML regulations. There is a need to comprehensively understand how KYC and AML regulations can be applied to DApps, DAOs, NFTs and others.

Cybersecurity is of a huge concern in the current world and will continue to be a concern in the upcoming era of Web3 too. Web2 cybersecurity issues like hacking, international cyberwarfare, corporate espionage and ransomware attacks will eventually find their way into the Web3 space because enterprises are investing money in there. Let us take a look at one such issue that is unique to Web3. Crypto-mining is the process of mining existing blocks on Proof-of-Work blockchain networks to validate transactions and add the block to the existing network. In the case of Bitcoin, miners are rewarded with Bitcoin, making this activity very lucrative for them. To mine new blocks, miners will have to solve complex hash puzzles. They need computers, Graphics Processing Units (GPUs) and other specific hardware and software tools that can perform this computation-intensive task. Since this task requires high computational power, miners pool resources sometimes to divide the reward amongst themselves, if fruitful. The security issue arises when this pooling of resources is done illegally without the permission of the user of the computer. This process is called crypto-jacking. Crypto-miners can slip mining software into someone's computer secretly and use that device to harness computation power for their mining purposes. This is not just compromising the privacy of the user under attack here, but also the performance of their device and the consequent electricity bills. This is, therefore, a new form of cybersecurity issue that arose with Web3.

Moving on to cybersecurity issues arising with the technology that Web3 is built upon, while the data on blockchain is nearly impossible to tamper with, there is still a possibility that data on the blockchain is mutable. Through attacks like 51% attack on a blockchain, attackers can corrupt the network.

In a traditional enterprise, the responsibility of foreseeing, anticipating and handling these breaches and attacks fall to the higher management of the company which comprises directors and other such officers. In the United States of America, the directors act under the business judgement rule which provides them immunity from liability if they are sued on the grounds of not doing their duty of care as long as their actions fall under the defined rules of the judgement. The rules ensure that the director acted 1) in good faith, 2) with care that a reasonably prudent person would do, 3) the best interests of the corporation. To be able to operate successfully as specified in these rules, the directors go through appropriate training and corporate compliance programs. In this context, the community-owned decentralised nature of DAOs poses a problem. Since the stakeholders in the decision-making process are members of the DAO with tokens, there is no guarantee that these members will be informed enough, take timely decisions and foresee the security risks that their organisation might face.

F. Online Gaming

The Indian gaming industry is rapidly growing. Lumikai - an interactive media venture capital fund - released a report on the gaming industry of India in 2022. It notes that the Indian gaming industry is valued at $2.6 billion in FY 2022 and is expected to have a compound annual growth rate (CAGR) of 27% to reach $8.6 billion by FY 2027. Of the 507 million gamers in India, 120 million users are paying users. In-game purchases are set to grow at a CAGR of 37%. The groundwork for a new era of Web3 gaming is being laid down well. One of the most popular examples of Web3 gaming is a leading Play-to-Earn game called Axie Infinity, built on blockchain, in which players can earn Axie's native crypto asset called Smooth Love Potion (SLP) by training and fighting monsters. Another way in which Web3 is infiltrating the gaming industry is also through in-game purchases. Ubisoft forayed into NFT gaming by introducing NFTs into the game Ghost Recon: Breakpoint. While there is a long way to Web3 adoption in the gaming world, there is great potential in uptake of Web3 technologies through the indirect funnel of gaming. Therefore, the gaming industry becomes an important domain to observe, as online gaming often serves as the earliest adopters and scalers of such paradigm-shifting technologies as Web3.

Key issues arising from online gaming fall under a wide spectrum of regulatory sectors.

There are questions pertaining to existing regulatory structures such as intellectual property rights, gaming laws, consumer protection, privacy, etc. With the introduction of Web3 into the mix, issues of interoperability of identities and currencies, money transmission through crypto-assets and general regulation of cryptocurrencies are some of the immediate challenges.

Money paid beyond the initial subscription or fee - called 'in-game purchases' - occur in the gaming world for multiple reasons. A user might want to buy skins for their character, unlock a new level or character of the game or buy extra lives. In-game purchases, in gaming history, have been used to launder money or trick the user into losing their money. These unintended consequences can, therefore, invoke regulations surrounding gaming laws and consumer protection requirements. The assets acquired in the game could be non-convertible or convertible to real-life fiat money. In order to adhere to local laws in most cases, games (like Roblox or Linden) emphasise that their in-game currency does not have any real-life value.

In the Web3 era, the lack of regulation creates further questions for online gaming. Gaming after the advent of the blockchain technology enables the transfer of assets and value amongst users without borders. Users can easily transfer their assets to one another via a blockchain network. As interoperability between games increases, so will the value of these crypto-assets purchased in the game. Regulation of money transmission over Web3 will face newer challenges than that of the traditional online gaming world.

Web3 gaming is also incredibly complicated because of the interaction with technologies like NFTs and metaverse that present difficult regulatory use-cases independently. Hence, the policy treatment of Web3 gaming has to differ significantly from the paradigm of online gaming that exists right now.

This brief was authored by Srijoni Sen and Srija Gadamsetti with the support of All India Gaming Federation.
The authors would like to thank Dhruv Garg and Suman Kasana for useful comments. Any errors are the authors' alone.