Metaverses

Afonso Ferreira, João Peres

10 Metaverses

10.1 Introduction

Despite what many readers may think, the metaverse is not a product, not even a brand of some social network company, but a name given to a set of technologies applied in platforms for the Web on the Internet. In fact, the concept of virtual worlds dates back at least to the 19th Century [21]. Still, the term metaverse was used to name a futuristic concept, described in a science fiction book in 1992, which popularised it [198], and was shown in a visual format in a movie 20 years later (i.e. 10 years ago) [140]. Metaverse in practice today, refers to a new type of Web platform, which is supported through a comprehensive set of technologies, some of which already consolidated and others in evolution, which will allow users greater interactivity and socialisation in immersive 3D digital environments, represented by a universe of new digital virtual worlds, preferably mirrored in the physical world.

Metaverse research witnessed a first wave of "hype" between the years 2000 and 2006, with many results and visibility. Currently, in 2022, it is going through a second wave of interest, now brought about by commercial players that started to market their metaverses and events held inside them, but also by a widely publicised metaverse-related public announcement by one of the Western Big-Techs in late 2021.

Today, it is possible to understand what metaverses are, or could be, by browsing through Web platforms such as Second Life, Decentraland, Somnium Space, The Sandbox, Roblox, Horizon Worlds, Avakin Life, Mesh, among others.

The concepts of digital virtual worlds of today's metaverses are typically based on Web 2.0 technologies that include 2D and 3D Virtual Reality spaces, with computer graphics images ranging from low to high resolution, and some platforms using Augmented Reality technologies in various activities. The representation of users is always through avatars, and, as access to platforms depends on an exclusive login, there is a lack of interoperability, as avatars are confined to a single metaverse and its worlds, not being allowed

to move from one metaverse to another, on another platform, without logging in again in the physical world.

The means of accessing the platforms can be done through various devices that include smartphones, tablets, laptops, desktops, workstations, and even head-mounted displays or virtual reality glasses. Some platforms already use monetisation through blockchain and cryptocurrencies, with the adoption of smart contracts and fungible and non-fungible tokens (NFTs) that enable mercantile activities. Note, however, that today there are still few platforms for metaverses that use Web 3.0 technologies, the HTTP/3 protocol, and other more advanced and secure technological resources, but this is clearly the path for the future.

To support these features, the most advanced technologies such as Web 3.0 (latest Internet version), Artificial Intelligence, Brain-Computer Interfaces, IoT (Internet of Things), Blockchains, and Virtual, Augmented, Extended, and Mixed Reality will usher in a large number of opportunities that will probably impact large parts of our societies, just like Social Networks did.

10.2 Who Is Going to Be Affected?

In order to analyse the plausible impact of metaverses in future, let's embrace in this chapter their full vision as digital worlds that are massive, immersive, persistent, open and economically developed, as follows [80].

- **Massive:** They can host an unlimited number, or at least a very high number of concurrent users, as the computing power of the Web platforms and of the users' machines evolves in terms of graphics processing and connectivity.

- **Immersive:** They offer three-dimensional and embodied experiences, based on Virtual Reality (VR) and Extended Reality (XR). Imagine that after work you go to a small room in your house or neighbourhood, dress up in a connected "sensory suit", and tell the computer the metaverse of your choice and, from there, you enter the site, having the sensation of being present and living "inside" a chosen digital virtual world, controlling many things with your thoughts. This is in contrast to the current experience of most game universes, which are two-dimensional, confined to screens, and mediated by clicks, typing, and either screen or mouse.

- **Persistent:** Metaverses will never stop or reset. Or at least that will be the perception of their users. The life and society of a metaverse will continuously evolve, even if some avatars are not present, as it happens to normal life in our world.

- **Open:** Anyone with good Internet connectivity and VR/XR computing power can go into metaverses, move within them as an avatar, interact with other avatars, socialise, trade, build, produce intellectually, and so on.

- **Economically developed:** There will be extensive trade in goods and services within the metaverses, which may or may not have an impact in the physical world outside them. They will likely be supported by Decentralized Finance (DeFi) architectures and digital monetary systems that encompass blockchain technologies, cryptocurrencies, smart contracts, and fungible and non-fungible tokens that will enable property rights assurance practices.

Clearly, such an ambitious vision points to a high likelihood of a renewed collision between Industrial Age Governance and Digital Age Governance, which would affect all layers of the population, from simple metaverse users to policy makers.

In fact, governments are already nervous. In the EU the European Parliament is concerned mainly about Competition, Data Protection, Responsibilities, Financial Transactions, Cybersecurity, Health, Accessibility, and Inclusion [126], while the EU Council's main points of preoccupation are Geopolitics, Economic growth, Jurisdiction, Health, Consumer protection, Civil and Penal codes, and Climate change [15]. We note that massive intellectual investment would be required in order for practical solutions to be found and implemented in each of these areas. Besides, there will be thorny issues around reaching consensus in any of these topics. These are some reasons why the European Commission has just included metaverse policy among its priorities [36, 42].

10.3 What Is Expected to Happen?

An analysis of the evolution of metaverse support technologies, such as those described above, the Internet, and the Web – from the Web 1.0 version and the current Web 2.0, to the new level of Web 3.0, especially when thinking about Web platforms with great interactivity and greater social reach –, brings many question and concerns, especially regarding cybersecurity, privacy and protection of (personal) data, regulations, and various aspects of the governance of such digital worlds [191].

Take governance *inside* of metaverses as an example. The concept of "inside" is highlighted because it is different from the concept of interface between the digital world of a metaverse and our physical world since such an

interface is becoming regulated, at least in the European Union (EU), since 2016.

In the EU, the rule-of-law is dominant and its institutions are mostly fit for purpose. However, in this new technological frontier that are metaverses, it is not clear what will be regulated, who will establish and enforce rules, or how this will be done. But any place, physical or digital, at some point of population density will need some kind of order maintenance, including the notion of fundamental rights.

Indeed, thinking of unregulated parallel digital universes is worrisome. And as commerce will be ubiquitous, products, transactions, property rights, and other businesses will need some kind of protocols for markets to thrive. Then all kinds of conflicting situations will have to be resolved by some form of authorities, police, and courts. As well, there must be rules of trade, taxation, income, etc. But then, if a large set of rules has to be established, another important question is who is going to set them: Are they going to be the owners of the platforms of metaverses, since these universes are privately owned? Will they put users to help set up local rules? Or are public authorities from the physical world starting out and expanding their reach into the digital world as well? Whose public authorities to start with? Or are libertarians thinking about creative technologies to govern the metaverses, promoting the ideology that "code is law"? Likewise, what form does such a body of rules take? Accordingly, we can think of the following forms of regulation.

- Signing of usage contracts. However, they may be as long as constitutions.
- Replication of laws and regulations from the physical world. However, this may hinder innovation, and good justifications would be expected for the choice of one model over another.
- Distributed models, based on digital technologies, like blockchain, bitcoins, NFTs, smart contracts (i.e. , persistent scripts).

In addition, the very technological offer of interactivity and immersion of next-generation metaverses will heavily depend on wearable devices monitoring both biometric (e.g., gait, facial expressions, temperature) and neurometric (e.g., fear, satisfaction, attention) data, which will imply continuous and full surveillance of users. In Western societies, where privacy and protection of personal data are fundamental rights, commercial and public interests will have a very difficult relationship concerning this topic.

To compound such issues, the attack surface for security breaches and privacy invasions can become very large in the metaverse, because it integrates a variety of older, current, as well as untested new technologies and systems

whose intrinsic vulnerabilities and flaws will be inherited by the larger system. As a consequence, existing security threats will be amplified, with more severe effects. They include the following (non exhaustive) [216]:

- Lack of security culture from the part of users in such new environments,
- Mismanagement of massive data streams,
- Widespread user-profiling activities,
- Unfair results from Artificial Intelligence (AI) algorithms,
- Digital twins security,
- Security of metaverse physical infrastructures,
- Personal data involved in the metaverse will be more granular and biometric, including emotional, etc.

Finally, the enlargement of the attack surface brought by metaverses will facilitate existing threats in physical and cyber spaces, like persecution, harassment, and espionage, which may increase in frequency and impact. The use of emerging technologies will make more likely security incidents, like hijacking wearable devices or cloud storage, virtual currency theft, or AI misconduct to produce fake news autonomously within metaverses [57].

10.4 What Is the Worst That Can Happen?

Many things can go wrong if provision and usage of metaverses run amok in future, and most of them are related to the notion of trust in them.

It is certain that the vast majority of metaverse users are and will be law-abiding citizens and people who value civilised behaviour. However, among the users is also certain that there will be cheaters and other less honest persons who will join in just to try and make easy money out of what would be defined in most parts of the physical world as criminal activity. Such an environment would not invite trust from users, and licit commercial returns over investment may plunge as a consequence, while illicit undertakings may flourish.

On another, perhaps more important registry, metaverses place major challenges to privacy and governance and they may have the potential to accelerate the geopolitical shift of power from Nation States to private companies. Remind that already today some social network companies have populations that are larger than that of the largest country on Earth. If national governments cannot trust that metaverses will treat their citizens in a legal manner,

then governments may decide to over-regulate metaverses, hampering innovation and increasing fragmentation.

Accordingly, the lack of trustworthy governance and of security and privacy regulations inside metaverses may turn this high-tech Eldorado into a 21st Century Wild-West, where fortunes will be made and lawlessness will be the rule rather than the exception.

10.5 Research Gaps

As seen above, the field for State regulation of metaverses is vast, ranging from issues at macro levels (e.g., geopolitics) to micro levels (e.g., selling a digital bracelet in the metaverse). In a nutshell, the major current EU legislation and policies governing the digital sphere are as follows.

- Digital Markets Act : Regulation of competition for online markets. It establishes harmonised rules that define and prohibit unfair practices, such as the use of competitors' data and lack of interoperability, on the part of "gatekeepers" of the Web.
- Digital Services Act : Due diligence obligations on all digital services that connect consumers to goods, services, or content, including procedures for faster removal of illegal content as well as comprehensive protection for the fundamental rights of online users [38].
- GDPR : Protection of personal data. Due diligence and cybersecurity [41].
- Data Governance Regulation and Data Act: While the Data Governance Regulation creates the processes and structures to facilitate data, the Data Act clarifies who can create value from data and under which conditions. [40]
- Various in cybersecurity: Cybersecurity Act (eg certification), NIS2, ENISA , ECCC / NCCs , Joint Cyber Unit, Cyber Resilience Act, etc. [37]

However, from a governance and policy viewpoint such existing legislation are probably not sufficient to induce trust in the domain, and perhaps not even suitable for metaverses. Consequently, much research is needed in these areas in the near future. For instance, there will be a need to regulate security and privacy in multiple universes that are being built from scratch. Questions may be simple extensions of existing concerns, like whether metaverses should be subject to existing laws for the physical world and, if so, how not to hinder innovation and creativity. Or they may be turned much more towards future concepts, like whether avatars should be given citizen status.

Likewise, the technologies needed to build metaverses as envisioned here are just emerging, and a great deal of technological research will be required in the next few years. Moreover, one likely result of market forces is that several metaverses will be created, representing parallel universes, not only between them, but also to the physical one we are used to live in.

What is certain is that a new gold rush has already begun. Required research areas can be presented in clusters, as follows.

10.5.1 Building trustworthy metaverses

One governance research area should analyse all aspects within metaverses that would impact individual users. These encompass inter alia Data protection, Liability, Digital Identities, Cybersecurity at the user level, Mental and Physical Health, Accessibility, Inclusion, Financial transactions, and Consumer protection.

10.5.2 Metaverses and the physical world

Another governance research area should propose new societal systems for metaverses and their interrelation with existing forms of governance and government. These would include Cybersecurity at physical infrastructure and at systems levels, Privacy, Competition, Global governance, Jurisdiction, Civil rights, Penal code, Climate change, Innovation.

10.5.3 Compliance by design

The emergence of metaverses raise a wide range of concerns regarding their compatibility with the law, as seen above. Therefore, it will be necessary to go beyond the well-known concepts of security-by-design and privacy-by-design towards an encompassing compliance-by-design paradigm, if at all possible. For instance, research will be required about adapted technical regulations to guide hardware manufacturers and software developers with respect to compliance, including data governance and operational governance rules.

Such governance topics should be addressed together with research in the new technologies and systems integration that will be needed in order to achieve the full metaverse concept described above in this chapter. Some technological and systems research areas are as follows. Note that they are intrinsically transdisciplinary.

10.5.4 Interactivity and immersive technologies

Making the metaverse fully interactive and immersive is an evolutionary research area. it should be focused on the massive capture and fast analysis of data (telemetry, biometric, and neurometric tracking, among others) of

users and their avatars. Data will be collected through "wearable interfaces" (wearable devices) of different types that will gradually bring to metaverse XR platforms more and more sensitive personal information, which will need systemic protection.

10.5.5 Metaverses design

The area of research on the establishment of structured projects and design of digital virtual worlds in a metaverse environment now has great potential to study and establish a minimum necessary architecture. These can be platform infrastructures, usual protocol standards, security systems, or even the constructive and operational aspects of the application of XR in 3D. The establishment of a minimum standard should not make creativity unfeasible, but encourage the effective construction of interoperable metaverses with rules for social coexistence among avatars, which are acceptable in ethical and moral terms, universally, whether in digital or physical worlds.

10.5.6 Interoperability between metaverse platforms

Interoperability of metaverses needs to be intensified, so that it should be possible for avatars (users) who are experiencing a digital virtual world on a particular metaverse platform of a company, to be able to move, without impediments and in a transparent way, into another platform of metaverse, from another company, without the need to identify themselves again in the physical world. Research on interoperability in metaverse environments would touch upon digital identities and allow the establishment of a seamless collection of metaverses, maybe using the concept of self-sovereign digital identities and digital passports [220].

10.5.7 Metaverses and Environmental, Social, and Governance (ESG) issues

One of the key research points concerning metaverses relates to their impact on climate change, because of their need to rely on huge data centres, high performance computing, and even blockchain platforms, all of which necessitate very high electricity consumption. This area of research requires advances in architectures and algorithms, but also in other areas such as cooling techniques, that can enable the use of those technologies without major environmental impact. ESG considerations will play a major role in the provision and adoption of metaverses in future.

It's worth noticing that in the areas mentioned above, isolated and unconsolidated actions are already ongoing, which aim to cover the existing gaps in metaverse research. We can mention the actions of: the World Economic Forum [70], the Metaverses Standards Forum [131], the Open Metaverses In-

teroperability Group [154], and the Metaverses Interoperability Community Group at the W3C [202], among others.

10.6 Example problems

Tangible example problems include:

Data protection inside the metaverse. Personal data collected in the metaverse will be more granular, biometric, and neurometric. The question is then how to reconcile the fundamental need of metaverse immersion technologies to implement widespread user-profiling and the fundamental right to data protection, including bioethics. Note that such a question touches upon protecting the data from both the physical user and the digital avatar. More specifically, it should be investigated how to ensure that metaverses will not make illegal use of such data, for example for sales and monetisation (such as social networks already do), for promoting media influence, or in the effective production of subliminal advertisements, among other aspects of active and interactive persuasion.

Protecting avatars from identity theft. The protection of avatars' identity is a very important issue to be solved. Although there are already several proposals and strategies for applying security in databases, with the use of technologies such as distributed ledgers and scatter or hash tree structures, such as Merkle Trees (which are, by the way, key elements of Blockchain), there is still no consensus on how to keep avatars' digital identities without compromising their Lifelogging (metaverses life history).

Regulation of creation of metaverses. The technologies currently applied by many Web platforms already provide easy-to-use tools that allow users to create their own metaverses. Even if these are simple, they are totally under the users' control. The problem here is centred on the improper creation of metaverses that camouflage digital worlds meant to harbour avatar gangs for criminal practices, social activism, racism, and terrorism, among other unethical and illegal practices.

Equal opportunities in the metaverse. Ensure accessibility and inclusion in the metaverse in order to safeguard equal opportunities. The Web platforms that host metaverses will be able to segregate avatars based on their physical users' hardware characteristics, computing capacity, personal profile, or according to the geographic region of their access, giving more privileges to some than others.

Cryptocurrencies and NFTs usage in the metaverse. Issues of ownership, misuse, interoperability and portability. As the Web platforms are proprietary, they maintain control over the digital assets owned by avatars, as well as, determine the monetary standards used. Some platforms have their own internal cryptocurrencies, a fact that can jeopardise the portability and interoperability of avatars' digital assets between platforms.