EU Blockchain
Observatory and Forum

BLOCKCHAIN-ENABLED VIRTUAL WORLDS

About this report

This is the third of a series of reports that will be published addressing selected topics following European Commission priorities. The aim is to reflect on the latest trends and developments and discuss the future of blockchain in Europe and globally.

This report has been produced by the EU Blockchain Observatory and Forum Experts Panel and team.

The EU Blockchain Observatory and Forum team:

- Lambis Dionysopoulos, Prof. George Giaglis, Institute for the Future, University of Nicosia
- Ioannis Revolidis, Ismael Arribas, Ingrid Vasiliu-Feltes, Inigo Mores, Tadej Slapnik and Antonio Lanotte – EUBOF Expert Panel

Note

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this report.

Disclaimer 1:

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for any use which may be made of the information contained herein.

Disclaimer 2:

This report, in its essence, adopts a conceptual and exploratory approach that diverges from traditional methodologies commonly seen in EUBOF publications. As such, it does not adhere to the usual practice of citation and referencing. The content is derived from a synthesis of innovative ideas rather than established sources, aiming to foster discussion and exploration in emerging areas of study. Therefore, traditional references are not applicable in this context.

Introduction

We define virtual worlds as a paradigm shift in digital interaction, merging virtually enhanced physical reality and physically persistent virtual reality into a single, immersive network. This collective virtual shared space, inclusive of all virtual worlds, augmented reality, and the internet, represents a technology-driven shift that is poised to effect significant changes across norms, disciplines, cultures, and other barriers.

Our report focuses on open virtual worlds, a vision of virtual worlds that underscores the importance of open standards and interoperability. Open virtual worlds is conceived as a decentralised network, free from the control of any single entity. It champions individual ownership rights, freedom of expression, and the ability to freely traverse and interact across different virtual environments.

Our exploration traces the historical evolution of virtual worlds and proto-virtual worlds, from the text-based environments of the 70s, like multi-user-dungeons (MUDs), to the current state of virtual worlds. We acknowledge that open virtual worlds is a product of advancements in technology, particularly virtual reality (VR) and augmented reality (AR), which have enabled a greater sense of immersion in virtual worlds.

We delve in the political, economic, social, technological, legal, and environmental aspects to examine the feasibility of open virtual worlds from these various perspectives, noting the significant considerations that lie ahead. Politically, it necessitates international cooperation for uniform standards and regulations, while economically, it is influenced by factors like economic stability, income disparity, and regulatory frameworks. Socially, digital literacy, privacy concerns, and societal norms play a role in its adoption. Technologically, it relies on advancements in connectivity, blockchain, hardware, and data storage. Legally, it must address issues like data privacy, digital rights, and cybercrime. Environmentally, its carbon footprint and the impact of hardware production and disposal need to be considered, necessitating sustainable practices and societal prioritisation.

Finally, we provide a comprehensive overview of the legal considerations surrounding open virtual worlds, including interoperability, privacy and data security, the monopoly power of big tech companies, and the digital divide are significant hurdles that must be overcome to realise the full potential of virtual worlds.

Defining (Open) Virtual Worlds

DEFINING VIRTUAL WORLDS

As defined in the latest report from EUBOF, virtual worlds represent a shift in the way individuals interact with digital environments, effectively combining virtually enhanced physical reality and physically persistent virtual reality into a single immersive network. This collective virtual shared space, which includes all virtual worlds, augmented reality, and the internet, can be understood as a technology-driven shift that leads to significant and generalised changes across norms, disciplines, cultures, and other barriers, creating new opportunities on a global scale.

Virtual worlds, unlike existing digital experiences, is primarily characterised by persistent and cohesive shared experiences that create a sense of a new ‘world’. These experiences can be immersive and interactive, but also adaptable to limited interaction, making virtual worlds flexibly immersive. Hence, virtual worlds can be defined as

'the product of a technology-driven shift with generalized impact through persistent and adaptable digital experiences'.

Potential use cases of virtual worlds are vast and encompass various industries. Education and learning could be significantly transformed with immersive and engaging virtual classrooms, labs, and experiences that transcend physical constraints. In entertainment, immersive and shared experiences – such as virtual concerts, sports, and other events – could be broadcast to a global audience. For business and work, virtual offices, meetings, and collaboration platforms could provide a more interactive and efficient means of communication and collaboration, transcending geographic barriers. The retail industry could see the evolution of virtual shopping and augmented fitting rooms, giving customers a more comprehensive experience. Healthcare might benefit from VR-based therapy and remote surgery. Furthermore, real estate could be revolutionized with virtual property tours and the creation of a 'virtual real estate' market. Virtual worlds also offer immense possibilities for social connectivity, allowing individuals to build and manage their digital avatars and engage in virtual communities and activities. Finally, in terms of governance, virtual worlds could enable more participative models of democracy and consensus-building, while open virtual worlds vision could become a platform for new forms of digital citizenship and economy. The historical evolution of virtual worlds and proto-virtual worlds has been a gradual process, resembling other technological advancements in the past. It began with text-based environments like multi-user dungeons (MUDs) in the 70s, which evolved from fantasy tabletop games. Over time, visual elements were added, leading to more social interactions in virtual worlds. The development of massively multiplayer online role-playing games (MMORPGs) further emphasized the social aspect and gave rise to social or recreational virtual worlds, where users became deeply engaged as 'virtual residents'.

With advancements in technology, commercially available virtual reality (VR) and augmented reality (AR) enabled a greater sense of immersion in virtual worlds and paved the way for proto-virtual worlds. These proto-virtual worlds facilitated even more social and recreational activities, fostering persistence and adaptability. Many VR-AR-based virtual worlds already exist, and other digital platforms are integrating VR and AR elements to enhance the continuity of virtual experiences.

However, while this evolution from more primitive and siloed virtual worlds to the more holistic and impactful virtual world is driven by a combination of technological and business factors, there have also been significant advances in the social and governance front, what is known as an 'open' virtual world.

DEFINING OPENNESS IN THE CONTEXT OF VIRTUAL WORLDS

Open virtual worlds is a vision for virtual worlds that emphasizes open standards and interoperability. It is envisioned as a decentralized network where no single entity has control. It supports individual ownership rights, freedom of expression, and the ability to freely move and interact across different virtual environments. This vision of virtual worlds allows for the broadest possible participation and innovation, ensuring that the opportunities it provides are accessible to all on a global scale.

Firstly, blockchain technology, with its decentralized and transparent nature, ensures the robustness of open virtual worlds by allowing for the creation of a shared, global database that is not controlled by any single entity. This database can store any form of data, including ownership records of digital assets, user identities, and transaction histories. It can provide a reliable and secure method of keeping track of all interactions within open virtual worlds, without requiring a central authority to manage it.

Secondly, non-fungible tokens (NFTs) are a type of cryptographic token on a blockchain that represents a unique item or piece of content. In the context of open virtual worlds, NFTs can be used to authenticate and prove ownership of digital assets, such as virtual real estate, digital art, and avatar items. This is essential in a virtual environment, where copying digital items is incredibly easy, as NFTs can provide a definitive, immutable record of ownership and provenance.

Finally, cryptocurrencies, as decentralized digital currencies, offer a means to conduct transactions within open virtual worlds, without the need for traditional banking or monetary systems. They can be used to buy, sell, or trade digital assets and services, thus enabling an economy within virtual worlds. Cryptocurrencies can also incentivize users and creators to contribute to the development of virtual worlds, for example, through rewards, payments, or staking mechanisms.

Importantly, decentralized autonomous organisations (DAOs) also play a key role in this open virtual world. DAOs are organisations represented by rules encoded as a computer program that is transparent, controlled by the organisation members and not influenced by a central government. DAOs can be leveraged in virtual worlds to manage virtual spaces, communities, and economies, essentially serving as self-governing entities. They are decentralised and democratic, where decisions are made through a voting system based on token holdings, allowing for a fair and transparent decision-making process. This embodies the ethos of open virtual worlds, as it empowers its participants and ensures that no single entity has control.

DAOs can be instrumental in facilitating collective ownership and decision-making over digital resources in virtual worlds. For instance, a DAO could own a piece of virtual land in virtual worlds, and its members could vote on how to use or develop that land. This level of autonomy and decentralisation is fundamental in an open virtual world, promoting collective governance and fairness, and fostering creativity and innovation.

The potential of algocratic sub-worlds within open virtual worlds further extends these concepts. ‘Algocratic’ – derived from ‘algorithm’ and ‘democracy’ – refers to decision-making processes governed by algorithms. In these sub-worlds, rule sets and governance structures can be algorithmically determined and enforced, providing unique, self-regulating environments.

Algocratic sub-worlds can range from virtual economies regulated by algorithmic monetary policy to social spaces where interpersonal interactions are guided by algorithmically mediated rules. This could enable more nuanced and context-specific governance structures within virtual worlds, allowing for a diverse array of social, economic, and political experiments. As with DAOs, the key principle here is decentralisation: power and control are distributed among participants, with algorithms serving to automate, enforce, and facilitate the agreed-upon rules.

BLOCKCHAIN IN THE OPEN VIRTUAL WORLDS

In the context of virtual worlds, blockchain emerges as a foundational technology, underpinning various facets of this expansive digital realm, including decentralised ownership, interoperability, economy, agreements, and governance. For decentralised ownership and asset verification, blockchain's decentralised nature ensures that assets within virtual worlds are owned and controlled by individuals rather than centralised entities. This decentralised ownership model is crucial for open virtual worlds vision, where individual ownership rights are paramount. Furthermore, blockchain provides a mechanism for verifying the authenticity and provenance of digital assets, ensuring that they are unique and not duplicated. In terms of interoperability across virtual environments, it

allows assets and identities to be recognised and used across various platforms and virtual worlds. Blockchain also provides the infrastructure for digital currencies, which are instrumental in facilitating economic transactions within virtual worlds. These currencies enable users to buy, sell, and trade assets, services, and experiences in a secure and transparent manner. Another important feature is smart contracts, or self-executing contracts, with the terms of the agreement directly written into code, which enable automated and trustless transactions within virtual worlds. These contracts can govern various interactions, from asset sales to complex multi-party agreements, without the need for intermediaries. Additionally, and given the increasing concerns about data privacy and security in digital realms, blockchain offers a solution by providing a transparent and immutable ledger. This ensures that transactions and interactions within virtual worlds are recorded in a way that is both secure and verifiable. Finally, the decentralised nature of blockchain aligns with the vision of an open virtual world free from the control of any single entity. Blockchain can facilitate decentralised governance models, allowing for community-driven decision-making processes and ensuring that power dynamics are equitably distributed.

Overall, we summarise the differences and similarities between open virtual worlds, and other proprietary solutions are summarised below:

Aspect	Open Virtual Worlds	Non-open Virtual Worlds
Governance	Decentralized, collective decision-making	Centralized control
User Rights	Individual ownership, freedom, open traversal	Restrictions possible
Economic Model	Decentralized, crypto, NFTs for assets	Centralized
Technological Integration	Embraces VR, AR, blockchain	Reliance on proprietary tech
Inclusivity	Global participation, worldwide community	Access restrictions possible
Legal Framework	Focus on privacy, digital rights, anti-monopoly	Aligned with controlling entity

CURRENT STATE OF THE VIRTUAL WORLDS

The present virtual world landscape encompasses a variety of platforms, each displaying distinct capabilities and adoption rates. These platforms can be classified as follows:

- **Gaming virtual world:** These include Roblox, Minecraft, Fortnite, and Zepeto. Roblox, for instance, reportedly hosted around 43.2 million daily active users as of Q1 2023.
- **Social virtual world:** this category comprises VRChat, Spatial, Somnium Space, Neos, Mozilla Hubs, Meta's Horizon Worlds, and AltSpaceVR.
- **Web3 virtual world:** Decentraland, The Sandbox, Otherside, OVER, and Axie Infinity are representatives of this class.
- **Utility-based virtual world:** Google Streetview and Google and Apple Maps AR overlays fall in this group.

Industrial virtual world: platforms such as Varjo's Reality Cloud and NVIDIA's Omniverse define this category.

However, the growth and development of virtual worlds are beset by significant challenges. Interoperability – defined as the ability of computer systems or software to exchange and use information – is a major hurdle. Presently, different virtual world platforms operate in isolation, each employing their own standards, systems, and user policies, thereby disrupting the smooth transfer and use of data, digital assets, and user identities across these platforms.

Efforts are ongoing to address this challenge. Ready Player Me, for instance, is a project that aims to enhance interoperability by allowing users to generate 3D avatars that are deployable across numerous platforms. Despite this, the issue of differing rendering standards among platforms persists. The World Metaverse Council is also working on creating an open interoperable virtual world, which involves defining technological requirements for virtual worlds ecosystem, including advanced 3D modelling, AR, AI, blockchain, smart contracts, geospatial technology, and integration with Web2 portals.

The potential of virtual worlds is immense, ranging from reshaping social interactions to introducing novel means of entertainment, e-commerce, and education. Nonetheless, several challenges need to be overcome to realise this potential. These include addressing issues surrounding interoperability, privacy and data security, the monopoly power of big tech companies, and the digital divide. Possible solutions include the integration of Web3.0 principles into virtual worlds and the creation of comprehensive regulatory frameworks to balance the encouragement of innovation and the protection of user interests. With these approaches, we can move towards a more equitable, user-centred, and immersive virtual world.

On the Feasibility of Open Virtual Worlds: PESTLE Analysis

POLITICAL CONSIDERATIONS

From a political standpoint, the lack of a centralised authority within open virtual worlds implies that there will be low bargaining power or even the resources to generate the necessary political capital for the regulations needed to facilitate openness and interoperable standards in virtual worlds. This is in stark contrast to the experiences of the private virtual world by large companies that have the resources and central planning to ensure that their voice is heard. This means that existing governmental and regulatory frameworks will have to evolve to accommodate the inherent decentralisation required in virtual worlds, by regulatory initiative, especially when considering the potential perils of privately owned virtual worlds operating in a non-interoperable manner as silos.

*Table 1: **PESTLE Analysis for the Feasibility of Open Virtual Worlds***

Factor	Considerations
Political	Lack of centralised authority might impede the development of necessary regulations for openness and inter-operability in virtual worlds. Need for international cooperation to standardise regulations concerning digital assets, cryptocurrencies, and virtual space governance.The role of political stability in technology adoption.
Economic	Robust economic conditions facilitate rapid adoption of virtual worlds, but economic instability and interest rate increases slow down infrastructure development. Income disparity could limit access to technology necessary for virtual world participation. Regulatory and tax frameworks related to digital assets significantly impact economic feasibility.
Social	Societal comfort with digital interactions and virtual realities could facilitate adoption, but digital divides and low technology literacy rates could hinder it. Privacy concerns and societal norms about screen time and cyberbullying also play a role.
Technological	Open virtual worlds require advanced technologies like 5G/6G networks, edge computing, high-speed internet, blockchain technologies, powerful VR/AR hardware, decentralised storage solutions, and secure cryptographic techniques.
Legal	Virtual worlds must navigate legal issues concerning digital rights management, intellectual property rights, data privacy and security, identity theft, and cybercrime. Compliance with data protection regulations like the GDPR, despite virtual worlds's decentralised architecture, is also important.

Specifically, there is a need for international cooperation to foster uniformity in standards and regulations concerning digital assets, cryptocurrencies, and virtual space governance. Concurrently, governments worldwide must ensure data privacy and security to protect users from potential malicious entities within virtual worlds. Stability of political systems also plays a significant role in the speed and efficiency of technological adoption, with more stable regions being better equipped to incorporate and regulate new technologies like open virtual worlds. Finally, ensuring that those standards are upheld will help foster necessary competition that will lead to innovative and useful products and experiences for consumers and businesses alike. Finally, there is a need for skilled talents/professionals to develop and sustain the technologies necessary for open virtual worlds.

ECONOMIC CONSIDERATIONS

The economic environment plays a vital role in the development and propagation of open virtual worlds and its standards. On one hand, robust economic conditions can facilitate the rapid adoption of open virtual worlds, as with other technologies. A thriving economy means more capital for investment in new technologies, increased consumer spending on innovative products and services, and a strong job market, where skills needed for virtual world-related industries are rewarded.

However, the current economic instability, which has led to numerous consecutive interest rate hikes by central banks to curb persistently double-digit inflation in most major markets, has translated into decreased capital flows into the infrastructure projects necessary for the widespread adoption of open virtual worlds, slowing its progression. Similarly, subpar macroeconomic conditions have slowed the growth of cryptocurrencies, NFTs, and other abutting technologies, further contributing to the slowing down of open virtual worlds infrastructure building.

In parallel, income disparity is another economic factor that can impact the adoption of new technologies, but virtual worlds in particular. Inequalities in income distribution could result in only a certain segment of the population having access to the technology and digital literacy necessary to fully participate in it. While this is the case for every technology, it is particularly true in the case of virtual worlds, where the hardware requirements, infrastructure cost, and literacy required to interact with its various components are historically high, compared to the introduction of other technologies, such as the launch of the iPhone as the first modern smartphone.

Lastly, regulatory and tax frameworks related to digital assets and transactions within open virtual worlds could significantly impact its economic feasibility. Open virtual worlds necessitate a comprehensive regulatory framework to prevent illicit activities such as money laundering and tax evasion. Failure to establish such a framework could undermine the economic viability of open virtual worlds.

SOCIAL CONSIDERATIONS

One of the key social facilitators for open virtual worlds could be society's increasing comfort with digital interactions and virtual realities. This comfort has been notably accelerated by recent global events such as the COVID-19 pandemic, which forced much of the world to interact digitally. Societies that are more open to technology and have higher digital literacy rates would likely facilitate the faster adoption of open virtual

worlds.

At the same time, however, the ubiquity of digital experiences has also led to increased scepticism. When digital literacy remains low, technology might be demonised, especially when its introduction is coupled with increasing social divides and a worsening of living conditions for parts of the population (for instance, the introduction of automation tools that leave individuals job- less). Similarly, other issues around the digital divide could pose significant challenges. If access to the requisite technology or internet connectivity is limited to certain socioeconomic classes or geographical regions, whether due to prohibitive costs or due to a lack of the required literacy, it could result in a sizeable portion of society being excluded from open virtual worlds and even its demonisation as a technology. This could slow overall adoption.

Another significant social factor is societal views on privacy and data security. As open virtual worlds involve digital identities and the potential sharing of personal data, societies that prioritize data privacy highly may have concerns about participating, which could slow its adoption.

Moreover, societal norms and regulations around screen time and its associated health implications, cyberbullying, and digital well-being will also play a crucial role in the acceptance and regulation of open virtual worlds. If these concerns are not adequately addressed, they could pose significant barriers to the widespread acceptance of open virtual worlds.

TECHNOLOGICAL CONSIDERATIONS

Technologically, open virtual worlds will rely on technological leaps in computational, connectivity and storage technology areas to create and maintain a persistent, user-generated, and fully immersive digital universe.

Firstly, it will require the widespread deployment of technologies such as 5G or even 6G networks, edge computing, and high-speed internet to ensure seamless, real-time interactions within virtual worlds. This is particularly important as latency issues can break immersion, disrupt activities, and overall diminish the user experience within virtual worlds. Those networks are also important for smartphones and communication and are being developed independently of open virtual worlds, meaning that their potential implementation does not rely on open virtual world-specific considerations.

Secondly, open virtual worlds are heavily reliant on blockchain technologies for secure, decentralised transactions, digital identities, and to facilitate the ownership of digital assets. In that area, significant advancements will be needed to accommodate the scale of open virtual worlds, particularly around transaction throughput, interoperability between different blockchains, and energy efficiency.

Thirdly, widespread adoption of virtual worlds will require significant advancements in hardware. This could include more powerful and accessible VR devices, AR glasses, haptic feedback suits, and other forms of immersive technology. Such advancements will not only enhance the user experience but also reduce the barrier to entry. Just as with connectivity and networks, the development of this hardware is not open virtual world-reliant but rather abuts with other industries, such as entertainment and gaming, leading to a positive synergy that will benefit open virtual worlds space.

Lastly, open virtual worlds, as a decentralised entity, will require advancements in decentralised storage solutions, secure cryptographic techniques, and privacy-preserving technologies, ensuring user data is secure, private, and cannot be manipulated.

LEGAL CONSIDERATIONS

Legal considerations for open virtual worlds are vast and complex, covering a multitude of areas such as digital rights management, intellectual property rights, data privacy and security, identity theft, and cybercrime, to name just a few. The present document provides a more detailed overview in a dedicated section, but briefly, an open virtual world must prioritise user privacy and data protection, which is at risk due to persistent monitoring, deeper profiling, and collection of special categories of data. The European Data Protection Supervisor (EDPS) highlights these considerations, with users being constantly monitored via wearable devices and data collection becoming more comprehensive.

Geographical scope is also an issue, with the GDPR requiring data protection laws to be applicable regardless of the location of digital environments. The GDPR broadly defines personal data, but in an open virtual world, data processing includes sensitive information such as names, addresses, and even wearable device data. Assigning data protection roles is also a concern, especially identifying data controllers in a decentralised environment like open virtual worlds. Despite these issues, the GDPR can potentially empower open virtual world users with various data protection rights. However, open virtual worlds' decentralised architecture might complicate the exercise of these rights, highlighting the importance of data protection by design and default, with solutions like blockchain-based systems playing a vital role.

ENVIRONMENTAL CONSIDERATIONS

As a technology that also relies on blockchain and high-performance computing devices, the carbon footprint of open virtual worlds could be considerable.

At this point, it is worth noting that many products and experiences that individuals value, including but not limited to smartphones and other electronic devices, international travel, and national security, generate considerable carbon. It is a matter of what society values the most to decide where to expend its carbon until we are collectively ready to transition to more sustainable ways of achieving the same results. This discussion applies not only to virtual worlds but also to energy-heavy PoW blockchains such as Bitcoin. Whether we collectively deem the existence of money that can operate in the absence of established institutions – in extremely adverse digital environments – worthy, or the ability to interact in interoperable and open digital environments, or to have access to a world of information through our smartphones beneficial, or whether we prefer one over the other, is a broad and different discussion.

Despite this, open virtual worlds' reliance on high-throughput systems will likely necessitate a flexible and fast blockchain, such as Ethereum, and equally highly programmable systems. These usually do not use energy-heavy consensus mechanisms.

On the hardware side, the production, operation, and disposal of the hardware required to access virtual worlds, like VR/AR devices, have an impact on the environment. This impact arises from the extraction of raw materials, the energy used in manufacturing, and the electronic waste when devices are discarded.

Additionally, the energy required to power the data centres and network infrastructure necessary to support open virtual worlds also contributes to its overall environmental impact.

Hence, the development of open virtual worlds must take into consideration its environmental footprint and strive towards sustainable practices, such as renewable energy sources for data centres, energy-efficient hardware, and circular economy practices for the lifecycle management of electronic devices. It will also necessitate a sincere discussion around what we want to prioritise as a society.

Key Regulatory Considerations

SAFEGUARDING USER PRIVACY AND DATA PROTECTION

Open virtual worlds aim to redefine the relationship of average users with their digital applications and environments. Web 1.0 and Web 2.0 have come a long way in establishing a rich digital user experience. Open virtual worlds, nonetheless, aims to take this experience to a different level. While maintaining some of the key characteristics of existing digital spaces, such as the more decentralized architecture of Web1.0 and the interactive nature of Web 2.0, open virtual worlds strive to create authentic and immersive digital environments, where the limits between the physical and digital lives of the users become more porous and blurred.

However, this transition to more immersive digital experiences must not come at the expense of user privacy and data protection (see Art. 7 and 8 of the Charter of Fundamental Rights of the EU). This key consideration is explored in depth in the present, given the increased consumer and regulatory concern regarding data security and ownership.

Indeed, the creation of immersive digital spaces comes with considerable challenges for the privacy and data protection rights of EU citizens. Perhaps the most comprehensive assessment of the data protection risk profile of virtual worlds has been proposed by the EDPS, which identified three major data protection considerations in immersive digital spaces.

CONTINUOUS AND PERSISTENT MONITORING:

Life in virtual worlds is an always-connected immersive life. Although average users of digital environments are already constantly online, virtual worlds is expected to raise the level of their exposure to monitoring since access to virtual worlds is only possible through wearable tracking and data-collecting devices. Current internet providers usually collect information based on user interaction with websites and mobile apps. Such collection, while expansive and intrusive, is usually more focused on the digital breadcrumbs left behind by users during digital sessions. In open virtual worlds, on the other hand, data collection will happen in a much more comprehensive way. Most importantly, apart from monitoring the digital presence of users, open virtual world instances will most likely have access to data collected from wearable devices and, therefore, they will also be able to monitor the physiological and mental state of their users, obtaining full access to user experiences during each individual session.

DEEPER PROFILING:

As mentioned in the previous paragraph, virtual world platforms (closed or open) will obtain richer and more complicated data from users. This will allow them to create more detailed profiles about each individual user and, therefore, their potential intrusions into user privacy will be much more intense and multifaceted than

what is currently observed in more traditional and non-immersive platforms.

COLLECTION AND PROCESSING OF SPECIAL CATEGORIES OF DATA:

A second life in an open virtual world is a life rich in sensitive data. In open virtual worlds, users will experience physiological and psychological stimuli within immersive digital environments. Wearable devices will continuously monitor and transmit user responses to such stimuli, revealing the full spectrum of their mental and physical state during each session.In addition, user experiences in open virtual worlds will create more dense and complex social interactions. Open virtual world users will express a more comprehensive part of their personality within these immersive spaces and will generally be more invested in their digital alter egos in comparison to their current Web 2.0 digital identities. The possibility of revealing aspects of their private life that relate to their health and mental status or political opinions, ethnic origin, sexual orientation, etc., is, therefore, much higher in open virtual world spaces than it is in traditional digital spaces.

The aforementioned will put user privacy and data protection under pressure. It is, therefore, important to understand the potential relationship between open virtual worlds and the GDPR. While a detailed discussion can be found in the Appendix of this document, a brief overview would be as follows:

- **GDPR's Geographic Scope:** The GDPR could apply to open virtual worlds targeting EU users, irrespective of virtual worlds's physical infrastructure locations.
- **Personal Data in Virtual Worlds:** The GDPR broadly defines personal data, including user account details and avatars in open virtual worlds, with the context determining its applicability.
- **Data Protection Roles:** Identifying data controllers in the decentralized open virtual world is complex, involving core developers and server operators, while users primarily act as data subjects.
- **Identifying Data Controllers:** In the decentralized virtual world, pinpointing data controllers focuses on entities managing the ecosystem's infrastructure and decision-making.
- **User Rights and Privacy:** The decentralized nature of open virtual worlds may challenge the exercise of GDPR rights, underscoring the need for built-in privacy and data protection measures.

Conclusions

ENVISIONING A CONNECTED, INCLUSIVE AND INNOVATIVE FUTURE

The EU can be a key player in shaping virtual worlds, particularly in terms of legal and regulatory frameworks. The GDPR has set a global standard for data privacy and security, a crucial aspect in virtual worlds where user data could be persistently monitored and collected. Inthe realm of digital assets and cryptocurrencies, the MiCA regulation can provide a comprehensive legal framework, fostering transparency and stability in virtual worlds's financial transactions. This could be particularly important for open virtual worlds, which emphasises decentralisation andinteroperability.

In bridging the gap between potential and reality, the EU's role in open virtual worlds becomes pivotal. By harmonizing its established regulatory frameworks with the unique aspects of virtual worlds, the EU can ensure the protection of user rights and the integrity of digital transactions. This synergy would not only uphold high standards of data privacy and financial transparency but also enhance user confidence and participation. Such regulatory guidance is essential for nurturing a thriving, equitable, and secure digital ecosystem, setting a global benchmark for responsible digital innovation.

The resulting open virtual world paradigm, with its potential to fundamentally revolutionize the virtual landscape, would present unique opportunities. Through leveraging cutting-edge technologies and fostering inclusive communities of creators, developers, and enterprises, this new horizon can catalyze unprecedented levels of innovation and competition. These are vital attributes for the long-term sustainability of the virtual space.

The collaborative and open nature of a virtual world could not only accelerate innovation but also ensure fair competition. An open virtual world could prioritize diversity, equity, and inclusion, presenting a viable platform for breaking down socioeconomic barriers and reducing the global digital and financial divide. Such an environment can contribute significantly towards achieving various sustainable development goals, fostering economic growth, job creation, and environmental sustainability.

Appendix

Considerations in Geographical and Subject Matter Scope: Could the GDPR Always Apply in an Open Virtual World? ***Considerations concerning the geographic scope of application of the GDPR.***

Open virtual worlds are by design a cross-border environment, where basic infrastructure and user experiences defy geographical limitations. Nonetheless, Art. 3 of the GDPR will most likely ensure the applicability of the GDPR in open virtual world spaces. Indeed, according to Art. 3, the applicability of the GDPR does not depend on the location of the infrastructure of digital environments but on the geographical footprint of the available goods and services. As long as an open virtual world targets user in the Union, the GDPR will be applicable.

The issue of the scope of the GDPR: What Qualifies as personal data in an open virtual world?

The GDPR provides a very wide definition of the notion of personal data. According to Art. 4(1) of the GDPR: '... personal data means any information relating to an identified or identifiable natural person . . .'. The notion of personal data might appear straightforward. In reality, though, it is heavily context-dependent (see recital 26 of the GDPR) and, therefore, rife with uncertainty. In that sense, the core principles developed by the EDPB (in its former iteration as Article 29 Working Party) and the CJEU in various decisions (e.g., C-582/14 (Breyer) or C-434/16 (Nowak)) will remain important interpretative tools for the adaptation of the notion of personal data to the specific issues and circumstances surrounding open virtual worlds.

In open virtual world environments, there will be many operations that will entail the processing of user personal data. For example, when creating open virtual world accounts/profiles, users will usually have to share personal information with their virtual world instances, such as their name, email, address, or payment and financial details. Such information will qualify as personal data under the GDPR. It must be stressed that the deployment of blockchain-based financial infrastructures instead of traditional banking applications will not necessarily render the GDPR inapplicable. It is generally accepted, for example, that blockchain-based public keys qualify as personal data under the GDPR since they can enable the identification of the users behind them. Open virtual world identities will not be limited to blockchain-based public keys, however. Usually, the registration process will be concluded with the creation of an avatar (i.e., a digital alter ego of each user by which they will participate in the immersive virtual world environments). Whether such avatars constitute personal data under the GDPR or not is a complicated question. On the one hand, the avatar will not always correspond to the real identity of a user. Users can customize the name, appearance, and other characteristics of their digital representations, and they can, therefore, create digital alter egos that are not related to their real-life identities. On the other hand, while avatars might obfuscate the real identity of users and make their identification more difficult, they might also prove to be a rich source of personally identifiable information. The complexity and density of social graphs in an open virtual world will leave ample room for comprehensive user profiling and inferences that might allow open virtual world stakeholders to trace the real identities of users behind their avatars.

The potential to re-identify users in an open virtual world will be substantially reinforced by the quality of interaction in these spaces. Indeed, open virtual world users will not be passive, but they will reinvent their entire digital life in complicated ways, revealing a wealth of personally identifiable information in the process

(including special categories of personal data). In addition, open virtual world operators will also probably have access to the personal data generated by the wearable devices of their users. They will, therefore, obtain real-time information not only about the digital representation of their users but also about their real-life surroundings and whereabouts. This unprecedented wealth of information might make the identification of open virtual world users less difficult than one might originally expect it to be.

Assigning Data Protection Roles and, Most Importantly, Identifying Data Controllers

Out of the three major data protection stakeholders regulated by the GDPR, the roles of the data subject and the data controller will predominantly come into the spotlight in open virtual worlds. The data subjects constitute the main beneficiaries of the GDPR since the entire network of the provisions of the latter aims to empower their position vis-a-vis the other data protection stakeholders. The data controllers, on the other hand, are, quite reasonably, the major recipients of compliance obligations since they define the purposes and means of the processing of personal data (see Art. 4(7) of the GDPR) and benefit from the added value created by such processing.

The assignment of the role of a data subject will generally remain straightforward in an open virtual world. Natural persons who create open virtual world accounts and interact with open virtual world environments will assume the role of data subject since their registration and interaction with the ecosystem will expose their personal information to processing.

The assignment of the role of the data controller, on the other hand, might prove to be more challenging (although not necessarily impossible). Open virtual worlds is a decentralized virtual world. The exact technical underpinnings of open virtual worlds are still under development. Nonetheless, the creation of a federated open virtual world that will draw from the free and open-source traditions and will also incorporate the decentralized ethos of blockchain-based solutions seem rather plausible at this stage. In that sense, open virtual worlds will create governance challenges and, ultimately, GDPR compliance conundrums since the identification of a central controlling entity that will define the means and purposes of the various processing activities will be difficult. This is an issue that appears in many decentralized spaces, most importantly in permissionless blockchains. In that regard, it has been proposed in legal scholarship that decentralized systems ought to be examined on different layers when searching for data controllers.

In the grand scheme of things, the effort to assign the role of the data controller in a decentralised open virtual world should focus on processing activities related to the creation and maintenance of the digital environment. Viewed from this angle, open virtual world spaces will usually depend on core developer teams and a nucleus of fundamental instances that will be in control of the major decisions related to the ecosystem. A decentralised open virtual world might not necessarily be a fully decentralised open virtual world (full decentralisation might even not be tenable or desirable), but it might include certain points of centralisation. While the identification of such controlling entities will not always be straightforward, it will also not be impossible. In addition, if open virtual worlds is supported by a federated architecture, the individual open virtual world servers might also constitute data controllers, at least with regards to the creation, development, and maintenance of their individual open virtual world access points.

When one looks beyond the core processing activities related to the creation and maintenance of open virtual worlds space and focuses on peer-to-peer interactions, open virtual world environments might not be very different from other digital spaces. In peer-to-peer interactions, the users will be in control of the purposes and means of the processing activities. For example, if user A wishes to interact with user B in an open virtual world and personal information is mutually disclosed in the process, then users A and B will assume the roles of the data controller vis-a-vis one another since they are the only stakeholders deciding about the purposes

(i.e., their individual interaction) and the means (i.e., the particular open virtual world platform of their choice) of their interactions.

User Rights and Privacy by Design

The previous sections discussed the major applicability questions of the GDPR in open meta- verse environments.

Provided that the applicability of the GDPR is established, this will allow open virtual world users to benefit from the set of data protection rights established in the GDPR: information rights (Art. 12-14 GDPR), the right to access one's personal information (Art. 15 GDPR), the right of rectification (Art. 16 GDPR), the right to erasure (Art. 17 GDPR), the right to restriction of processing (Art. 18 GDPR), and data portability (Art. 20 GDPR) will all become available to open virtual world users, setting the framework of their data protection empowerment.

Nonetheless, the open and decentralised architecture of open virtual worlds might create obstacles to the exercise of such rights. It might also have an impact on their effectiveness. In closed and centralised systems, the exercise of GDPR rights is usually more straightforward. A decentralised open virtual world, on the other hand, might lack a core centralised entity that is in control of the ecosystem. It might not, therefore, be equally capable of ensuring full compliance with the GDPR since the diffusion of power and control might make the compliance process more resource-intensive and demanding.

Privacy and data protection by design and default (see Art. 25 of the GDPR) might, therefore, play a major role in open virtual world environments. Indeed, if the decentralised architecture of open virtual worlds renders an ex-post enforcement of user GDPR rights impracticable, ex-ante data protection assurances incorporated and hard-coded into the system will be necessary. Blockchain-based solutions might provide strong foundations for key data protection qualities such as self- sovereign identity management, data minimisation, accuracy, and integrity of user personal data, although further research and development of GDPR-compliant architectures will still be necessary.