



The Metaverse:

Policy Implications For A New Digital Frontier

FOREWORD



This white paper addresses some important policy implications of the metaverse. This seminal document reflects our commitment to facilitate the shaping of our shared digital future and promoting responsible and inclusive participation in the digital space.

Recent advancements in technology have ushered in an unprecedented era, blurring the lines between the physical and digital realms. The emergence of the metaverse holds tremendous potential to reshape our lives and revolutionize the way we work, learn, socialize, and interact with one another. The metaverse can unlock novel economic opportunities and empower individuals with new means of expression and creativity. By 2026, a quarter of the world's population will spend at least one hour every day in the metaverse.

Indeed, this new frontier for human interaction and innovation has the capacity to address some of the pressing global challenges using solutions that were previously unimaginable. However, as with any revolutionary advancement, the metaverse accompanies a myriad of complexities and policy implications that demand our collective attention. It is incumbent upon us, as global leaders and policymakers, to craft policies that ensure that the metaverse's development is human-centric, and its adoption and utilization are open, inclusive, sustainable, and safe.

To achieve these objectives, collaboration between governments, industry, civil society, and academia is paramount. The Digital Cooperation Organization is committed to playing a key role in facilitating collaboration and coordination among diverse stakeholders, fostering international cooperation and global consensus on metaverse-related policies and regulations.

In this white paper, the combined expertise of the Digital Cooperation Organization and Whiteshield is leveraged to navigate this uncharted terrain. The paper examines the architecture and transformative power of the metaverse and its challenges and presents key insights and recommendations – while differentiating between policies that impact

the broader ecosystem and those that shape user experiences within it. With an emphasis on building an agile and balanced, innovation friendly regulatory framework, this paper underscores the need for proactive multistakeholder approach to policymaking, engaging diversified stakeholders, especially the private sector, and avoiding excessive restrictions.

We encourage policymakers and stakeholders to engage in constructive dialogue and collaborative endeavors to shape the metaverse's policy landscape for the benefit of all. By promoting responsible practices and fostering sustainable growth, we can strike a balance between nurturing an environment of innovation and safeguarding individuals and businesses from potential negative implications.

The Digital Cooperation Organization stands ready to support these joint efforts, providing guidance, expertise, and resources to navigate this evolving digital realm. When we uphold human-centric values and work together in the spirit of cooperation, we harness the potential of transformative technologies in ways that enhance lifestyles, strengthen connectivity, drive economic growth, and contribute to global prosperity – bringing forth a more inclusive, innovative, and safe digital era that enables prosperity for all.

Finally, I extend my gratitude to the dedicated teams from the Digital Cooperation Organization and Whiteshield who have contributed their expertise, research, and insights to this white paper. Their commitment to advancing global dialogue on the metaverse is commendable, and I have full confidence that this white paper will serve as a cornerstone for future policy discussions.

Deemah AlYahya
Secretary-General
The Digital Cooperation Organization

EXECUTIVE SUMMARY

The purpose of this white paper is to offer insights into the definition, development, and functionality of the metaverse, and to elaborate on its policy implications. It presents recommendations for policymakers and stakeholders to harness the opportunities presented by this transformative technology and address the challenges associated with its development and adoption.

Metaverse, as a progressing paradigm of the next generation internet, and a natural extension of Web 3.0 intends to create a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space for humans to interact, play, work, and socialize. Various surveys and studies have revealed that the metaverse economy will experience exponential growth soon. According to Gartner, by 2026, 25% of the world's population is likely to consume at least one hour a day in the metaverse for activities like entertainment, working, shopping, attending schools, and socializing¹. Analysts forecast that by 2030, there will be up to five billion metaverse users, and the metaverse economy by then, according to different estimates, could grab between US\$5 trillion to US\$13 trillion of value^{2 3}.

This paper provides an overview of what the metaverse means, articulates some of its policy implications, and introduces a set of its potential applications and use cases. The paper starts by defining the metaverse based on its key features, attributes, and current uses. To support the definition, we first explore its historic evolution through the lens of three distinct waves of technological development: Web 1.0, 2.0, and 3.0. While Web 1.0 focused on static content consumption and while Web 2.0 emphasized user-generated content and social networking, Web 3.0 is now introducing decentralization, interoperability, and AI-powered personalization.

The metaverse extends these advancements by integrating immersive VR and AR technologies, and fostering a digital universe where users can dynamically interact in real-time with each other and their digital environments. The paper will expand on these evolutionary waves in more detail.



As an interconnected and immersive space, the metaverse builds on prior web generations to push the boundaries of digital experiences. This new wave represents the next frontier in internet evolution, enabling richer interactions and greater possibilities for creativity, collaboration, and innovation across various sectors, from entertainment and socialization to education and commerce. The metaverse is a complex layered system that enables users to interact, create, and collaborate in a virtual ecosystem. It encompasses digital infrastructure, network protocols (a set of rules to send or receive data over the computer networks), consensus mechanisms, transaction execution, and user applications.

We also explore several challenges and opportunities related to the development and growth of the metaverse. These challenges span digital identity, property rights and ownership, transacting and exchanging, accountability, security, interoperability, and digital inclusion.

The paper then details a set of policy implications of the metaverse for the stakeholders, particularly for the policymakers, with an aim to understand how they can shape a human-centric, accessible, sustainable, and inclusive metaverse. The modality of doing so entails a pronounced focus on a range of principles that are treated separately. This section establishes the policy recommendations, highlighting the need for having effective multi-stakeholder engagement and collaboration amongst national and international stakeholders and across the governments.

Finally, the paper explores some notable use cases of the metaverse, discussing both their potential and current limitations or challenges, and presenting some policy considerations associated with each use case.

TABLE OF CONTENTS

Introduction	07
Defining The Metaverse	11
Possible Architecture Of The Metaverse	12
Transformative Power Of The Metaverse	14
Challenges And Potential Obstacles	15
Policy Recommendations	20
Recommendations That Are Exogenous To The Metaverse	21
Recommendations That Are Endogenous To The Metaverse	26
Metaverse Use Cases And Policy Considerations	32
Entertainment	33
Work And Education	35
Socialization	36
Healthcare	37
Commerce	38
Industrial Metaverse	40
Conclusion	42
Bibliography	45

Disclaimer, and Copyrights

The analysis and drafting of 'The Metaverse: Policy Implications For A New Digital Frontier' was conducted by Whiteshield and the DCO based on direct advisory experience by Whiteshield and the DCO team. The Paper and any opinions expressed in this publication are views of the authors, and may not necessarily reflect those of Whiteshield and the DCO. All efforts were made to compile data that is as accurate and as recent as possible based on available international sources. Whiteshield and the DCO do not take any responsibility for data that may be inaccurate.

Copyright © 2023 by Whiteshield and the DCO

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise without the prior permission of Whiteshield and the DCO.



METaverse

INTRODUCTION

The concept of the metaverse has gained significant attention in recent years. Advances in technology are progressively enabling the creation of boundless virtual ecosystems where people can interact, create, and collaborate in ways that were previously impossible. Industries are also leveraging virtual technologies to improve their efficiency and productivity and investing heavily in harnessing their full potential. This paper targets policy and decision makers including government officials, regulators and representatives from relevant industries and seeks to provide an overview of what we mean by the metaverse and to provide recommendations to the stakeholders including policymakers on how they can effectively and collectively respond to the challenges that arise from its development and adoption.

History and evolution

The notion of the metaverse has its roots in science fiction, with early references dating back to Neal Stephenson's 1992 novel "Snow Crash". Stephenson's metaverse is a virtual reality universe where users can interact with one another as well as with various digital objects. Since then, the concept made its way to other books, movies, and games including "The Matrix", "Ready Player One", and "Second Life". However, only now does the vision of a fully operational and functioning metaverse seem close to becoming a reality.

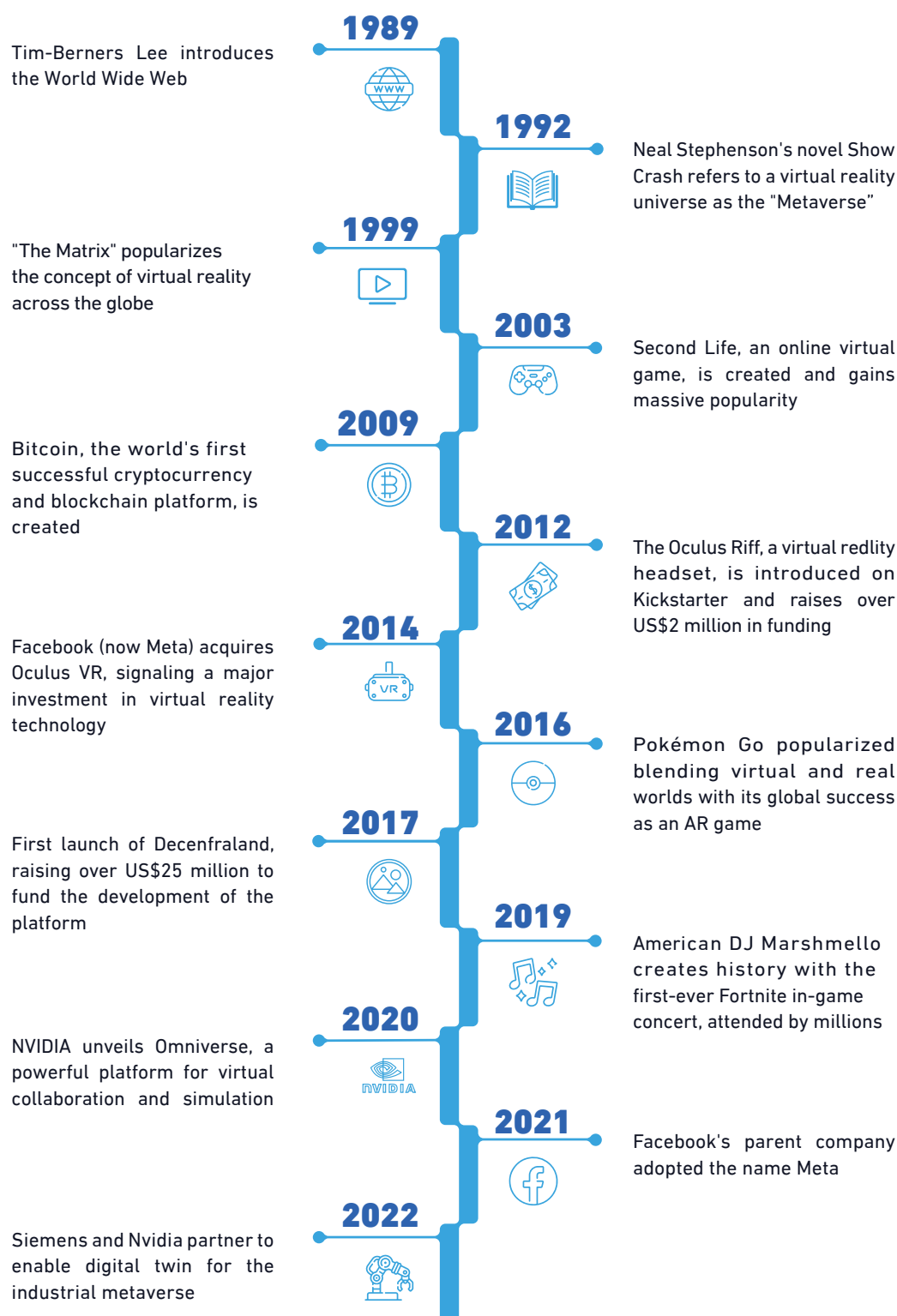


Figure 1: Evolution of the Metaverse

Source: Whiteshield.

Prior to offering a definition of the metaverse, it may be valuable to understand the historical development of one of its fundamental enablers and building blocks - the Web. The evolution of the internet as we know it is often depicted through the lens of three distinct technological waves.

The first wave, or Web 1.0 emerged in the early 1990s, with the creation of the World Wide Web. It democratized “access to information” with an emphasis on static content consumption produced predominantly by companies and institutions. Users were restricted in the scope of their activities and limited to viewing information on web pages.

The second wave or Web 2.0 emerged in the early 2000s and emphasized user-generated content and social networking. As a result, it came to be known as the period of the “participative social web” and helped democratize “content generation”. Platforms such as Facebook, Twitter, and YouTube emerged as dominant players, and enabled users to interact with each other and share content in real-time. Most importantly, this second evolution validated the willingness of many users to engage with each-other by creating and sharing information and to actively participate in online communities that reflected their interests, aspirations, or ideals.



Web 3.0 is the third wave of this evolutionary journey. While still unfolding, it is characterized by the convergence of various emerging technologies that span virtual and augmented reality, artificial intelligence, and decentralized ledger technologies among others.

The confluence of these and other disruptive technologies is radically transforming the way we interact with and utilize digital and virtual platforms. It is rapidly paving the way to a more immersive and interconnected experience built around new forms of digital assets and economies. Web 3.0 is ushering in an era of a personal and immersive web, focused on peer-to-peer interactions where data is personalized and the reliance on middlemen minimized⁴.

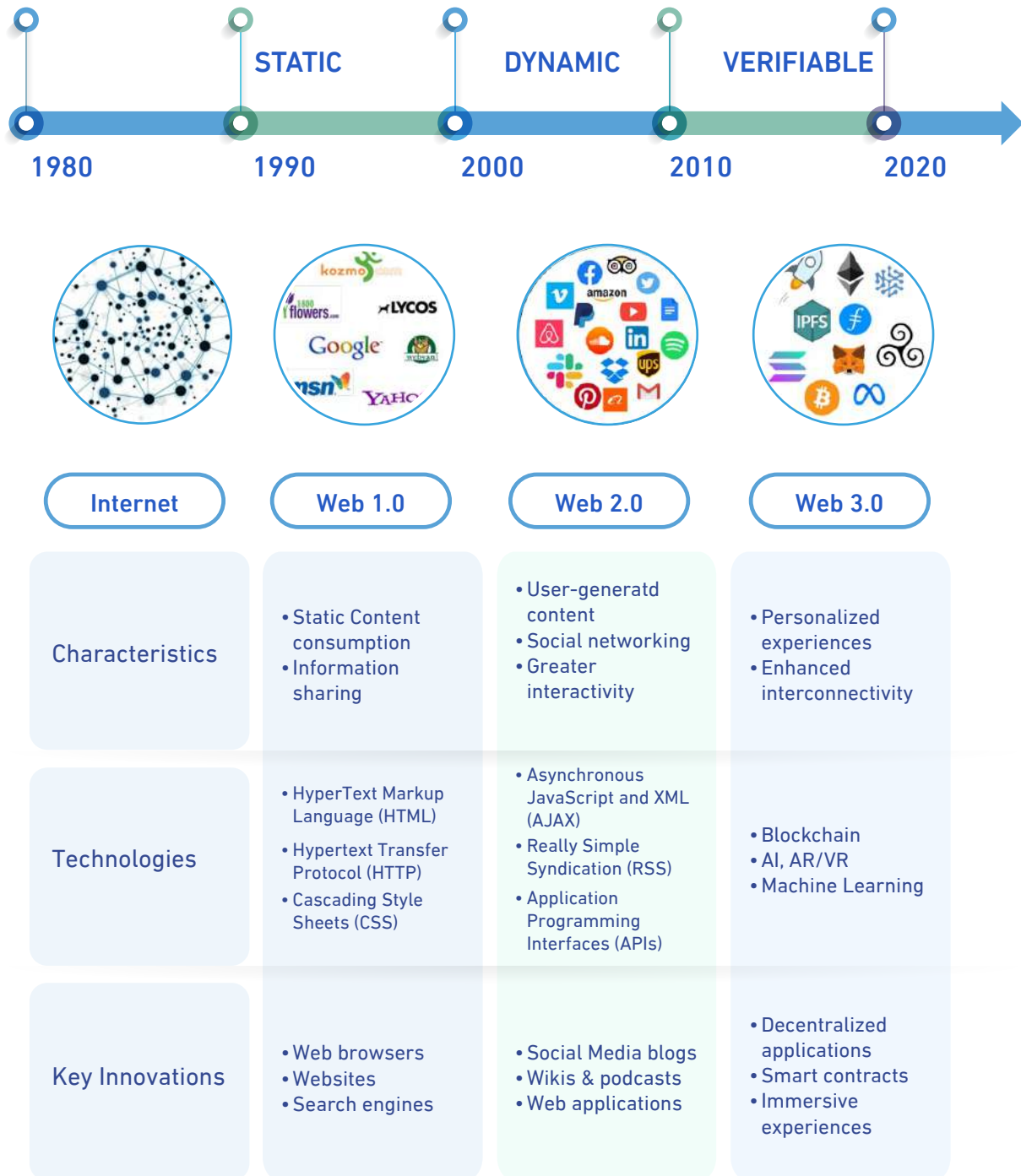


Figure 2: Evolution of the Web

Source: Whiteshield.

Defining The Metaverse



In light of this on-going evolution, many definitions of the metaverse have emerged. A widespread description refers to the metaverse as the medium through which netizens will eventually experience future manifestations of the internet.

Under such a depiction, Web 3.0 and the metaverse are perceived as separate evolutions of the internet with the former focused on its underlying governance, its decentralized nature, and its modus operandi, and the latter confined to an interactive layer that manifests itself in the way users work, socialize, interact, and immerse themselves on the internet.

Clearly, such a focus emphasizes the role played by a subset of disruptive technologies that can transform the way users interact with the web and that includes, without being limited to, Augmented, Virtual and Mixed Reality, and Digital Twin technology. However, our definition transcends this immersive and experiential nature to include other enabling building blocks that form an integral part of Web 3.0.

In this paper we define the metaverse as a natural extension of Web 3.0 with a pronounced focus on the immersive aspect of the users' experience.

Possible Architecture of the Metaverse

Consequently, and akin to the internet, we describe the metaverse as a complex layered system. Each layer is built atop its predecessor and contributes to an ever-increasing universe of functions and services meant to provide users with unique avenues to interact, create and collaborate. In this system, users can

interact in real-time with one another, digital objects, or their environment. This is typically done with the help of avatars which serve as a digital representation of users within a virtual ecosystem. Beyond enabling social interactions, avatars can also offer a means of self-expression and identity formation.

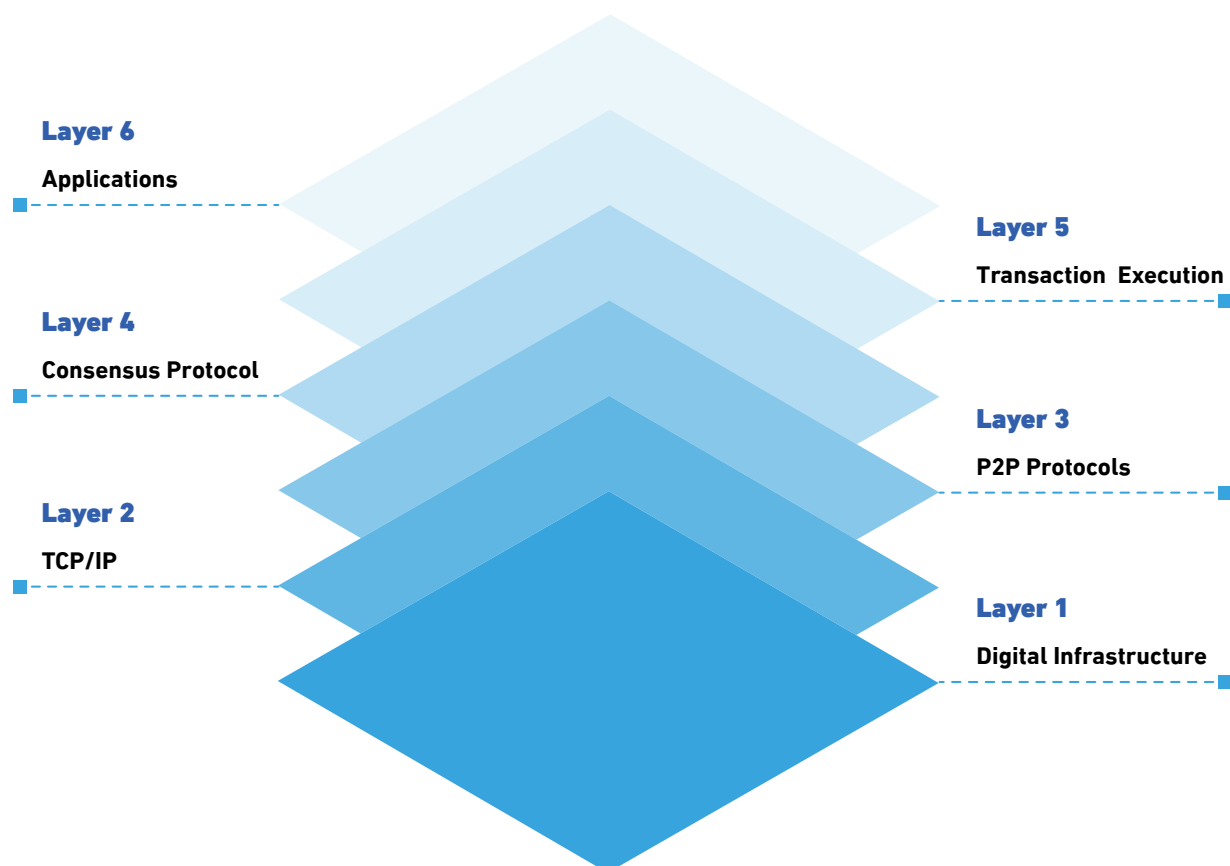


Figure 3: Layers of the Metaverse

By virtue of being an extension of Web 3.0, the metaverse inherits its foundational principles. A particular subset of those principles that includes decentralization and interoperability carries significant implications for its underlying architecture. More specifically, the metaverse layered system would revolve around:

Layer 1 – Digital Infrastructure

A first layer, consisting mainly of digital infrastructure, hardware, and devices that also encompasses network, storage, and compute functionalities. This layer comprises a range of essential components such as 5G and future-generation 6G, cutting-edge AR/VR headsets for immersive experiences, powerful quantum computing systems and efficient edge computing solutions for low-latency processing.

Layer 2 – Network and Transport

A second layer, consisting of the Transmission Control Protocol and the Internet Protocol (TCP/IP), and which corresponds to the internet as we know it.

Layer 3 – Peer-to-Peer Protocols

A third layer encapsulating peer-to-peer (P2P) protocols to allow individual users to interact and communicate with each other without relying on a central server. Such a layer is a necessary building block of a decentralized governance model that our definition of the metaverse should cater for.

Layer 4 – Consensus Protocol

A fourth layer that implements the desired consensus protocol and that embeds relevant cryptography primitives. This too, is an essential ingredient to the successful implementation of decentralized governance. Simply put, a consensus protocol defines and upholds the rules of the game and implements algorithms to ensure that agreement is reached among the network participants. The resilience and immutability of consensus has far-reaching implications on the security and reliability of the network.

Layer 5 – Transaction Execution

A fifth layer focused on execution and successful completion of interactions and transactions. Payment processing, value transfer, and content exchange would be conducted at this level. While the previous layer optimizes the security and the decentralization of the metaverse, this layer is mainly concerned with scalability and speed. This layer covers elements like Digital Identity, Smart Contracts, Digital Assets etc.

Layer 6 - Applications

A sixth layer that includes the web browser, user platforms, various software applications and services that run on top of the metaverse and that serve as the main point of touch for most users.

Transformative Power of the Metaverse

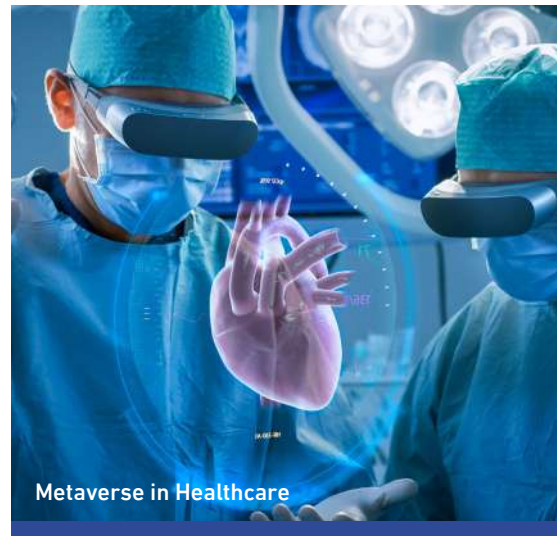


It is no secret that the metaverse has the potential to significantly elevate the levels of its users' collaboration and innovation. Users can interact, share ideas, and create content in new ways that could lead to the development of ground-breaking products, services, and solutions.



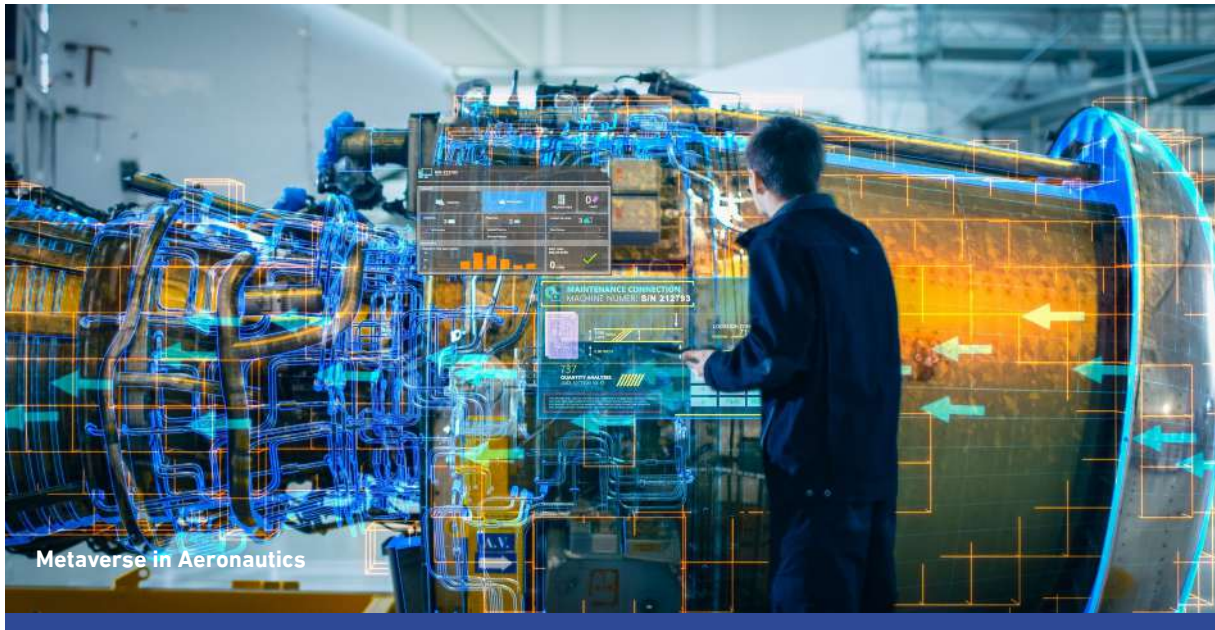
Metaverse In Education

In education, for example, virtual environments can provide immersive and interactive learning experiences that are not possible in traditional classrooms. The metaverse can enable students to visit virtual museums, travel to different parts of the world, explore complex scientific concepts, collaborate, boost teamwork, and benefit from lifelong learning and training platforms regardless of location or socioeconomic status.



Metaverse in Healthcare

Similarly, in healthcare, virtual environments can be used to simulate medical procedures and train healthcare professionals in a safe and controlled way. This could pave the way to improved access to healthcare, particularly for individuals in remote or underserved areas.



Furthermore, the coupling of virtual environments with Digital Twin technology can play a significant role in improving industrial efficiency and safety. For example, the industrial metaverse can help optimize production processes, reduce downtime, run immersive training programs, perform simulation-based testing, and support with remote assistance, maintenance, and repair.

Challenges and Potential Obstacles

While the metaverse represents a new frontier for human interaction and innovation, several challenges remain to be addressed. The emerging complications tend to be of four types:

Those related to the user's identity in the metaverse

Those associated with ownership and usage of digital goods and services

Those pertaining to the user's immersive experience and the way users transact and interact

Those affecting various enablers of collective user experience on the metaverse

These challenges should guide and inform future policymaking to ensure an optimal resolution that guarantees the successful adoption of a well-functioning metaverse.



Digital Identity: One of the main complications in the metaverse consists of creating and maintaining a secure and reliable digital identity. Users' successful interactions in virtual environments will be contingent upon proving their identity to participate in various activities.

At a bare minimum, the path to resolution will require a framework that facilitates digital identity authentication, reins in identity theft and fraudulent activity, and protects users' privacy by default.

Property Rights And Ownership:

The metaverse is a space where digital content is created, owned, shared, and consumed. As such, this digital dynamic pose numerous challenges pertaining to the custody and control of digital property, the lending, renting, and sharing of digital assets, as well as personal data ownership, data management and the protection of other intangibles such as intellectual property rights. These complications highlight the importance of a robust legal framework and resilient infrastructure that safeguards the scarcity of digital property and upholds ownership rights in all its manifestations.

Accountability: Decentralization can make it difficult to hold individuals and entities accountable for their actions. For example, in virtual environments, there may be instances of harassment, fraud, or other illegal activities, and it may be challenging to identify and hold the responsible party accountable. This calls for mechanisms to ensure that users are protected and that the metaverse remains a safe and secure environment for everyone.

Transacting And Exchanging: In the metaverse, transactions involving virtual assets in all their forms can be executed at the speed of light, in real-time, twenty-four hours a day, seven days a week. This contrasts with traditional settlement platforms where execution timelines are usually laxer. Such a regime would require rethinking the dynamics of assets custody, lending and rehypothecation. Furthermore, the metaverse built on top of a decentralized governance would pave the way to a higher degree of freedom in transacting and exchanging as enabled by its peer-to-peer nature.

A major implication is that the level of transparency around interactions may be significantly reduced and in turn, could limit the effect of traditional regulatory enforcement techniques. Another implication is that the treatment of taxes will likely be more challenging.

Data Privacy: Within the metaverse, platforms and service providers will have the capability to gather extensive personal data from users, including



sensitive information like healthcare records or individual preferences obtained through methods such as eyeball tracking. There remains a risk of malicious actors impersonating other users in order to acquire personal data, or the data could potentially be leaked to third parties. It is essential to address these privacy concerns and ensure that robust measures are in place to protect individuals' personal information within the metaverse.

Security: A necessary condition for the implementation and adoption of the metaverse is to have robust security protocols embedded across all its building layers. Achieving the highest levels of security can prove to be extremely challenging. The consensus and cryptography layer would play a critical role toward achieving this endeavor, especially that it helps provide a reliable source of truth that can be leveraged by all applications.

Interoperability: The metaverse is not a monolith and will likely consist of a multitude of platforms, that might be heterogeneous in their design and

functionality. As a result, it is critical that any implementation addresses the challenge of accessibility and interoperability to ensure that users can seamlessly move between different platforms without compromising their data or jeopardizing their identity.

Digital Inclusion: The metaverse has the potential to create new opportunities and experiences for people, but it also has the potential to exacerbate existing social inequalities due, in part, to relatively high costs and inadequate digital literacy to use the requisite advanced technologies. It is important that the metaverse remains sustainable and accessible to all, regardless of socioeconomic status, abilities or disabilities, and geographic location.

Big Data Challenge: The metaverse will contain a massive amount of structured and unstructured data generated through different sources including XR or IoT devices. This could generate a number of challenges regarding how big data is gathered, integrated, stored, analyzed, and shared with stakeholders.



COMPLEXITIES

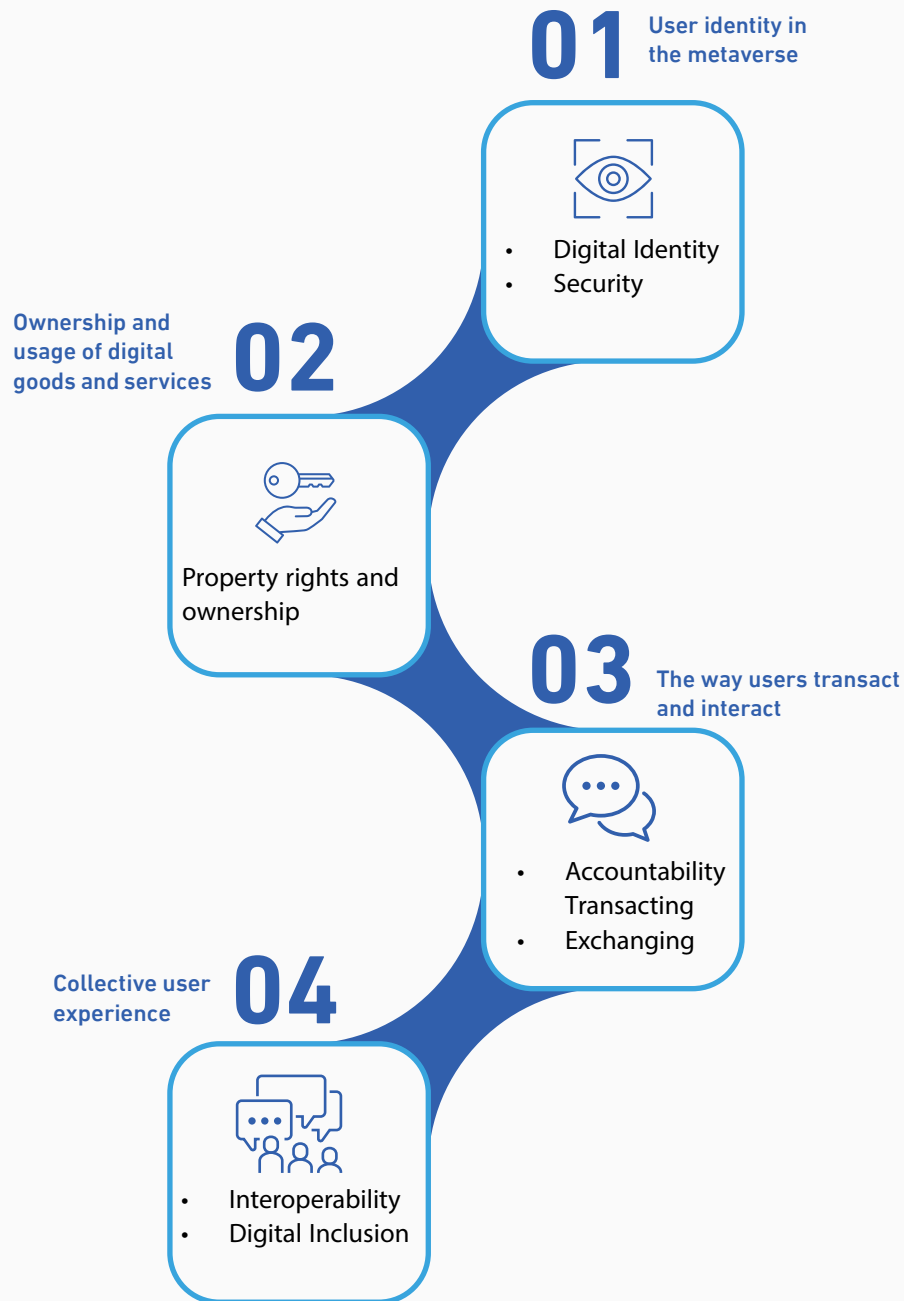
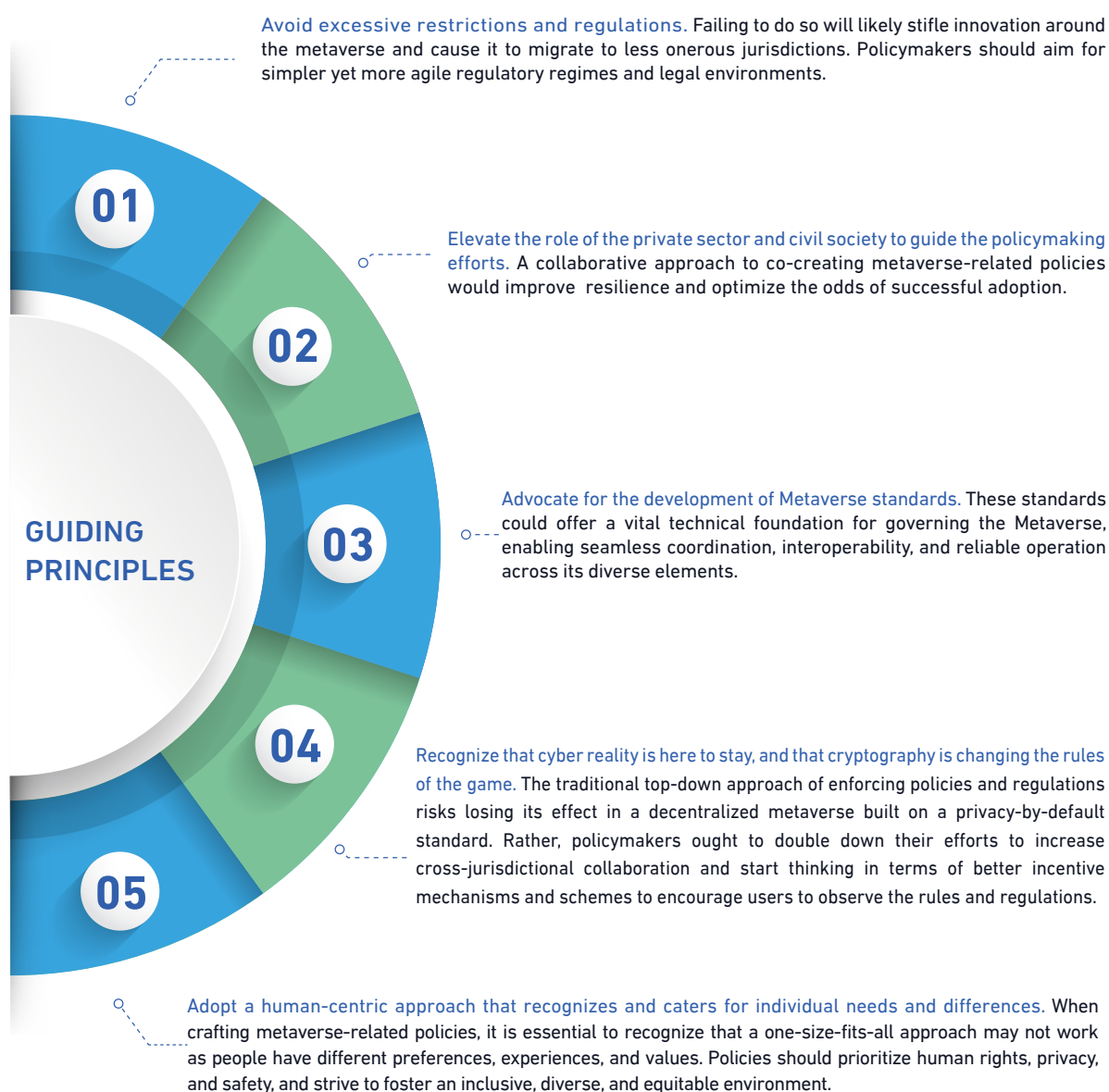


Figure 4: Complications and Challenges

Governments and policymakers should always aim to enhance the quality of life in their societies, and one way to achieve this is by promoting the seamless integration of technology into the daily lives of their residents. Far from being a straightforward task, the effective integration of the metaverse could pose an uncommon challenge to the policymakers: navigating a new paradigm of decentralized governance.

Before discussing some of the potential implications on policymakers in the next section, we conclude this introduction with a set of guiding principles to formulate more effective policies and prepare better for the advent of the metaverse:





POLICY RECOMMENDATIONS

The evolution of Human civilizations points in a direction of rising structure. The collective genius of men, women and increasingly, intelligent machines, enables the advent of ever more complex systems with an ever-larger degree of order and richer set of relationships. This apparent order is often designated as a source of predictable behavior and recognized as a basis for efficiency gains and productivity.

However, orderly behavior is illusive. Many decision makers struggle to grasp that our world is best described as a complex system. Although deterministic in nature, such systems remain highly sensitive to initial conditions and require complete knowledge of the present state to be able to make any meaningful projection. As a result, in such systems, it remains hard to predict the evolutionary course of events, let alone meaningfully control outcomes of planned actions.

The emergence of exponential technologies, including the metaverse, are adding to the complexity of our world. This premise implies that a more judicious approach for policymakers would be to part way with the prevalent thinking that “more is better”.

In the policymaking realm, onerous rules, not necessarily based on evidence, could immediately turn counterproductive and in the process, cause many policies to fail at

fulfilling their *raison d'être*: enhancing the living standards and conditions of citizens.

As the metaverse continues to take shape, policymakers ought to distinguish between two broad sets of policies: those that affect the wider ecosystem that enables the emergence, development, and continuous innovation around the metaverse, and those that impact a user's immersive experience within it.

Recommendations that are Exogenous to the Metaverse

A. Continuously promote and enable entrepreneurial ecosystems.

The metaverse is a project in gestation. Its evolutionary path, like that of many previous ground-breaking technologies, will be significantly influenced and shaped by entrepreneurs and startups that dare to challenge the status quo and push the boundaries of what is possible. Metaverse will provide entrepreneurs and startups with an opportunity to redefine their human interactions, hence offering novel and innovative products and services.

Rather than constraining the very foundation of innovation around it, policymakers are encouraged to put forth policies that enable creativeness and empower the conception of new value-adding functionalities, products, and services for the metaverse. At the very least, such policies would facilitate access to finance, incentivize enhanced business support, mitigate onerous consequences of a legacy regulatory environment, protect intellectual property, reduce barriers to

cross-border expansion, enable cross-jurisdictional mobility of entrepreneurs, and expedite commercialization.

More specifically, policymakers should pave the way to the emergence of a financial infrastructure that answers the needs of entrepreneurs and startups. National financial policies could be revised to cater to this need.

This would include the promotion of angel investing, the anchoring of a seed funding ecosystem, the improvement of public capital markets, access to crowdfunding and other forms of granular capital support, and the streamlining of debt markets.

In addition, policymakers should enable a more sustained level of entrepreneurial business support geared toward risk takers that are advancing the development and adoption of the metaverse. For example, they could embed frameworks to incentivize industry network support, the creation of incubation and acceleration platforms, and the access to necessary utilities and shared services such as telecom, internet, legal,

and accounting services. Governments can incentivize or partner with the private sector to develop state of the art facilities to encourage innovation using emerging technologies.

Visa, for example, operates multiple innovation centers and runs initiatives around the world to provide their partners and clients with the facilities to conduct pilots/ proof of concepts on the financial solutions using emerging technologies, and offer them training and mentorship⁵.

In line with the principles of the New Digital Deal, the Ministry of Science and ICT (MSIT) in the Republic of Korea has unveiled a range of government-backed initiatives to foster an enabling ecosystem for the metaverse. These initiatives encompass the establishment of a Metaverse Academy to cultivate skilled professionals, the provision of dedicated facilities and metaverse hubs to support specialized companies, and the facilitation of core immersive content and technology development for the realization of a hyper-immersive metaverse. By actively promoting these measures, the MSIT aims to fuel the growth of the metaverse and empower innovative enterprises in this transformative realm⁶.

Furthermore, policymakers should collaborate internationally to lower the barriers that challenge the cross-border expansion of innovative digital start-ups. These barriers can hinder innovation by preventing entrepreneurs from accessing new markets, resources, and talent. By lowering these barriers, tech entrepreneurs and startups can benefit from increased access to capital, expertise,

and customer bases, enabling them to scale their businesses more effectively.

In many instances, legacy regulations around bankruptcy treatment, intellectual property protection, labor, and contract enforcement demotivate creative individuals from initiating their entrepreneurial journey. By revisiting their jurisdiction's older regulatory regimes, policymakers could catapult entrepreneurial activity and play a fundamental role in enabling innovation.

B. Support experimentation and enable accelerated pathways to gain regulatory approvals for metaverse innovators.

Regulatory sandboxes and live-testing environments are controlled systems where innovators can test their metaverse projects and applications without the risk of regulatory penalties. A direct consequence of such a model is bringing regulators closer to the industry. It helps set-up a constructive bilateral communication channel between regulators and innovators and enables a nimbler regime whereby regulators can accelerate their learning and innovators can test the impact of their creations in a risk-minimized environment.

The broader societal, cultural, and economic implications of the metaverse remain unknown. Considering this uncertainty, tools such as regulatory sandboxes, can mitigate the spreading of undesired and adverse effects by testing the practicality of an innovation prior to its full-fledged market deployment. Furthermore, if such testing reveals strong consumer and end-user benefits, access to the market could be further accelerated through the grant of faster authorization.

As an example, The Saudi Arabian Monetary Authority (SAMA) has updated its regulatory sandbox framework to promote collaboration between fintech startups, financial institutions, and regulators. The new framework streamlines the testing and evaluation process for new products and services, and includes guidelines on data protection, privacy, anti-money laundering, and cybersecurity⁷.

Furthermore, the EU Commission has recently adopted a new strategy on Web 4.0 and virtual worlds. Through this strategy, the commission aims to pave way for the needed assistance and funding to the digital creators in the virtual space so they can test new tools, improve dialogue and collaboration between developers and industrial users. The strategy also recommends developing regulatory sandboxes for virtual worlds and Web 4.0 to encourage innovation⁸.

As part of the New Digital Deal, the Republic of Korea's government is actively improving metaverse-related laws and regulations, developing ethics principles, and establishing a self-regulation system. These initiatives aim to create a responsible and accountable metaverse ecosystem that prioritizes user protection and privacy while promoting ethical conduct⁹.

C. Promote investment in Research and Development (R&D) and encourage a sustainable evolution of the metaverse.

The sustainability, inclusivity, and accessibility of the metaverse depend heavily on its enabling infrastructure. The observance of this triad necessitates high-speed internet

connectivity, significant computing power, and sustainable energy resources.

To achieve this, policymakers would need to enable the expansion of broadband access to underserved communities and rural areas and prioritize the usage of environmentally friendly energy resources.

To further encourage R&D in metaverse-critical technologies including e.g., Artificial Intelligence, blockchain, Virtual, and Augmented Reality, policymakers could help extend financial incentives to eligible investors. They could encompass tax credits, grants, as well as other forms of financial assistance to help reduce the risks and costs associated with investing in new and untested technology. Most importantly, such mechanisms would signal to the broader community that the government is committed to supporting the growth and development of metaverse.

Policymakers could also play a more pronounced role by working alongside the private sector to fund dedicated research and facilitate the relevant institutions to set-up metaverse research labs, incubation centers and innovation hubs to attract and retain talented researchers and metaverse builders.

To foster the development of metaverse technology, KPMG has joined forces with Microsoft, Ericsson and MetaKey to launch a Metaverse and Digital Twin Hub in Saudi Arabia. The initiative will leverage a series of investments, including Microsoft's development of a new cloud data center, and help drive the digitalization of the Kingdom in various industries¹⁰.

D. Uphold the neutrality of relevant protocols and support interoperability standards

Simply put, protocols consist of rules that govern how information is communicated and exchanged between different parties. One could argue that the success of the internet is in big part due to the neutrality of its underlying protocols which include e.g., TCP/IP (Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hyper Text Transfer Protocol), or FTP (File Transfer Protocol). Such protocols remained open and were jointly developed by a consortium of disparate entities including representation from the government, the private sector, academia, and Non-Profit Organizations (NGOs). Most importantly, these protocols were never subjugated to the control of any particular entity.

The metaverse's layered architecture relies on the internet's enabling protocols. However, it also relies on a gamut of new protocols concerned with the exchange of value, the communication of identities, and the management of digital property among others. Like the internet, it can be argued that the metaverse's future success and widespread adoption is contingent on the openness and neutrality of many of its enabling protocols.

However, such openness does not preclude policymakers from participating in the definition of specific metaverse standards. In this context, a standard can be thought

of as a formalization of a protocol with the objective of securing acceptance by a majority of stakeholders. The Republic of Estonia is an example of a country whose government has successfully created a digital society and an enabling infrastructure through an approach that factored in neutrality and interoperability¹¹.

In a collaborative effort, leading standards organizations and companies joined forces in 2022 to establish the "Metaverse Standards Forum." Open to any organization, this initiative seeks to provide a venue for cooperation between standards organizations and companies to foster the development of interoperability standards for an open and inclusive metaverse, and accelerate their development and deployment through pragmatic, action-based projects. By fostering collaboration and setting standards, the forum seeks to facilitate seamless interaction and connectivity across diverse metaverse environments¹².

A direct consequence of enabling seamless exchange through an interoperability standard would be to spur innovation and improve the overall end user's experience. Policymakers could then reserve a more pronounced regulatory intervention to the metaverse's application layer, where they could create compliance requirements tailored to the specificities of each sector and activity.



E. Build bridges and foster cross-jurisdictional collaboration.

One of the main challenges that ensue from the global nature of the metaverse is the need for cross-jurisdictional harmonization. In the absence of such large-scale coordination, there exists a substantial risk that users will be subject to conflicting standards and regulations. For example, different jurisdictions may have different rules governing data privacy or intellectual property. This would make it challenging for companies to seamlessly operate in the metaverse, or for creators to ubiquitously protect the fruits of their labor.

A necessary condition for the successful deployment of the metaverse is to ensure a productive multi-stakeholder collaboration especially between the governments. In this regard, the promotion of inter-governmental collaboration is critical to

the development of a global perspective on standards that can in turn prevent the establishment of fragmented regulatory regimes.

It is worth noting that the European Parliament has highlighted the need for a “shared model” as the absence of borders will likely challenge the prevalent notion of territorial sovereignty¹³.

The International Telecommunication Union (ITU) has recognized the importance of fostering cross-jurisdictional collaboration and building bridges across the metaverse ecosystem. To this end, it has created a focus group to examine the technical, economic, and policy implications of the metaverse and promote cooperation among a wide range of stakeholders from different regions and jurisdictions¹⁴.

Recommendations that are Endogenous to the Metaverse



F. Devise a framework to anchor the metaverse's identity management and data protection model on solid ground.

We previously articulated the importance of creating and maintaining a system that safeguards the security and reliability of digital identity in the metaverse. Such a system should address challenges associated with identity authentication, identity theft, and more broadly, challenges around upholding users' data privacy.

In all likelihood, enabling the creation of such a system cannot be accomplished in isolation. Earlier, we highlighted the need for multi-stakeholder collaboration.

Specifically, policymakers should work closely with the technology industry to put forth standards and best practices for digital identity management. One of the merits of such a joint effort is to help elucidate the technological capabilities and limitations of digital identity systems and to ensure their alignment with the principles of privacy, security, and user control.

Collaboration with the technology industry would be a step forward in helping policymakers conceive of a clear legal framework to regulate digital identity systems and protect users' privacy rights. In addition to understanding the limits of what is technically capable, policymakers should define a governance model that outlines the responsibilities of different stakeholders, including technology companies, government agencies, and general users.

In this new paradigm, policymakers ought to consider the increasing ubiquity of AI-intermediaries that can collect, store, share and decide on data permission rights independently of a human agent. The identity and data governance framework should reign in potential adverse effects that may ensue from delegating some aspects of data management to autonomous agents.

Perhaps one of the most promising initiatives that policymakers could influence is the development of decentralized identity systems that would give users more control over their personal data and reduce the risk of a centralized system's single point of failure. To that end, an existing public blockchain with large network effects and high security standards can act as a tamper-proof ledger of identity data, distributed across multiple nodes in the network.

First announced in May 2019, Microsoft's ION serves as a good example of a decentralized identity system. To allow individuals and organizations to create, manage, and own their digital identities, the ION network was built atop the Bitcoin blockchain and introduced Decentralized Identifiers (DIDs) to enable a self-sovereign identity model¹⁵.

However, the paradigm of a decentralized identity system hinges on the ability of users to assume a greater level of responsibility as safety nets typically offered by centralized systems cease to apply.

For example, the loss of access to a user's private key could imply the perpetual loss of critical user information that would otherwise be recoverable under a centralized model. Consequently, policymakers should invest in educating users about the tradeoff at stake and the importance of digital identity security.

Policymakers should also work towards making their digital identity systems globally or regionally interoperable.



G. Safeguard intellectual property and digital ownership rights on the metaverse.

The metaverse is a space that can accelerate not only the volume of digital content created, but also its variety. Tokenized securities across numerous sectors and activities, Non-Fungible Tokens (NFT), cryptocurrencies, digital bearer assets, as well as other forms of digital assets, are ushering in an era of digital property ownership that up until recently was mainly confined to the physical.

Policymakers have a pivotal role to play. For a starter, they can help clarify the different types of ownership in the metaverse including when asset ownership ought to be governed through e.g., a contractual or a property framework.

Equally important are the matters of ownership verification, protection, and transfer. To ensure compliance with existing financial regulations including Anti Money Laundering (AML), policymakers should pay particular attention to the question of transparency around ownership as it manifests itself in the context of a decentralized governance structure. In this respect, an existing public blockchain that adheres to the highest security standards and that is visible to all network participants could prove useful in serving as a single and immutable source of truth.

A treatment of ownership rights could not be comprehensive if it does not consider the question of custody. Technology allows bearers of digital assets to assume full custody. However, many users in the metaverse, individuals and institutions alike, may opt for outsourcing custody to a third party.

As part of their regulatory framework, policymakers should clarify the liabilities associated with various custody models and help address and mitigate some of their adverse effects.

For example, educating users on the advantages of cryptographic multi-signatures for shared custody purposes can help protect users from the risks of theft or loss. Furthermore, the regulatory framework could underscore the importance of having specific insurance models for third-party custody, as well as robust cybersecurity standards to ensure the safety of custodied assets.

A bigger question for policymakers to contemplate is under what circumstances should digitally owned assets be firmly subjected to bailment law. An important implication would be to help avoid instances of rehypothecation that at times can prove fatally detrimental to the original bearer of the asset.

Insofar as intellectual property is concerned, policymakers need to ensure that creators and innovators are protected within the metaverse.

This may involve implementing measures such as digital rights management (DRM) technology to protect copyrighted content, establishing mechanisms to report and address instances of piracy and infringement, and working with law enforcement agencies to enforce the law within the metaverse.



H. Ensure the adoption of robust cybersecurity standards to optimize the metaverse users' experience and prevent potential harm.

Cyber-attacks are becoming more frequent and are increasingly calling for adequate cybersecurity measures to prevent unauthorized access, data theft, and other malicious activities. For example, Distributed Denial-of-Service (DDoS) attacks have increased in frequency and scale, with a 2021 report from Kaspersky indicating a 52% YoY increase in DDoS attacks targeting educational resources and online gaming platforms during Q4 2021¹⁶.

The ever-expanding roster of devices spanning Augmented and Virtual Reality sets, coupled with the cambrian explosion in Internet of Things sensors and actuators, will continuously introduce new cyber-attack vectors in the metaverse. Clearly, collaborating with industry experts and relevant stakeholders will be instrumental to developing and improving prevalent cybersecurity standards.

Rather than passively collaborating, policymakers should proactively promote investment in cybersecurity infrastructure. For example, they could facilitate investments in critical infrastructure such as data centers and connectivity networks. Such infrastructure would be endowed with robust cybersecurity protocols and advanced physical security measures including biometric authentication, 24/7 surveillance, intrusion detection and prevention schemes, frequent vulnerability assessment and penetration testing, as well as incident response and recovery capabilities.

In big part, the metaverse's underlying security relies on various cryptographic primitives and protocols. Policymakers benefit from a privileged position to specifically promote investment in cryptographic infrastructure encompassing the deployment of key management systems and the on-going integration of advanced encryption techniques. However, cybersecurity standards are as

good as their users' abilities to integrate and adopt them.

Consequently, policymakers should invest in cybersecurity training for individuals, corporations and metaverse developers to educate them about best practices and raise their awareness about cyber risks.

I. Collaborate with technology industry players, developers, and behavioral scientists to ensure harmless interaction in the metaverse and enforce optimized transparency and accountability standards.

The exercise of enforcing acceptable behavioral standards under a decentralized governance structure is more challenging than the one usually carried out under a centralized governance model. In a decentralized context, no single party or entity detains the monopoly over the rules of interaction. Enforcing penalties at will naturally becomes a more difficult endeavor.

Policymakers could always contemplate stricter enforcement mechanisms at the application layer. However, the metaverse offers an unprecedented opportunity to rethink the traditional top-down approach of enforcing policies and to explore further avenues better adapted to a decentralized paradigm. Such avenues would rely in big part on well-designed incentive schemes to encourage users to observe the rules and regulations.



For such a game-theoretic approach to yield optimal outcomes, it is recommended to anchor it at the level of the metaverse's consensus layer. For example, Bitcoin's decentralized governance model is built around a consensus protocol that incentivizes the network's mining nodes to abide by the rules of the game to maximize their reward and economic return. Indeed, for miners to participate in the network, they initially spend capital on mining hardware and then incur ongoing operational cost, mainly in the form of electricity consumption. Such capital expenditure and operational expenses cannot be recouped unless miners observe the pre-defined consensus rules, for only then will they be rewarded with digitally native tokens, Satoshis. In this context, these tokens naturally emerge as a solution to align incentives on the decentralized network.

Despite its expected benefits, the metaverse could still be ground for misuse that spans inappropriate content exchange, cases of harassment and abuse, and a manifestation of stronger forms of addiction.

Likely, such manifestations would be associated with a non-negligible impact on users' wellbeing and mental health. To that end, policymakers are encouraged to establish clear guidelines and standards to instill transparent review processes and frequent audits. Clearly, such an effort must be developed in tandem with the metaverse's underlying identity management and data protection framework.

Furthermore, policymakers can play a central role in developing various educational resources to encourage healthy and respectful behavior on the metaverse, support parents and guardians better manage their minors' exposure to it, reduce the stigma around mental health issues, and provide mental health support and resources.

A new framework such as Whiteshield's "Quantum Governance" would be instrumental in ensuring a balance between the policymakers' actions and capabilities on the one hand and the absorptive capabilities of the people on the other hand¹⁷.



J. Continuously adapt labor regulations to the new employment opportunities that are integral to the metaverse and that have the potential of shaping the future of work.

The metaverse is bound to introduce a new form of labor dynamic where corporations progressively move to the digital realm, and the employment of individuals becomes increasingly tied to the rules of a virtual environment. Policymakers must navigate the challenge of imagining and continuously adapting to a market model that is still in gestation. The World Economic Forum's Future of Jobs report highlights this shift and emphasizes the need for inclusive and sustainable employment opportunities¹⁸.

No matter its final form, the guiding principles of policymakers in that regard remain unchanged and anchored around the provision of inclusive and sustainable employment opportunities. In particular, they must focus on employee protection including access to fair compensation, safe working conditions, and social safety net programs.

Considering these principles, it will be critical for policymakers to study, analyze and assimilate the potential ramifications of a radically new model that revolves around smart contracts. This becomes even more critical especially when contracts are algorithmically defined, written, and upheld as part of an autonomous organization. In this context, policymakers should ponder the fundamental questions of contract enforcement, amendment, arbitration, and mediation among other things.

Furthermore, the emergence of the metaverse will most likely catapult the sharing economy forward as individuals will more easily be able to access freelance opportunities and engage in peer-to-peer working relationships. In addition to putting this emerging "future-of-work" model on solid regulatory footing, policymakers could play a pivotal role in preparing and training the next generation of metaverse workers. They could promote a stronger emphasis on STEM education, a better access to resources and training for teachers to incorporate the metaverse into educational curricula, and a more fluid collaboration between educational institutions and industry experts to develop programs related to emerging technologies.



METaverse USE CASES AND POLICY CONSIDERATIONS

A recent survey of 3,400 consumers and executives conducted by McKinsey & Co. revealed that business leaders remain optimistic about the metaverse's impact on their respective industries with 95% expecting a positive impact within the next 5 to 10 years¹⁹.

In this section, we explore some notable use cases of the metaverse which are already being harnessed by numerous industries to create innovative opportunities in different sectors including education and training, healthcare, entertainment, commerce, and manufacturing.

However, as is the case with any emerging technology, the path to successful deployment and adoption of the various use cases is paved with obstacles that include accessibility features, data privacy, standardization, digital equity, labor laws, content moderation, and user safety.

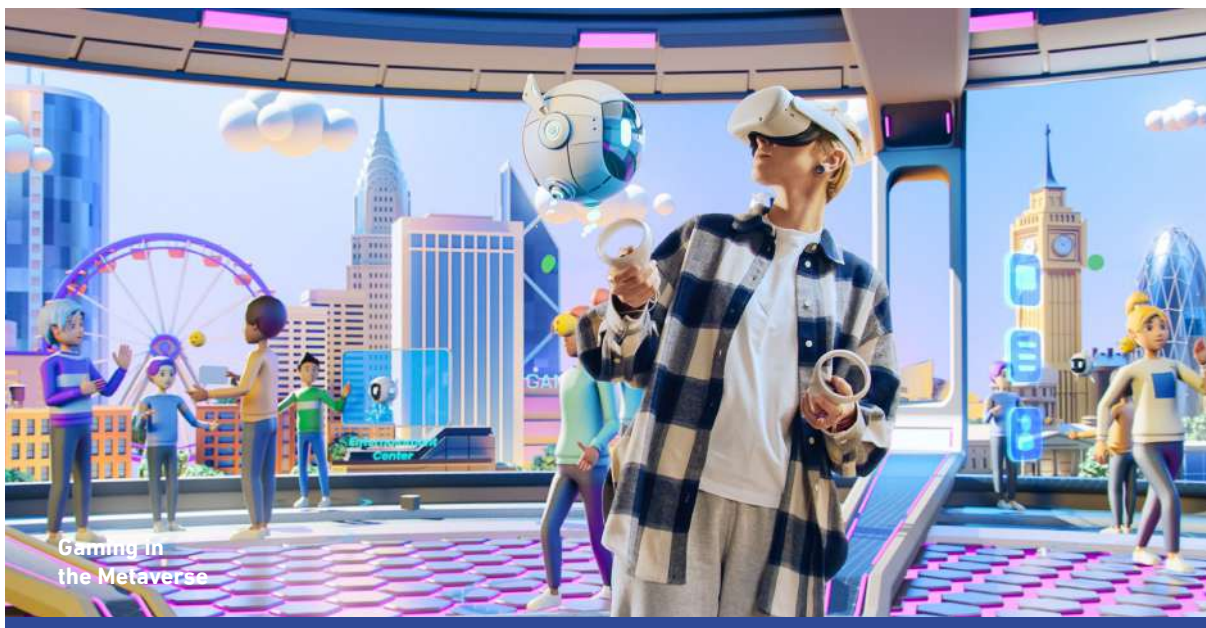


Entertainment

The metaverse is often associated with videogames and interactive entertainment, which have driven the commercialization and technological innovation of Virtual Reality (VR) since Sega's 1991 announcement of the VR headset for the Mega Drive / Genesis home console. Technological advancements, such as rotational tracking and lag-free displays, have provided the foundation for VR to expand into other use cases. As of 2020, the VR gaming market is valued at over US\$180 billion, and is expected to grow to up to US\$400 billion by 2025 ²⁰.

Entertainment experiences in the metaverse include games, concerts, and live events either through the augmentation of a local space or the creation of a virtual space in which users can participate. Examples include the 2023 Imagine Dragons concert by AT&T THANKS, which allowed virtual attendance and backstage access on the Oculus headset, and the Mario Kart Live Home Circuit (2020), which enabled players to create racetracks in their homes to challenge other racers.





The gaming industry has always been at the forefront of technology, and it has embraced the metaverse as a new frontier for creating unique experiences that can be shared with players from all over the world.

Game developers can leverage the vast array of tools and platforms including e.g., Decentraland, Roblox, Epic Games and Sandbox, to create immersive gaming experiences unlike anything else experienced in the traditional gaming world.

For example, Decentraland was established as an innovative virtual world platform to empower users to buy and develop virtual plots of land, create digital accessories, interact, and play games²¹.

Despite its significant growth potential, the entertainment metaverse industry is also facing several challenges. One of those is the high cost of entry, as VR headsets and hardware prices are still relatively expensive for mainstream adoption. Additionally, concerns such

as motion sickness, discomfort during extended usage, and the need for adequate physical space for immersive experiences can affect user adoption. While developers focus on addressing these concerns, policymakers can support technological progress by addressing critical issues around privacy and data security.

For policymakers, the metaverse entertainment industry could also serve as an example of regulatory expansion. Regulations applicable to standard video games and music, including copyright and ownership of digital assets, could be transferable to their virtual counterparts. However, the challenge for regulators lies in managing content specifically created within the metaverse, such as the sale of user-created virtual experiences or the licensing of music and art assets used in virtual spaces.



Work and Education

The COVID-19 pandemic has led to a rapid adaptation of remote work and distance learning with an increased offering of digital coursework and e-learning through services like Khan Academy and Coursera, and a renewed interest in applications such as Zoom and Microsoft's Teams.

The video conferencing market was valued at US\$6.8 billion in 2021, with an expected annual growth rate of more than 11%²².

As virtual workspaces continue to evolve, the future of distance learning and work may move further towards enriching virtual spaces to increase the quality of meetings and collaborations

Despite the rapid adoption of remote work and distance learning in virtual spaces, certain limitations need to be addressed. One of the main challenges is the potential for decreased social interaction

and collaboration in virtual compared to in-person settings. Additionally, the technology for communication and collaboration depends in big part on the reliability of internet connectivity and access to adequate equipment and amenities.

Furthermore, virtual spaces can pose new challenges, as evidenced by a beta tester in Meta's platform who reported being sexually harassed by another participant in the metaverse²³. Defining and prosecuting such crimes in the often-anonymous virtual world will likely prove to be challenging.

As virtual work and education spaces continue to evolve, policymakers and stakeholders must carefully consider the potential benefits and limitations while creating regulatory frameworks that ensure safety, privacy, and inclusivity.



Socialization

The virtual world has created new avenues for socialization beyond the usual entertainment and productivity spaces. Before the advent of VR headsets, applications like Second Life were successful in creating virtual spaces for enthusiasts. The potential of virtual social spaces is expected to be significant as it caters to the basic human need for socialization and connection.

However, its fulfillment depends on the innovation and creativity of developers to build new features and functionalities and augment early developments, such as personalization of avatars and creation of digital homes and town squares.

As VR technology continues to advance, there is potential for even more diverse and immersive social experiences in the metaverse where virtual social spaces could gain significant traction.

However, the development of virtual social spaces comes with its own set of challenges. One of the main concerns is tied to the type of content created within these spaces. Ownership and licensing issues surrounding personalized items and other intellectual property will have to be addressed.

Also, issues such as harassment within virtual social spaces must be resolved to ensure that users have a safe and respectful virtual experience. In light of these concerns, policymakers need to tread carefully and adopt a balanced approach to govern the development of virtual social spaces.



Healthcare

Augmented and Virtual Reality (AR/VR) applications have gained considerable attention in healthcare in recent years notably with respect to five use cases including remote consultations, medical education and training, pain management, physical therapy and rehabilitation, and mental health therapy.

The future potential of AR/VR in healthcare is expected to be significant, with an anticipated global market size of US\$18-20 billion by 2030, up from US\$2.1 billion in 2021²⁴.

Furthermore, Artificial Intelligence (AI) capabilities are expected to advance personalized medicine, enabling patients to provide their personal data and genomics to obtain AI-generated personalized diagnostics and treatment plans. Virtual clinical trials could gain further traction and smart hospitals could drive market growth

by incorporating AI-enhanced surgeon robots and virtual reality treatments for patients.

However, the collection and use of patient's personal data in AI-generated diagnostics and treatment plans may raise data privacy and security concerns. Additionally, regulatory limitations may impact the development and adoption of AR/VR technologies in healthcare, including concerns related to patient safety, liability, and reimbursement.

Collaboration among stakeholders, including healthcare providers, technology developers, regulators, and patients, is vital to address some of these concerns and ensure responsible and ethical use of AR/VR while further R&D is necessary to enhance the maturity and effectiveness of innovative healthcare offerings.



Commerce

The metaverse has the potential to transform traditional business models. Several notable use cases of the metaverse in commerce have emerged.

In immersive shopping, consumers can interact with products in a 3D environment, try on virtual clothes, and customize products. This can enrich their online experience and potentially drive sales.

Virtual marketplaces allow the creation of virtual economies and in the process, enable creators, entrepreneurs, and startups to identify new business opportunities.

Remote collaboration in virtual environments can enhance teamwork, creativity, and business outcomes, surpassing the benefits of the traditional video conferencing experience.

Virtual events and conferences can offer businesses cost savings and enable them to reach a broader audience.

Virtual advertising can create more engaging experiences for consumers, generate valuable data for targeted advertising, and help brands reach a younger and tech-savvy audience.

These use cases offer novel and innovative ways to engage with consumers and provide personalized experiences. Additionally, the embedding of crypto assets into the metaverse offers new avenues for cross-border transactions and commerce.

However, as the amount of personal and sensitive data generated, stored, and shared in the metaverse increases, data management, including data privacy and security become major concerns. A 2020 study suggests that five minutes of VR tracking data can produce “information that can identify a user out of a pool of 511 people with an accuracy of 95.3%”, indicating the increasing privacy risks of the metaverse’s growing data ecosystem²⁵.



Policymakers must therefore ensure adequate measures are in place to for proper data management, and to protect users' privacy and data security.

The regulatory landscape around metaverse commerce is still developing, and policymakers must address issues such as taxation, consumer protection, and intellectual property rights to ensure fair competition and prevent fraud. There is also a risk of a digital divide, where the benefits of metaverse commerce may not be accessible to everyone, particularly those in developing countries or those who cannot afford the necessary technology.

It is recommended that policymakers collaborate with stakeholders from the commerce industry, technology companies, and consumer advocacy groups to develop appropriate regulations and ensure a balanced approach that promotes digital literacy, innovation and growth while safeguarding the interests of consumers.



Industrial Metaverse

The industrial metaverse allows industries to create digital twins of their physical assets, using virtual and augmented reality technologies, thereby providing real-time monitoring, predictive maintenance, and optimized operations.

This progressive approach to industrial automation is expected to bring significant benefits in terms of efficiency and productivity, and policymakers should develop a deeper understanding of its potential to inform a regulatory framework that promotes its responsible and sustainable development.

As an example, Siemens and NVIDIA announced a partnership to collaborate on enabling the industrial metaverse. They plan to connect NVIDIA Omniverse, a platform for 3D-design and collaboration, and Siemens Xcelerator, the open digital business platform, to create a digital twin that simulates and visualizes industrial processes. This partnership aims to bring real-time simulation and collaborative workflows to industrial manufacturing and design²⁶.

One of the noteworthy advantages of the industrial metaverse is its potential to enhance safety. By developing digital models of work environments, industries can simulate hazardous scenarios without exposing workers to harm, enabling them to be better trained and prepared and thus reducing the occurrence of accidents and injury incidents. Furthermore, the industrial metaverse offers opportunities for increased innovation, allowing companies to test new designs and ideas rapidly without incurring costs and risks typically associated with traditional physical testing.

However, policymakers should also take note of the potential impact of the industrial metaverse on the workforce especially since the automation and virtualization of manufacturing processes could lead to job loss or at the very least require retraining and reskilling.

According to the World Economic Forum's Future of Jobs report, the rapid advancement of technology and the integration of the metaverse in industrial



sectors could significantly transform traditional manufacturing practices. For example, the implementation of virtual factories and digital twins may reduce the need for manual labor in certain areas²⁷.

Policymakers must proactively address these changes to ensure a smooth transition for workers and facilitate the acquisition of new skills that align with the evolving demands of the industrial metaverse.

Policymakers must also establish clear standards and regulations to address concerns related to data privacy and establish measures to ensure that the use of these technologies does not result in the violation of workers' rights.

CONCLUSION

We may be standing at the cusp of a new digital era where the metaverse and by extension AI that plays a significant role in creating and enhancing the virtual world of the metaverse could very well represent the next iteration of the internet and introduce a profound shift in the way we interact with one another and with our environment.

At its core, the metaverse is a complex layered system enabling an entirely new digital ecosystem within which users can create, collaborate, and express their individuality in a myriad of ways. As we move forward and as its enabling technologies continue to develop, we can expect the metaverse to expand in ways we can barely imagine. A group of industry leaders even warned in June 2023 that AI technology “might one day pose an existential threat to humanity and should be considered a societal risk on a par with pandemics and nuclear wars”²⁸.

To prepare better for its advent, policymakers may want to observe certain rules and guiding principles to ensure its responsible management while aiming for an agile regulatory regime that protects the end user and ensures cross-sectoral cooperation without stifling innovation. To that end, the policymaking effort should avoid excessive restrictions and regulations, elevate the role of the private sector and civil society in the policy formulation process, recognize that cyber reality and cryptography are changing the rules of the game, and adopt a human-centric approach whenever designing new policies. Human-centricity is key, especially in the context of a policymaking realm that is far from static. To that end, policymakers are invited to recognize the fundamental role of the individual and the citizen in driving successful metaverse policy formulation. More specifically, governments at times tend to initiate and execute programs that do not consider the absorptive capacity of the individuals as it relates to their interaction with public policies and their potential to transform these policies into tangible achievements.

To optimize their impact, policies should strive to resolve the various complications that naturally arise in the context of the metaverse including the management of digital identity, metaverse data ecosystem, property rights and ownership, accountability, transactions and exchanges, security, interoperability, and digital inclusion.

Most importantly, the success of policymakers in creating a seamless and sustainable metaverse experience that transcends physical boundaries hinges on their capability to foster cross-jurisdictional collaboration and selectively involving a broad set of stakeholders including industry representatives and technology players.

International organizations have a key role to play in fostering an effective multilateral cooperation that will be necessary to shape an inclusive and safe metaverse. International organizations can be instrumental in helping governments, private sector, civil society, and academia navigate the developments around the metaverse and understand the relevant policies, infrastructure, tools, and protocols needed to harness its potential.

About the Digital Cooperation Organization



The DCO is a global Intergovernmental Organization founded in November 2020 that aims to enable digital prosperity for all by accelerating the inclusive and sustainable growth of the digital economy. The DCO is focused on empowering the youth, women, and entrepreneurs, leveraging the accelerative power of the digital economy, and leapfrogging with innovation to drive economic growth and increase social prosperity. Through enhanced cooperation and dialogue, the DCO seeks to establish a conducive environment for the rapid development of digital economies within which all individuals, businesses and societies can innovate and thrive.

In pursuit of its purpose, the DCO fosters multilateral collaborations across sectors to allow governments, private sector, international organizations, and civil society to cocreate, and codesign initiatives that enable more inclusive digital transformation and the growth of digital industries. The DCO's main flagship interventions include programs and initiatives that aim to enhance cross-border data flows, market access for SMEs, digital entrepreneurs' empowerment, digital taxation, and digital inclusion.

About Whiteshield



Whiteshield is a global advisory firm known for its ability to respond to global challenges rapidly and incisively. Whiteshield uses the most advanced tools and technology and combines them with their team of leading international experts to engage decision-makers in tackling society's most significant challenges. They are recognized for their rapid decision support, innovation, data science algorithms and deep policy expertise. They are specialists in “connecting the dots” between policy, business and enhancing the lives of citizens.

CONTRIBUTORS

We would like to express our gratitude to all of those with whom we have had the pleasure to work on this paper. The larger contributing team from Whiteshield and the DCO employees includes:

LEAD AUTHORS

Ahmad Bhinder
Policy Innovation Director
DCO

Rodrigue Kamel
Policy Advisor
Whiteshield

Bassam Khoury
Partner & Director
Whiteshield

ACKNOWLEDGEMENTS

Whiteshield

Avery Shipton
Policy Advisor
Whiteshield

Gianmarco Mazzochi
Manager
Whiteshield

Arthur Pendaries
Manager
Whiteshield

The DCO

Alaa Abdulaal
Chief of Digital Economy Foresight
DCO

Khaldoon Said
Marketing & Communications Director
DCO

Tiphaine Lagarde
Digital Ecosystem and Partnerships Director
DCO

Syed Iftikhar
Digital Research Director
DCO

BIBLIOGRAPHY

1. <https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026>
2. https://icg.citi.com/icghome/what-we-think/citigps/insights/metaverse-and-money_20220330
3. McKinsey, Value Creation in the Metaverse <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse>
4. a16z, How to Win the Future: An Agenda for the Third Generation of the Internet: <https://a16z.com/wp-content/uploads/2021/10/How-to-Win-the-Future-1.pdf>
5. <https://visainnovationprogram.com/#program> <https://usa.visa.com/about-visa/global-innovation-centers.html>
6. <https://www.msit.go.kr/eng/bbs/view>
7. <https://www.sama.gov.sa/en-US/News/Pages/news-849.aspx>
8. European Commission, Communication, "An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition," Strasbourg, 11 July 2023, COM (2023) 442/final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023D-C0442&qid=1696221355432>
9. <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIdx=&bbsSeqNo=42&nttSeqNo=657&searchOpt=ALL&searchTxt=>
10. <https://www.computerweekly.com/news/365531002/KPMG-launches-metaverse-and-digital-twin-hub-in-Saudi-Arabia>
11. <https://www.sps.nyu.edu/homepage/metaverse/metaverse-blog/the-estonian-miracle-e-estonia-and-the-future-of-digital-infrastructure.html>
12. <https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse> ; <https://metaverse-standards.org/>
13. <https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf>
14. <https://www.itu.int/en/mediacentre/Pages/PR-2023-01-19-TSB-Focus-Group-metaverse.aspx>
15. <https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/toward-scalable-decentralized-identifier-systems/ba-p/560168>; <https://identity.foundation/ion/>
16. https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021
17. <https://www.project-syndicate.org/commentary/data-governments-businesses-partnerships-public-good-by-christopher-pissarides-et-al-2022-10>; <https://whiteshield.com/>
18. World Economic Forum, Future of Jobs Report 2023: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf?_gl=1*vcwxgw*_up*MQ..&gclid=Cj0KCQjw98ujBhCgARIsAD7QeAjW0f6wrfY19hIfosKC5U-nhJQP7cYEN3IBQDTTSi9vC3s0qCm77REaAnt5EALw_wcB
19. McKinsey & Company, Value Creation in the metaverse: https://www.mckinsey.com/~/_media/mckinsey/Value-creation-in-the-metaverse.pdf

BIBLIOGRAPHY

20. Grayscale The Metaverse Web 3.0 Virtual Cloud Economies, https://www.digitalcapitalmanagement.com.au/wpcontent/uploads/2022/02/Grayscale_Metaverse_Report_Nov2021.pdf
ARK Investment Management LCC, White Paper “Big ideas 2021” https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/ARK%E2%80%93Invest_BigIdeas_2021.pdf
21. Decentraland, a blockchain-based virtual world: <https://decentraland.org/whitepaper.pdf>:
22. “Video Conference Market Size, Share, & COVID-19 Impact Analysis,” Fortune Business Insights, <https://www.fortunebusinessinsights.com/industry-reports/video-conferencing-market-100293>
23. “The metaverse has a groping problem already,” Tanya Basu, MIT Technology Review, <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>
24. Convergence from market reports including Precedence Research, Grand View Research, Global Market Insights (2022)
25. https://www3.weforum.org/docs/WEF_Demystifying_the_Consumer_Metaverse.pdf: Miller, M. R., F. Herrera, H. Jun, J.A. Landay and J.N. Bailenson, “Personal identifiability of user tracking data during observation of 360-degree VR video”, Scientific Reports, vol. 10 no. 1, 2020.
26. Siemens and NVIDIA to enable industrial metaverse: <https://press.siemens.com/global/en/pressrelease/siemens-and-nvidia-partner-enable-industrial-metaverse>
27. World Economic Forum, Future of Jobs Report 2023: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf?_gl=1*vcwxgw*_up*MQ..&gclid=Cj0KCQjw98ujBhCgARIsAD7QeAjW0f6wrfY19hlfosKC5U-nhJQP7cYEN3IBQDTTSi9vC3s0qCm77REaAnt5EALw_wcB
28. <https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html>



Follow Us on

   @dcorg |  www.dco.org