UNIVERSITY OF
GLOUCESTERSHIRE

This is a peer-reviewed, final published version of the following document and is licensed under Creative Commons: Attribution 4.0 license:

Wynn, Martin G ORCID logoORCID: https://orcid.org/0000-0001-7619-6079 and Jones, Peter ORCID logoORCID: https://orcid.org/0000-0002-9566-9393 (2023) New technology deployment and corporate responsibilities in the metaverse. Knowledge, 3 (4). pp. 543-556. doi:10.3390/knowledge3040035

Official URL: https://doi.org/10.3390/knowledge3040035
DOI: http://dx.doi.org/10.3390/knowledge3040035
EPrint URI: https://eprints.glos.ac.uk/id/eprint/13237

Disclaimer

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.

The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.

The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

PLEASE SCROLL DOWN FOR TEXT.

knowledge

MDPI

Article

New Technology Deployment and Corporate Responsibilities in the Metaverse

Martin Wynn * and Peter Jones

The School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL50 2RH, UK; pjones@glos.ac.uk
* Correspondence: mwynn@glos.ac.uk

Abstract: The term "metaverse" came to the fore in 2021 when Facebook rebranded its corporate identity to Meta and signalled its intention to invest at least USD 10 billion in developing the concepts and related products that year. However, there is still little consensus in defining what constitutes the metaverse, although there is a widespread, though not universal, agreement that it will bring a wide range of benefits across society. More specifically, the advent and continuing evolution of the metaverse has strategic and operational implications for, and impacts on, industry and business at large. Adopting an inductive, interpretivist approach, this exploratory research article presents case examples of the guidance on the responsible development of the metaverse provided by two IT business services companies. This article identifies the major risks and responsibilities associated with the metaverse and assesses how companies might address these responsibilities. Very little research has been published in this area, and this article attempts to make a small contribution to filling this gap in the literature. This article finds that these responsibilities are largely in line with those currently associated with corporate digital responsibility, and concludes that the strategic impact and extent of regulatory change will depend on the nature of the metaverse that materialises in the forthcoming decade.

Keywords: metaverse; corporate digital responsibility; CDR; regulation; digital technologies

check for updates

Citation: Wynn, M.; Jones, P. New Technology Deployment and Corporate Responsibilities in the Metaverse. *Knowledge* **2023**, *3*, 543–556. https://doi.org/10.3390/knowledge3040035

Academic Editor: Constantin Bratianu

Received: 4 September 2023
Revised: 19 September 2023
Accepted: 26 September 2023
Published: 27 September 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The metaverse as a concept is not new, having been introduced in the sci-fi novel Snow Crash [1] over 30 years ago. Today, the metaverse is widely discussed and is generally seen to be the next "big thing" in the application of technology in business and society. While the benefits claimed for the metaverse span many areas of activity, the continuing evolution of the metaverse has a potentially wide range of implications for industry in areas currently related to corporate social responsibility (CSR), or more precisely, corporate digital responsibility (CDR). The parameters of CDR include trust, privacy, security, information transparency, customer engagement, employee upskilling, culture change, environmental impact, and ethics [2]. The advent of the metaverse will increase focus on these responsibilities and the possible need for regulation.

In this context, Madiega et al. [3] (pp. 1–2), writing under the banner of the European Parliamentary Research Service, argued that "it is essential to consider how to attribute responsibility" for such impacts, and that "the multitude of entities present in the metaverse will create a web of relationships making it very difficult to determine responsibilities and liabilities". Governments are increasingly coming under pressure to regulate the metaverse, and KPMG [4] argued that governments have a unique opportunity to play a more proactive role in the regulation of the metaverse. At the same time, the corporate sector will also need to recognise its metaverse responsibilities and their strategic implications. Anshari et al. [5] (p. 1) argued that, as businesses increasingly use the metaverse to expand their service networks, they "may need to carefully assess the ethical implications of their data collection and utilisation procedures".

Although the metaverse is beginning to attract attention in the academic literature [6,7], there has been little consideration to date on how companies could and should approach their responsibilities regarding the development and use of the metaverse. This paper focuses on this gap in the literature and addresses two research questions (RQs), in the context of the metaverse in business and industry. First, what are the main risks and responsibilities associated with the metaverse? Second, how will the metaverse be regulated and how will companies report on their metaverse responsibilities to their stakeholders?

Following this introduction, this paper includes a section on the research method, and a section that reviews some of the relevant literature. The results section then reports on the findings from two case studies (in Section 4.1) and then addresses the two RQs noted above (in Section 4.2). The concluding section summarises the contribution of the article and outlines possible areas for future research.

2. Research Method

The research method is interpretivist and inductive, and consists of two main elements: a scoping literature review, and two case studies drawn from secondary sources. For the literature review, recently published academic literature and information obtained from various web sources were reviewed to provide the material presented in the following section. This scoping review supported the development of the two research questions to be addressed using evidence from the case studies. Scoping reviews "are best employed when there is limited literature to inform the research question of interest" [8] (p. 5), and can help to lay the foundations for subsequent research endeavours. This paper then examines how two major companies—Accenture and A3Logics—are approaching their responsibilities related to the metaverse. The case studies draw heavily on reports published in 2023 by Accenture, an international professional services company specialising in information technology services and consulting, based in Dublin, and A3Logics, a global information technology services, consulting and business solutions company, based in California. Both the Accenture report "Building a Responsible Metaverse" [9], and the A3Logics report "Why companies Need to be Socially Responsible in Metaverse Development" [10] look to focus on the ethical, environmental and social issues involved in building and developing metaverse technologies. As such, this paper might best be seen as an opportunistic endeavour designed to shed some preliminary light on an issue that has received very little attention in the academic literature.

While these case studies do not offer a complete picture of how the two companies are approaching the metaverse, the authors believe that they provide some valuable insights into how such international companies will have to transition their CDR strategies and operations in response to the changes introduced by the metaverse. The authors looked to capture the companies' approach to the metaverse in their own words, in the belief that such quotations help to convey corporate authenticity. Document analysis was thus the main technique used in the case studies. Bowen [11] (p. 27) defined this as a "procedure for reviewing or evaluating documents—both printed and electronic (computer-based and Internet-transmitted) material", noting that "like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge". This helped the authors identify emergent themes and address the research questions, this being an iterative, cyclical process involving the working and re-working of common themes and related issues.

3. Relevant Literature

3.1. Concept and Definition

There is little by way of a consensus on how the metaverse should be defined, which is partly due to the continuing evolution of its constituent technologies, but a small sample of working definitions of the metaverse is provided here, and some of its perceived charac-

teristics are discussed. Conceptualising the metaverse and how it will work in practice is challenging. Tucci [12] (paras. 1–2) offers the following vision of the future:

> "Imagine a virtual world where billions of people live, work, shop, learn and interact with each other—all from the comfort of their couches in the physical world. In this world, the computer screens we use today to connect to a worldwide web of information have become portals to a 3D virtual realm that's palpable—like real life, only bigger and better. Digital facsimiles of ourselves, or avatars, move freely from one experience to another, taking our identities and our money with us".

This, however, remains just a vision, and it remains unclear as to how it will develop in practice. McKinsey [13] (2022, para. 4) sees the metaverse as "best characterized as an evolution of today's internet—it is something we are immersed in instead of something we look at. It may realize the promise of vast digital worlds to parallel our physical one". More starkly, in addressing "responsibly strategizing the metaverse", Marabelli and Newell [14] (para. 3) argued that "the immersive and potentially ubiquitous and pervasive characteristics of this technology hold strategic implications for organizations, and have the potential to change the future of work and society". Deloitte [15] (p. 6) set out three possibilities regarding how the metaverse may develop by the early 2030s. The more conservative (basic) assessment is that the metaverse "excels for the things it's good at, but never becomes a general-purpose platform", and remains "a speciality market for specific uses that will complement but not replace other technologies". A more sophisticated (intermediate) possibility would see multiple metaverses in which there are "a handful of major players vying for share of a dynamic marketplace", and "a mainstream market for many applications but split among the next generation of tech leaders". Finally, the most advanced (dominant) perspective envisions "an open, interoperable metaverse", which becomes "the dominant interface through which we conduct most of our daily activities", and entails "the full migration of today's internet and more into an immersive world in which most businesses and consumers operate".

It is thus not surprising that the definitions of the metaverse differ or are couched in rather vague terms. Mystakidis [16] (p. 486) offers a brief definition, namely "the metaverse is a post-reality universe, a perpetual and persistent multiuser environment merging physical reality with digital virtuality", whilst for PWC [17] (para. 5) "the metaverse promises a stunningly realistic 3D digital world where you can do almost anything that you can in the real world—and more besides. . .. . .. one day the metaverse won't run on platforms whose owners control data, governance and transactions. Instead, customers (and businesses) will be able to take their identities, currencies, experiences and assets anywhere they wish".

3.2. Metaverse Technologies and Business Applications

Mager and Matheson [18] (para. 3) see the metaverse as "a confluence of technologies that allow new forms of experience and engagement across industries through 3D activity and the use of simulations based on artificial intelligence". Underpinning the metaverse are a range of technologies—a "technology stack"—that are generally viewed as facilitating the metaverse (Figure 1). The metaverse space is made possible by the new, decentralised iteration of the Internet called Web3 [19], which provides access to a range of digital technologies that support the metaverse–blockchain [20], the Internet of Things [21], spatial and edge computing [22], artificial intelligence [23], 3D modelling software [24], extended reality [25], and brain–computer interfaces (BCIs) [26] (Table 1). However, as Pratt and Daniel [27] (para. 18) point out, "the technology is simply not ready to support a fully immersive and shared metaverse—interoperability, computing power, software protocols, networking capacity and the degree of sophistication don't exist to create a true metaverse today—and it may never get there". McKinsey [13] (para. 8), however, is more optimistic, noting "constant improvements in computing power allow larger virtual worlds to exist. Cloud and edge computing let intensive large-data processes, such as graphics

rendering, move off local devices. The rapid adoption of 5G is enabling mobile devices to access these large worlds more easily and with lower latency. And the cost of production for augmented- and virtual-reality hardware is declining".

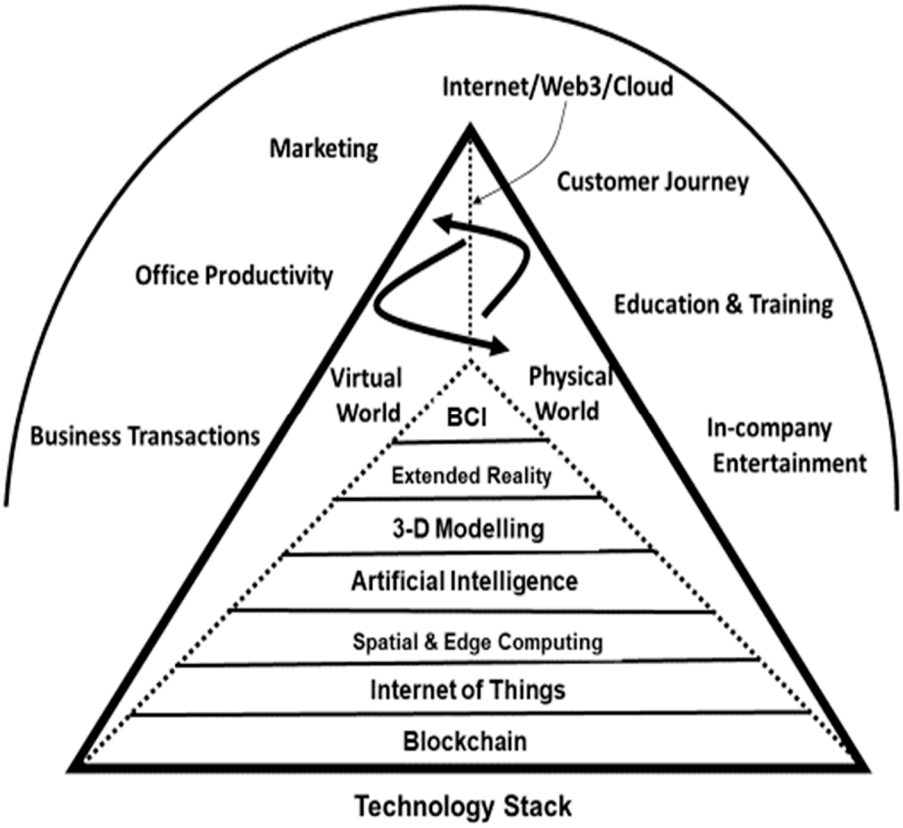

Figure 1. The metaverse technology stack and application areas.

Table 1. The technologies supporting the metaverse.

Digital Technology	Role in the Metaverse
Web3 [19]	The new version of the World Wide Web, still in development, that will provide the window into the metaverse, using blockchain and artificial intelligence to support operations in both the physical and virtual worlds.
Brain–computer interfaces [26]	Still largely under development, these will replace or augment extended reality interfaces and provide more direct brain-to-computer connectivity.
Extended reality [25]	Extended reality technologies (AR, VR and MR) will be used to provide user access to the virtual side of the metaverse. Headsets and glasses will provide users with virtual reality experiences that parallel the physical world.
3D modelling [24]	Three-dimensional modelling technologies will be used to create the virtual world images, products and other objects.
Artificial intelligence (AI) [23]	AI will be integral to the robotics functions in the metaverse, including chatbots and avatars. AI will also have wider applications to support human activities.
Spatial/edge computing [22]	IoT and other data will be processed in real-time to provide the information that supports the physical and virtual worlds and oils the metaverse machinery.
Internet of Things (IoT) [21]	A full range of devices, monitors and controllers for data collection within the physical and virtual environments.
Blockchain [20]	Blockchain technology will support cryptocurrency and non-fungible tokens, providing the secure and immutable storage of digital property, payments and other transactions.

In outlining the commercial capabilities of the metaverse, Accenture [9] emphasised the future role and importance of the metaverse in imagining, designing and delivering innovative extended reality experiences, in using blockchain to drive resilience across supply chains, to facilitate trust [28], verify digital identity, and build new revenue models, in digital engineering and manufacturing, and in technology innovation. More specifically, Pratt [29] identified a number of possible areas of application in the metaverse, not only in business operations [30], but also in education and training [31], customer experiences [32], work meetings [33], healthcare [34] and marketing [13] (Figure 1).

In terms of the impact on work meetings, Choder [33] (para. 6) notes that "the metaverse could allow people from around the globe to come together in one space (albeit online) in ways that were previously unobtainable or prohibitively costly". More specifically, as regards customer experience, Purdy [32] (para. 1) claims that "the metaverse presents a once-in-a-generation opportunity to reinvent the consumer experience", and identified three ways in which this could unfold: firstly " by creating new ways to discover and explore products"; secondly " by helping to fuse physical and virtual product experiences in more meaningful ways", and thirdly "by reestablishing connections between people and brands through 'digital humans'—AI-powered bots that can interact with users in virtual environments". In a similar vein, McKinsey [13], in discussing the potential of the metaverse for marketeers, suggests that "for marketers, the metaverse represents an opportunity to engage consumers in entirely new ways while pushing internal capabilities and brand innovation in new directions" (para. 4).

3.3. Risks, Responsibilities and Regulation

Nichols [35] (para. 1) notes that "when companies and users decide to adapt the technologies of the coming metaverse, they will also expose themselves to a new class of security risks and vulnerabilities". Research into who is to take responsibility for the metaverse is still in its infancy, and is emerging from a variety of disciplines, including information science, law, and systems engineering. Rosenberg [36] suggested that, as major corporations have begun investing billions to deploy immersive worlds, proposals for its regulation will soon be required. More specifically, he claimed that the fundamental risks were the monitoring, manipulation and the monetisation of users. Pratt and Daniel [27] (para. 32) take a broader perspective on the risks involved in the metaverse, and provide "just a short list" including "environmental concerns; cybersecurity issues; legal issues; sexual harassment and other forms of harassment; privacy issues; scams; misinformation; and effects on mental health, including lowered self-esteem and increased feelings of isolation".

Charamba [6] (p. 110) argued that "the dawn of metaverses" could mean that "BigTech control over our digital lives could be all consuming", and we be could be "ensconced in digital, state-like walled gardens that are controlled by a handful of companies wielding sovereign-like authority". This leads Charamba [6] to question how we can understand corporate responsibility in relation to human rights in a digital environment, and he discusses the United Nations Guiding Principles for Business and Human Rights, and proposes a corporate responsibility to respect and protect digital human rights. In exploring the sustainability of the metaverse, De Giovanni [37] further suggested that companies should not exclusively focus on the metaverse merely as a booster to enhance economic performance, but rather that they should carefully evaluate its role in terms of its environmental effects and social goals. In illustrating his argument that taking a responsible digitalisation approach seems to be quite urgent, De Giovanni [37] asserts that environmentally, the metaverse will entail an interesting trade-off, because it demands a high level of energy consumption. At the same time, while the metaverse favours social interactions within the digital world, an attendant decline in social interactions in the real world may have psychological implications.

Schobel and Leimeinster [38] claimed that the creation of metaverse ecosystems and integrated platforms results in different responsibilities for complementors/service providers, consumers, platform owners, and orchestrators, who handle the transfer of one platform

into other ecosystems. However, in mapping out the complex dynamic nature of the metaverse, Schobel and Leimeinster [38] argued not only that the responsibilities of these four groups will be continually changing, but also that it is important to rethink governance structures. Here, a distinction is made between governance by the metaverse and the governance of the metaverse, with the former involving rules to guide the behaviours of all stakeholders, while the latter involves things that cannot be programmed, such as in the real world, where rules can be broken.

In addressing the social and ethical challenges of the metaverse, Benjamins et al. [39] suggested that the potential negative consequences of the massive use of technology demanded attention. Here, the metaverse was seen not only to face a range of technical, legal, business, economic, security, and user experience challenges, but also to face risks stemming from deliberately malicious, usually forbidden, actions, and from the unintended consequences of supposedly innocent actions. The authors look to learn from the experiences of artificial intelligence in identifying direct and indirect challenges. The direct challenges of the metaverse are those that companies can handle by themselves, and those that require government involvement, while indirect challenges refer to problems that begin to surface after some time, and were mainly unseen at the time of market launch. Benjamins et al. [39] also suggested that the metaverse could exacerbate existing mental health and liberty challenges, as well as "dual world" challenges, in that, if people spend ever more time in virtual worlds, they may become less sensitive to the consequences of their actions in the real world.

In turning to regulation, Rosenberg [36] effectively assumes that companies will not adopt trusted norms that would eliminate risks without government oversight, not least because the history of social media suggests that self-regulation, while often espoused by large and powerful corporations, may not be effective when implemented. He also argues that it is unrealistic to expect consumers to simply opt-out of the metaverse to avoid violations of their privacy and other abuses, not least because metaverse platforms could be one of the primary access points to digital content. Furthermore, Rosenberg [36] suggests that some level of government regulation will be required to prevent the exploitation of users within the metaverse. Such regulatory measures could include restricting both the monitoring and the emotional analysis of metaverse users, and restricting both virtual product placements and virtual personas within the metaverse.

4. Results

4.1. Case Study Findings

In its introduction to "Building a Responsible Metaverse", Accenture [9] (p. 3) claimed that "the world needs a responsible metaverse that is built with past lessons and existing challenges in mind so we can better anticipate—and account for—what lies ahead", and that "as companies look to build their own metaverse experiences, they must put trust at the core of their strategy". With this in mind, in 2022, Accenture [9] (p. 3) conducted a global survey of consumer experiences of the metaverse across 19 countries, and the results revealed "that consumers care about more than just the front-end experience and that organizations must dig deeper to earn their trust".

Accenture [9] (p. 4) argued that "to earn and maintain users trust, companies must make sense of a complex array of questions and trade-offs, related to technology, policy, ethics and business strategy", and that "companies will also have to apply past lessons to entirely new paradigms around data, ownership and governance". In addressing privacy, for example, Accenture claimed that the primary purpose in collecting, processing and sharing user data should be to deliver value to the user. To this end, Accenture [9] (p. 6) argued that "design decisions should feature privacy defaults that are intuitive given the context of the use case or experience", and that "companies should implement innovative strategies to educate users about the privacy options within the metaverse". In a similar vein, in addressing security, Accenture [9] (p. 6) argued "security by design should focus on hardening infrastructure and software against novel threats, particularly cybercrime,

fraud and disinformation", that "companies should use an adaptive zero-trust security model", and that "data protection should be in place to protect the confidentiality and integrity of experiences, data, and applications".

Accenture [9] (p. 7) describe safety as "the top priority in virtual environments", and maintains that "platforms must proactively implement policies, technologies and practices, to discourage harmful content and behaviours", and that "companies should invest in predictive and real-time detection capabilities as well as in-world features to enable users to manage their own safety". In focusing on sustainability, companies are advised "when deciding how to build and select hardware, software and platforms for the metaverse, companies should evaluate environmental impact, such as energy usage, emissions and e-waste", and that "users, creators and operators should be educated about what they can do to reduce the environmental footprint of the metaverse".

Accenture [9] (p. 9) identified six critical areas of focus that companies should start "exploring and understanding" and "building in guardrails", which "will provide a greater chance of alignment between the intended and the actual experiences of the metaverse". Here, the argument was that the closer this alignment, the greater the trust, and the more successful the metaverse will be. The six areas were: privacy by design and by default; the risks and rewards of tokenisation; interoperability; digital safety; sustainability; and identity and inclusion. As regards interoperability, for example, Accenture suggests that while the communities, platforms, marketplaces, and worlds of the metaverse are likely to operate with different degrees of openness, users will want to act seamlessly with applications and providers across virtual and digital asset platforms. Ultimately, operators will need to address several challenges to achieve interoperability, not least that the technology must be engineered to enable inoperability, which involves "the mobilization of vast resources as well as collective agreement and action from metaverse platforms" [9] (p. 13).

A3Logics [10] argued that, if the metaverse was to truly benefit humanity, social responsibility issues must guide its platform development from the start. More specifically. A3Logics [10] (p. 3) argued that "as the metaverse becomes more developed and adopted, social responsibility issues will become increasingly important to ensure that this new digital realm evolves positively and ethically". Five social responsibility issues were identified, namely safety and well-being; inclusivity; responsible innovation; governance; and combatting illegal activity.

In examining safety and well-being, it was argued that, as the metaverse caters to all ages, it will be crucial to implement safety features, parental controls, and policies to protect users from harm, violence, harassment, and addiction. At the same time, it was suggested that the metaverse must be designed so as to be accessible to people of all backgrounds, abilities and demographics, and thus issues such as diversity, accessibility and fairness, will clearly need attention. In outlining the importance of governance, A3Logics [10] (p. 3) noted that new rules, regulations, norms and standards should be developed to provide governance in the metaverse, and that "self-regulation by companies alone may not suffice".

Furthermore, environmental sustainability, inclusivity and combatting online harassment and toxicity are addressed. A3Logics [10] argued that, as the metaverse continues to develop, so there will be increasing concerns about its potential environmental impact. Here, the issues are seen to include energy consumption, e-waste, the reliance on rare earth metals, carbon dioxide emissions and material sourcing. Metaverse technologies will see huge increases in global energy demand to run the data centres, servers, and devices that power the metaverse, and this, in turn, will lead to substantial increases in carbon dioxide emissions and to further global warming. Looking to the future, A3Logics argued that the priority is to improve the efficiency of metaverse technologies by using more renewable energy sources and designing low-power options. The reliance of the metaverse technologies on rare earth metals and minerals, used in speakers, sensors and screens, for example, can have harmful environmental and social impacts related to their mining extraction and disposal.

While there are arguments that the metaverse could establish a more inclusive, diverse and connected world, such arguments are seen to largely depend on proactively designing inclusivity and diversity into the development process, and ensuring accessibility for users with disabilities and for underrepresented groups from the start. A3Logics [10] argued that this can be easily done by metaverse developer companies, that education can help awareness around inclusivity and diversity, and that challenging biases and broadening representation will be an ongoing process as the metaverse develops. There is also recognition that the metaverse will have the potential to amplify issues of online harassment and toxicity. Here, A3Logics [10] highlighted a number of critical considerations including identity anonymity and avoiding avatar designs and representations that promote stereotyping and dehumanisation.

Arguably more positively, A3Logics [10] (p. 3) claimed that "embedding social responsibility into metaverse development can help unlock several benefits", including gaining user trust; fostering innovation; avoiding regulation; and improving metaverse experiences. In focusing on trust, for example, the argument is that prioritising issues such as safety, privacy and inclusion can help convince users that their interests receive due consideration. Perhaps more tellingly, A3Logics [10] also argued that self-regulation through a culture of social responsibility could pre-empt the need for external intervention, that the case for government regulation would be seen to be less imperative, if concerns about privacy, security and safety were being proactively addressed, and that would allow the metaverse to develop with fewer restrictive regulations, and that the need for government regulation is less imperative when issues such as privacy, security and safety are proactively addressed.

4.2. Analysis

This sub-section assesses the case study findings and extant literature to address the two RQs set out in the introduction.

4.2.1. What Are the Main Risks and Responsibilities Associated with the Metaverse? (RQ1)

Figure 2 depicts the main risks and range of responsibilities associated with the metaverse evidenced either in the case studies and/or in the extant literature reviewed earlier. It is clear that many of these issues are inter-related and need to be treated accordingly, i.e., in a comprehensive manner. Here, user privacy and security, and then environmental impact and sustainability, are explored in more detail to illustrate the interrelationship and complexity of these issues.

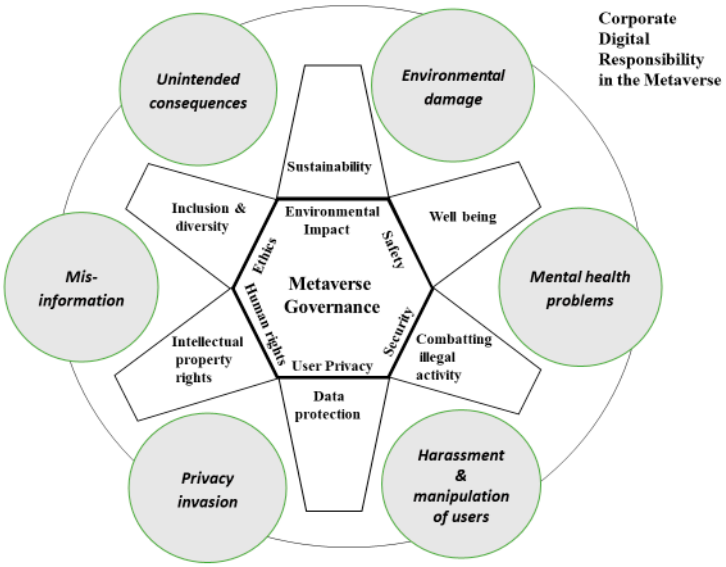

Figure 2. Risks (grey-shaded) and main elements of CDR in the metaverse.

Firstly, in addressing issues of user privacy and security, Madiega et al. [3] (p. 8) suggested that "the massive volumes of data circulating in the metaverse and the ways in which this data will be used constitute a growing risk for users". Here, issues were seen to include the security of metaverse-enabling devices, building secure protocols to mitigate the risk of the transfer of harmful code between platforms and thus enable the seamless movement of users between virtual spaces, as well as identify identity theft, avatar duplication and misuse. More generally, Flick [40] suggested that there are significant ethical concerns about the use of non-fungible tokens, and recommended that they should not be used unless these concerns are addressed or mitigated.

At the same time, the massive volume of personal and financial data available in the metaverse will continue to fall prey to hacking, sexual abuse, phishing and malware, while new forms of cybercrime, such as selling fake non-fungible tokens, malicious smart contracts and the illicit use of crypto-currencies may pose increasingly common challenges. There are also concerns that the metaverse will allow criminals and terrorists to use its multi-layered structure to hide behind encryption and untraceable non-fungible tokens to conceal their identity. Nair et al. [41], for example, reported on their empirical research which revealed that virtual reality attackers can access personal data from the seemingly anonymous users of popular metaverse applications such as VRChat. More generally, there are also growing concerns about links between the metaverse and the dark web.

Secondly, the potential development of the metaverse introduces new perspectives on the environmental impact of digital technology deployment. APlanet [42], the technology and sustainability consultancy, for example, questioned whether the metaverse will mean a waste, or a saving, of resources, and whether its environmental benefits will outweigh the negatives in terms of sustainability, suggesting that such questions are "shrouded in mystery" (para. 1). At the same time, Kshetri and Dwivedi [43] suggested that different metaverse applications vary widely in terms of their carbon footprints and environmental impacts, and that while the leisure and enjoyment activities of the consumer metaverse will have adverse energy and environmental consequences, many industrial metaverse applications are likely to have a positive environmental impact. Zhao and You [44] recognised that the metaverse is becoming a booming industry, but claimed that its climate impacts have not been quantitatively understood, and showed that it will facilitate climate change mitigation in five ways, namely working, traveling, education, non-fungible token, and gaming. More specifically, Zhao and You [44] suggested that increasing metaverse adoption can reduce global surface temperatures by up to 0.02 degrees centigrade before the end of the century, and lower greenhouse gas emissions. There are also claims that metaverse growth will accelerate decarbonisation and improve air quality, but that the environmentally responsible adaptation of the growth of the metaverse requires the transformation of the domestic energy supply. De Giovanni's [37] research into digital transformation and the metaverse also highlighted several negative consequences, including the environmentally unfriendly nature of blockchain.

There are thus differing and contrasting views on this issue. On the one hand, under the banner "sustainability in the metaverse", EY [45] (para. 3) claimed that "the metaverse holds the promise of substantial reductions in carbon emissions, whether through the substitution of physical goods with digital ones, replacing real world presence with digital interactions, or digital twins that will help us optimise the physical world, from the planet to individual humans", and that "the immersive nature of metaverse experiences could also help us to overcome our behavioural barriers to climate change". On the other hand, environmental and climate action pressure groups claim that the increasingly widespread use of the metaverse and the massive increase in computational power it will demand, will, for example, generate greatly increased carbon dioxide emissions. More generally, the Geneva Environment Network [46] (para. 7) claimed that "digital activity has become a multifaceted entity, comprising everything from video streaming and online gaming, to cryptocurrency trading and digital banking", that "these mediums come with an environmental price", that "despite its seemingly separate

existence from the physical world, digital technology has created its own unlikely carbon footprint", and that its impact on global sustainability is widespread.

4.2.2. How Will the Metaverse Be Regulated and How Will Companies Report on Their Metaverse Responsibilities to Their Stakeholders? (RQ2)

For the past two decades, a growing number of companies have produced corporate social responsibility (and sustainability, and more recently environmental, social and governance) reports to communicate how they manage and mitigate the impacts of their business activities. If companies operating in the metaverse choose to report on how they are discharging their metaverse responsibilities, though currently there is no statutory requirement for them to do so, they may use their existing corporate social responsibility reporting processes, within which CDR is increasingly recognised as a fifth arm, alongside environmental, philanthropic, ethical and economic responsibility [2].

However, the growth and development of the metaverse will entail new forms of corporate responsibilities that require greater regulation, probably from both within the corporate environment and from outside via individual platform controls and government agencies. In looking to the responsible regulation of the metaverse, and more particularly to the safety, privacy, and well-being of users, GMSA [47], identified a number of policy challenges, namely interoperability, safety and well-being, data privacy, cybersecurity, misinformation and competition. Interoperability, for example, is seen as a primary challenge to the effective functioning of the metaverse, but its promotion may require systems architects to work closely together to safeguard against closed systems and to implement common standards. At the same time, as the metaverse assumes an ever-greater business role, new privacy considerations, particularly involving data portability between digital platforms, and collecting personal information, will become increasingly important. Anshari et al. [5] suggested that any business must have a transparent policy regarding its metaverse applications to foster a culture of ethics and that to leverage the potential of the metaverse for business strategies, a number of ethical concerns have to be addressed. These concerns include keeping track of who will use or benefit from the massive volumes of data provided by the customer, and who will guarantee that no user profiling or digital personality mining will be undertaken for marketing or promotional purposes. Companies will need to protect users' privacy and rights, and will have an obligation to secure users' data by ensuring their data are not vulnerable to hackers.

In due course, it may thus be most appropriate, as suggested by Mihale-Wilson et al. [48] (p. 18), to view corporate digital responsibility as "distinct" from corporate social responsibility, and thus to see it as requiring its own distinct reporting process. At present, whether companies will choose to pursue such a route in communicating on the discharge of their responsibilities for the metaverse remains to be seen, and will depend to some extent on which metaverse emerges over the next decade. If the more advanced dominant metaverse outlined by Deloitte [15] comes to fruition in the next decade, then the implications for CDR and the need for regulation are similarly moved forward at pace (Table 2).

Table 2. Regulatory measures in the metaverse variations.

Type of Metaverse	Uses and Applications in Corporate Environment	Probable Regulatory Measures
Basic	Team collaboration and conferences, augmented training/learning, and immersive digital twins.	No consistent external regulation specific to the metaverse. Access and usage regulated within CDR at the company level.
Intermediate	Businesses use a variety of metaverse platforms for different company operations. Ecosystems compete on the basis of offered services offered.	Platforms enact strong and effective self-governance to complement CDR company norms.
Dominant	The full migration of the developed Internet into an immersive world in which most businesses and consumers operate.	Government, platform-specific and corporate regulations provide strong governance, strict and enforceable rules around digital ownership, privacy, security and other CDR aspects.

In parallel with its practical development, it is vitally important to develop theoretical perspectives to help understand the nature of the metaverse, its relationships with corporate social responsibility and locate it within the business environment, but also more widely within social structures. Whilst work in this field is still very much in its infancy, Anshari et al. [5] identified two sets of theories, namely utilitarian theory, and stakeholder theory, as offering some guidance regarding the possible ethical, and the responsibility-related, risks generated by the metaverse. On the one hand, Anshari et al. [5] argued that utilitarian theory is useful in understanding why organisations would choose the metaverse to develop their business activities despite the risks. Put simply, adopting the metaverse is seen to be appropriate if it results in greater happiness than adverse reactions, for example, stress and suffering. On the other hand, Anshari et al. [5] also point out that stakeholder theory emphasises the importance of making sure that all stakeholders are aware of both the risks and the benefits of the metaverse. Hemphill [49] looked to take this issue further by integrating stakeholder theory with responsible innovation scholarship, and by focusing on the questions, consequences and ethical dilemmas that companies will need to address when creating and manufacturing future products for the metaverse. Hemphill [49] argued that his approach will bring a sense of legitimacy that businesses will be able to harness in the social and public policy arenas, when looking to establish formal standards and eventually in commercial product implementation.

Whichever version of the metaverse is developed and implemented in the business community, it will be important to ensure that what is reported can be understood by all stakeholders, especially the users. The independent external assurance and verification of the claims that companies make about the impact of their business activities, and how they manage those impacts, will surely determine the credibility of the reporting process. Here, there may be concerns that few companies will have the expertise to undertake assurance process, and that many of those that are may be major players in the metaverse themselves, and thus commercial sensitivities may be seen as a problem. The platform providers will almost certainly have to impose some measure of self-regulation, but external regulation by governments and other agencies also seems inevitable, given the already considerable concern expressed by global governments regarding the current use of artificial intelligence and other digital technologies [23].

5. Conclusions

The case studies outline many of the responsibilities associated with the development of the metaverse, but in some ways, the outline of these responsibilities, and the issues surrounding them, raises as many, perhaps more, questions than it answers. While many companies may initially look to focus their strategic thinking on creating immersive marketing opportunities, expanding audience engagement and digital advertising, if companies lose sight of their strategic responsibilities for the metaverse, and in so doing lose consumers' trust, then they may find it increasingly difficult to reap the potential business benefits claimed for the metaverse. This paper has tried to illuminate and illustrate the complexities and uncertainties of discharging the strategic responsibilities inherent in the future development of the metaverse.

However, this paper has a number of limitations, not least in that it is not based on empirical corporate data, and in that it draws its information exclusively from Internet sources. Nevertheless, it offers some insights into the guidance available to companies who are looking to lay the foundations for the responsible metaverse, and as such, helps to fill a gap in the academic literature. At the same time, this paper might provide a platform for future research into how companies are addressing their responsibilities for the metaverse. While a wide range of specific research avenues might be identified, two general themes would seem to stand out. On the one hand, it is important to develop a theoretical framework to help to locate corporate responsibility for the metaverse within the wider business and social context, and to provide a framework to underpin what will surely be a diverse and rapidly growing body of research work on corporate responsibilities for

the metaverse. On the other hand, a variety of empirical studies might profitably explore how companies are addressing, introducing, and reporting on their responsibilities for the metaverse, and on consumers' awareness and understanding of how companies discharge such responsibilities.

Author Contributions: Conceptualisation, M.W.; methodology, M.W. and P.J.; formal analysis, M.W. and P.J.; investigation, M.W. and P.J.; data curation, M.W. and P.J.; writing—original draft preparation, M.W. and P.J.; writing—review and editing, M.W. and P.J.; project administration, M.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are available via the referenced sources.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Stephenson, N. *Snow Crash*; Bantam Books: New York City, NY, USA, 1992.
2. Wynn, M.; Jones, P. Corporate responsibility in the digital era. *Information* **2023**, *14*, 324. [CrossRef]
3. Madiega, T.; Car, P.; Niestadt, M.; Van de Pol, L. *Metaverse: Opportunities, Risks and Policy Implications*; European Parliamentary Research Service: Brussels, Belgium, 2022; Available online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557 (accessed on 6 September 2023).
4. KPMG. The Metaverse: Why Governments Should Care. 2023. Available online: https://kpmg.com/xx/en/blogs/home/posts/2023/01/the-metaverse-why-governments-should-care.html (accessed on 28 August 2023).
5. Anshari, M.; Syafrudin, M.; Fitriyani, N.L.; Razzaq, A. Ethical Responsibility and Sustainability (ERS) Development in a Metaverse Business Model. *Sustainability* **2022**, *14*, 15805. [CrossRef]
6. Charamba, K. Beyond the Corporate Responsibility to Respect Human Rights in the Dawn of a Metaverse. *Univ. Miami Int. Comp. Law Rev.* **2022**, *30*, 110–149.
7. Mogaji, E.; Wirtz, J.; Belk, R.W.; Dwivedi, Y.K. Immersive time (ImT): Conceptualizing time spent in the metaverse. *Int. J. Inf. Manag.* **2023**, *72*, 102659. [CrossRef]
8. Hanneke, R.; Asada, Y.; Lieberman, L.; Neubauer, L.; Fagan, M. *The Scoping Review Method: Mapping the Literature in Structural Change Public Health Interventions, SAGE Research Methods Cases Part 2*; Department of Public Health Scholarship and Creative Works, 2017; Volume 94, pp. 1–14. Available online: https://digitalcommons.montclair.edu/public-health-facpubs/94 (accessed on 6 May 2023). [CrossRef]
9. Accenture. Building a Responsible Metaverse. 2023. Available online: https://www.accenture.com/gb-en/insights/technology/responsible-metaverse (accessed on 3 August 2023).
10. A3Logics. Why Companies Need to Be Socially Responsible in Metaverse Development. 2023. Available online: https://www.a3logics.com/blog/why-companies-need-to-be-socially-responsible-in-metaverse-development (accessed on 29 July 2023).
11. Bowen, G.A. Document analysis as a qualitative research method. *Qual. Res. J.* **2009**, *9*, 27–40. [CrossRef]
12. Tucci, L. *What Is the Metaverse? An Explanation and In-depth Guide*; TechTarget: Newton, MA, USA, 2022; Available online: https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know#:~:text=The%20metaverse%20is%20a%20vision,not%20in%20the%20physical%20world (accessed on 30 June 2023).
13. McKinsey. Marketing in the Metaverse: An Opportunity for Innovation and Experimentation. 2022. Available online: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/marketing-in-the-metaverse-an-opportunity-for-innovation-and-experimentation (accessed on 29 June 2023).
14. Marabelli, M.; Newell, S. Responsibly strategizing with the metaverse: Business implications and DEI opportunities and challenges. *J. Strateg. Inf. Syst.* **2023**, *32*, 101774. [CrossRef]
15. Deloitte. A Whole New World: Exploring the Metaverse and What It Could Mean for You. 2022. Available online: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-what-is-the-metaverse-new.pdf (accessed on 2 July 2023).
16. Mystakadis, S. Metaverse. *Encyclopedia* **2022**, *2*, 486–497. [CrossRef]
17. PWC. Demystifying the Metaverse. 2023. Available online: https://www.pwc.com/us/en/tech-effect/emerging-tech/demystifying-the-metaverse.html (accessed on 6 September 2023).
18. Mager, S.; Matheson, B. Rising Technologies for Marketers to Watch. Deloitte Insights. 2023. Available online: https://www2.deloitte.com/uk/en/insights/topics/marketing-and-sales-operations/global-marketing-trends/2023/rising-technology-trends-for-marketing.html (accessed on 17 August 2023).

19. Stackpole, T. What Is Web3? Harvard Business Review. The Big Idea Series. 2022. Available online: https://hbr.org/2022/05/what-is-web3 (accessed on 4 September 2023).
20. Huynh-The, T.; Gadekallu, T.R.; Wang, W.; Yenduri, G.; Ranaweera, P.; Pham, Q.-V.; Benevides da Costa, D.; Liyanage, M. Blockchain for the metaverse: A Review. *Future Gener. Comput. Syst.* **2023**, *143*, 401–419. [CrossRef]
21. Kiran, M.B.; Wynn, M. The Internet of Things in the Corporate Environment. In *Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies*; Wynn, M., Ed.; IGI-Global: Hershey, PA, USA, 2022; pp. 132–148. ISBN 9781799877127. Available online: https://eprints.glos.ac.uk/10497/ (accessed on 12 July 2023).
22. Lawton, G. *Spatial Computing*; TechTarget: Newton, MA, USA, 2023; Available online: https://www.techtarget.com/searchcio/definition/spatial-computing (accessed on 16 September 2023).
23. Jones, P.; Wynn, M. Artificial Intelligence and Corporate Digital Responsibility. *J. Artif. Intell. Mach. Learn. Data Sci.* **2023**, *1*, 50–58.
24. Ripert, D. *The Pathway to the Metaverse Begins with 3D Modelling*; Entrepreneur Science and Technology: Irvine, CA, USA, 2022; Available online: https://www.entrepreneur.com/science-technology/the-pathway-to-the-metaverse-begins-with-3d-modelling/425643 (accessed on 5 September 2023).
25. Xi, N.; Chen, J.; Gama, F.; Riar, M.; Hamari, J. The challenges of entering the metaverse: An experiment on the effect of extended reality on workload. *Inf. Syst. Front* **2023**, *25*, 659–680. [CrossRef]
26. Abdelghafar, S.; Ezzat, D.; Darwish, A.; Hassanien, A.E. Metaverse for Brain Computer Interface: Towards New and Improved Applications. In *The Future of Metaverse in the Virtual Era and Physical World*; Hassanien, A.E., Darwiish, A., Torky, M., Eds.; Studies in Big Data; Springer: Cham, Switzerland, 2023; Volume 123, pp. 43–58. [CrossRef]
27. Pratt, M.; Daniel, D. The CIO's Guide to Understanding the Metaverse. 2022. Available online: https://www.techtarget.com/searchcio/feature/The-essential-introduction-to-the-metaverse-for-CIOs?utm_campaign=20220316_The+CIO%27s+essential+guide+to+the+metaverse&utm_medium=EM&utm_source=NLN&track=NL-1808&ad=940624&asrc=EM_NLN_211154075 (accessed on 23 August 2023).
28. Mollajafari, S.; Bechkoum, K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy. *Sustainability* **2023**, *15*, 13401. [CrossRef]
29. Pratt, M. 10 Metaverse Use Cases for IT & Business Leaders. Computer Weekly.com E-guide. 2022. Available online: https://www.computerweekly.com/ehandbook/10-metaverse-use-cases-for-IT-and-business-leaders (accessed on 28 June 2023).
30. Capgemini. The Metaverse—Opportunities for Business Operations. 2023. Available online: https://www.capgemini.com/insights/research-library/the-metaverse-opportunities-for-business-operations/ (accessed on 5 September 2023).
31. Collins, C. Looking to the Future: Higher Education in the Metaverse. *Educ. Rev.* **2008**, *43*, 50–52.
32. Purdy, M. Building a Great Customer Experience in the Metaverse. Harvard Business Review. 3 April 2023. Available online: https://hbr.org/2023/04/building-a-great-customer-experience-in-the-metaverse (accessed on 7 September 2023).
33. Choder, B. Meetings in the Metaverse: Is this the Future of Events and Conferences? *Forbes*. 13 January 2022. Available online: https://www.forbes.com/sites/forbescommunicationscouncil/2022/01/13/meetings-in-the-metaverse-is-this-the-future-of-events-and-conferences/?sh=1d2089728a1f (accessed on 5 September 2023).
34. Lee, C.W. Application of Metaverse Service to Healthcare Industry: A Strategic Perspective. *Int. J. Environ. Res. Public Health* **2022**, *19*, 13038. [CrossRef]
35. Nichols, S. Metaverse Rollout Brings New Security Risks, Challenges. 2022. Available online: https://www.techtarget.com/searchsecurity/news/252513072/Metaverse-rollout-brings-new-security-risks-challenges (accessed on 30 July 2023).
36. Rosenberg, L. Regulation of the Metaverse: A roadmap: The Risks and Regulatory Solutions for Largescale Consumer Platforms. 2022. Available online: https://dl.acm.org/doi/abs/10.1145/3546607.3546611?casa_token=nzlplVhYPnUAAAAA:fWQ9iX6aNy0PaW_-69iRVgITMoXMlDy62gSSVHTBUgLCWbwS3oDnLH9mLX-B_hnqXUtYuTKI2Zy1lA (accessed on 7 June 2023).
37. De Giovanni, P. Sustainability of the Metaverse: A transition to industry 5.0. *Sustainability* **2023**, *15*, 6079. [CrossRef]
38. Schobel, S.M.; Leimeinster, J.M. Metaverse platform ecosystems. *Electron. Mark.* **2023**, *33*, 12. [CrossRef]
39. Benjamins, R.; Vinuela, Y.R.; Alonso, C. Social and ethical challenges of the metaverse. *AI Ethics* **2023**, *3*, 689–697. [CrossRef]
40. Flick, C. A critical professional ethical analysis of nonfungible tokens (NFTs). *J. Responsible Technol.* **2022**, *12*, 100054. [CrossRef]
41. Nair, V.; Garrido, G.G.; Song, D. Exploring the Unprecedented Privacy Risks of the Metaverse. 2022. Available online: https://arxiv.org/abs/2207.13176 (accessed on 5 May 2023).
42. Aplanet. Metaverse and Sustainability: Friends or Foes. 2022. Available online: https://aplanet.org/resources/metaverse-and-sustainability-friends-or-foes/ (accessed on 6 September 2023).
43. Kshetri, N.; Dwivedi, Y.K. Pollution-reducing and pollution-generating effects of the metaverse. *Int. J. Inf. Manag.* **2022**, *69*, 102620. [CrossRef]
44. Zhao, N.; You, F. The growing metaverse sector can reduce greenhouse gas emissions by 10 Gt CO_2e in the united states by 2050. *Energy Environ. Sci.* **2023**, *16*, 2382–2397. [CrossRef]
45. EY. Metaverse: Could Creating A Virtual World Build A More Sustainable One? 2022. Available online: https://www.ey.com/en_uk/digital/metaverse-could-creating-a-virtual-world-build-a-more-sustainable-one (accessed on 2 September 2023).
46. Geneva Environment Network. Data, Digital Technology, and the Environment. 2021. Available online: https://www.genevaenvironmentnetwork.org/resources/updates/data-digital-technology-and-the-environment/ (accessed on 23 July 2023).

47. GSMA. The Year Ahead in Digital Policy; Regulating the Metaverse. 2023. Available online: https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse#:~:text=Given%20that%20the%20metaverse%20is,kinds%20of%20interactions%20and%20transactions (accessed on 10 September 2023).
48. Mihale-Wilson, C.; Hinz, O.; van der Aalst, W.; Weinhardt, C. Corporate Digital Responsibility. *Bus. Syst. Inf. Eng.* **2022**, *64*, 127–132. [CrossRef]
49. Hemphill, T.A. The Metaverse and the challenge of responsible standards development. *J. Responsible Innov.* **2023**, *10*, 2243121. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.