Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)108

09.12.2022

DIGITAL COMMITTEE HEARING ON "WEB 3.0 AND THE METAVERSE"

RESPONSES TO WRITTEN QUESTIONS

ELIZABETH M. RENIERIS
hackylawyer@protonmail.com

1. **What are the concepts and considerations underpinning, respectively, "Web 3.0" (in the sense of the semantic web), "Web3" and "the Metaverse", what are the differences between them and what are the anticipated opportunities and risks associated, and what do they each mean for the structure and architecture of an open, free and also secure and user-centred network – in short, do they represent a version of the internet that is to be prevented?**

At present, there is no consensus as to what the terms "Web 3.0," Web3" and "the Metaverse" mean or represent. Rather, they are often used interchangeably and in different ways to support the varied, and sometimes competing, interests of various stakeholders. That said, they all refer to ideas and machinations about what the future of our digital experience might look like, particularly in contrast to our experience today.

"Web 3.0" is an older, narrower term of art, generally associated with Sir Tim Berners Lee's description of a third generation of the Web, which he first articulated several decades ago. In this paradigm, Web 1.0 refers to a "read only" version of the web, consisting largely of static web pages and content; Web 2.0 refers to a "read-write" version, which enabled the rise of user-generated content, social media, and increased interactivity; and Web 3.0 refers to a "read-write-execute" or "semantic web" (sometimes also referred to as a "web of data") in which everything is connected at the level of data. According to Berners Lee, Web 3.0 neither requires nor benefits from the use of blockchain technology.

Although often used interchangeably with Web 3.0, "Web3" is a broader, more nebulous term used to describe a theoretically more decentralised web than we have today; it is sometimes referred to as the "read-write-own" web. It typically involves a combination of blockchain or distributed ledger technology (DLT), self-executing lines of code (known as "smart contracts"), non-fungible tokens (NFTs), and cryptocurrencies. From a technical standpoint, Web3 is purported to represent a shift away from the existing web's traditional client-server architecture, whereby data is concentrated in and funneled through centralized servers belonging to large corporations, to more peer-to-peer arrangements and protocols, allowing network resources to communicate and exchange data directly.

"Web 3.0" and "Web3" are often positioned as "better" versions of the digital ecosystem than we have today and presented as solutions to the ongoing privacy and security concerns posed by the Web's concentration of power in a handful of large corporations. However, both concepts are problematic because they attempt to solve non-technical problems, such as this concentration of wealth and power in a small handful of private corporations, with mostly technological interventions, while ignoring the social,

political, economic, and cultural factors that gave rise to these problems in the first place. In other words, they represent largely techno-solutionist perspectives.

Finally, "the Metaverse" or "metaverse" is a concept that emanates from science fiction and was first used by Neal Stephenson in a 1992 novel titled *Snow Crash*, which depicted the metaverse as an internet-based virtual reality space with avatars and software agents. Today, it broadly refers to a network of virtual worlds or a kind of immersive internet enabled by a suite of extended reality (XR) technologies such as virtual reality (VR), augmented reality (AR), and mixed reality (MR); hardware such as headsets, wearables, and other connected devices; the use of physical and behavioral biometrics; avatars and other digital identity tools; and artificial intelligence (AI) and machine learning-powered systems. Rather than refer to any kind of "metaverse" as a fully formed concept or ecosystem, however, I prefer to characterize these technologies as *metaversal technologies*.

While none of these terms or concepts represents a "version of the internet that is to be prevented" per se, those who promote visions of Web 3, Web 3.0, and the metaverse often make claims that must be challenged (and sometimes embrace ideologies that are socially, politically, and economically problematic, as further described below). As such, law and policymakers, academics, members of civil society, and other stakeholders should seek to apply a critical lens to Web3 or metaverse-related projects, and place the evidentiary burden of proof on promoters to demonstrate clear benefits.

2. What are the technical, security-related, infrastructure-critical, conceptual, social, financial policy, foreign policy and societal risks of Web3, what are the risks in terms of personal rights and civil liberties?

From a technical, security-related, and infrastructural perspective, Web3 largely relies on a combination of untested, unreliable, and insecure technologies that introduce additional layers of complexity, which, in turn, increases the risks of failures and vulnerabilities. For example, its proponents often claim that Web3 will give individuals back "control" over the privacy and security of their data from large, centralised intermediaries such as Meta and Google. In reality, however, Web3 typically offers two equally bad alternatives to the existing model. In one version, existing intermediaries are replaced with newer, less accountable ones (and, even then, those intermediaries often still rely on the services and infrastructure of traditional intermediaries, e.g., Amazon Web Services or Google Cloud Platform, replicating the associated challenges). In the other version, individuals are unreasonably burdened with having to manage and secure their own wallets, keys, and data, with no recourse or remedy when things inevitably go wrong. This approach disproportionately impacts different individuals and communities, often imposing the highest burden on the most vulnerable.

From a conceptual perspective, Web3 proponents also exhibit a kind of imaginative obsolescence whereby one vision of the future rapidly replaces the next, while existing technologies and systems, which billions

of people presently rely on every day, suffer decay and disrepair. In other words, the promise of Web3 diverts our imaginations and resources from fixing known problems or rehabilitating what exists, to conjuring up technological utopias in which these problems don't resurface. This also upends efforts at effective technological governance and "kicks the can down the road" while we wait for new laws and regulations to emerge, while failing to apply existing ones. It also represents a kind of longtermism in the sense of neglecting to confront and address real and present dangers of existing sociotechnical systems in favour of some future utopian ideals.

From an economic and societal standpoint, Web3 also risks exacerbating our commercial exploitation via digital interactions. Whereas the early Web was largely a non-commercial content distribution network until e-commerce introduced the offering of products and services online, blockchain-based versions of Web3 would use "smart contracts" to turn every digital interaction into a financial transaction with a corresponding micropayment in the form of a cryptocurrency, often with one or more opaque intermediaries taking transaction fees. With this "financialization of everything," as some have described it, comes the risk that we are no longer capable of being passive users of content or digital citizens of the Web but rather that we come to view ourselves first and foremost as commercial actors or wholly commodified entities in an increasingly complex financial system.

The above concerns, taken together, also present grave risks to our personal rights and civil liberties. If we overemphasise and overinvest in technical solutions to nontechnical problems, resulting in a kind of imaginative obsolescence that neglects existing challenges and allows for the unchecked commodification of human experience, there will be little left of rights and liberties. For example, if we consider how meaningless "consent" has become in the context of asymmetrical digital interactions that harvest personal data, consider how a micropayment or explicit financialization of such interactions would afford them a kind of false legitimacy, rubberstamping the transactional nature of our experience. If we accept the financialization of everything and come to view ourselves as principally commercial actors, we also undermine the civil and human rights that attach to being citizens or humans.

3. **Are the existing European regulatory approaches (such as DSA, DMA and GDPR) sufficient and which regulatory measures beyond these do you view as suitable or necessary in order to contain the risks of Web3 and what options do you see for otherwise mitigating the risks mentioned?**

It is difficult to say whether existing European regulatory approaches are sufficient, particularly with respect to recently introduced laws such as the DSA, DMA, DGA, Data Act, and AI Act, among others, as they are mostly new and untested at this stage. That said, the key to their applicability and effectiveness will be the extent to which law and policymakers can challenge and dissect the claims of Web3 promoters to see their activities and institutions for what they are, rather than what they are claimed to be. For example, distributed technical architecture (e.g., geographically distributed nodes in a blockchain network)

is not the same as decentralised sociopolitical or economic control; a technically decentralised app (or dApp) does not automatically imply the absence of intermediaries or enhanced data security or privacy; and the anonymity of decisionmakers in a DAO is not a basis for avoiding responsibility or evading accountability. By applying a critical lens and sticking to first principles, we can avoid the endless quest for "perfect laws" that may never come.

With specific regard to the GDPR, it should continue to apply in all aspects to Web3 as most permutations and Web3 systems still consist of entities who can be deemed to be data controllers, data processors, and data subjects, despite the sometimes-increased difficulty and complexity in identifying their respective roles and responsibilities. For example, that a blockchain-based personal data management system allows individuals to manage and store personal data in a user-controlled digital wallet does not imply the absence of a data controller-data subject relationship, in so far as the system is designed in ways that dictate the purposes and means for processing data. Moreover, where there are inherent and irreconcilable tensions as between the GDPR and proposed technical architectures, they should be deemed non-compliant with the existing regulations and held accountable for addressing compliance gaps.

Here it is important to note that the GDPR only addresses data protection, which is only one of many important civil and human rights and freedoms implicated by Web3 systems (and metaversal technologies more generally). While important, we must not lose sight of the way in which even data protection-compliant systems can result in unfair and discriminatory outcomes, inequitable treatment, a lack of due process, and significantly undermine privacy, autonomy, personal dignity, and more collective economic, social, and cultural rights. In other words, in a version of the web built on linked data and code-based commercial transactions, ensuring the privacy or security of data will not be enough to ensure the privacy or security of people.

4. How do you assess the opportunities and risks of cryptocurrencies — in general and in the context of Web 3.0?

On balance and based on the evidence that we have to date, cryptocurrencies present more risks than opportunities. Cryptocurrencies purport to disintermediate financial transactions, disrupt traditional banking, and promote financial inclusion. But according to a recent report from Cambridge University, cryptocurrencies lack the stability, usefulness, and accessibility to achieve any of these ends. Instead, to date, cryptocurrencies have introduced a host of new, opaque, and unaccountable intermediaries; posed little threat to the traditional financial system or large conventional banks (whose innovation labs have embraced blockchain and cryptocurrencies as a marketing tool); and done little to address financial inclusion. In fact, one of the only inclusive aspects of cryptocurrencies to date has been the widespread economic devastation of millions of cryptocurrency investors who have lost money in uncollateralized schemes—losses that have disproportionately impacted minority investors.

Specifically in the context of Web3, cryptocurrencies are also being injected into all manner of sociotechnical systems in ways that present serious risks of discrimination, exclusion, harassment, and invasions of privacy and autonomy. For example, Web3 digital identity projects such as WorldCoin, which are largely being tested in the developing world, use invasive biometric technologies such as iris-scanners to establish blockchain-based identities for a "global digital currency" scheme. But although WorldCoin, and blockchain-based digital identity projects in Myanmar, Turkey, and the Netherlands, among other places, purport to support financial and social inclusion, they fail to address the underlying social, political, and economic causes for exclusion in existing financial and identity systems, positioning technology as a comprehensive solution. In other words, they again exhibit a high degree of techno-solutionism.

Even in the limited instances where cryptocurrencies may result in financial or social inclusion, these systems typically rely on combinations of opaque technologies that introduce significant complexity. It is widely appreciated that intermediaries, whether banks in the financial context or digital platforms in the online context, offer significant benefits in terms of security, accessibility, and convenience. But Web3 projects often expect individuals to manage their own wallets, keys, and cryptographic protocols, burdening individuals with the responsibility for the privacy and security of their data or other assets and leaving them without any recourse or remedy when things (inevitably) go wrong, while neglecting the disproportionate impacts this has on the accessibility or usability of the tech for different people and communities.

Despite these risks, cryptocurrency promoters argue that it is still early days for the technology and the benefits remain to be realised, but that is not in fact the case. Bitcoin, the most widely known cryptocurrency, has been around for more than a decade, and remains highly concentrated in the hands of a few, with limited real-world applicability or utility beyond speculative purposes. Moreover, notions of blockchain and electronic money or "ecash" (precursors to cryptocurrencies) have been around for nearly four decades, and the underlying cryptographic concepts and methods have been around for much longer. Meanwhile, other digital technologies, such as smart phones and certain IoT devices, have had demonstrable benefits in significantly shorter time horizons.

A deeper problem still with cryptocurrencies is the ideologies that promoters often espouse, typically featuring a kind of neoliberalism centered on the supremacy or self-sovereignty of the individual, sometimes also expressed as an absolute freedom to transact. Not only does this unduly burden the individual (with an uneven and disparate impact on certain populations) but this orientation is particularly problematic at a time of great collective challenges like climate change, racial injustice, and rising authoritarianism, and risks undermining important collective goals, whether social, political, environmental, or economic. Moreover, the elevation of one right above all others also threatens core international human rights principles regarding the interrelatedness, interdependence, and indivisibility of rights.

5. What specific application areas and added value, aside from virtual gaming, can metaverses offer (e.g., in medicine or engineering)?

In so far as we consider the metaverse to be any immersive or virtual digital experience, there are potentially valuable applications in terms of jobs or skills training. For example, augmented and virtual reality have long been used in the aeronautical and aerospace industries to train pilots and astronauts in different skills and simulate in-flight scenarios. Increasingly, VR is also being used to train medical students and practitioners by allowing them to practise medical or surgical techniques and procedures through virtual simulations. Beyond training, there are also potentially valuable applications in practice, as in the case of virtual remote medical consultations. VR tools are now also being used by military and law enforcement personnel for training exercises and investigations.

As these use cases gain traction, there are mounting concerns that virtual training environments do not always effectively replicate or account for the complexities of real-world activities or scenarios and can result in an overinflated degree of confidence in one's abilities or expertise when applied in practice. Additionally, metaverses or virtual spaces may not always be designed with accessibility in mind and can therefore be of limited use to individuals with cognitive, sensory, or physical limitations or impairments, and potentially limit their professional development or skills training in an inequitable fashion. Where the use of VR and other metaversal tools is deemed appropriate, they should ideally be deployed in combination with or alongside other modalities to promote inclusion and accessibility.

6. Unlike Web 3.0, Web3 describes a new generation of the internet, based on blockchain and in which users are to have control of their data (the concept for Web3 includes, for example, decisions on DAOs, the establishment of a token-based economy, financial services using DeFi protocols). What is your assessment of the potential of Web3, especially in light of the fact that without a central intermediary, the user often forgoes convenience?

It is important to separate the claims that Web3 promoters make with respect to user control over data from the realities of these projects in practical effect. While there is widespread agreement that the existing web is riddled with a concentration of power in the hands of a few large corporations who have over-exploited personal data for commercial gain, often resulting in harmful outcomes for individuals and communities, and while the desire to address these challenges is laudable, there is no evidence that Web3 will in fact solve or address them.

First, as already noted above, Web3 interventions often do not actually result in any kind of disintermediation. Rather, they often replace existing intermediaries with newer, more opaque and unaccountable ones who are not subject to the same incentives or levers that can be used to hold existing intermediaries to account (such as the existence of known and identifiable executives and accountable parties; existing laws and regulations; business continuity and emergency planning, mandatory

transparency reporting, shareholder accountability, and other corporate governance mechanisms; compliance programs and expertise that can be leveraged for new technologies; and relationships with regulators, among others). Web3 and crypto intermediaries often hide behind anonymity or pseudonymity, code, and jurisdictional arbitrage (frequently operating through offshore entities to avoid tax liability and compliance obligations).

But even where they might result in any kind of meaningful disintermediation, this is not necessarily a benefit to impacted individuals or communities. Take, for example, personal data management. While many would like to control and manage their own data in theory, few would like to do so in practice. Given the scope and scale of digital, data-based interactions and transactions that an individual faces in daily life today, it is simply not reasonable or practical to expect fully self-managed systems. It would be a recipe for behavioural failures, including overwhelm and consent fatigue. Thus, in the case of actual disintermediation, individuals would forego more than mere convenience. They would sacrifice safety and security, tasked with managing complex technical tools and systems (the mantra "not your keys, not your crypto" comes to mind here). They would also forego effective recourse and remedy, without easily identifiable entities or individuals to hold accountable, and possibly diminish their privacy based on the false confidence that the overly inflated cryptographic capabilities of these systems might induce.

Web3 promoters often claim that blockchain is key to privacy and autonomy in the digital age, but "censorship-resistant" technologies actually pose a major threat to our privacy and autonomy. Blockchain's most frequently cited benefits include greater transparency, improved traceability, and increased speed and efficiency—core features that do not disappear when the technology is applied to humans. In worrying about the "censorship resistance" of transactions, we lose sight of the impact on humans. By creating a permanent, digital record of our transactions, we make ourselves more vulnerable to external control and self-censorship. In this way, Web3's proposition of rebuilding our digital ecosystem on top of blockchain, risks leaving people more transparent (i.e., exposed), traceable (i.e., surveillable), and efficient (i.e., transactional)—qualities which are also conducive to authoritarian impulses.

7. **Which political measures are advisable in order to ensure that metaverse spaces currently being created are based on European values–in particular data and consumer protection–and the principles of the digital EU single market–in particular fair competition and sustainable ("green IT") and manipulation-free (no "dark patterns") design?**

While important, data protection and consumer protection are too narrow a lens to protect important values in relation to metaverse spaces and the use of metaversal technologies. After all, we are more than just data subjects and consumers in these virtual spaces. We remain citizens and human beings with important civil and political rights. As such, to best ensure that metaverse spaces respect European values, companies offering such virtual services and metaversal technologies should be held to a duty to respect

long-standing human rights standards and principles, with particular regard for the European Convention on Human Rights and the EU Charter of Fundamental Rights, as well as for international human rights law more generally, in accordance with the UN Guiding Principles on Business and Human Rights.

Moreover, rather than attempt to regulate a "metaverse" as such, law and policymakers should focus on applying existing laws and regulations to the constituent products and services that make up a given metaverse-based offering. For example, metaverses in the form of virtual workspaces and workplace tools should be subject to existing rules and obligations that bind employers and required to afford employees the same rights and protections as they enjoy in non-virtual contexts, including through existing labour laws. In line with the EU's principle that "what is illegal offline should also be illegal online," what is illegal in non-virtual spaces must also be illegal in virtual ones. In other words, the metaverse should not enjoy any kind of exceptional treatment or escape existing laws and regulations.

8. What specific starting points are there, with regard to the development of the internet so far (Web1, Web2), for transferring development towards a user-oriented, decentralised and secure internet into global governance mechanisms?

I am not convinced that a "user-oriented, decentralised, and secure internet" is possible or even desirable. Too often "user-oriented" means overburdening individuals with an unmanageable number of decisions, choices, and trade-offs, in a way that leaves the individual more vulnerable than the alternatives. For example, a long-standing paradigm in data protection and privacy law is the "notice and choice" or "notice and consent" framework. Though it was long heralded as promoting the privacy, security, and autonomy of individuals online, the reality in practice has been quite the opposite. This hyper-individualistic approach has left individuals exceedingly vulnerable as they are inundated with opaque legalese in the form of corporate privacy notices, terms and conditions, cookie consent popups, and more, to create the illusion of user control over privacy. Imagine extending this broken framework to virtual spaces, where qualitatively new and different user interfaces (beyond the graphical user interface) introduce additional challenges to providing meaningful notices and obtaining real-time consent. It's simply the wrong paradigm.

Moreover, as already explored above, "decentralised" is another buzz word that has not panned out in practice. In earlier iterations of the Web, ideological subgroups also promoted the idea of decentralisation as a kind of holy grail. At the height of the dot com boom, John Perry Barlow and the cyberlibertarians depicted "cyberspace" as a wholly separate and new reality, not subject to the laws of man or physics. Modern-day crypto libertarians follow in this same tradition, seeking exceptional treatment of their products and services, arguing that existing laws and regulations do not apply to their ecosystems.

But intermediaries are valuable, as are institutions, in providing individuals with a degree of safety, security, and recourse when things go wrong. On the other hand, many cryptocurrency and Web3

promoters undermine institutions (whether governments, universities, or banks) even as they free ride on existing legal and political infrastructure, recreate new institutions with the same challenges, and refuse to accept the same levels of responsibility or accountability. More important than any kind of technical decentralisation is to address the concentration of economic and political power in digital governance and to ensure that the rules and standards applied reflect a broad range of global stakeholders, rather than serving the interests of a few.

Moreover, a "secure internet" is not just a matter of blockchain or any other technical architecture, as proponents of Web3 or the metaverse would have us believe. Even the best technical security is vulnerable to political corruption, perverse economic incentives (such as harmful underlying business models), and challenges and vulnerabilities associated with scale. Web3 and the metaverse represent increased interactivity and commercialization of the web, which comes with heightened risks. When everything becomes a financial transaction, corporate values and incentives will inevitably crowd out more democratic ones. Without addressing incentives, there can be no adequate security, no matter the levels of cryptography employed.

Finally, one of the biggest security vulnerabilities that we are failing to adequately consider in this conversation has to do with digital identity. As Web3 and the metaverse lead to a more expansive internet, more immersive experiences, and additional touchpoints between digital and physical surfaces, our approach to digital identity becomes critical. Whereas the early web allowed for a high degree of anonymity, and encouraged multiple contextual identities (for gaming, commerce, blogging, or social networking, for example), Web3 and the metaverse risk imposing a single digital identity (tied to our legal identity) across all surfaces. This could mean the end of anonymity, which would also threaten the notion of digital public spaces. As such, we need to protect anonymity and not impose an identity layer for people in every digital interaction (an alternative is to improve the identity of machines and hardware).

9. **How do you assess digital civil society's stance on the topic of Web 3.0 and blockchain/DLT, which, among others, indicate a significant potential for abuse along with consequences drawing criticism from a social and socio-political perspective (see for example Jürgen Geuter/"tante", Molly White with the blog "Web3 is going just great", letter from crypto experts to the US Congress)? Is your impression that policymakers are giving appropriate consideration to the views expressed?**

Civil society actors are understandably concerned with the potential for abuse of Web3, Web 3.0, and blockchain/DLT, as they do not stand to profit from their proliferation in the way that private actors promoting them do, nor do they face the same political challenges around their adoption and use as government actors. In general, civil society organizations hold great institutional knowledge and expertise; take a more arms-length, independent stance, including from this absence of commercial or political incentives; and can more objectively evaluate the relative risks and opportunities of these concepts and

technologies. Moreover, digital civil society stakeholders can be viewed as stewards and protectors of the digital public sphere, a space that is increasingly threatened by the extension of privately controlled spaces into virtual worlds, augmented real-world spaces, and notional metaverses.

I largely agree with the issues enumerated and the views expressed in the materials you cite in this question, and particularly echo the concerns raised in the letter from crypto experts to the US Congress regarding the need to push back against the claims, and challenge the narratives of, those who stand to profit from cryptocurrency, Web3, and blockchain schemes. I also strongly agree with the letter's concerns around the unfounded privacy claims made by blockchain promoters, in particular that privacy mechanisms are "antithetical" to the technology's basic design.

In my experience, however, policymakers are not giving appropriate consideration to the views and concerns of civil society (and in the U.S., they are disproportionately influenced by the industry's aggressive political and economic lobbying efforts). It is understandable that policymakers are as frustrated as individuals with the status quo and seeking to address shortcomings of the existing digital ecosystem by whatever means possible. We are primed to look for alternatives and exhibit a strong bias towards the claimed potential and benefits of new technologies, even when there is little evidence to support it. This can induce a naive optimism that the next thing or the next iteration will be better, despite its increasing complexity, when we haven't been able to solve existing challenges. But we must overcome this bias and take an evidence-based approach to our evaluation and assessment of these technologies.

10. Are you aware of applications for blockchain technology beyond cryptocurrencies that cannot be performed more efficiently and with less damage to the environment, etc. with existing technologies. How can the balance of opportunities and risks be assessed from a sociopolitical perspective?

First, I am not an expert on the environmental impacts of these technologies. That said, I am not at present familiar with any use cases where the benefits would exceed the environmental costs. From a sociopolitical perspective, it is important to push back on the way that these technologies are often characterised as not having an environmental footprint or material impact. For example, just as big tech has leveraged terms like "AI" and "the cloud" to distract from the environmental toll of those technologies, cryptocurrency promoters also use terms like "ether," "Ethereum virtual machine," "digital twin," and others to connote a kind of immateriality or non-physicality. The reality is that these technologies are expensive, extractive, and highly material, with great environmental impact, and that should factor into each and every decision regarding their use or suitability.

11. Does research offer a unanimous definition of the metaverse and if not, which definition would you recommend to policymakers when dealing with this concept and what role in this do the

existing concepts of Augmented Reality, Assisted Reality, Virtual Reality and Extended Reality play?

As I noted in my response to question 1, there is no consensus on the precise definition or contours of the metaverse as it does not apply to any single technology or specific combination of technologies. Rather, a variety of stakeholders use the term to mean different things.

Private companies tend to define the metaverse in terms of their own commercial opportunities, i.e., for the new proprietary offerings and expanded monetizable surfaces it can enable through virtual spaces and VR-enabled experiences. Examples include Meta's Horizon Worlds, a VR-based social network and Horizon Workrooms, a VR-based conferencing product, as well as Microsoft Mesh for Microsoft Teams. While private companies tend to imagine separate independent metaverses (i.e., walled gardens), other stakeholders sometimes imagine a more unified singular metaverse where individuals can virtually move between different virtual spaces.

Academic researchers, and computer scientists in particular, tend to define the metaverse in relation to the technologies that it implicates, including extended reality (XR) technologies such as virtual reality (VR), augmented reality (AR), and mixed reality (MR); hardware such as headsets, wearables, and other connected devices; physical and behavioural biometrics; digital identity tools and avatars; and AI and machine learning-powered systems. One computer scientist has defined the metaverse as a "3D virtual shared world where all activities can be carried out with the help of augmented and virtual reality services." Other disciplines, such as anthropologists, might define the metaverse in relation to past experiences like Second Life or PlayStation Home.

Another way to think about the notion of a "metaverse" that may be useful for law and policymakers in broader conversations about its social, political, or economic desirability is that it acts as a kind of virtual layer or barrier between ourselves and our experience of reality. In other words, the metaverse layers a virtual dimension on top of our existing social, professional, and commercial interactions, thereby extending the monetizable and surveillable surface area of our lives. To the extent that metaverses are controlled by private companies, this also threatens to impose commercial incentives and corporate values onto these experiences and shape these interactions in ways that might further undermine civil and human rights, core democratic values and principles, and collective action.

12. What is your assessment of the research situation in Germany on the topic of metaverses compared with the rest of the world in terms of professorships, publications, state research funding and third-party financing for metaverses and Web 3.0?

I cannot speak to this question.

13. **In your assessment, how have companies in Germany prepared for the metaverse so far, in particular when compared with the USA and China, and do you see the risk that due to a lack of prioritization of the topic, we in Germany could miss out in technological and economic terms on keeping up with the global frontrunners?**

I cannot speak to this question.

14. **What risks may arise from state attempts to regulate the new technology at too early a stage, what basis for standardisation can already be used for dealing with metaverses, what is your assessment of how things stand in Germany and Europe regarding framework conditions that would enable metaverses and in terms of funding programmes, and what measures would you recommend to policymakers as a priority in order to utilize as best as possible the economic and societal opportunities of the metaverse?**

First, I would challenge that these technologies are at an early stage. In the case of blockchain and cryptocurrencies, as described above, the technology is not very new, and the benefits remain largely theoretical. Similarly, virtual ecosystems or metaverse-style spaces are also not new. In fact, as many scholars and technologists have pointed out, there are limited improvements on the version of the metaverse recently debuted by Mark Zuckerberg over the look and feel of the virtual world known as Second Life launched in 2003.

While certain enabling technologies of the metaverse, such as AR, VR, and XR, and their hardware components, have made some gains in the intervening decades, they have not yet evolved to a point to encourage their organic adoption. For example, the well-known Google Glass technology, unveiled a decade ago, has famously failed to attract a market, while VR headsets like Meta's Quest (formerly the Oculus Rift) have faced slow growth and significant hurdles to adoption. As adoption grows, however, it is important to ensure that these technologies comply with existing laws and regulations, including consumer protection, product liability, and competition laws.

While the technologies involved are not quite as early stage as some would contend, there are some qualitative differences between contemporary versions of the metaverse put forward by industry and older versions like Second Life. Most important among these differences is that modern-day metaverses are privatized, commercial spaces that require economic and regulatory systems that support the "enclosure of virtual spaces." In this way, they pose a direct threat to notions of a "digital public sphere" and introduce commercial incentives that inevitably shape individuals' experiences in them. In this regard, it is also important to examine the procurement and use of privately designed, developed, and operated metaversal technologies in the provision of public sector services and activities.

15. What business form are DAOs and do they need to be regulated in order to protect end customers from fraud and misuse?

For some blockchain or cryptocurrency promoters, DAOs are not so much a business or corporate form as they are a philosophical or organising principle representing what they believe to be a new form of community governance and participation. Whereas corporations traditionally govern and make decisions through a board of directors and named executives who represent the interests of shareholders, DAOs instead make decisions and steer the direction of an organisation through anonymous, token-based voting mechanisms enforced through "smart contracts." A famous example is the Constitution DAO, a failed attempt to crowdfund the purchase of a rare copy of the U.S. Constitution in November 2021. While some DAOs feature a "one token, one vote" system, governance models vary across DAOs.

In some cases, however, a DAO is effectively a limited liability corporation (LLC) by another name, whether legally recognized as such or not. Where not legally recognized, DAOs may seek to avoid corporate governance obligations and other requirements. Some jurisdictions, including a handful of states in the United States, such as Wyoming, Vermont, and Tennessee, allow DAOs to register as a type of LLC. These so-called "compliant DAOs" can then benefit from the privileges and protections of traditional LLCs, including limited liability, asset protection, and favourable tax treatment. However, corporate registration requirements can be difficult to reconcile with DAOs that feature anonymous or pseudonymous membership or governance structures. Where DAOs function like LLCs, and seek to benefit from the associated protections, they should be required to register as such and comply with all relevant requirements.

16. How can consumer protection rights and principles be implemented in decentralised blockchain systems such as those of Web3?

A high level of consumer protection is a fundamental right enshrined in Article 28 of the EU Charter. In general, policymakers must ensure that blockchain systems, whatever the degree of technical centralisation or decentralisation, respect consumers' rights to safe and healthy products, fair terms, proper information (free from misleading advertising and marketing), and rights of cancellation, which might be particularly challenging in the context of immutable, append-only ledgers.

It is also important to push back against the narrative of decentralisation as, upon closer examination, very few of these projects or systems are truly decentralised. Rather, it is usually possible to identify entities or actors who exercise substantial control over them, including the purposes and means of any data processed by them (for example, blockchain systems consisting of thousands of nodes around the world that can "read" the ledger often have just a handful of nodes that can "write" to it, thereby concentrating control in the hands of a few). Such entities and actors should be held liable for their decisions, actions, and omissions in proportion to the level and degree of control that they exercise over the design, development, and

operation of a given system. In this way, clear liability rules and frameworks will be essential to effective consumer protection over Web3 systems and services.

The particularities of consumer protection principles as applied to blockchain systems and offerings may also depend on the use case or sector implicated. For example, a blockchain crowdfunding platform may be subject to certain registration requirements, limits on fundraising, reporting obligations, and other consumer protections required of financial services or fintech providers. Meanwhile, blockchain systems used to manage other types of digital assets, which are not subject to financial regulations, should be subject to alternative frameworks, such as the Markets in Crypto-Assets Regulation. Others still might be subject to unique health and safety or product liability requirements, such as for blockchain systems used in healthcare or certain industrial applications. In other words, existing laws, regulations, and standards do not disappear simply because a Web3 system or service uses blockchain or DLT.

17. "Web 3.0", which to date remains only a vision, is celebrated for its decentralised structure, for limiting the power of larger platforms and for locating data sovereignty with the users. What entity, in your opinion, would at all be in a position to replace the existing infrastructure systems of platforms and access nodes with blockchain technology? And where would the energy to operate the blockchain technology come from?

I do not fully understand the question. That said, I would agree that these concepts are largely still imaginations and push back on the claims around decentralisation. Regarding the claim that they would locate data sovereignty with users, I have already discussed the significant risks and downsides of such an approach in my response to questions above. By way of summary, these proposals would unduly and unreasonably burden individuals with managing their own data in a way that exacerbates existing problems, while adding a layer of perverse commercial incentives on top. Regarding the question of energy usage, I am not an expert on the matter but would refer back to my comments regarding the need to push back against ethereal narratives and acknowledge the materiality of these technologies.

18. In your view, are the visions of a "Metaverse" and/or a "Web 3.0" suitable for substantiating and strengthening the digital sovereignty of Germany and Europe vis-à-vis China or the USA, for example? What exactly would have to happen in terms of hard and software used, and–where applicable–at regulatory level?

As presently conceived of, I do not believe that visions of a metaverse and/or Web 3.0 (or Web 3 for that matter) will strengthen the digital sovereignty of Germany and Europe vis-à-vis China or the USA. From both a hardware and software standpoint, China and the United States are leaders when it comes to metaversal technologies. For example, China's Tencent and Baidu filed the most AR and VR-related patent applications of any companies worldwide in 2020 and 2021. China also leads the world in VR adoption, with wide usage in real estate and property development, retail, education, and other sectors. And finally,

China is leading on strategic planning, including through its recent Virtual Reality and Industry Application Integration Development Action Plan (2022-2026) issued by the Ministry of Industry and Information Technology, which includes a comprehensive set of policies for developing virtual spaces.

In the United States, globally dominant technology companies like Meta, Google, Microsoft, and others continue to dominate the imaginative discourse and narratives around the metaverse and Web 3 and could adapt their existing platforms and vast user bases to drive adoption towards new virtual spaces. Similarly, corporations like Apple and Google could leverage their market dominance in respect of smartphone technologies to capture mobile-enabled markets in the metaverse. The metaverse will also boost the demand for cloud-based computing and storage services, bolstering already dominant US cloud providers like Amazon, Microsoft, Google, and IBM.

However, while China and the US may lead on metaverse-related hardware and software products and services, Germany and Europe have an opportunity to provide ethical, moral, legal, and policy leadership in this area, and should focus their efforts accordingly.