Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)110

12.12.2022

Molly White
www.mollywhite.net
molly@mollywhite.net

Statement for the public hearing on
"Web 3.0 and the Metaverse"

Committee on Digital Affairs
German Bundestag
December 14, 2022

Introduction

Thank you for inviting me to speak at today's hearing. I am Molly White, and I research web3, cryptocurrencies, and blockchain-based technologies. My educational and professional background is in computer science and software engineering, and for the past year I have maintained the website *Web3 is Going Just Great*,[1] where I aim to highlight the many issues in the web3 and cryptocurrency space. I have also written and spoken about blockchain technologies more broadly, including in a collection of longer-form writings.[2] I have done some research into the concept of the metaverse, though to date I have primarily focused on where it intersects with the cryptocurrency industry.

I am a fellow at the Harvard Library Innovation Lab. I am not speaking on their behalf today; the views I am expressing today are solely my own.

Prepared statement

Web3—an imagined future era of the web that would be based around blockchains—became a prominent buzzword over the past two years as the cryptocurrency industry sought to frame their products as revolutionary technologies that might usher in a new frontier of technological innovation.

The web3 sales pitch can be compelling at surface level, because it often points out real flaws in existing technological, financial, legal, or political systems, and heavily features compelling (albeit vague) buzzwords around topics like "decentralization", "democratization", "self-sovereignty", and "censorship-resistance". But when it comes to fulfilling these promises, the technologies and products fall far short, and in fact often provide *worse* alternatives to existing flawed systems.

Web3 projects have made so many grand promises about the potential of blockchains that it would be impossible to address them all. I will touch on a few:

---

[1] Available: https://web3isgoinggreat.com.

[2] Available: https://blog.mollywhite.net/blockchain.

On ownership: The poorly-defined concept of "owning one's own data" has become popular in the web3 space. Many platforms making this promise simply mean that, instead of storing user data privately on their own servers, they store it publicly on a blockchain (or in decentralized filestorage systems like IPFS,[3] but connected to cryptocurrency wallet addresses). However, this opens the content up to scraping by even *more* marketing firms and data analytics companies than already seek to gain access to the types of data that users provide private companies today. Furthermore, one does not truly "own" their data when they don't have the ability to modify or delete it, as is the case when it is stored on a blockchain or in many decentralized storage systems.

In some cases, projects use similar language when describing "ownership" of digital assets much like ones people already purchase today—for example, representing purchasable upgraded weapons in video games as non-fungible tokens (NFTs). This marketing deliberately dodges the fact that, in the case of game assets, a video game creator can still arbitrarily choose to stop supporting the use of an asset in the game, rendering the "ownership" of it no different in practice from existing systems of digital ownership. The same general issue applies more broadly to the long list of web3 projects suggesting to use crypto assets to represent all kinds of products beyond just video game items, such as concert and event tickets, club and restaurant membership cards, virtual "real estate", and so on.

On decentralization: Blockchain advocates typically point to decentralization as an advantage of blockchain-based technologies. However, they tend to gloss over the incredibly important distinction between network decentralization and the decentralization of power. They also tend to exaggerate the network decentralization of blockchain projects, at that.

It is true that public blockchains such as Bitcoin, Ethereum, and others are fairly decentralized in terms of the network, which consists of thousands of nodes distributed throughout the world. However, that is not all that different from something like Amazon Web Services, which is also a network made up of many thousands of servers in tens of geographically distributed datacenters, and which no one would normally describe as "decentralized" in the sense that blockchain proponents mean the term. This is because it is the *power* distribution that is significant. The power distribution remains

---

[3] InterPlanetary File System, see J. Benet, "IPFS – Content addressed, versioned P2P file system," 2014 [Online]. Available: https://arxiv.org/abs/1407.3561

enormously centralized in blockchain projects.[4] Furthermore, even if a given blockchain network *was* decentralized, in practice very few people interact with blockchains without going through numerous centralized intermediaries such as API providers.[5]

Many web3 evangelists have adopted talking points around removing power from large tech companies and other powerful firms, and restoring it to the users. Among those making these claims are the powerful firms themselves. See, for example, Andreessen Horowitz's statement that "web3 will put power in the hands of communities rather than corporations",[6] despite establishing themselves as an enormously powerful figure in the web3 space with investments in major crypto companies across all facets of the industry.[7]

On financial inclusion, or "banking the unbanked": The cryptocurrency industry has rightfully identified as a problem that there are many people globally who do not have access to bank accounts, or to loans and other services typically provided through banks. However, the industry often chooses not to examine and address the primary reasons why various communities are unbanked, but instead seek only to sell their target customers—often marginalized and/or low-income people—on cryptocurrency-based financial products that are poorly regulated and subject to few consumer protections, often enormously volatile, and prone to hacks and scams.[8]

The cryptocurrency industry has taken to arguing against regulations and consumer protection measures by claiming that such regulatory boundaries would "stifle innovation". In practice, the "innovation" that evangelists claim web3 and blockchains will usher forth has not been realized in terms of removing power from tech

---

[4] D. S. H. Rosenthal, "Can we mitigate cryptocurrencies' externalities?" presented for EE380: Computer Systems Colloquium, Dept. of Comp. Sci., Stanford University, Palo Alto, CA, USA, spring 2022 [Online]. Available: https://www.youtube.com/watch?v=twrduL8aNGE

[5] M. Marlinspike, "My first impressions of web3," Moxie Marlinspike, blog, January 7, 2022 [Online]. Available: https://moxie.org/2022/01/07/web3-first-impressions.html

[6] Andreessen Horowitz, "The web3 landscape," 2021 [Online]. Available: https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf

[7] "Where Andreessen Horowitz Is Investing in Crypto," Blockdata, September 4, 2022 [Online]. Available: https://www.blockdata.tech/blog/general/where-andreessen-horowitz-is-investing-in-crypto

[8] T. Carmona, "Debunking the narratives about cryptocurrency and financial inclusion," The Brookings Institution, Washington, DC, USA, 2022 [Online]. Available: https://www.brookings.edu/research/debunking-the-narratives-about-cryptocurrency-and-financial-inclusion/

monopolies or opening new opportunities for financial inclusion; rather, we have seen impressive innovation in the realm of fraud, theft, and predatory financial products which have flourished thanks to minimal regulatory attention.

List of questions

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?

Web3 is, more than anything, a marketing term that has come to be used to describe an imagined future era of the web that would be based around blockchains.

The terms "Web 3.0" and "web3" are sometimes used interchangeably to refer to the blockchain-based future era of the web that some predict may emerge. However, there are some who still use "Web 3.0" to refer to the earlier prediction by Tim Berners-Lee and others that the next era of the web would be the "semantic web". The semantic web has little overlap with the topics discussed here today, besides sharing a similar name.

The metaverse is also a vague marketing term that seems to be defined differently by every person. It is generally used to refer to immersive virtual environments that are sometimes accessed through virtual reality and similar technologies. Some metaverses directly incorporate crypto assets, which are used as currency, represent in-world assets like clothing for one's avatar, or create a market in which people trade virtual "land".

While advocates suggest that web3 is crucial for an "an open, free and also secure and user-centred network", in practice it has produced anything but. Web3 is typically hyperfinancialized, open only to those who can afford to pay to join, and controlled by those who hold the most tokens—often project founders, venture capitalist investors, or people who are already extremely wealthy.

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?

In addition to the concerns I described in my statement, proponents of blockchain-based technologies often describe them as inherently more private than existing systems. To examine this, first we must describe the degrees of privacy that exist in traditional technological and financial systems, which roughly form three categories. *Public* data is information that is available to any who wishes to find it; *private* data is information that is completely secret; and *limited* data is that which is available only to a limited set of trusted institutions (e.g. a bank, or a technology company with whom an individual has an account).

The original blockchain ideology seeks to do away with the "limited" category as a part of its quest to eliminate trusted intermediaries.[9] Instead, all information is either completely private or completely public. On most major blockchains, all transaction data is public, and anyone can look up a wallet address to see a complete list of its transactions with other parties and the wallet balances. Increasingly, blockchain developers and companies are exploring storing other personal data in connection to users' crypto wallet addresses, as well: personal credentials,[10] records of attendance at in-person events,[11] etc. All of this data is stored in perpetuity, meaning that pseudonymity must be maintained indefinitely. Some blockchain projects, particularly in the web3 space, seek to store *very* personal data such as medical records in publicly accessible, decentralized filestorage. Users must not only trust these projects to use proper encryption practices, but because the data is stored publicly and indefinitely they must trust that the keys will never be compromised and that the encryption algorithm will never be seriously broken. It is worth noting that this perpetual storage of private data, even psuedonymized, means that some blockchain-based systems may not be able to comply with regulations such as the GDPR.

The connection between a wallet address and a person's real-life identity is, at least in the idealized forms of these systems, private. However, if a person chooses to publicly connect their wallet to their identity, or if they do so inadvertently, or if a trusted party leaks this connection, or if the public blockchain activity is sufficient to deduce this person's real-life identity, then all this public data (transaction history, wallet balances, and other public personal data connected to their wallet address) becomes connected to them. In practice, it is difficult to set up, fund, and secure a completely private wallet with no connections to one's real identity, and it is difficult to maintain this privacy.[12]

Many people use centralized platforms (Binance, FTX, and Coinbase being several examples) because they are considerably easier to use. Because they must comply with

---

[9] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] E. G. Weyl, P. Ohlhaver, and V. Buterin, "Decentralized society: finding web3's soul," 2022 [Online]. Available: https://ssrn.com/abstract=4105763

[11] M. Marcobello, "POAPs: what is a proof of attendance protocol?" *CoinDesk*, Aug. 23, 2022 [Online]. Available: https://www.coindesk.com/learn/poaps-what-is-a-proof-of-attendance-protocol/

[12] For further discussion of the difficulties in maintaining the privacy of a cryptocurrency wallet, see M. White, "Anonymous cryptocurrency wallets are not so simple," Molly White, blog, February 12, 2022 [Online]. Available: https://blog.mollywhite.net/anonymous-crypto-wallets/

anti-money laundering laws, these platforms typically require identification documents, reintroducing the limited level of data disclosure that cryptocurrency originally sought to do away with. However, people who use these platforms *still* have the same public transaction data associated with their crypto wallets, unlike in traditional banking systems where this data is also limited. Customers of these platforms are exposed to additional vectors through which their identities may be connected to their wallet addresses: for example, through malicious data breaches,[13] or—as we've seen more recently—as required in bankruptcy proceedings when those platforms fail.[14]

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?

I am not sufficiently familiar with the details of European regulatory approaches to speak to this, although I will direct to my earlier comment in question 2 that blockchain-based projects may find themselves fundamentally unable to comply with the GDPR.

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

It is important to carefully evaluate the pros and cons of blockchains and cryptocurrencies. While doing so, it is crucial to not get hung up in conversations about what someday *might* be enabled by these technologies, which tends to be where proponents of them try to direct the conversation.

In the fourteen years that cryptocurrencies have existed, they have produced minimal opportunities outside of financial speculation. They do not work well as currencies due to their volatility, and attempts to reduce this volatility by pegging cryptocurrencies to a traditional currency ("stablecoins") have been shady at best and disastrous at worst.[15] Besides those who became wealthy from crypto speculation, perhaps the most

---

[13] *E.g.* F. Munawa, "Major Canadian crypto exchange Coinsquare says client data breached," *CoinDesk*, Nov. 26, 2022 [Online]. Available: https://www.coindesk.com/tech/2022/11/26/major-canadian-crypto-exchange-coinsquare-says-client-data-breached/

[14] *E.g.* A. Greenberg, "Celsius exchange data dump is a gift to crypto sleuths—and thieves," *Wired*, Oct. 13, 2022 [Online]. Available: https://www.wired.com/story/celsius-user-data-dump-crypto-tracing-scammers/

[15] A. Osipovich and C. Ostroff, "TerraUSD crash led to vanished savings, shattered dreams," *The Wall Street Journal*, May 27, 2022 [Online]. Available: https://www.wsj.com/articles/terrausd-crash-led-to-vanished-savings-shattered-dreams-11653649201

revolutionary positive impact of cryptocurrencies has been on the lives of cybercriminals and fraudsters, who have used them to great success over recent years.[16]

For average people, who may be tempted by the 1000x returns once experienced by early Bitcoin adopters, the landscape is not so bright. They are often trading at an unfair knowledge disadvantage against powerful players who can manipulate markets, being sold on too-good-to-be-true returns by Ponzi projects that later collapse, or losing their assets to the many hacks and exploits that are practically a daily occurrence. Recent research suggests that "an estimated 73-81% of retail investors have likely lost money on their initial investment".[17]

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

It is important to distinguish the promises of virtual or extended reality from the hype and marketing of "metaverses". The fields of VR and XR are well established and far predate recent attempts to burnish the reputations of unimpressive technological projects in hopes of attracting venture capital and retail investment.

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?

Blockchains have shown themselves to be not well-suited to the stated goals of web3. If the next iteration of the web is to involve any of the many admirable goals sometimes stated by web3 proponents—more user privacy, or more self-governing communities, for example—it is important that technologists not shackle ourselves to technologies that have shown little promise towards achieving those goals, and instead seem to be pushing the web toward a hyperfinancialized, extractive environment that enriches crypto startup founders and investment funds at the expense of individual users.

---

[16] N. Weaver, "The ransomware problem is a Bitcoin problem," *Lawfare*, May 27, 2021 [Online]. Available: https://www.lawfareblog.com/ransomware-problem-bitcoin-problem

[17] R. Auer, G. Cornelli, S. Doerr, J. Frost, and L. Gambacorta, "Crypto trading and Bitcoin prices: evidence from a new database of retail adoption," working paper, Bank for International Settlements, Basel, Switzerland, 2022 [Online]. Available: https://www.bis.org/publ/work1049.pdf

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?

Once again, "metaverse" should be carefully defined. In many cases the products are now being branded as "metaverses" are not meaningfully different from platforms like *Second Life*, a virtual world that is now twenty years old.

If this question is meant to address questions around VR and XR, it will be important to build frameworks for the enormous degree of data collection enabled by a much broader range of sensors than are utilized in most consumer computers or smartphones, such as eye tracking, haptics, etc.

There are many pertinent questions around dark patterns and manipulation in VR/XR/"metaverse" platforms, particularly as these platforms prominently market themselves to children and teenagers. I am not an expert in these subjects but urge you to seek them out.

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, decentralized and secure internet into global governance mechanisms?

The Internet began as a highly decentralized network and grew more decentralized over time. The enormous financial incentives introduced with advertising and data brokerage have made it very profitable for tech companies to form monopolies and operate in extractive, abusive ways. The incentive to create healthy, user-centric, responsibly-governed online spaces simply cannot compete against those financial incentives, and projects that seek to do so often fail due to lack of funding or are crushed by larger tech corporations. More attention should be paid toward other models of running organizations that are not based around the for-profit corporation model, such as non-profits, platform co-operatives, or publicly-owned utilities.

We are not facing a crisis because we lack the *technology* to create a better web. We've been working on web technology for thirty years, and its improvement in that time has been impressive. The real crisis stems from the extractive, hypercommercialized nature of web corporations; the broad view of user data as a commodity to be extracted and user behavior as a thing to be molded; and the power that enormously powerful technology companies wield within the web but also in much broader areas of society and politics.

Those problems are not ones that will be fixed with technology. We are already watching these same tech monopolies establishing profitable footholds in the web3 landscape, even as we are being told that web3 will somehow subvert their power and profitability.

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"1, letter from crypto-experts to the US Congress2)? Is your impression that policymakers are giving appropriate consideration to the views expressed?

With rare exception, my perception is that policymakers fall into one of two categories: they are either fearful of sounding out of touch if they express too much skepticism around crypto/web3, or they have bought in to the sales pitch that blockchains and cryptocurrencies are a revolutionary innovation despite minimal evidence to support it.

The crypto lobbyist argument that crypto cannot be regulated without stifling innovation seems to have hit home among policymakers, despite being completely farcical. If regulations against financial fraud can't be enforced on an industry without destroying that industry, it should be worth taking a look at what that industry is really doing.

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?

No. Cryptocurrencies (and financial products built around them) are the primary use case for blockchains, and they have enormous negative externalities that tend to far outweigh any benefits.

Besides that, the strongest use case for blockchains has been the associated hype bubble. At least in the recent few years, blockchains have attracted massive interest from institutional investors and retail speculators, and so even if a product benefits in no way from the addition of a blockchain, it can sometimes get funding by claiming to use one.

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?

It does not. I would recommend avoiding the use of the term entirely, and instead using the more specific term that is relevant (for example, "virtual reality" or "massively multiplayer online platform").

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 am not sufficiently familiar with German metaverse research to answer 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 am not sufficiently familiar with German metaverse companies to answer 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?

Again, it is more useful to address the specific topics of concern, be it VR/XR, massively multiplayer online worlds, or the use of crypto assets. Each of those has its own specific sets of regulatory concerns, though I do not have sufficient expertise in the first two topics to offer an assessment.

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

Although the term "DAO" is intended to refer to a member-controlled organization with token-based governance, in practice the term is widely used including to refer to

organizations with no governance systems at all, or with governance centralized in a small team of founders.

Even within organizations that are constructed more in the way that the term "DAO" is intended, there is so much variance in actual structure that it is not likely to be feasible to define a singular business form that would be well-suited to all. I am most familiar with DAOs as they operate in the United States, and I have seen them formulated as LLCs, Unincorporated Nonprofit Associations, C corporations, etc.

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

There is a long list of consumer protections that could be put into place, including requiring crypto platforms to responsibly segregate customer funds, perform proper audits, disclose proof of assets and liabilities to outside agencies, operate separately from firms that may have conflicting interests, etc. Existing regulations around fraud should be strongly enforced.

It's also critical that regulations are carefully formulated so as not to expose people to *additional* risk by allowing cryptocurrency platforms to become tightly integrated with traditional finance, by possibly exposing traditional finance and people who do not use cryptocurrencies to contagion from the frequent cryptocurrency collapses.

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 system of platforms and access nodes with blockchain technology? And where would the energy to operate the blockchain technology come from?

It is neither desirable nor feasible to "replace the existing infrastructure system of platforms and access nodes with blockchain technology". This question is also based on the flawed premise that web3 is inherently decentralized; refer to the "On decentralization" portion of my prepared statement.

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?

I am not able to answer this question without a better understanding of what is meant by "digital sovereignty".