**Deutscher Bundestag**
Ausschuss für Digitales

Ausschussdrucksache
20(23)113
13.12.2022

**Berlin, 13.12.2022**

# Stellungnahme zum Fragenkatalog des Ausschusses für Digitales in der Sache „Web 3.0 und Metaverse“

**von Lilith Wittmann (mail@lilithwittmann.de)**

**1) Was sind die Konzepte und Überlegungen, die jeweils „Web 3.0“ (im Sinne des semantic web), „Web 3“ und „Metaverse“ zugrunde liegen, wodurch unterscheiden sie sich, was sind die damit erhofften Chancen und Risiken und was bedeuten sie jeweils für die Struktur und Architektur eines offenen und freien sowie eines sicheren und nutzerzentrierten Netzes - kurz: Stehen sie für das Internet, das es zu verhindern gilt?**

Da es sich hier um drei völlig unterschiedliche Themenfelder handelt, werden diese getrennt beantwortet:

**1. Das Semantic Web**

Das Web 3.0 oder Semantic Web ist eine Idee – geprägt von Tim Berners Lee – um die Daten dieser Welt maschinenlesbar zu verknüpfen. Es geht also darum, offene Daten gut nutzbar für alle bereitzustellen[1].

Zu der Zeit, in der an den grundlegenden Konzepten des Web 3.0 gearbeitet wurde, sprach man viel über das Web 2.0 - ein Internet, in dem Menschen nicht nur Inhalte konsumieren können, sondern auch selbst Texte und Bilder teilen. Damals wow, heute halt das Internet. Aber schon damals erkannten einige Menschen, dass unstrukturierte Texte und Bilder zwar toll sind, strukturierte – also maschinenlesbare – Daten aber noch viel mehr Möglichkeiten bieten könnten. Deshalb hatte unter anderem Tim Berners-Lee schon sehr früh den Gedanken, dass man über Internet-Technologien auch Daten miteinander verknüpfen könnte. Wie Linked Open Data funktionieren kann, ist heute schon gut in der Wikipedia sichtbar. Dort werden Fakten einmal im System Wikidata definiert und können dann automatisch in die Artikel der verschiedenen Sprachversionen der Wikipedia eingebunden und aktualisiert werden.

Ein Konzept mit einem unglaublichen Potenzial für Staat, Wirtschaft und Gesellschaft.[2]

Seit mindestens 2012[3] fordern deshalb verschiedene zivilgesellschaftliche Initiativen, dass sich auch die deutsche Verwaltung in diese Richtung weiterentwickelt. In der Regel unter dem Stichwort Linked Open Data[4]. Linked Open Data gilt gemeinhin als die Zielvorstellung von Open Data Bestrebungen. Projekte, welche die Ideen hinter LOD

---

1 https://web.archive.org/web/20171010210556/https://pdfs.semanticscholar.org/566c/1c6bd366b4c9e07fc37eb372771690d5ba31.pdf

2 https://video.codefor.de/w/791d6351-2fbe-4335-bc98-5e99d6dc10fb

3 https://media.ccc.de/v/vortrag_mp6_og_-_2012-05-19_19_00_-_linked_open_data_-_angelo_veltens_-_7

4 https://5stardata.info/en/

aufgreifen, sind z.B. Wikidata[5] oder der “Linked Open EP” Datensatz des europäischen Patentamts[6].

Die Prinzipien von Linked Open Data wurden von der Bundesverwaltung leider bis auf wenige Ausnahmen bis heute nicht aufgegriffen. Die einzigen mir bekannten Projekte sind einige Meta-Datensätze sowie das Projekt DCAT-AP.de[7], welches die Gemeindeschlüssel Deutschlands als ein LOD-artiges Datenformat bereitstellt.

Auch regulatorisch wurde Linked Open Data bisher in Deutschland nirgends verankert: Im Datennutzungsgesetz ist davon keine Rede. Auch nicht in ganz frisch verabschiedeten Initiativen, zum Beispiel der Ratifizierung der EU-Richtlinie 2019/1151, also der Online-Zugänglichmachung des Handelsregisters. Sie hätte ein sehr gutes Beispiel dafür sein können, welche Chancen in einem semantischen Web mit maschinell erschließbaren und offenen Daten liegen. Der Gedanke ist einfach: Man gibt einen Namen ein und findet alle Firmen, die diesem Menschen gehören. Ein einfaches Tool für Steuerfahnder*innen und Journalist*innen – es wurde aber technisch so nicht umgesetzt. Sondern es wurde ein digitales Papier ins Internet gestellt, wo leider auch Daten drinstanden, die da gar nicht hätten drinstehen dürfen – aber das ist eine andere Geschichte.[8] Ein Phänomen, das wir häufiger sehen. Man könnte auch sagen: Anstelle von Linked Open Data sind eingescannte PDFs in Deutschland immer noch der Standard.

**2. Web 3**

Das Web 3, vereinzelt auch von seinen Fans als Web 3.0 bezeichnet, ist eine Sammlung von Technologien, welche es ermöglichen, den Besitz von digitalen Währungen und Gütern im Internet abzubilden.

Technisch reden wir hier eigentlich nur über Technologien, um Daten in eine nicht veränderbare Datenbank abzuspeichern. Das kann seit vielen Jahren mit verschiedenen Maßnahmen zentral oder dezentral erreicht werden.
Daten in eine öffentlich verteilte Ledger-Datenbank, also eine Datenbank, aus der man nichts löschen kann, zu schreiben, ist eben ein Weg, das zu tun. Das nennen wir Blockchain.

So eine Ledger-Datenbank ist für bestimmte Anwendungen, insbesondere in ihrer zentralisierten Form ganz praktisch. Banken nutzen z.B. einen Ledger, um alle Transaktionen, die sie durchführen, sicher zu speichern.

[5] https://www.wikidata.org/
[6] https://www.epo.org/searching-for-patents/data/linked-open-data.html
[7] https://www.dcat-ap.de/
[8] https://www.zeit.de/2022/38/lilith-wittmann-handelsregister-digitalisierung-buerokratie-datenschutz

Die erste bekannte dezentrale Ledger-Anwendung war Bitcoin, also eine digitale Währung. Seitdem haben sich in den letzten Jahren zahlreiche weitere ledger-basierte Währungen auf ähnlicher Technologiebasis entwickelt. Das hat dazu geführt, dass jeder Mensch – auch ohne viel technischen Sachverstand – einen solchen Ledger aufsetzen und so seine eigene Währung erfinden kann. Über Einträge in den Ledger und digitale Signaturverfahren, bei denen nur die Inhaber des Tokens über das zur Signatur gehörende Geheimnis verfügen, können sie die Inhaberschaft ihres virtuellen Geldes beweisen.

Neben Währungen können auf so einer Blockchain aber auch beliebige andere Informationen gespeichert werden, z.B. Verträge oder Informationen über den Besitz von digitalen Gütern. Die Idee solcher Smart Contracts stammt ursprünglich auch aus Ende der 90er Jahre[9], erreichte aber erst im Kontext der Ethereum Blockchain Relevanz.

Über die von Staaten unabhängigen digitalen Währungen und die Möglichkeit, Verträge in Programmcode-Form abzulegen, wollen einige Anhänger des Web 3 gerne heute kernstaatliche Leistungen von Code in einer dezentralen Datenbank übernehmen lassen statt von staatlichen Strukturen. Einige Web 3 Anhänger wollen also Aufgaben, für die heute Staaten zuständig sind, ausschließlich in ihren Ledgern regeln.

**3. Metaverse**

Das Metaverse ist ein ursprünglich in einem dystopischen Roman von Neal Stephenson erfundener Begriff für eine digitale Welt. Dieser Begriff wurde von Facebook wieder aufgegriffen, um diese dystopische Welt in Spielform umzusetzen. Bisher mit mäßigem Erfolg, wie auch die EU kürzlich in ihrem eigenen Metaverse feststellen durfte. Zu deren 387.000 Euro teurer Metaverse-Party erschienen fünf Menschen[10]. Auch der Aktienkurs von Meta, ehemals Facebook – die mit ihrer Umbenennung eine All-In-on-Metaverse Strategie verfolgen – deutet darauf hin, dass der Markt von diesem Konzept nicht überzeugt ist.

Web 3 und Metaverse werden oft zusammen erwähnt, weil das Web 3 als ein Teil eines möglichen Wirtschaftssystems des Metaverse gesehen wird.

Wo genau jetzt der Unterschied zwischen Spielen der Frühen 2000ern – wie z.B. “Second Life” und dem Metaverse liegt, ist mir nicht ganz erklärlich. (Außer der Anzahl der Dimensionen und der benötigten Hardware natürlich.)

[9] https://web.archive.org/web/20140115142013/http://szabo.best.vwh.net/securetitle.html
[10] https://www.politico.eu/article/eu-threw-e387k-meta-gala-nobody-came-big-tech/

Da meine Kompetenzen im Bereich der Computerspiele eher eingeschränkt sind, werde ich mich zu den Fragen zu diesem Themenkomplex nicht äußern.

**2) Was sind die technischen, sicherheitstechnischen, Infrastruktur-kritischen, konzeptionellen, sozialen, finanzpolitischen, außenpolitischen und gesellschaftlichen Risiken von Web 3, was sind die Risiken mit Blick auf die Persönlichkeits- und Freiheitsrechte?**

**Risiken für Persönlichkeits- und Freiheitsrechte**

Digitalen Projekten auf Basis von Blockchains und Web 3-Konzepten sind Stand heute i.d.R. nicht mit den europäischen Standards im Datenschutz vereinbar. Dies lässt sich sehr gut an einigen Beispielen aus der deutschen Verwaltung aufzeigen:

**– BAMF-Blockchain**
In der Blockchain des Bundesamts für Migration und Flüchtlinge sollten die Antragsunterlagen sowie Informationen zum Verlauf des Asylverfahrens in einer internen Blockchain abgelegt werden.[11]
Das Ganze hat nur den kleinen Haken, dass in Deutschland ja jeder Mensch im Rahmen der DSGVO ein Recht auf die Korrektur und Löschung seiner eigenen Daten hat. Daten in Blockchains sind aber eben genau unveränderbar.

Da sich dies auf Basis einer Blockchain nicht umsetzen lässt – man also nicht im Sinne der DSGVO rechtskonform Daten einer Person auf einer Blockchain speichern kann – entschied man sich in diesem Fall dazu, nur Referenzen der Dokumente, die bearbeitende Stelle sowie den Antragsstatus auf dem Ledger abzulegen.
Auch das erfüllt meiner Rechtsauffassung nach nicht die Anforderungen an das Recht auf Vergessen im Sinne der DSGVO, weil somit weiterhin Referenzen auf Dokumente nicht gelöscht werden können – und die Echtheit und das Vorhandensein eines Dokumentes und auch der garantiert echte Status eines Asylantrags zu einem bestimmten Zeitpunkt zweifelsfrei belegbar sind.
Wenn nun ein solcher Ledger öffentlich wird, kann für jeden auf der Blockchain abgelegten Asylfall also festgestellt werden, wie dieser bearbeitet wurde.

[11] https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/blockchain-whitepaper.pdf?__blob=publicationFile&v=6

**– ID Wallet: Ausweis und Führerschein auf Blockchain-Basis**
Im September 2021 gab es für etwa 3 Tage einen digitalen Personalausweis und einen Führerschein auf Blockchain-Basis in Deutschland[12]. Der wurde sofort wieder eingestellt, weil das Prinzip von Ausweisdokumenten auf einer Blockchain – aus der man bekanntlich nichts löschen kann – in Verbindung mit der Idee, dass man die Ausweisdokumente auf seinem eigenen Smartphone speichert und von dort aus weitergibt, so viele konzeptionelle Sicherheitsprobleme hatte, dass es unverantwortbar war, dieses Projekt weiterzuführen.

Hier zeigt sich ein Problem, dass wir in der Web 3 Welt oft beobachten können: Der Schutz der digital signierten Güter liegt in der Verantwortung der Nutzer*innen und das führt schon jetzt dauernd zu Problemen. Hardware und Software wird unsicherer, je älter sie wird. Nicht alle können sich immer die modernste Hardware und Software leisten. Wir hätten also in Zukunft mit Ausweisen oder anderen digitalen Gütern auf den Smartphones der Bürger*innen das Problem, dass sich reiche Menschen besser vor dem Diebstahl ihrer Digitalen Identität (also eine Datei mit kryptografischem Verweis auf die Blockchain oder Wurzelzertifikat) schützen könnten als ärmere.
Wie schwierig es ist, solche Daten zu schützen, sieht man daran, wie oft technisch versierten Web 3-Fans ihre digitalen Güter abhandenkommen. Nur dass es sich hierbei heute eben i.d.R. noch eher um NFTs, also so etwas wie digitalisierte Fußball-Sammelbildchen mit fragwürdigem monetären Gegenwert handelt und nicht um eine digitale Brieftasche mit allen Dokumenten drin, um Bankkonten zu eröffnen oder Kredite zu beantragen.

Weil aber die Web 3-Welt Eigenverantwortung so wichtig findet, würde in einem solchen Fall dann nicht die Bank ein Problem haben, weil sie einem Betrüger einen Kredit gegeben hat. Sondern die Person, die ihren digitalen Ausweis verloren hat. Für die Bank wäre auch gar nicht feststellbar, welche natürliche Person da wirklich gerade mit ihr interagiert hat.

Wenn nun also Menschen ihr digitaler Ausweis abhandenkommt, dann kann dieser zwar – nachdem dies bemerkt wurde – gesperrt werden. Dass es sich dabei um den echten Ausweis der Person handelt, der da geklaut wurde, ist dank der Blockchain, aber für immer nachvollziehbar. Diese Funktion einer öffentlichen Blockchain oder eines Ausweissystems auf Basis von Wurzelzertifikaten bietet somit komplett neue Geschäftsmodelle für Datenhändler*innen. Das erste Modell ist der Identitätsdiebstahl: Hier kann ein geklauter Ausweis auch schon vor dem Kauf im Darknet auf seine Echtheit überprüft und dann so lange benutzt werden, bis auffällt, dass es eine Kopie davon gibt – im Zweifel also sehr lange.

[12] https://lilithwittmann.medium.com/

Das andere Modell ist, dass eine Nutzer*in sich gegenüber einem Unternehmen ausweist und das Unternehmen die garantiert echten Daten verliert oder sie an einen Datenhändler verkauft. Alle, die an die Daten, der Bürger*innen kommen, können zukünftig also auch die Echtheit dieser Daten zu jedem Zeitpunkt zweifelsfrei belegen. Das macht die Daten der Bürger*innen um ein Vielfaches wertvoller als z.B. eine pseudonyme Identität auf Basis einer E-Mail-Adresse.

Wie das Projekt "ID Wallet" überhaupt online gehen konnte, obwohl es eine Bewertung des BSI gab, die genau diese Probleme aufzeigte (und noch viele mehr), ist bis heute nicht abschließend geklärt.[13] Es bleibt ein gutes Beispiel, warum "Technologie First, Bedenken Second" kein guter Ansatz ist.

Auf EU-Ebene machen wir gerade dieselben Fehler noch mal – und das BMI ist mit der Bundesdruckerei mit einem "Large Scale Prototype" dabei, das konzeptionell kaputte Modell "ID Wallet" einfach noch mal auszuprobieren.

**– Schulzeugnis auf Blockchainbasis**

Dasselbe Konzept mit denselben Fehlern und fatalen / unbedachten Folgen gab es dann beim digitalen Schulzeugnis, an dem u.a. das BMBF mit der Bundesdruckerei gearbeitet hat, einfach noch mal. Wieder entgegen der Empfehlung des BSI[14]. Außerdem war die dazugehörige Verwaltungsanwendung so unsicher, dass es mit einfachsten Mitteln möglich war, darin beliebige Daten zu speichern.

Nur, dass dort nicht nur alle Erwachsenen mit verlierbaren, garantiert echten staatlichen Dokument ausgestattet werden sollten, sondern auch Kinder. Man wollte und will nun auch wieder im Rahmen des Projektes "Enmeshed" nach demselben Prinzip einer besonders vulnerablen Gruppe signierte Dokumente ausstellen, die besonders schützenswerte, personenbezogene Informationen (im Sinne von Art. 9 DSGVO) enthalten. Diese sollen dann beliebig an Schulen, potenzielle Arbeitgeber und Weitere verteilt werden. Es ist nur eine Frage der Zeit, bis das schiefgeht.

Wir haben jetzt an drei Beispielen gesehen, dass die Blockchain-Technologie und die darauf basierenden Web 3 Konzepte wie z.B. die sogenannten "Selbstbestimmte Identitäten" (SSI)[15] nicht zur Lösung von Problemen im Rahmen unserer juristischen Normen nutzbar sind. Und dabei gleichzeitig auch Standards des Verbraucher*innenschutzes weitestgehend ignoriert werden.

[13] https://fragdenstaat.de/dokumente/141932-bmi_idwallet/
[14] https://www.mdr.de/nachrichten/sachsen-anhalt/digital-zeugnis-blockchain-hintergrund-100.html
[15] https://doi.org/10.48550/arXiv.2203.00398

Anstatt dass wir versuchen, unsere Normen an eine Technologie anzupassen, sollten wir nach Technologien suchen, die unsere Normen tatsächlich erfüllen. Nicht die Technologie sollte das Soziale definieren, sondern das Soziale die Technologie. Es ist besonders erschütternd, dass der Staat solche Technologien an besonders vulnerablen Gruppen wie Kindern testet. Ganz nach dem Motto "Erst mal mit denjenigen ausprobieren, die sich eh nicht wehren können".

Es ist bedauernswert, wie lange der Staat mit solchen Technologien spielen muss, Millionen an Steuergeld verbrannt werden[16] und dass dabei bis heute von außen keinerlei Lernerfolge erkennbar sind. Dabei gibt es die notwendige technische Kompetenz, solche Projekte aus einer IT-Sicherheits-Perspektive einzuschätzen, in der deutschen Verwaltung durchaus[17].

**Technische Risiken**

Bei den im Web 3 eingesetzten Technologien handelt es sich häufig noch um Technologien in einem eher experimentellen Stadium. Allerdings seit nun bald 15 Jahren. Es kommt bei Transaktionsplattformen noch immer im Wochentakt zum Abfluss von personenbezogenen Daten und digitalen Gütern. Es ist fraglich, ob die Technologie diese Phase – auch mit entsprechender Regulierung – jemals verlassen kann.

Weil Nutzer*innen oder ein durch sie betrauter Treuhänder die Verantwortung über ihre digitalen Güter hat und diese im Falle von technischen Problemen oder Diebstahl in der Regel nicht mehr rückholbar und i.d.R. auch unversichert sind, herrschen hier signifikant höhere Risiken als z.B. bei klassischen Banken.

**Soziale Risiken**

Wie bereits unter *"Risiken für Persönlichkeits- und Freiheitsrechte"* benannt, sehe ich hier Risiken unter anderem darin, dass Nutzer*innen nicht über die Fähigkeiten verfügen, ihre digitalen Credentials zu schützen und diese verlieren. Dies kann schwere Folgen wie den Verlust ihrer Finanzwerte oder den Abfluss ihrer Daten haben. Dies wird übermäßig marginalisierte Gruppen betreffen.

---

16 https://www.schwarzbuch.de/aufgedeckt/steuergeldverschwendung-alle-faelle/details/digitale-brieftasche-floppt

17 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3

Eine Welt, in alle Interaktionen auf Tokens und Transaktionen heruntergebrochen wird, kann schon per Definition nicht sozial sein. Transaktionen, die idR von sehr privilegierten Menschen in der Tech Branche definiert werden und selbstverständlich deren Weltbild abbilden.

Zwar richten sich Web 3 basierte Angebote oft an Menschengruppen, die z.B. bisher keinen Zugang zu klassischen Finanzsystemen haben. Allerdings nicht aus sozialem Gedanken, sondern um von der Situation der Menschen zu profitieren.

**Gesellschaftliche und Finanzpolitische Risiken**
Die Idee des Web 3 ist, staatliche Ordnungssysteme in technische Lösungen unabhängig vom Staat auszulagern. Der Staat soll also im Kontext von Web 3 per Definition seine Rechte und die seiner Bürger*innen gar nicht nicht durchsetzen können.

**Wirtschaftliche Risiken**
Mehrere Studien belegen, dass Blockchain-Projekte eine sehr sehr niedrige Erfolgsrate haben. Es ist also davon auszugehen, dass durch die nutzlosen Investitionen in Blockchainprojekte auch ein immenser wirtschaftlicher Schaden entsteht[18].

Abschließend lässt sich sagen, dass Web 3-Technologie und Konzepte völlig unüberblickbare soziale und technische Risiken mit sich bringen. Deshalb ist von ihrem Einsatz abzuraten.

**3) Sind die bestehenden europäischen Regulierungsansätze (etwa DSA, DMA und DSGVO) ausreichend und welche regulatorischen Maßnahmen sehen Sie darüber hinaus als geeignet oder notwendig an um diese Risiken von Web 3 einzudämmen und welche Möglichkeiten sehen Sie, die angesprochenen Risiken anderweitig zu mitigieren?**

Wie bereits in Frage 2 ausgeführt, sind die Ideen und Konzepte des Web 3 nicht mit den Standards der DSGVO – insbesondere dem Art. 17, Recht auf Vergessen – vereinbar.

Ich halte es darüber hinaus für notwendig, Kryptowährungen stärker zu regulieren. Insbesondere in folgenden Bereichen:

- Verbraucher*innenschutz
- Finanzspekulationen
- Geldwäsche: Herkunftsnachweis und Meldepflichten für Kryptowährungen

[18] https://www.theregister.com/2018/11/30/blockchain_study_finds_0_per_cent_success_rate/

Da Kryptowährungen kein inhärenter Wert innewohnt, müssen wir einen Diskurs darüber führen, welche Regulierungen dafür greifen sollen. Vielleicht könnten hier Aspekte aus der Regulierung von Glücksspiel mit entsprechender Besteuerung und Verbraucherschutzregelungen übernommen werden.

**4) Wie bewerten Sie Chancen und Risiken von Kryptowährungen – im Allgemeinen und im Kontext des Web 3?**

Siehe *Frage 3.*

**5) Welche konkreten Anwendungsfälle und Mehrwerte, abgesehen von virtuellen Spielwelten, kann das Metaversum (z. B. in der Medizin oder im Ingenieurswesen) bringen?**

Siehe *Frage 1.*

**6) Im Gegensatz zum Web 3.0 beschreibt das Web 3 eine neue Generation des Internets, das auf Blockchain basiert und in dem die Nutzer die Kontrolle über ihre Daten innehaben sollen (das Konzept des Web 3 beinhaltet z. B. Entscheidungen über DAOs, den Aufbau einer tokenbasierten Wirtschaft, Finanzdienstleistungen über DeFi-Protokolle). Wie schätzen Sie das Potential des Web 3 ein, v.a. vor dem Hintergrund, dass der Nutzer ohne zentrale Intermediäre häufig auf Convenience verzichtet?**

Die Annahme, dass das Web 3 ohne Intermediäre auskommt, ist leider falsch. Es sind nur andere, weniger regulierte Intermediäre. Unter anderem deshalb sehen wir eine unfassbare Menge an Betrugsfällen im Kontext des Web 3.[19]

Die Kontrolle über seine Daten könnten die Nutzer*innen zwar rein theoretisch übernehmen – allerdings nur bis zu dem Punkt, an dem sie ihre Daten verlieren, einen Fehler begehen, weil sie die Technologie nicht beherrschen oder von jemandem betrogen wurden. Da dies – Stand heute – ständig und wie wir in Frage 2 lernten, ja ganzen Staaten passiert, ist das schon ganz schön viel **“Convenience”** auf die Nutzer*innen da verzichten müssen.

[19] https://web3isgoinggreat.com/

**7) Welche politischen Maßnahmen sind angezeigt, um sicherzustellen, dass in Entstehung befindliche Metaversen auf europäischen Werten – insbesondere Daten- und Verbraucherschutz – und den Prinzipien des digitalen EUBinnenmarkts – insbesondere fairer und lauterer Wettbewerb sowie nachhaltiges („Green IT“) und manipulationsfreies (keine „Dark Patterns“) Design – beruht?**

Das kann ich Ihnen nicht sagen, da ich nicht weiß, was europäische Werte eigentlich sind. Ob nationalstaatliche Wertvorstellungen in Online-Spielen mit 3D-Welten allerdings relevant sind, wage ich zu bezweifeln.

**8) Welche konkreten Ansatzpunkte gibt es mit Blick auf die bisherige Entwicklung des Internets (Web 1.0, Web 2.0), die Entwicklung zu einem nutzerorientierten, dezentralen und sicheren Internet in globale Governance-Mechanismen zu überführen?**

Hier wäre insbesondere mehr Grundlagenforschung dazu nötig, wie denn solche Systeme langfristig nachhaltig, nicht kommerziell und mit sehr vielen Teilnehmenden betrieben werden können.

Stand heute werden solche dezentralen Systeme oft von Menschen mit vielen Privilegien und einer sehr technischen Perspektive konzipiert und betrieben. Hier wäre die Unterstützung von Initiativen von marginalisierten Gruppen wünschenswert, um so nicht dieselben Fehler bei der Abbildung sozialer Strukturen in Technik zu machen, wie sie bisher immer wieder passiert sind.

Darüber hinaus sind Initiativen wie die Mastodon-Instanz der Bundesverwaltung zu begrüßen. Und die weitere Förderung solcher ersten Ansätze von dezentralen sozialen Netzwerken ist wünschenswert.

**10) Sind Ihnen Anwendungen der Blockchaintechnologie außerhalb von Kryptowährungen bekannt, die nicht durch bestehende Technologien, effizienter, umweltschonender etc. geleistet werden können. Wie ist eine Abwägung von Chancen und Risiken aus gesellschaftspolitischer Sicht zu bewerten?**

Nein. Wobei ich auch daran zweifle, dass sich das Prinzip von Währungen durch die Blockchain-Technologie besser abbilden lässt als durch konventionelle Währungen.

**11) Gibt es eine in der Wissenschaft geeinte Definition von Metaverse und wenn nicht, welche Definition würden Sie der Politik für den Umgang mit dem Konzept empfehlen und welche Bedeutung spielen dabei jeweils die bisherigen Konzepte von Augmented Reality, Assisted Reality, Virtual Reality und Extended Reality?**

Wie eingangs erwähnt, kenne ich mich mit Spielen nicht aus. Ich verzichte deshalb auf die Beantwortung dieser Frage.

**12) Wie würden Sie die Forschungslage in Deutschland zum Thema Metaverse im internationalen Vergleich bewerten, was Professuren, Publikationen, staatliche Forschungsförderung und Drittmittelfinanzierung für den Forschungsbereich Metaverse und Web 3.0 angeht?**

Nicht nur in der Verwaltung wurde schon eine Menge Geld mit der Blockchain verbrannt. Sondern auch in an das Web 3 angelehnten Bereichen werden bereits hohe Summen an Wirtschafts- und Forschungsförderungen verteilt.

So werden z.B. im "Schaufensterprojekt ~~Sichere~~ Digitale Identitäten" über 55 Millionen Euro vom BMWK dafür bereitgestellt, dass von vier Konsortien Lösung zur Nutzung von blockchainbasierten digitalen Identitäten entwickelt werden[20].

Oder im Rahmen des Projektes Gaia-X Federation Services. Dort spielen ganz viele Unternehmen zusammen mit Blockchains und wie sie darüber Datenhandel abbilden können. Mit über 13 Millionen Euro Fördergeld.

Allein eine Suche nach "Blockchain" im Förderportal des Bundes[21] findet Förderungen mit einer Gesamtsumme von mehr als 65 Millionen Euro. Die beiden oben genannten Projekte sind da noch gar nicht inbegriffen. Der deutsche Staat scheint dabei wirklich völlig wahllos alles zu fördern, wo das Wort Blockchain auch nur drin vorkommt. Von Wahlen über Züge bis zu Gesundheitsdaten in der Blockchain wird mit allem gespielt, was die KRITIS Verordnung und Art. 9 DSGVO so hergeben.

[20] https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/edt_bekanntmachung_foerderrahmen.pdf;jsessionid=304E35F234325A8F768133818028BC7F?__blob=publicationFile&v=3

[21] https://foerderportal.bund.de/foekat/jsp/SucheAction.do#

**13) Wie haben sich Ihrer Einschätzung nach die Unternehmen in Deutschland bisher auf Metaverse vorbereitet, gerade was den Vergleich zu den USA und China angeht und sehen Sie das Risiko, dass wir in Deutschland durch eine mangelnde Priorisierung des Themas Metaverse den technologischen und wirtschaftlichen Anschluss an die Weltspitze verpassen könnten?**

Siehe *Frage 11*.

**14) Welche Risiken könnten von zu frühen staatlichen Regulierungsversuchen der neuen Technologie ausgehen, auf welche Grundlagen bei Normierung und Standardisierung kann bereits für den Umgang mit Metaverse zurückgegriffen werden, wie sind wir in Deutschland und Europa Ihrer Einschätzung nach bei ermöglichenden Rahmenbedingungen für Metaverse aufgestellt, was Förderprogramme angeht und welche Maßnahmen möchten Sie der Politik vorrangig mitgeben, um die wirtschaftlichen und gesellschaftlichen Chancen von Metaverse möglichst gut nutzbar zu machen?**

Siehe *Frage 11.*

**15) Welche Geschäftsform sind DAOs und wie müssten sie reguliert werden, um Endkund*innen vor Betrug und Missbrauch zu schützen?**

Wie in *Frage 2* ausgeführt, erscheint mir das unmöglich.

**16) Wie können die Rechte und Prinzipien des Verbraucherschutzes in dezentralen Blockchain-Systemen wie denen des Web 3 umgesetzt werden?**

Nach meinem Rechtsverständnis: gar nicht.

**17) Das sogenannte Web 3.0 wird, bislang nur als Vision, dafür gefeiert, dass es dezentral aufgebaut sei, dass es die Macht großer Plattformen begrenze und dass die Datenhoheit bei den Nutzern liege. Welche Instanz wäre denn Ihrer Auffassung nach überhaupt in der Lage, das bisherige infrastrukturelle System der Plattformen und Zugangsknoten durch die Blockchain-Technologie zu ersetzen? Und woher sollte die Energie zum Betreiben der Blockchain-Technologie kommen?**

Das lange Zeit herrschende Energieproblem von Blockchainprojekten wurde tatsächlich von den meisten Projekten durch eine Umstellung von Proof-of-Work (Lösung einer komplizierten Rechenaufgabe, deren Lösung unglaublich viel Strom verbraucht) zu Proof-of-Stake (Verfahren auf Basis einer Token-basierten Sicherheitsleistung und dem Zufall) gelöst.

Für alles Weitere: *Fragen 2 & 3.*

**18) Sind Ihrer Auffassung nach Visionen eines „Metaverse“ und/oder eines „Web 3.0“ geeignet, die digitale Souveränität Deutschlands und Europas gegenüber etwa China oder den USA zu begründen und zu verstärken? Was genau müsste dafür seitens der eingesetzten Hard- und Software und gegebenenfalls auf der Ebene der Regulierung geschehen?**

Wie ein Einsatz von digitalen Signaturen sowie dezentralen Datenbanken die nationale Souveränität steigern soll, ist mir nicht erklärlich. Des Weiteren scheint eine Technologie, welche kernstaatliche Leistungen in einen unregulierten Raum überführen soll, nicht unbedingt für die Stärkung staatlicher Strukturen geeignet.

Was die Souveränität der deutschen Verwaltung gegenüber des Internets angeht, sollte deutlich mehr Kompetenz bei den Ermittlungs- und Finanzbehörden aufgebaut werden. Denn blockchainbasierte Währungen sind in Deutschland noch immer ein wunderbarer Weg, um Geld zu waschen. Dabei bietet der öffentliche Ledger ja tatsächlich den Vorteil, dass Transaktionen nachvollzogen werden können - diesen Vorteil sollten Ermittlungsbehörden zu nutzen lernen.