Elizabeth M. Renieris
HACKYLAWYER LLC

Anhörung im Ausschuss für Digitales am 14.12.2022
"Web 3.0 und Metaverse"

ANHÖRUNG IM AUSSCHUSS FÜR DIGITALES "WEB 3.0 UND METAVERSE"

ANTWORTEN AUF SCHRIFTLICHE FRAGEN

ELIZABETH M. RENIERIS

hackylawyer@protonmail.com

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 und 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 nutzer-zentrierten Netzes - kurz: stehen sie für das Internet, das es zu verhindern gilt?

Gegenwärtig gibt es keinen Konsens über die Bedeutung der Begriffe „Web 3.0", „Web3" und „Metaverse" (oder „Metaversum") oder was sie darstellen. Vielmehr werden sie oft synonym und unterschiedlich verwendet, um die vielfältigen und manchmal konkurrierenden Interessen der verschiedenen Interessengruppen zu unterstützen. Dennoch beziehen sie sich alle auf Ideen und Pläne, wie die Zukunft unserer digitalen Praxis aussehen könnte, insbesondere im Vergleich mit unserer heutigen Erfahrung.

„Web 3.0" ist ein älterer, enger gefasster Kunstbegriff, der im Allgemeinen mit der von Sir Tim Berners Lee vor einigen Jahrzehnten erstmals formulierten Beschreibung einer dritten Generation des Webs in Verbindung gebracht wird. In diesem Paradigma ist das Web 1.0 eine „Nur-Lesen"-Version des Webs, die größtenteils aus statischen Webseiten und Inhalten besteht, das Web 2.0 ist die „Lesen-Schreiben"-Version, die das Aufkommen von nutzergenerierten Inhalten, sozialen Medien und verstärkter Interaktivität ermöglichte, und das Web 3.0 ist das „Lesen-Schreiben-Ausführen"- oder „semantic Web" (manchmal auch als „Web der Daten" bezeichnet), in dem alles auf der Datenebene miteinander verbunden ist. Laut Berners Lee erfordert das Web 3.0 weder den Einsatz der Blockchain-Technologie noch profitiert es davon.

„Web3" wird zwar häufig als Synonym von Web 3.0 verwendet, ist aber ein weiter gefasster, nebulöser Begriff, der ein Web beschreibt, das theoretisch stärker dezentralisiert ist als wir es heute kennen. Gelegentlich wird es auch als das „Lesen-Schreiben-Besitzen"-Web bezeichnet. In der Regel handelt es sich dabei um eine Kombination aus Blockchain- oder Distributed-Ledger-Technologie (DLT), selbstausführenden Codezeilen (bekannt als „Smart Contracts"), kryptografisch eindeutige, unteilbare, unersetzbare und überprüfbare Token (Non-Fungible Tokens, NFTs) und Kryptowährungen. Aus technischer Sicht soll das Web3 eine Abkehr von der traditionellen Client-Server-Architektur des Webs darstellen, bei der die Daten in zentralen Servern großer Unternehmen konzentriert und darüber geleitet werden, und eine Hinwendung zu Peer-to-Peer-Konstruktionen

und -Protokollen, über die die Netzressourcen direkt miteinander kommunizieren und Daten austauschen.

„Web 3.0“ und „Web3“ werden im Vergleich zu den heutigen oft als „bessere“ Versionen des digitalen Ökosystems bezeichnet und als Lösungen für die anhaltenden Datenschutz- und Sicherheitsbedenken präsentiert, die aufgrund der Machtkonzentration im Web bei einer Handvoll großer Unternehmen entstehen. Beide Konzepte sind jedoch problematisch, weil sie versuchen, nicht-technische Probleme, wie die Konzentration von Reichtum und Macht bei einer kleinen Handvoll privater Unternehmen, mit meist technologischen Eingriffen zu lösen, während sie die sozialen, politischen, wirtschaftlichen und kulturellen Faktoren, die diese Probleme überhaupt erst verursacht haben, außer Acht lassen. Mit anderen Worten: Sie vertreten weitgehend techno-solutionistische Perspektiven.

Der Begriff „Metaverse“ stammt aus der Science-Fiction und wurde erstmals 1992 von Neal Stephenson in seinem Roman „Snow Crash“ verwendet, in dem das Metaverse als ein internetbasierter virtueller Realitätsraum mit Avataren und Software-Agenten dargestellt wird. Heute bezieht er sich im weitesten Sinne auf ein Netzwerk virtueller Welten oder eine Art immersives Internet, das durch eine Reihe von „realitätserweiternden“ Technologien (Extended-Reality-Technologien, XR-Technologien) wie Virtual Reality (VR), Augmented Reality (AR) und Mixed Reality (MR), Hardware wie Headsets, Wearables und andere vernetzte Geräte, den Einsatz physischer und verhaltensbiometrischer Daten, von Avataren und anderen digitalen Werkzeugen für eine digitale Identität sowie künstlicher Intelligenz (KI) und auf maschinelles Lernen gestützten Systemen ermöglicht wird. Ich ziehe jedoch vor, diese Technologien als metaversale Technologien zu bezeichnen, anstatt von einem „Metaversum“ als voll ausgebildetem Konzept oder Ökosystem zu sprechen.

Obwohl keiner dieser Begriffe oder keines dieser Konzepte per se eine „Version des Internets, die es zu verhindern gilt“ darstellt, stellen jene, die Visionen von Web 3, Web 3.0 und dem Metaverse propagieren, oft Behauptungen auf, die in Frage gestellt werden müssen (und vertreten manchmal Ideologien, die sozial, politisch und wirtschaftlich problematisch sind, wie weiter unten beschrieben). Daher sollten Gesetzgeber und politische Entscheidungsträger, Wissenschaftler, Mitglieder der Zivilgesellschaft und andere Interessengruppen versuchen, Web3- oder Metaverse-Projekte kritisch zu betrachten und die Last der Darlegung und des Nachweises eindeutiger Vorteile auf die Befürworter zu übertragen.

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

Aus technischer, sicherheitsbezogener und infrastruktureller Sicht stützt sich das Web3 weitgehend auf eine Kombination aus unerprobten, unzuverlässigen und unsicheren Technologien, die zusätzliche Komplexitätsebenen einführen, wodurch wiederum das Fehler- und Schwachstellenrisiko erhöht wird. Die Befürworter von Web3 behaupten beispielsweise häufig, dass der Einzelne die „Kontrolle“ über seine Privatsphäre und die Sicherheit seiner Daten von großen, zentralisierten Intermediären wie Meta und Google zurückerhält. In Wirklichkeit bietet Web3 jedoch in der Regel zwei gleich schlechte Alternativen zum bestehenden Modell. In einer Version werden bestehende Intermediäre durch neuere, weniger rechenschaftspflichtige Intermediäre ersetzt (und selbst dann stützen sich diese Intermediäre oft noch auf die Dienste und die Infrastruktur traditioneller Intermediäre, z. B. Amazon Web Services oder Google Cloud Platform, was dazu führt, dass sich die damit verbundenen Herausforderungen wiederholen). In der anderen Version wird der Einzelne in unzumutbarer Weise damit belastet, seine eigenen Wallets, Schlüssel und Daten zu verwalten und zu

sichern, ohne dass er einen Regressanspruch hat oder Abhilfe schaffen kann, wenn – was zwangsläufig geschieht – Probleme auftreten. Dieser Ansatz wirkt sich unverhältnismäßig stark auf verschiedene Personen und Gemeinschaften aus und belastet die Schwächsten oft am stärksten.

Aus konzeptioneller Sicht legen die Web3-Befürworter auch eine Art erfinderische Obsoleszenz an den Tag, bei der sich Zukunftsvisionen in schneller Folge einander ablösen, während die bestehenden Technologien und Systeme, auf die sich aktuell Milliarden Menschen täglich verlassen, als veraltet und vernachlässigbar betrachtet werden. Mit anderen Worten: Das Versprechen des Web3 verlagert unsere Vorstellungskraft und unsere Ressourcen von der Lösung bekannter Probleme oder den Erhalt des Vorhandenen auf das Heraufbeschwören technologischer Utopien, in denen diese Probleme nicht wieder auftauchen. Das unterläuft auch die Bemühungen um eine wirksame technologische Governance, weil der Gesetzgeber ständig gezwungen ist, mit neuen Gesetzen und Vorschriften darauf zu reagieren, ohne dass die bestehenden Anwendung finden können. Es handelt sich auch um eine Art von Denken im Sinne der philosophischen Denkschule des „Longtermism“, nach der reale und gegenwärtige Gefahren bestehender soziotechnischer Systeme zugunsten einiger zukünftiger utopischer Ideale vernachlässigt werden.

Aus wirtschaftlicher und gesellschaftlicher Sicht birgt das Web3 auch die Gefahr, unsere kommerzielle Ausbeutung durch digitale Interaktionen zu verschärfen. Das frühe Web vor Einführung des Online-Angebots von Produkten und Dienstleistungen durch den elektronischen Handel war ein nicht-kommerzielles Netzwerk zur Verbreitung von Inhalten. Blockchain-basierte Versionen des Web3 dagegen würden mittels „intelligenter Verträge“ (Smart Contracts) jede digitale Interaktion in eine finanzielle Transaktion mit einer entsprechenden Mikrozahlung in Form einer Kryptowährung umwandeln, wobei ein oder mehrere undurchsichtige Intermediäre häufig Transaktionsgebühren einziehen. Mit dieser „Finanzialisierung von allem“, wie dies von einigen bezeichnet wurde, geht die Gefahr einher, dass wir Inhalte nicht mehr passiv nutzen oder digitale Bürger des Webs sein können, sondern dass wir uns in erster Linie als kommerzielle Akteure oder als vollständig zu einer Ware gewordene Einheiten in einem immer komplexeren Finanzsystem wiederfinden.

Die oben genannten Bedenken sind in ihrer Gesamtheit ebenfalls eine große Gefahr für unsere persönlichen Rechte und bürgerlichen Freiheiten. Wenn wir technische Lösungen für nicht-technische Probleme überbetonen und zu viel in sie investieren, was zu einer Art erfinderischer Obsoleszenz führt, die bestehende Herausforderungen vernachlässigt und die unkontrollierte Kommerzialisierung menschlicher Erfahrungen ermöglicht, wird von Rechten und Freiheiten wenig übrig bleiben. Wenn wir beispielsweise bedenken, wie bedeutungslos die „Einwilligung“ im Kontext asymmetrischer digitaler Interaktionen geworden ist, bei denen personenbezogene Daten gesammelt werden, sollten wir bedenken, dass eine Mikrozahlung oder eine explizite Finanzialisierung dieser Interaktionen ihnen eine Art falscher Legitimität verleihen würde, da sie den transaktionalen Charakter unserer Erfahrung absegnet. Wenn wir die Finanzialisierung von allem akzeptieren und uns als hauptsächlich kommerzielle Akteure betrachten, untergraben wir auch die mit dem Bürger- und Menschsein verbundenen Bürger- und Menschenrechte.

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?

Es ist schwer zu sagen, ob die bestehenden europäischen Regulierungsansätze ausreichend sind, insbesondere im Hinblick auf die kürzlich eingeführten Gesetze wie das Gesetz über digitale Dienste (DSA), das Gesetz über digitale Märkte (DMA), den Daten-Governance-Rechtsakt (DGA), das Datengesetz (Data Act) und das Gesetz über künstliche Intelligenz (AI Act), da sie größtenteils neu

und noch nicht erprobt sind. Der Schlüssel zu ihrer Anwendbarkeit und Wirksamkeit liegt jedoch in dem Umfang, in dem Gesetzgeber und politische Entscheidungsträger die Behauptungen der Web3-Promoter hinterfragen und zerlegen können, um ihre Aktivitäten und Institutionen als das zu erkennen, was sie sind, und nicht als das, was sie vorgeben zu sein. So ist beispielsweise eine verteilte technische Architektur (z. B. geografisch verteilte Knoten in einem Blockchain-Netzwerk) nicht dasselbe wie eine dezentrale gesellschaftspolitische oder wirtschaftliche Kontrolle, eine technisch dezentralisierte App (oder dApp) bedeutet nicht automatisch, dass es keine Intermediäre gibt oder dass die Datensicherheit oder der Datenschutz verbessert werden, und die Anonymität der Entscheidungsträger in einer dezentralisierten autonomen Organisation (DAO) ist keine Grundlage, um sich der Verantwortung zu entziehen oder der Rechenschaftspflicht zu entgehen. Wenn wir eine kritische Sichtweise anwenden und uns an die ersten Grundsätze halten, können wir die endlose Suche nach „perfekten Gesetzen“, die es vielleicht nie geben wird, vermeiden.

Was speziell die Datenschutz-Grundverordnung angeht, so sollte sie weiterhin in allen Aspekten für Web3 gelten, da die meisten Permutationen und Web3-Systeme nach wie vor aus Einrichtungen bestehen, die als für die Datenverarbeitung Verantwortliche, Datenverarbeiter und betroffene Personen angesehen werden können, obwohl die Bestimmung ihrer jeweiligen Rollen und Verantwortlichkeiten manchmal schwieriger und komplexer ist. Wenn beispielsweise ein Blockchain-basiertes System zur Verwaltung personenbezogener Daten Einzelpersonen ermöglicht, personenbezogene Daten in einer vom Nutzer kontrollierten digitalen Wallet zu verwalten und zu speichern, bedeutet das nicht, dass es keine Beziehung zwischen dem für die Verarbeitung Verantwortlichen und der betroffenen Person gibt, sofern das System so konzipiert ist, dass es die Zwecke und Mittel der Datenverarbeitung diktiert. Darüber hinaus sollten in Fällen, in denen es inhärente und unvereinbare Spannungen, z. B. zwischen der Datenschutz-Grundverordnung und den vorgeschlagenen technischen Architekturen gibt, diese als nicht den bestehenden Vorschriften entsprechend gelten und für die Behebung von Konformitätslücken verantwortlich gemacht werden.

In diesem Zusammenhang muss darauf hingewiesen werden, dass sich die Datenschutz-Grundverordnung nur auf den Datenschutz bezieht, der nur eines von vielen wichtigen Bürger-, Menschen- und Freiheitsrechten ist, die von Web3-Systemen (und metaversalen Technologien im Allgemeinen) betroffen sind. Auch wenn dies wichtig ist, dürfen wir nicht aus den Augen verlieren, dass selbst datenschutzkonforme Systeme zu ungerechten und diskriminierenden Ergebnissen, ungleicher Behandlung und einem Mangel an ordnungsgemäßen Verfahren führen und die Privatsphäre, die Autonomie, die persönliche Würde und allgemeinere wirtschaftliche, soziale und kulturelle Rechte erheblich beeinträchtigen können. Mit anderen Worten: In einer Version des Webs, die auf verknüpften Daten und codebasierten kommerziellen Transaktionen beruht, wird die Gewährleistung der Privatsphäre oder der Sicherheit der Daten nicht ausreichen, um die Privatsphäre oder die Sicherheit von Menschen zu gewährleisten.

4. Wie bewerten Sie Chancen und Risiken von Kryptowährungen – im Allgemeinen und im Kontext des Web 3.0?

Alles in allem und auf der Grundlage der uns bisher vorliegenden Erkenntnisse bergen Kryptowährungen mehr Risiken als Chancen. Kryptowährungen geben vor, bei Finanztransaktionen ohne Intermediäre auszukommen, dadurch umwälzende Veränderungen für das traditionelle Bankwesen hervorzurufen und die finanzielle Integration zu fördern. Einem aktuellen Bericht der Universität Cambridge zufolge fehlt es den Kryptowährungen jedoch an Stabilität, Zweckmäßigkeit und Zugänglichkeit, um diese Ziele zu erreichen. Stattdessen haben Kryptowährungen bisher eine Vielzahl neuer, undurchsichtiger und nicht rechenschaftspflichtiger Intermediäre hervorgebracht. Sie stellen kaum eine Bedrohung für das traditionelle Finanzsystem oder große konventionelle Banken dar (deren Innovationslabore Blockchain und Kryptowährungen als Marketinginstrument entdeckt

haben), und sie haben wenig zur finanziellen Integration beigetragen. Tatsächlich ist einer der wenigen integrativen Aspekte von Kryptowährungen bislang der weit verbreitete wirtschaftliche Ruin von Millionen Kryptowährungsinvestoren, die Geld in unbesicherten Systemen verloren haben – Verluste, die unverhältnismäßig viele Minderheitsanleger betroffen haben.

Speziell im Zusammenhang mit Web3 werden Kryptowährungen auch in alle möglichen soziotechnischen Systeme auf eine Art eingebracht, die ernsthafte Risiken der Diskriminierung, Ausgrenzung, Belästigung und Eingriffe in die Privatsphäre und Autonomie mit sich bringt. Web3-Projekte für digitale Identitäten wie WorldCoin, die größtenteils in Entwicklungsländern getestet werden, nutzen beispielsweise invasive biometrische Technologien wie Iris-Scanner, um Blockchain-basierte Identitäten für ein „globales digitales Währungssystem“ zu erstellen. Doch obwohl WorldCoin und Blockchain-basierte digitale Identitätsprojekte unter anderem in Myanmar, der Türkei und den Niederlanden vorgeben, die finanzielle und soziale Eingliederung zu unterstützen, versäumen sie, die zugrunde liegenden sozialen, politischen und wirtschaftlichen Ursachen für die Ausgrenzung in den bestehenden Finanz- und Identitätssystemen anzugehen und die Technologie als umfassende Lösung zu positionieren. Mit anderen Worten: Sie zeigen wieder ein hohes Maß an Techno-Solutionismus.

Selbst in den wenigen Fällen, in denen Kryptowährungen zu finanzieller oder sozialer Eingliederung führen können, beruhen diese Systeme in der Regel auf einer Kombination undurchsichtiger Technologien, die eine erhebliche Komplexität mit sich bringen. Es wird allgemein anerkannt, dass Intermediäre, seien es Banken im Finanzkontext oder digitale Plattformen im Online-Kontext, erhebliche Vorteile in Bezug auf Sicherheit, Zugänglichkeit und Bequemlichkeit bieten. Bei Web3-Projekten wird jedoch häufig erwartet, dass der Einzelne seine eigenen Wallets, Schlüssel und kryptografischen Protokolle verwaltet. Dadurch wird dem Einzelnen die Verantwortung für den Schutz seiner Privatsphäre und die Sicherheit seiner Daten oder anderer Vermögenswerte aufgebürdet, und er hat keine Möglichkeit, sich zu wehren oder Abhilfe zu schaffen, wenn – wie unvermeidlich – Probleme auftreten, wobei die unverhältnismäßigen Auswirkungen auf die Zugänglichkeit oder Nutzbarkeit der Technologie für verschiedene Menschen und Gemeinschaften vernachlässigt werden.

Trotz dieser Risiken argumentieren die Befürworter von Kryptowährungen, dass die Technologie noch in den Kinderschuhen steckt und die Vorteile erst noch realisiert werden müssen, aber das ist nicht der Fall. Bitcoin, die bekannteste Kryptowährung, gibt es seit mehr als einem Jahrzehnt. Sie befindet sich nach wie vor in den Händen einiger weniger, und ihre reale Anwendbarkeit oder ihr Nutzen jenseits von Spekulationszwecken ist begrenzt. Außerdem gibt es die Konzepte der Blockchain und des elektronischen Geldes oder „E-Cash“ (Vorläufer der Kryptowährungen) schon seit fast vier Jahrzehnten, die zugrunde liegenden kryptografischen Konzepte und Methoden sind noch viel länger bekannt. In der Zwischenzeit haben andere digitale Technologien, wie Smartphones und bestimmte IoT-Geräte, in wesentlich kürzerer Zeit nachweisbare Vorteile gebracht.

Ein tiefergehendes Problem bei Kryptowährungen sind die Ideologien, die von den Befürwortern oft vertreten werden. Typischerweise handelt es sich dabei um eine Art Neoliberalismus, in dessen Mittelpunkt die Vorherrschaft oder Selbstsouveränität des Einzelnen steht, die manchmal auch als absolute Transaktionsfreiheit dargestellt wird. Das führt nicht nur zu einer übermäßigen Belastung des Einzelnen (mit uneinheitlichen und unterschiedlichen Auswirkungen auf bestimmte Bevölkerungsgruppen), sondern ist in Zeiten großer kollektiver Herausforderungen wie Klimawandel, Rassenungerechtigkeit und zunehmendem Autoritarismus besonders problematisch und birgt die Gefahr, dass wichtige kollektive Ziele, seien sie sozialer, politischer, ökologischer oder wirtschaftlicher Natur, untergraben werden. Darüber hinaus bedroht die Erhebung eines Rechts über

alle anderen auch zentrale internationale Menschenrechtsgrundsätze hinsichtlich der Wechselbeziehung, Interdependenz und Unteilbarkeit von Rechten.

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

Wenn wir das Metaversum als eine immersive oder virtuelle digitale Erfahrung betrachten, gibt es potenziell wertvolle Anwendungen für Arbeitsplätze oder die Ausbildung von Kompetenzen. So werden Augmented und Virtual Reality in der Luft- und Raumfahrtindustrie seit langem eingesetzt, um Piloten und Astronauten in verschiedenen Fertigkeiten zu schulen und Szenarien während des Fluges zu simulieren. Zunehmend wird VR auch in der Ausbildung von Medizinstudenten und Ärzten eingesetzt, die medizinische oder chirurgische Techniken und Verfahren in virtuellen Simulationen üben. Über die Ausbildung hinaus gibt es auch potenziell wertvolle Anwendungen in der Praxis, wie z. B. virtuelle medizinische Fernkonsultationen. VR-Tools werden inzwischen auch vom Militär und von Strafverfolgungsbehörden für Übungen und Ermittlungen eingesetzt.

In dem Maße, in dem diese Anwendungsfälle an Bedeutung gewinnen, wächst die Sorge, dass virtuelle Schulungsumgebungen die Komplexität realer Handlungen oder Szenarien nicht immer effektiv nachbilden oder berücksichtigen und in der Praxis zu einem überzogenen Vertrauen in die eigenen Fähigkeiten oder das eigene Fachwissen führen können. Daneben sind Metaversen oder virtuelle Räume nicht immer barrierefrei gestaltet und können daher für Personen mit kognitiven, sensorischen oder körperlichen Einschränkungen oder Beeinträchtigungen nur von begrenztem Nutzen sein und damit ihre berufliche Entwicklung oder ihre Kompetenzschulung möglicherweise auf ungerechte Weise einschränken. Wenn der Einsatz von VR und anderen metaversalen Werkzeugen als angemessen erachtet wird, sollten sie idealerweise in Kombination mit oder neben anderen Modalitäten eingesetzt werden, um Inklusion und Zugänglichkeit zu fördern.

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 Web3 ein, v. a. vor dem Hintergrund, dass der Nutzer ohne zentrale Intermediäre häufig auf Convenience verzichtet?

Es ist wichtig, die Behauptungen der Web3-Befürworter zur Kontrolle der Daten durch die Nutzer von der Realität dieser Projekte in der Praxis zu trennen. Es besteht zwar weitgehende Einigkeit darüber, dass das bestehende Web mit einer Machtkonzentration in den Händen einiger weniger Großunternehmen behaftet ist, die personenbezogene Daten zu kommerziellen Zwecken ausbeuten, häufig mit schädlichen Folgen für Einzelpersonen und Gemeinschaften, und obwohl der Wunsch, diese Probleme anzugehen, lobenswert ist, gibt es keine Anzeichen dafür, dass das Web3 diese Probleme tatsächlich lösen oder angehen wird.

Erstens führen, wie bereits oben erwähnt, Web3-Interventionen häufig nicht zu einer tatsächlichen Ausschaltung von Intermediären (Disintermediation). Vielmehr ersetzen sie häufig bestehende Intermediäre durch neue, undurchsichtigere und nicht rechenschaftspflichtige Intermediäre, die nicht denselben Anreizen oder Ansatzpunkten unterliegen, mit denen bestehende Intermediäre zur Rechenschaft gezogen werden können (wie z. B. die Existenz bekannter und identifizierbarer Führungskräfte und rechenschaftspflichtiger Parteien, bestehende Gesetze und Vorschriften, Geschäftskontinuität und Notfallplanung, obligatorische Transparenzberichterstattung, Rechenschaftspflicht gegenüber den Aktionären und andere Corporate-Governance-Mechanismen, Compliance-Programme und Fachwissen, das für neue Technologien genutzt werden kann, Beziehungen zu Aufsichtsbehörden etc.). Web3- und Krypto-Intermediäre verstecken sich häufig

hinter Anonymität oder Pseudonymität, Code und Rechtsprechungsarbitrage (sie operieren häufig über Offshore-Unternehmen, um Steuerpflicht und Compliance-Verpflichtungen zu vermeiden).

Aber selbst dort, wo sie zu einer sinnvollen Disintermediation führen könnten, ist dies nicht unbedingt ein Vorteil für die betroffenen Personen oder Gemeinschaften. Nehmen wir zum Beispiel die Verwaltung personenbezogener Daten. Theoretisch würden viele gerne ihre eigenen Daten kontrollieren und verwalten, aber nur wenige wollen das auch in der Praxis tun. Angesichts des Umfangs und des Ausmaßes digitaler, datengestützter Interaktionen und Transaktionen, mit denen der Einzelne heute im Alltag konfrontiert ist, ist es einfach nicht sinnvoll oder praktikabel, vollständig selbstverwaltete Systeme zu erwarten. Dies wäre ein Einfallstor für Verhaltensfehler, einschließlich Überforderung und Einwilligungsmüdigkeit. Im Falle einer tatsächlichen Disintermediation würde der Einzelne also auf mehr als nur Bequemlichkeit verzichten. Er würde Sicherheit und Schutz opfern, wenn er es mit der Verwaltung komplexer technischer Tools und Systeme konfrontiert ist (man denke nur an das Mantra „nicht dein Schlüssel, nicht dein Krypto“). Er würde ebenso auf wirksame Rechtsmittel und Rechtsbehelfe verzichten und auf die Möglichkeit, leicht identifizierbare Einrichtungen oder Personen zur Rechenschaft zu ziehen sowie möglicherweise den Schutz seiner Daten gefährden aufgrund eines trügerischen Vertrauens in die übermäßig aufgeblähten kryptografischen Fähigkeiten dieser Systeme.

Web3-Befürworter behaupten oft, dass Blockchain der Schlüssel zu Datenschutz und Autonomie im digitalen Zeitalter ist, tatsächlich jedoch stellen „zensurresistente“ Technologien eine große Bedrohung unserer Privatsphäre und Autonomie dar. Zu den am häufigsten genannten Vorteilen von Blockchain gehören größere Transparenz, bessere Nachverfolgbarkeit sowie höhere Geschwindigkeit und Effizienz – Kernmerkmale, die auch bei der Anwendung der Technologie auf Menschen nicht verschwinden. Bei der Sorge um die „Zensurresistenz“ von Transaktionen verlieren wir die Auswirkungen auf die Menschen aus den Augen. Mit der Erstellung einer permanenten, digitalen Aufzeichnung unserer Transaktionen machen wir uns für externe Kontrolle und Selbstzensur anfälliger. Auf diese Weise birgt das Versprechen von Web3, unser digitales Ökosystem auf Blockchain-Basis neu aufzubauen, die Gefahr, dass die Menschen transparenter (d. h. exponierter), nachverfolgbarer (d. h. überwachbar) und effizienter (d. h. transaktionsbezogener) werden – Eigenschaften, die auch für autoritäre Impulse förderlich sind.

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 EU-Binnenmarkts – insbesondere fairer und lauterer Wettbewerb sowie nachhaltiges („Green IT“) und manipulationsfreies (keine „Dark Patterns“) Design – beruht?

Datenschutz und Verbraucherschutz sind zwar wichtig, bieten aber eine zu stark verengte Perspektive, wenn es darum geht, wichtige Werte im Zusammenhang mit metaversen Räumen und der Nutzung metaversaler Technologien zu schützen. Schließlich sind wir in diesen virtuellen Räumen mehr als nur Datensubjekte und Verbraucher. Wir bleiben Bürger und Menschen mit wichtigen bürgerlichen und politischen Rechten. Unternehmen, die diese virtuellen Dienstleistungen und Metaverse-Technologien anbieten, sollten sicherstellen, dass Metaversen die europäischen Werte respektieren, und verpflichtet werden, die seit langem bestehenden Menschenrechtsstandards und -grundsätze einzuhalten, insbesondere die Europäische Menschenrechtskonvention und die EU-Grundrechtecharta sowie die internationalen Menschenrechtsnormen im Allgemeinen gemäß den UN-Leitprinzipien für Wirtschaft und Menschenrechte.

Anstatt zu versuchen, ein „Metaversum“ als solches zu regulieren, sollten sich Gesetzgeber und politische Entscheidungsträger darauf konzentrieren, bestehende Gesetze und Vorschriften auf die einzelnen Produkte und Dienstleistungen anzuwenden, aus denen ein bestimmtes Metaversum-

basiertes Angebot besteht. So sollten beispielsweise Metaversen in Form von virtuellen Arbeitsräumen und Arbeitsplatz-Tools den bestehenden Regeln und Verpflichtungen unterliegen, die Arbeitgeber verpflichten, den Arbeitnehmern die gleichen Rechte und den gleichen Schutz nach dem geltenden Arbeitsrecht wie in nicht-virtuellen Kontexten zu gewähren. Gemäß dem EU-Grundsatz „was offline illegal ist, muss auch online illegal sein“, muss das, was in nicht-virtuellen Räumen rechtswidrig ist, auch in virtuellen Räumen rechtswidrig sein. Mit anderen Worten: Das Metaversum sollte keine Sonderbehandlung erfahren und sich nicht den bestehenden Gesetzen und Vorschriften entziehen.

8. Welche konkreten Ansatzpunkte gibt es mit Blick auf die bisherige Entwicklung des Internets (Web1, Web2), die Entwicklung zu einem nutzerorientierten, dezentralen und sicheren Internet in globale Governance-Mechanismen zu überführen?

Ich bin nicht davon überzeugt, dass ein „nutzerorientiertes, dezentralisiertes und sicheres Internet“ möglich oder gar wünschenswert ist. Allzu oft bedeutet „nutzerorientiert“, dass der Einzelne mit einer unüberschaubaren Zahl von Entscheidungen, Wahlmöglichkeiten und Abwägungen überfordert wird, und zwar in einer Weise, die ihn verwundbarer macht als die Alternativen. Ein seit langem bestehendes Paradigma im Datenschutzrecht ist zum Beispiel der Rahmen „Benachrichtigung und Wahlmöglichkeit“ bzw. „Benachrichtigung und Zustimmung“. Obwohl er lange Zeit als Mittel zur Förderung der Privatsphäre, der Sicherheit und der Autonomie des Einzelnen im Internet angepriesen wurde, hat sich in der Praxis das genaue Gegenteil herausgestellt. Dieser hyperindividualistische Ansatz hat den Einzelnen äußerst verwundbar gemacht, da er mit schwer verständlicher Rechtssprache in Form von Datenschutzhinweisen der Unternehmen, Geschäftsbedingungen, Popup-Fenstern für die Zustimmung zu Cookie-Richtlinien und vielem mehr überschwemmt wird, um die Illusion zu erwecken, der Nutzer habe die Kontrolle über seine Privatsphäre. Stellen Sie sich vor, Sie würden diesen unzureichenden Rahmen auf virtuelle Räume ausdehnen, in denen qualitativ neue und andere Benutzeroberflächen (über die grafische Benutzeroberfläche hinaus) zusätzliche Herausforderungen für die Bereitstellung aussagekräftiger Hinweise und die Einholung von Einwilligungen in Echtzeit darstellen. Es ist einfach das falsche Paradigma.

Ferner ist „dezentralisiert“, wie oben bereits erwähnt, ein weiteres Schlagwort, das sich in der Praxis nicht bewährt hat. In früheren Versionen des Web propagierten ideologische Untergruppen auch die Idee der Dezentralisierung als eine Art heiligen Gral. Auf dem Höhepunkt des Dotcom-Booms stellten John Perry Barlow und die Cyberlibertären den „Cyberspace“ als eine völlig eigenständige und neue Realität dar, die nicht den Gesetzen des Menschen oder der Physik unterliegt. Die heutigen Krypto-Libertären stehen in derselben Tradition und streben eine Sonderbehandlung für ihre Produkte und Dienstleistungen an, mit dem Argument, dass die bestehenden Gesetze und Vorschriften nicht für ihre Ökosysteme gelten.

Aber Intermediäre sind ebenso wertvoll wie Institutionen, da sie dem Einzelnen ein gewisses Maß an Sicherheit und Regressmöglichkeiten bieten, wenn ein Problem entsteht. Auf der anderen Seite untergraben viele Kryptowährungs- und Web3-Befürworter Institutionen (ob Regierungen, Universitäten oder Banken), auch wenn sie sich auf die bestehende rechtliche und politische Infrastruktur stützen; sie erschaffen neue Institutionen mit denselben Herausforderungen und weigern sich, dasselbe Maß an Verantwortung oder Rechenschaft zu übernehmen. Wichtiger als jede Art von technischer Dezentralisierung ist, die Konzentration wirtschaftlicher und politischer Macht in der digitalen Governance anzugehen und sicherzustellen, dass die angewandten Regeln und Normen ein breites Spektrum globaler Interessengruppen spiegeln, anstatt den Interessen einiger weniger zu dienen.

Außerdem ist ein „sicheres Internet“ nicht nur eine Frage der Blockchain oder einer anderen technischen Architektur, wie uns die Befürworter des Web3 oder des Metaverse glauben machen wollen. Selbst die beste technische Sicherheit ist anfällig für politische Korruption, perverse wirtschaftliche Anreize (z. B. schädliche zugrunde liegende Geschäftsmodelle) und Herausforderungen und Schwachstellen in einem bestimmten Ausmaß. Web3 und das Metaverse stehen für eine verstärkte Interaktivität und Kommerzialisierung des Webs, die mit erhöhten Risiken verbunden ist. Wenn alles zu einer finanziellen Transaktion wird, verdrängen der Wert und die Anreize für Unternehmen unweigerlich demokratischere Werte. Ohne die Berücksichtigung von Anreizen kann es keine angemessene Sicherheit geben, unabhängig vom Grad der eingesetzten Kryptographie.

Schließlich hat eine der größten Sicherheitslücken, die wir in dieser Diskussion nicht angemessen berücksichtigen, mit der digitalen Identität zu tun. Da Web3 und das Metaversum zu einem umfassenderen Internet, immersiveren Erfahrungen und zusätzlichen Berührungspunkten zwischen digitalen und physischen Oberflächen führen, wird unser Ansatz zur digitalen Identität entscheidend. Während das frühe Web ein hohes Maß an Anonymität ermöglichte und mehrere kontextabhängige Identitäten förderte (z. B. für Spiele, Handel, Blogging oder soziale Netzwerke), besteht im Web3 und im Metaverse die Gefahr, dass eine einzige digitale Identität (die fest an unsere rechtliche Identität gebunden ist) auf allen Oberflächen durchgesetzt wird. Dies könnte das Ende der Anonymität bedeuten, was auch die Vorstellung von digitalen öffentlichen Räumen bedrohen würde. Daher müssen wir die Anonymität schützen und dürfen nicht bei jeder digitalen Interaktion eine Identitätsebene für Menschen einführen (eine Alternative wäre, die Identität von Maschinen und Hardware zu verbessern).

9. Wie bewerten Sie die Positionierung der digitalen Zivilgesellschaft zum Thema Web 3.0 und Blockchain/DLT, die unter anderem auf großes Missbrauchspotenzial oder sozial und gesellschaftspolitisch zu kritisierende Folgen hinweisen (siehe z.B. Jürgen Geuter/"tante", Molly White mit dem Blog "Web3 is going just great"1, Brief von Kryptoexpert*innen an den US-Kongress2)? Haben Sie den Eindruck, dass die Politik die vorgebrachten Standpunkte entsprechend berücksichtigt?

Die Akteure der Zivilgesellschaft sind verständlicherweise besorgt über das Missbrauchspotenzial von Web3, Web 3.0 und Blockchain/DLT, da sie von ihrer Verbreitung nicht in demselben Maße profitieren wie die sie propagierenden privaten Akteure, und auch nicht mit den gleichen politischen Herausforderungen im Zusammenhang mit ihrer Einführung und Nutzung konfrontiert sind wie staatliche Akteure. Im Allgemeinen verfügen zivilgesellschaftliche Organisationen über ein großes institutionelles Wissen und Fachkenntnis; sie nehmen eine unabhängigere Haltung ein, auch weil sie keine kommerziellen oder politischen Anreize haben, und können die relativen Risiken und Chancen dieser Konzepte und Technologien objektiver bewerten. Des Weiteren können die Akteure der digitalen Zivilgesellschaft als Sachwalter und Schützer des digitalen öffentlichen Raums betrachtet werden, der zunehmend durch die Ausdehnung privat kontrollierter Räume in virtuelle Welten, erweiterte reale Räume und fiktive Metawelten bedroht ist.

Ich stimme weitgehend den Problemen und den Ansichten zu, die in den von Ihnen in dieser Frage zitierten Materialien geäußert werden, und schließe mich insbesondere den Bedenken an, die in dem Schreiben von Krypto-Experten an den US-Kongress geäußert wurden, wonach die Notwendigkeit besteht, gegen die Behauptungen der Akteure vorzugehen, die von Kryptowährungen, Web3 und Blockchain-Systemen profitieren wollen, und ihre Narrative zu hinterfragen. Ich stimme außerdem entschieden den Bedenken zu, die in dem Schreiben zu unbegründeten Datenschutzbehauptungen von Blockchain-Befürwortern geäußert werden, insbesondere, dass Datenschutzmechanismen dem grundlegenden Design der Technologie „entgegenstehen“.

Meiner Erfahrung nach berücksichtigen die politischen Entscheidungsträger jedoch nicht ausreichend die Ansichten und Bedenken der Zivilgesellschaft (und in den USA werden sie unverhältnismäßig stark durch die aggressive politische und wirtschaftliche Lobbyarbeit der Industrie beeinflusst). Es ist verständlich, dass die politischen Entscheidungsträger ebenso wie die Bürger über den Status quo frustriert sind und versuchen, die Mängel des bestehenden digitalen Ökosystems mit allen Mitteln zu beheben. Wir sind darauf programmiert, nach Alternativen zu suchen, und neigen dazu, das behauptete Potenzial und die Vorteile neuer Technologien anzuerkennen, selbst wenn es kaum Beweise dafür gibt. Das kann zu einem naiven Optimismus führen, der uns glauben lässt, dass die nächste Sache oder die nächste Iteration trotz ihrer zunehmenden Komplexität besser sein wird, wenn wir bestehende Herausforderungen nicht lösen konnten. Aber wir müssen diese Voreingenommenheit überwinden und bei der Bewertung und Beurteilung dieser Technologien einen evidenzbasierten Ansatz wählen.

10. 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?

Ich muss vorausschicken, dass ich keine Expertin für die Umweltauswirkungen dieser Technologien bin. Allerdings sind mir aktuell keine Anwendungsfälle bekannt, bei denen der Nutzen die Umweltkosten übersteigen würde. Aus gesellschaftspolitischer Sicht ist es wichtig, sich gegen die Art und Weise zu wehren, in der diese Technologien häufig als Technologien ohne ökologischen Fußabdruck oder materielle Auswirkungen dargestellt werden. So wie die Big-Tech-Branche Begriffe wie „KI“ und „Cloud“ genutzt hat, um von der Umweltbelastung durch diese Technologien abzulenken, verwenden auch die Befürworter von Kryptowährungen Begriffe wie „Ether“, „virtuelle Maschine von Ethereum“, „digitaler Zwilling“ und andere, um eine Art Immaterialität oder Nicht-Physikalität zu suggerieren. Die Realität ist, dass diese Technologien teuer, extraktiv und sehr materiell sind und große Auswirkungen auf die Umwelt haben, was bei jeder Entscheidung über ihren Einsatz oder ihre Eignung berücksichtigt werden muss.

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 ich in meiner Antwort auf Frage 1 festgestellt habe, gibt es keinen Konsens über die genaue Definition oder die Konturen des Metaversums, da es sich nicht auf eine einzelne Technologie oder eine bestimmte Kombination von Technologien bezieht. Vielmehr wird der Begriff von einer Vielzahl Akteuren in unterschiedlichen Bedeutungen verwendet.

Privatunternehmen neigen dazu, das Metaversum im Hinblick auf ihre eigenen kommerziellen Möglichkeiten zu definieren, d. h. für die neuen proprietären Angebote und erweiterten monetarisierbaren Oberflächen, die es durch virtuelle Räume und VR-gestützte Erfahrungen ermöglichen kann. Beispiele hierfür sind Horizon Worlds von Meta, ein VR-basiertes soziales Netzwerk und Horizon Workrooms, ein VR-basiertes Konferenzprodukt, sowie Microsoft Mesh für Microsoft Teams. Während private Unternehmen dazu neigen, sich getrennte, unabhängige Metaversen vorzustellen (d. h. Walled Gardens), stellen sich andere Akteure gelegentlich ein einheitlicheres, singuläres Metaversum vor, in dem sich Einzelpersonen virtuell durch verschiedene virtuelle Räume bewegen können.

Akademische Forscher und insbesondere Informatiker neigen dazu, das Metaversum in Bezug auf die damit verbundenen Technologien zu definieren, einschließlich Extended-Reality-Technologien (XR-