Grundkonzepte von Identität und digitaler Identität im Web3

Versuch der Systematisierung von Identitätsmanagement für den Zweck der Regulierung sowie eine Darstellung der Vorteile von Blockchain-basierten Web3-Lösungen anhand einiger Use Cases von KILT.

Text — Gustav Hemmelmayr

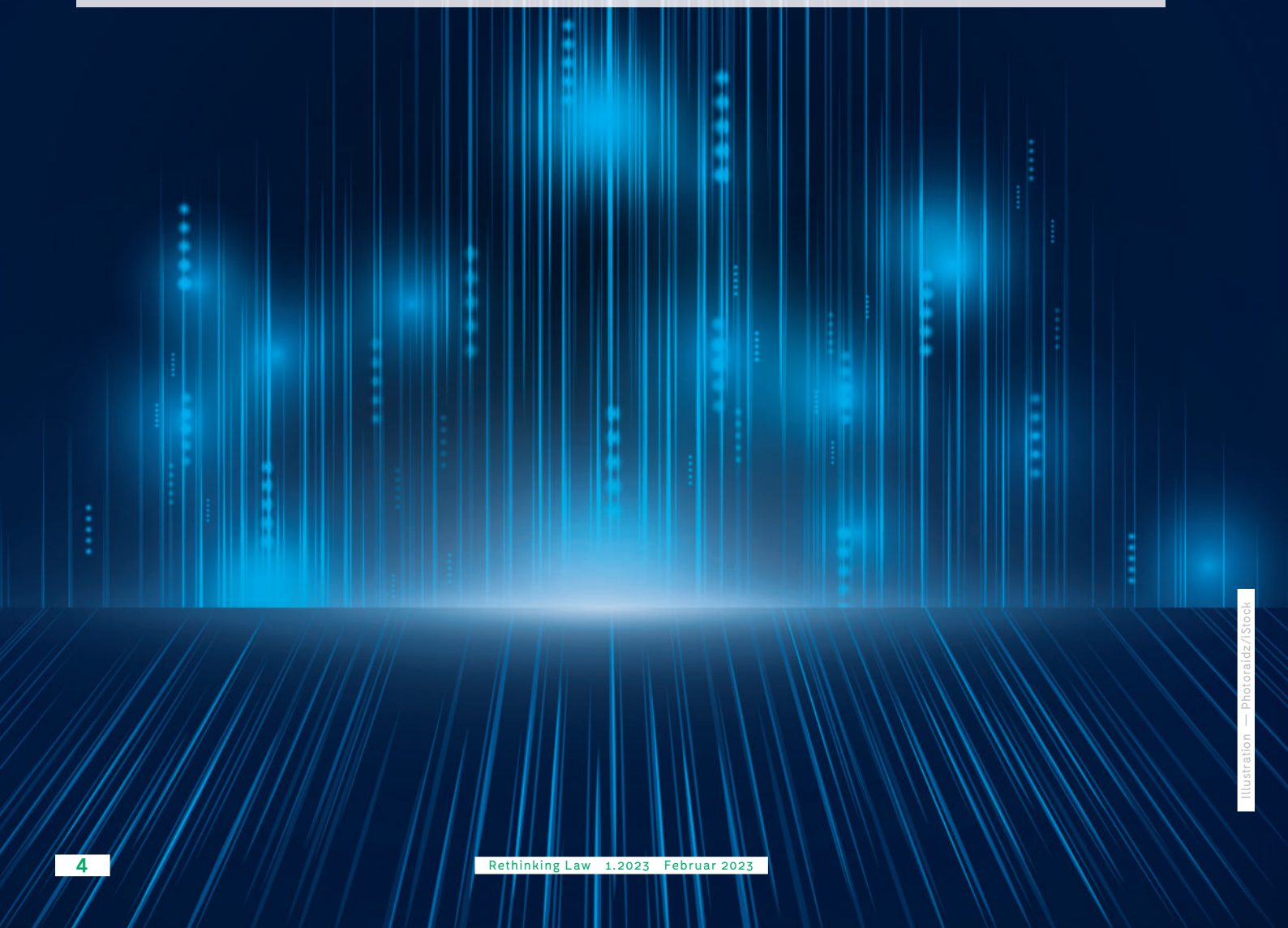

Illustration — Photoraidz/iStock

I. Offline-Identitäten und Ausweise

Identität und Identifier

In der realen Welt drück sich unsere Identität auf alle möglichen Arten und Weisen aus. Wir sind körperlich an einem Ort, können dort, wenn es ein öffentlicher Ort ist, gesehen werden.[1] Menschen erinnern sich aneinander, an das Gesicht, an die Augen, an Bewegungen, den Klang der Stimme, an Auffälligkeiten oder Unauffälligkeit, aber auch an Kleidung, Charakter, Gespräche und eine Vielzahl anderer individueller Merkmale einer Person. Oft weiß man, wo man jemanden getroffen hat, erinnert sich an die Situation, die Stimmung, an die Begleitung und das Umfeld einer Person, an ihre Aufgaben, Vorzüge, und dergleichen. Wir können so viele Details im Umgang miteinander aufnehmen und uns später daran erinnern.

Alle diese Dinge, die wir im Laufe der Zeit über eine Person lernen, machen das aus, was wir als die Identität dieser Person empfinden. Identität ist hier das Konzept, dass dies eine bestimmte Person ist.

Schon bei der Geburt werden an die Identität einer Person Daten geknüpft – es wird erfasst, wann und wo eine Person geboren ist, welchem Geschlecht diese Person angehört, welchen Familiennamen diese Person trägt und auf welchen Vornamen die Person hören soll. Diese Daten werden hoheitlich verwaltet und stellen die Grundlage für Personenstandsurkunden und Ausweise dar. Über die Jahre können sich manche dieser Daten ändern[2] und es kommen zahlreiche Daten dazu – das Erlernen von Fähigkeiten, das Absolvieren von Ausbildungen, die Änderung des Familienstandes, die Aufnahme oder Aufgabe von beruflichen Tätigkeiten oder anderen sozialen Aufgaben oder Rollen in Gemeinschaften. Der Datenpool wächst und wird in vielen Fällen begleitet von Zertifikaten und Dokumenten, die diese Daten bzw. ihre Änderungen belegen. Diese Daten sind Identifier, also Daten, die zu der unmittelbar erfahrbaren Identität einer Person zusätzliche Informationen geben.

Die Belege bzw. Credentials für diesen Daten sind Ausweise, Zeugnisse, Berechtigungsscheine, die von Stellen wie Verwaltungsbehörden, Schulen, Universitäten, Unternehmen und anderen Organisationen ausgestellt werden. Die zunächst privaten Daten aus dem Leben eines Menschen werden hoheitlich verwaltet und der Staat stellt dazu Ausweise zur Verfügung. Wenn jemand der ausstellenden Stelle vertraut, über ein Thema eine Aussage zu treffen, so vertraut man auch deren Nachweis.

Versucht man festzustellen, wer jemand ist, den man noch nicht kennt, kann man nicht auf eine komplexe Wahrnehmung einer Person zurückgreifen; man versucht daher, sich die Person durch Zuordnung eines Namens zu einem Gesicht zu merken, und hofft im besten Fall, sie das nächste Mal wiederzuerkennen. Man verknüpft also eine markante Ausprägung der Identität (Gesicht) mit einer Information (Namen). Wenn diese Person auch noch Credentials dafür hat, die belegen, dass ein bestimmter Name zu diesem Gesicht auch von einer Autorität überprüft wurde, so kann man, wenn man dieser Autorität traut, darauf vertrauen, dass auch andere und ggf. auch offizielle Stellen diese Person unter diesem Namen kennen.

Merkmale eines physischen Ausweises

Ausweise dienen als das Medium, mit dem wir nachweisen, wer wir sind. Die Identifizierung der jeweiligen Person wird anhand der biometrischen Daten vorgenommen – es wird das Gesicht mit dem Foto abgeglichen oder die Unterschrift auf dem Ausweis mit der auf einem Dokument. Diese Identifikatoren oder Kennzeichen sind Merkmale, die mit einer bestimmten Identität verknüpft sind und zur eindeutigen Identifizierung des tragenden Objekts oder Subjekts dienen können.[3]

Zur Überprüfung der Echtheit und Gültigkeit eines Personalausweises sind primär die physische Ausprägung des Ausweises vorhanden, die visuell oder mit maschineller Hilfe geprüft werden können.

1 Alle Aussagen sind private Ansichten des Autors. Er spricht dabei weder für erwähnte Unternehmen noch für sonstige Institutionen. Nichts in dieser Darlegung ist als Einladung oder Aufforderung zum Kauf von digitalen Vermögenswerten, Finanzinstrumenten oder Wertpapieren gedacht und dient auch nicht dazu, ebenso nicht als Rechts-, Anlage- oder Steuerberatung.

2 Auch die Änderung der Daten wird hoheitlich verwaltet und bedarf ggf. staatlicher Genehmigung. Die Regelungen dafür sind Teil eines gesellschaftlichen Aushandlungsprozesses, wie man derzeit anhand der Debatten um das Transsexuellen Gesetz beobachten kann. Mehr dazu hier von Seiten der Bundesregierung https://fmos.link/18947 oder hier von Jan Böhmermann aufgearbeitet: https://fmos.link/18948 (Abruf jew. 23.01.2023).

3 Mehr Informationen zu Identifikatoren: https://fmos.link/18949 (Abruf: 23.01.2023).

II. Zentralistische Ansätze des digitalen Identitätsmanagements

Identitätsmanagement in Web2

Grundlage für die Verwendung von Accounts oder anderen Online-Anwendungen in Web1- und Web2-Anwendungen ist die Überprüfung der digitalen Identität. Typischerweise wird eine Kombination aus Username/E-Mail-Adresse und Passwort abgefragt, die man bei einer erstmaligen Registrierung angelegt hat. Zusätzlich können in Web2 auch Anmeldedaten von bestehenden Accounts für neue Accounts verwendet werden (z.B. Facebook-Login). Allen diesen Anwendungen gemein ist, dass Zugangsdaten zentral verwaltet und überprüft werden. Die Betreiber der Seiten stellen also Mechanismen zur Verfügung, in denen die jeweiligen Daten eingegeben und anschließend zentral verifiziert werden. Stimmen die Anmeldedaten mit den anfangs hinterlegten Anmeldedaten überein, so öffnet sich die Anwendung und die Nutzer können diese direkt nutzen.

Diese zentrale Verwaltung von Zugangsdaten hat einige Vorteile, an die wir uns gewöhnt haben. Verliert oder vergisst man ein Passwort, gibt es einen Prozess, mit dem ein neues Passwort eingerichtet werden kann. Sie hat aber auch den Nachteil, dass die Verwendung von Mechanismen Dritter impliziert, dass dieser Dritte mitprotokolliert, wie Nutzer sich im Netz bewegen. Das erscheint praktisch, wenn man von einer App verständigt wird, dass jemand sich soeben von einem unbekannten Device eingeloggt hat, das heißt aber auch, dass wir gar nicht wissen, welche Verwendungs- und Bewegungsdaten unsere Apps über uns eigentlich speichern, wie lange sie diese vorhalten und wie sie diese monetarisieren. Darüber hinaus gibt es abseits der Interaktion der einzelnen Nutzer mit dem zentralen Unternehmen auch die Interaktion der Nutzer untereinander und die Kommunikation der Nutzer an die von ihnen gewählte Öffentlichkeit. Es gibt private Nachrichten, Gruppen, in denen man aktiv sein kann oder auch nur mitliest, Profile, auf denen Fotos, Texte und Links gepostet werden können, sowie Videotelefonie. Ähnlich divers wie in der realen Welt gibt es also allerlei wahrzunehmen. Es entsteht ggf. ein sehr komplexes und genaues Bild davon, wie eine Person ist und was ihre Identität ausmacht.

Forbes schreibt, dass sich das Problem ergibt, dass unsere Identität mit einer Vielzahl von Metadaten angereichert wird, die allein von den entsprechenden Unternehmen kontrolliert werden, ohne dass wir als Nutzer Mitsprache oder Kontrolle über diese immer detaillierter werdende Identität haben, die auf der anderen Seite von diesen Unternehmen wie eine Ware behandelt wird, die gekauft oder verkauft werden kann. Diese Identität ist damit weit mehr als nur die Anmeldedaten, die zur Verifizierung bzw. zum Einloggen verwendet werden, sondern eine Summe von Teilen, die Dinge umfasst wie das Gesicht einer Person, ihre persönliche Geschichte und wie sie sich selbst identifiziert. Damit kann ein echtes Profil einer Person erstellt werden, was insofern problematisch ist, als die Nutzer darüber keinerlei Verfügungsmacht haben.[4]

Identitätsmanagement in Regulierung

Regulierung, die als Reaktion auf das Ungleichgewicht zwischen Nutzern und Plattformbetreibern im Web2 entstanden ist, setzt ebenfalls an zentralistischen Konzepten an. So geht beispielsweise die DSGVO[5] so selbstverständlich von zentralen Verwaltern aus – „dem Verantwortlichen", der in Art. 4 Ziff. 7 DSGVO definiert ist als derjenige, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet –, dass Datenverarbeitung ohne einen Verantwortlichen nicht angedacht ist. Damit ist auch eine DSGVO-konforme Datenverarbeitung nur mit einem Verantwortlichen möglich. Dadurch droht in einem dezentralen System den Beteiligten z.B. Nodes, dass diese von der Regulierung als Verantwortliche mitgemeint sind, ohne dass diese in der tatsächlichen Durchführung ihrer Aufgaben wirklich über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.[6]

Aber auch die eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste[7] basiert weitgehend auf dem Gedanken, dass es eine zentrale Stelle gibt, die verantwortlich zeichnet, in diesem Fall die qualifizierten Ver-

4 Der diesbezügliche Forbes-Artikel findet sich unter dem Link: https://fmos.link/18950 (Abruf: 23.01.2023).

5 Datenschutzgrundverordnung im Volltext nachzulesen hier: https://fmos.link/18951 (Abruf: 23.01.2023).

6 Mehr zur Inkompatibilität von Blockchain und DSGVO hier: https://fmos.link/18952 (Abruf: 23.01.2023).

7 Informationen zur Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, kurz eIDAS-Verordnung, hier: https://fmos.link/11742 (Abruf: 23.01.2023).

trauensdiensteanbieter. So wird die elektronische Signatur beispielsweise in drei unterschiedliche Stufen – die einfache, die fortgeschrittene und qualifizierte elektronische Unterschrift – unterteilt und nur der qualifizierten elektronischen Signatur wird die gleiche Rechtswirkung zugesprochen wie der echten Unterschrift. Die qualifizierte elektronische Unterschrift ist aber an zahlreiche Bedingungen geknüpft, die nur mithilfe eines zentralen Diensteanbieters – dem qualifizierten Vertrauensdiensteanbieter – erfüllt werden können. Damit wird elektronischen Signaturen, die ohne Beteiligung eines Intermediärs – also eines Dritten, in dessen Prozessen diese Signatur von Nutzern erstellt wird, der aber auch die entsprechenden Dokumente, Zeitstempel etc. zentral vorhält – per se die Gleichwertigkeit abgesprochen. Auch hier gilt also die zentrale Verantwortung als das Element, das Vertrauen in einen Prozess erzeugen soll.

Das ist insbesondere deshalb kurios, da sowohl die Verwendung von Ausweisen als auch die Unterschrift in der realen Welt völlig dezentral vonstattengeht; Personen, die sich entschließen, sich auszuweisen, zücken ihr Dokument, ohne dass ein Dritter diesen Vorgang protokolliert oder auch nur darin involviert ist, und für eine rechtsgültige Unterschrift reichen ein handelsüblicher Stift und ein Blatt Papier.

Derzeit wird in eIDAS 2.0 an einer europäischen ID-Wallet[8] gearbeitet, in der es einheitliche Identitätsnachweise über eine europäische Wallet zur Verwaltung der eigenen Identität geben soll. Ziel ist es, eine einheitliche Wallet zu schaffen, die einerseits Credentials wie den europäischen Personalausweis und den digitalen Führerschein enthalten und andererseits Behörden und Banken, aber auch privaten, unregulierten Plattformen wie Facebook, Amazon und Google offenstehen soll. Die geplante Wallet stößt bei Datenschützern auf massive Bedenken, weil sie keine Schutzmaßnahmen gegen Missbrauch hinsichtlich Tracking, Profiling oder gezielter Werbung vorsieht. Dadurch kann die Werbung nicht nur auf bestimmte Nutzer zugeschnitten und an ihre jeweilige Identität gekoppelt, sondern auch ermittelt werden, wem welche Werbung angezeigt wurde und wie effektiv diese ist. Datenschutzexperten fordern angesichts der breiten Verwendung der Wallet, dass kurzfristig notwendige Daten nur für einen zeitlich begrenzten Zeitraum zu speichern und dann zu löschen sind.

Die geplante Wallet stößt bei Datenschützern auf massive Bedenken, weil sie keine Schutzmaßnahmen gegen Missbrauch hinsichtlich Tracking, Profiling oder gezielter Werbung vorsieht.

Laut epicenter.work[9] [10] wurden die Probleme bisher nicht behoben und der notwendige Schutz für die Privatsphäre nicht eingezogen und es droht somit eine panoptische Sicht auf alle Lebensbereiche sowie die Beförderung von kriminellem Missbrauch, sodass für sensible Gesundheits-, Finanz- und Identitätsdaten aller Europäer ein gefährliches und unkontrollierbares Umfeld geschaffen wird.

Ein weiterer Punkt und ein Kernelement der geplanten Wallet ist Identifizierung der Nutzer

8 Mehr zur Wallet-App aus eIDAS 2.0, sowie der Kritik daran hier: https://fmos.link/18953 (Abruf: 23.01.2023).

9 A.a.O. (Fn. 7).

10 Epicenter.works: eIDAS 2.0 – Beispiellose Risken für die Privatsphäre: https://fmos.link/18954 (Abruf: 23.01.2023).

durch Offenlegung ihres rechtlichen Namens gegenüber Dritten, die gem. Art 11a der neuen eIDAS-Verordnung die Mitgliedstaaten verpflichtet, jeder Person eine eindeutige alphanumerische Zeichenfolge zuzuordnen, die diese ihr Leben lang zur Identifikation begleitet. Gleichzeitig sollen Mitgliedstaaten verpflichtet werden, organisatorische und technische Maßnahmen zu ergreifen, um einen hohen Datenschutz zu gewährleisten und die Gefahr der Profilerstellung zu verhindern. Laut epicenter.work können die Mitgliedstaaten diese Verpflichtung nicht erfüllen, weil die dauerhafte Kennung es von Natur aus ermöglicht, Nutzerverhalten über Interaktionen hinweg zu verfolgen.[11]

III. Verwendung eines realen Ausweises im Vergleich zu digitalen Identitäten in Web2

Der Personalausweis wird von staatlicher Stelle ausgestellt und wird der jeweiligen Person physisch übergeben. In der Folge kann sich die Person mit diesem Ausweis zu jedem Zweck legitimieren. Der Ausweis bleibt zu diesem Zweck immer bei der Person, die diesen ggf. vorzeigt.

Beim Vorzeigen vollziehen sich drei Stufen der Überprüfung – die Identität, also ob Ausweis und Person zusammenpassen, die Echtheit, also ob es sich tatsächlich um einen echten und unverfälschten Personalausweis des jeweiligen Staates handelt und die zu prüfenden Informationen, also: handelt es sich tatsächlich um eine Person des verlangten Alters oder hat diese Person tatsächlich diesen Namen.

Die Verwendung des Ausweises wird der ausstellenden Stelle nicht gemeldet und da es sich um ein physisches, „dummes" Dokument handelt, wird die Verwendung auch auf dem Ausweis nicht angezeigt oder gespeichert.

Im Gegensatz dazu wird im Web2 potenziell jeder Schritt technisch aufgezeichnet. Es ist nicht öffentlich bekannt, was genau aufgezeichnet wird, wie diese Aufzeichnungen mit anderen Daten zusammengelesen werden, wie diese kommerzialisiert oder weitergegeben und auch nicht, ob und wann sie wieder gelöscht werden.

Nun zielt beispielsweise die oben erwähnte DSGVO ja genau darauf ab, den Nutzern Auskunftsrechte, Löschungsrechte etc. einzuräumen. Die Rechtsverfolgung gestaltet sich jedoch schwierig und nur selten bemerken Verbraucher Verstöße und können erfolgreich dagegen vorgehen.[12] [13]

IV. Vorteile von Web3-Lösungen

Im Folgenden sollen Kernelemente des Web3 dargestellt werden,[14] um deren Vorteile im Vergleich zum Web2 aufzuzeigen.

Eigentum an Daten

Die Dezentralisierung legt die Kontrolle in die Hände der Nutzer und beendet oder schwächt damit das Monopol von Web2-Unternehmen. Die Nutzer können selbst entscheiden, ob sie ihre Daten mit anderen teilen oder ob sie sie lieber für sich behalten wollen.

Datensicherheit

Daten, die in einer riesigen zentralisierten Datenbank gespeichert sind, sind per se unsicher, weil Hacker nur ein einziges System knacken müssen, um an wertvolle Benutzerdaten zu gelangen. Oft spielen Insider eine Rolle bei der Weitergabe von Schlüsselinformationen an externe böswillige Akteure. Dezentrale Systeme sind so konzipiert, dass sie gegen ein solches Verhalten eines Teils der Teilnehmer resistent sind.

Ungerechtfertigte Zensur

Zentralisierte Systeme setzen ihre Benutzer oft einer ungerechtfertigten Zensur aus. Durch die Dezentralisierung wird die Autorität auf die Teilnehmer übertragen, sodass es für ein einzelnes Unternehmen schwierig ist, Nachrichten zu beeinflussen.

Transparenz des Systems

Transparenz ist ein fester Bestandteil des Designs dezentraler Ökosysteme. Die Nodes arbeiten zusammen, um das reibungslose Funktionieren des Systems selbst zu gewährleisten, und kein einzelner Node kann eine Entscheidung isoliert treffen. Teilnehmer können sich bei der Entscheidungsfindung einbringen, indem sie an der Governance teilnehmen.

11 Mehr dazu im hier abrufbaren Dokument eIDAS Policy Analysis des epicenter.works vom 2 Februar 2022, https://fmos.link/18955, und in der aktuelleren Stellungnahme hier: https://fmos.link/18956 (jew. Abruf: 23.01.2023), Zitat übersetzt aus dem Englischen.

12 Max Schrems und seine Klagen gegen Facebook im Überblick hier: https://fmos.link/18957 (Abruf: 23.01.2023).

13 Abzurufen hier: https://fmos.link/18958 (Abruf: 23.01.2023).

14 Dieser Vergleich beruht weitgehend auf diesem Artikel in gekürzter Form: https://fmos.link/18959 (Abruf: 23.01.2023).

Transparenz der Algorithmen

Alle Algorithmen sind öffentlich einsehbar, sodass man sich nicht auf die Behauptungen eines Unternehmens verlassen muss, sondern unmittelbar überprüfen kann, ob der Code macht, was versprochen wurde.

V. Standardisierte Definition digitaler Identität für die Zwecke der Erstellung von digitalen Ausweisen

Das W3C – das World Wide Web Consortium, das Gremium zur Standardisierung der Techniken im World Wide Web, das beispielsweise HTML standardisiert hat – definiert als Identität einen Satz von Informationen zur Identifizierung einer bestimmten Entität. Entitäten sind dabei alles, was eine eindeutige Identität hat, z. B. eine Person, eine Organisation, ein Konzept oder ein Gerät. Um diese unsere Identität nachzuweisen, werden in Regel Ausweise, Berechtigungsnachweise oder Behauptungen anderer über die Identität verwendet.[15]

Mitte letzten Jahres hat die W3C schließlich Decentralized Identifiers (DIDs)[16] standardisiert. Im Abstract dazu heißt es, dass dezentralisierte Identifikatoren (DIDs) eine neue Art von Identifikatoren sind, die eine überprüfbare, dezentralisierte digitale Identität ermöglichen. Im Gegensatz zu typischen föderierten Identifikatoren wurden DIDs so konzipiert, dass sie von zentralisierten Registern, Identitätsanbietern und Zertifizierungsstellen entkoppelt werden können. Das Design ermöglicht dem Besitzer einer DID, die Kontrolle über die DID ohne Involvierung Dritter nachzuweisen.[17]

Damit kommt ein völlig neuartiges Konzept aufs Tableau, das auf den Ideen des Web3 basiert und in seinen Zielen[18] die Eliminierung der Notwendigkeit von zentralen Verantwortlichen und den damit verbundenen Schwachstellen anstrebt. Die Kontrolle über alle Daten samt der Verfügung über deren Privatheit wird damit jeweils an die einzelnen Entitäten selbst gegeben. Dabei sollen diese Systeme über genug Sicherheit verfügen, dass man sich auf die DID-Dokumente verlassen kann, unter anderem indem die DID eine Verifikation direkt über kryptographische Beweise ermöglicht. Zusätzlich sollen mit der Standardisierung interoperable Systeme entstehen und digitale Identifier von einem ins andere System mitgenommen werden können. Das alles soll möglichst einfach verstehbar, implantierbar und verwendbar sein sowie erweiterbar, sofern dies die Interoperabilität, die Übertragbarkeit oder die Einfachheit nicht stark beeinträchtigt.

VI. Beispiel: KILT Protocol, KILT DIDs und einige Identity-Lösungen

Das KILT Protocol[19] ist ein Blockchain-Identitätsprotokoll für die Ausstellung von selbstsouveränen, überprüfbaren Berechtigungsnachweisen und dezentralen Identifikatoren. Die Blockchain ist öffentlich einsehbar, ebenso der zugrunde liegende Code; die Nutzung steht jedem frei; es sind – ähnlich wie bei der Bitcoin- oder der Ethereum-Blockchain – nur die Gebühren für Transaktionen zu bezahlen. Auch die Verwendung des Protocols für eigene Anwendungen steht sowohl für kommerzielle als auch nichtkommerzielle Projekte offen. Die Blockchain ging im Polkadot-Ökosystem 2021 live und ist dort eine Parachain, die ihre Sicherheit von der Relaychain bekommt.

Grundgedanke bei allen Anwendungen basierend auf dem KILT Protocol ist, dass die Nutzer selbst die alleinige Hoheit über ihre Daten und ihre daraus generierte Identität haben. Dafür werden die Daten und Credentials, die sich direkt auf die Person der Nutzer beziehen, lokal auf dem Device der jeweiligen Nutzer generiert, gespeichert und auch nur mit Zustimmung der Nutzer ganz oder teilweise Dritten zur Verfügung gestellt – ähnlich, wie das mit Ausweisen in der realen Welt funktioniert.

Zur Überprüfung der Credentials in der Wallet der Nutzer, sind im Credential Daten referenziert, die sich auf der Blockchain finden lassen. Dafür werden die Daten des Credentials in eine alphanumerische Folge umgewandelt, die ohne das Credential keine Bedeutung hat und daher auch öffentlich in der Blockchain verankert werden kann.

15 Ebd.

16 Die vollständige W3C Recommendation vom 19.07.2022 abrufbar unter https://fmos.link/18960 (Abruf: 23.01.2023).

17 ebd, Übersetzung des Autors.

18 Ziele der Decentralized Identifiers und Verifiable Credentials s. URL a.a.O. (Fn. 15).

19 Website von KILT Protocol mit mehr Hintergrundinformationen: https://www.kilt.io/ (Abruf: 23.01.2023).

> **Niemand kann in die Abläufe eingreifen, diese kontrollieren oder Informationen sammeln.**

Die Credentials sind für ein Dreiecksverhältnis gedacht – es gibt einen Nutzer, der ein Credential ausgestellt bekommen möchte (Claimer), einen Attester, typischerweise ein Unternehmen oder ein automatischer Check über das Vorliegen der zu bestätigenden Eigenschaft, und einen Verifier, also jemanden, der kontrolliert, ob der Nutzer eine bestimmte Eigenschaft nachweisen kann. Die Technologie ist dabei die Ausstellungsmethode des Credentials – eine Software, die fälschungssicher und vor dem Zugriff Dirtter geschützt jene Inhalte vorhält, die Claimer und Attester in dem Credential festgehalten haben. Als Identifier für diese Credentials dient die KILT DID, eine DID nach der Standardisierung der W3C, die für jede Identität eines Nutzers erstellt werden kann.

Im Gegensatz zu Web2-Lösungen und dem zentralistischen Konzept, das die bisherigen Regulierungen vor Augen hatten, gibt es keine zentral gesteuerten Prozesse und keine Anhäufung von Daten. Stattdessen werden die Vorteile von Dezentralität genutzt. Niemand kann in die Abläufe eingreifen, diese kontrollieren oder Informationen sammeln. Stattdessen wird auf Privacy-by-design gesetzt, die Anwendungen werden also technisch so konzipiert, dass letztlich alle Informationen und Daten alleine bei denen verbleiben, denen sie gehören – den Nutzern selbst.

Sporran-Wallet – Wallet im Web3

Die Sporran-Wallet[20] kann wie viele andere Wallets für Transaktionen von Kryptowährung verwendet werden – in diesem Fall von KILT Coins, der nativen Währung des KILT Protocols. Darüber hinaus kann man den Sporran zum Speichern von DIDs und Credentials verwenden, um eine digitale Identität zu erstellen – ähnlich wie in der realen Welt in physischen Brieftaschen Geld und Ausweise verwahrt werden.

Im Sporran ist es nicht nur möglich, eine, sondern mehrere Identitäten zu erstellen – zum Beispiel eine Arbeitsidentität mit allen relevanten Qualifikationen, eine Gaming-Identität mit allen Rankings oder andere Credentials für weitere digitale Lebensbereiche. Sporran bietet eine Möglichkeit zur Verwaltung und Unterzeichnung von Transaktionen mit diesen digitalen Identitäten auf der KILT Blockchain. Dies ist die Basis, um Nutzern die Kontrolle über ihre eigenen Daten zurückzugeben.

Für jede dieser Identitäten wird jeweils eine unterschiedliche KILT-DID erstellt, die in der digitalen Interaktion als eindeutiger Identifier genutzt wird – ähnlich wie das Gesicht oder der Fingerabdruck in der realen Welt. Anders als in der eIADAS 2.0 können Nutzer für jede ihrer Identitäten eine andere KILT-DIDs erstellen, sodass sie beliebig viele für unterschiedliche Zwecke oder in anderen Zeitabschnitten halten können. Durch die Vielzahl an möglichen Identitäten und Identifiern können verschiedene Lebensbereiche oder -abschnitte getrennt gehalten werden und kompromittierte Identitäten durch neue ersetzt werden. Damit haben Nutzer die Möglichkeit, sich aktiv gegen Tracking zu wehren.

Die Wallet basiert auf Kryptografie, jede Identität kann mit einem eigens erstellten Passwort zur Bestätigung von Transaktionen verwendet und, basierend auf einer Seed-Phrase von zwölf Worten, jederzeit wiederhergestellt werden. Nur der Nutzer selbst hat Zugriff auf die Daten und das Vermögen, die über die Wallet verwaltet werden. Wenn Passwort oder Seed-Phrase geknackt werden, sollten Vermögen und Credentials in eine neue Identity umziehen.

20 Mehr Info zum Sporran hier https://fmos.link/18961 (Abruf: 23.01.2023) und die Software verfügbar als Browser-Extension hier: https://www.sporran.org/ (jew. Abruf: 23.01.2023).

SocialKYC – digitale Ausweise im Web3

Die Idee hinter SocialKYC[21] ist, dass quasi jeder bereits digitale Identitäten hat, unter denen man bekannt ist, die man öffentlich nutzt, um sich auszutauschen, um die Arbeit, Interessen oder das eigene Leben darzustellen. Dadurch entstehen reale private und geschäftliche Beziehungen und werden bestehende Beziehungen gepflegt. Folgerichtig sollten Nutzer die Möglichkeit haben, nachzuweisen, dass sie diejenige Person sind, die diese digitalen Identitäten betreibt, ohne dafür die Daten aus der realen Welt über Web2 zu verknüpfen.

Um diesem Gedanken gerecht zu werden, lassen sich mit SocialKYC dezentrale Credentials über soziale Anknüpfungspunkte einer Person erstellen. Ähnlich wie in der realen Welt schafft es mehr Vertrauen, dass es sich um dieselbe Person handelt, wenn es mehrere unterschiedliche Anknüpfungspunkte gibt. Nutzer können sich für ihre E-Mail-Adresse und ihre Social Media Accounts auf Twitter, Discord, GitHub, Twitch und Telegram, bzw. derzeit in Beta für ihren YouTube-Kanal, Credentials erstellen.

Für ein Credential über einen Account müssen die Claimer der SocialKYC-Software nachweisen, dass sie Zugriff auf diesen Account hat. Dies passiert beispielsweise durch einen öffentlichen Post auf dem Profil, zu dem die Software den Claimer auffordert und der sich automatisch überprüfen lässt. Sobald das nachgewiesen ist, bestätigt SocialKYC das Credential und postet eine Referenz zu diesem Credential auf der KILT Blockchain.

Das Credential liegt dann in der Wallet des Nutzers und dieser verfügt allein darüber. Möchte sie sich damit ausweisen, kann ein Verifier das Credential mithilfe der Referenz auf der Blockchain überprüfen; wobei die Referenz für Dritte, die über das Credential nicht verfügen, unlesbar bleibt.

SocialKYC selbst speichert, teilt oder verkauft keine Daten und vergisst den gesamten Vorgang, sobald das Credential bestätigt wurde. Für skeptische Menschen mit guten Fähigkeiten oder auch Datenschutzexperten und -organisationen liegt der gesamte Code von SocialKYC öffentlich auf GitHub, sodass man den beschriebenen Prozessen nicht glauben muss, sondern diese auch direkt überprüfen kann.

DIDsign – Signatur im Web3

Mit DIDsign[22] können Dateien mit dem Sporran signiert werden. Voraussetzung dafür ist, dass die Nutzer über eine KILT-Adresse mit einer KILT-DID verfügen. Dann geht sie einfach auf die DIDsign-Website und kann direkt in ihrem Browser die DIDsign-Software nutzen, um ihre Datei zu signieren, optional auch mit einem ergänzenden Credential oder unter gleichzeitiger Setzung eines Timestamps in der KILT Blockchain.

Im Gegensatz zu zentralisierten Diensten, die ebenfalls digitale Signaturen anbieten, werden bei DIDsign keine Daten gespeichert. Der Nutzer signiert und speichert die Dateien lokal auf seinem persönlichen Gerät (Laptop oder Mobiltelefon) ohne externen Server. Die Datei wird dabei lediglich in den Browser am eigenen Gerät geladen. Dort erfolgt die Signatur. Die daraus generierte signierte Datei kann am Gerät gespeichert werden, und sobald der Browser geschlossen ist, sind die Daten auch im Browser nicht mehr vorhanden, ohne dass die Daten jemals das Gerät verlassen haben.

Dient die Signatur der Datei als Beleg, so kann die Datei zu diesem Zweck einer anderen Person übergeben werden – beispielsweise per E-mail, per Übergabe auf einem Stick – und die andere Person kann überprüfen, ob diese Datei tatsächlich von der genannten Adresse signiert wurde und ggf. welche Credentials und welcher Timestamp in der Signatur hinterlegt sind. Dafür muss man die signierte Datei bloß in den Verify-Teil von DIDsign ziehen. Die Software überprüft die Signatur und die Unverfälschtheit der Daten wiederum direkt im Browser, ohne dass irgendwelche Daten irgendwohin übermittelt werden. Die andere Person kann ggf. auch die signierte Datei gegenzeichnen, indem sie diese ebenfalls mit ihrer Wallet signiert.

Diese Art von Signatur findet nicht nur auf Verträge Anwendung, sondern kann auch sonst

21 Zugang zum SocialKYC Service hier: https://socialkyc.io/ (Abruf: 23.01.2023).

22 Informationen zu DIDsign hier: https://fmos.link/18962 und hier https://fmos.link/18963, DIDsign zum selber ausprobieren hier: https://didsign.io/ (jew. Abruf: 23.01.2023).

als Beleg für die Authentizität von Video- oder Audiodateien, für den Beweis des Forschungsstandes, für den Nachweis über die Unverfälschtheit einer Software oder einen gesundheitlichen Zustand dienen. Der Fantasie der Anwendungsfälle sind hier keine Grenzen gesetzt. Da die Software weder irgendwelche Daten speichert noch verarbeitet, kann jegliches Datenformat signiert werden.

Dies bietet eine sichere und private Möglichkeit, Dateien dezentral zu signieren und empfangene Signaturen sowie die Unverfälschtheit von Dateien zu überprüfen.

VII. Ausblick

Auch wenn sich in den letzten 15 Jahren einiges getan hat, beginnt die generelle Umstrukturierung unserer digitalen Welt gerade erst. Wir sehen zwar immer klarer, in welche Richtung die Reise gehen könnte, viele Entwicklungen und Anwendungsmöglichkeiten werden wir aber erst in der nächsten Dekade finden. Im Mainstream sind rund um die letzten beiden Hype-Phasen Kryptowährungen als Investment und Spekulationsobjekt angekommen. Die anderen Nutzungsmöglichkeiten von Blockchain und Web3 sind den meisten noch weniger bewusst.

Laut dem Technology-Report von Bain & Company[23] wird eines der wichtigsten Themen des Web3 das Konzept der digitalen Identität sein. Demnach wird erwartet, dass digitale Web3-Wallets eine große Rolle spielen werden, wenn Unternehmen – nämlich Web2- und Web3-Unternehmen – darum konkurrieren, die Zukunft der Online-Identität zu gestalten. Denn die Web3-Wallets haben das Potenzial, die Art und Weise zu verändern, wie sich Nutzer mit Anwendungen verbinden, indem sie universelle Anmeldefunktionen bieten. Was bisher eine website-spezifische Anmeldung war, könnte bald nur noch die Auswahl von „connect wallet" erfordern. Viele Befürworter von Web3 hoffen, dass dieser neue Ansatz es dem Nutzer ermöglichen wird, mehr von ihren Daten und digitalen Gütern direkt zu besitzen, zu kontrollieren und zu monetarisieren, ohne dass Unternehmen unerwünschten Zugriff auf diese Daten oder Güter haben.

Use-Cases für Web3-Anwendungen im Identitätsbereich

Laut Verdict[24] werden, wenn sich Web3 durchsetzt und in der Web2-Welt Fuß fassen kann, DIDs ein wichtiger Eckpfeiler sein, um die Eintrittsbarriere zu senken. Blockchain-basierte Identitätssysteme werden das Tor zu nutzerorientierten Anwendungen im dezentralen Web3-Bereich sein. Use-Cases für Web3-basierte Identitäten sind laut Socialmediaexaminator[25] umfassend und weitreichend.

Beispielsweise werden die digitalen Identitäten aus den bestehenden Web2-Anwendungen übertragbar auf andere digitale Räume. Auch der Datenschutz im eCommerce-Bereich wird gefestigt, weil Nutzer direkt mit ihren Wallets einzelne Daten zur Verwendung freischalten können, ohne potenziell den Zugriff zu ganzen Profilen freizugeben. Im Gesundheitswesen können Daten auf Wallets gehalten werden, die allein mit Zustimmung der Nutzer weitergegeben werden, sodass bei jedem Arztbesuch alle potenziell hilfreichen Daten vorhanden sind, ohne diese sensiblen Informationen zu gefährden. Im Bildungsbereich können zu den Zeugnissen in Papierform digitale Credentials ausgestellt werden, die über die Wallet abgerufen, aber auch durch einen potenziellen Arbeitgeber direkt auf ihre Richtigkeit und Unverfälschtheit geprüft werden können.

Regulierung im Identitätsmanagement

Wie kann man nun dazu kommen, dass Regulierung de lege ferenda und die Chancen des Web3 miteinander verwoben und Nutzern die Hoheit über ihre Identität auch in der digitalen Welt zurückgegeben wird. Einige Punkte, an denen man ansetzen könnte:

Mindset und Voraussetzungen: Als erstes und am dringendsten braucht es mehr Web3-Kompetenz bei Verwaltung und Politik. Die Idee einer Anhörung im Bundestag zu Blockchain, im Jahr 2018[26] und die kürzlich stattgefundene Anhörung zu Web3 und Metaverse[27] sind erste Ansätze, dass Politik bzw. politische Institutionen sich öffentlich mit Sachverständigen zum Web3 aus-

23 Technology Report von Bain & Company hier: https://fmos.link/18964 (Abruf: 23.01.2023).

24 Zum Verdict-Artikel https://fmos.link/18965 (Abruf: 23.01.2023).

25 Hier: https://fmos.link/18966 (Abruf: 23.01.2023).

26 Die offiziellen Dokumente zur Anhörung „Blockchain" im Bundestag hier: https://fmos.link/18967 (Abruf: 23.01.2023).

27 Die offiziellen Dokumente zur Anhörung „Web3 und Metaverse" im Bundestag hier https://fmos.link/18968 (Abruf: 23.01.2023).

tauschen. Insbesondere die Anhörung 2022 sorgte allerdings schon im Vorfeld für Kritik[28] und alternative Stellungnahmen von nicht eingeladenen Sachverständigen.[29] In der Anhörung selbst wurde ein düsteres Bild[30] der technologischen Entwicklungen gezeichnet. Tatsächlich ist es wichtig, die Gefahren von neuen Technologien zu verstehen, um mit diesen richtig umgehen zu können. Allerdings stellt sich schon die Frage, ob die Anhörung in dieser Form dem Thema und der politischen Auseinandersetzung an sich dienlich war.[31]

Fakt ist jedenfalls, dass das Web3 gekommen ist, um zu bleiben. Die politische Entscheidung kann also nicht einfach dafür oder dagegen sein. Es ist an der Zeit, dass Politik und auch Verwaltung die immanenten Grundkonzepte von Web3 – wie Öffentlichkeit, Dezentralität, Datenhoheit, Erlaubnisfreiheit (bezogen auf die Teilnahme, nicht wertpapierrechtlich) – verstehen. Erst, wenn man diese Grundkonzepte durchdrungen hat, kann man über die Chancen und Gefahren diskutieren und sich damit auseinandersetzten, wie man sich als Staat, als Politik und als Verantwortlicher dazu verhält. Denn je mehr technisches und konzeptionelles Verständnis aufgebaut wird, desto mehr kann man self-sovereign Meinungen entwickeln, Ideen haben und letztlich Entscheidungen treffen.

Das Know-how dazu gibt es praktischerweise schon direkt in Deutschland. Berlin ist ein weltweiter Blockchain-Hotspot.[32] Es gibt in Deutschland Studiengänge zu Blockchain[33] und an denselben Universitäten Gratiskurse wie die Blockchain Autumn School und das Web3-Talents-Programm,[34] aus denen kontinuierlich Web3- und Blockchainexperten in die Welt verabschiedet werden.

Nur wenn dieses Know-how sich auch in öffentlichen Einrichtungen verbreitet, können wir in Deutschland darauf hoffen, dass Regulierung nicht mehr nur als untauglicher Versuch der Verhinderung einer weltweit stattfindenden technologischen Umwälzung, sondern als Ergebnis eines wirklichen politischen Diskurses entsteht, in dem das Augenmerk darauf liegt, wie wir als Gesellschaft diese Technologien nutzen wollen und wie wir auch in diesen Technologien unsere demokratischen Grundwerte, den Schutz der Verbraucher und deren Privatsphäre fördern und zugleich Diskriminierung oder Betrügereien verhindern.

Institutionalisierung von Web3 in Deutschland: Um in weiterer Folge dezentrale Strukturen als zumindest gleichwertige Technologien neben zentralistisch organisierten Technologien zu etablieren, ohne es dabei Verbrauchern selbst zu überlassen festzustellen, welcher Software man vertrauen kann, könnte man sich Institutionen vorstellen, die technologische Rechtssicherheit bieten – die also verlässliche Aussagen treffen können, ob beispielsweise eine Software das tut, was sie sagt, dass sie tut, oder auch bestimmte Software für bestimmte Zecke zertifizieren kann. Der Aufbau solcher technologischer Strukturen könnte neu institutionalisiert werden oder es könnten bestehende Strukturen für solche Zwecke ausgebaut werden.

Privacy-by-Design & Verbraucherschutz: Zusätzlich könnte man die Einrichtung von Verbraucherschutzorganisationen in Betracht ziehen, die Privacy-by-Design-Ansätze nicht nur auf ihre Validität prüfen können, sondern Verbrauchern auch für Fragen rund um technische Themen zur Verfügung stehen, Schulungen anbieten oder Ähnliches.

Inklusion von bestehenden Gruppierungen: Zusätzlich könnten bestehende Strukturen, die sich bereits in der Vergangenheit um Datenschutz oder Verbraucherschutz gekümmert haben, die Behörden bei der Prüfung und Zertifizierung von Software unterstützen. Gruppierungen könnten Gutachten abgeben, Kritikpunkte vorbringen und an der Verbesserung monierter Punkte mitarbeiten oder Schulungen erarbeiten, um den Umgang mit neuen Technologien besser bekannt zu machen.

Europäische Regulierung von Zielen statt Abläufen: Die deutsche Politik könnte das in Deutschland umfangreich vorhandene Wissen über Datenschutz und self-sovereign Identity-by-Design nutzen, um in europäischen Regulierungen eine Gleichstellung von dezentralen Lösungen mit den alten zentralis-

28 https://fmos.link/18969 (Abruf: 23.01.2023).
29 Hier die Stellungnahme des Blockchain Bundesverbands zu den Fragen für die Anhörung „Web3 und Metaverse" im Bundestag https://fmos.link/18970 (Abruf: 23.01.2023).
30 Hier ein Blog zur Stimmung in der Anhörung: https://fmos.link/18971 (Abruf: 23.01.2023).
31 Kritikpunkte waren etwa die zugrunde liegenden Fragen an sich, der Ablauf mit relativ kurzen Stellungnahmen von Sachverständigen und auch die Auswahl der Sachverständigen
32 Bericht über Berlin als Blockchain-Hotspot hier: https://fmos.link/18972 (Abruf: 23.01.2023).
33 Studiengänge zu Blockchain: https://fmos.link/18973 und https://fmos.link/18974 (jew. Abruf: 23.01.2023).
34 Blockchain Autumn School https://fmos.link/18975 und Web3-Talents https://web3-talents.io/ (jew. Abruf: 23.01.2023).

> **Im Web3 wird wieder Augenhöhe zwischen Unternehmen und Nutzern geschaffen, indem Datenschutz direkt mit der Technologie hergestellt wird.**

tischen Standards zu erwirken bzw. auf lange Sicht zu einer Umstellung der Regulierung beizutragen. Anstelle der zentralen Verantwortlichen sollten Ziele festgesetzt werden, die von einer Technologie erreicht werden müssen, damit eine dezentrale Lösung als gleichwertig anerkannt wird.

Verpflichtung zu Interoperabilität: Für die bestehenden Web2-Monopole genauso wie für neue Lösungen könnte man eine Verpflichtung zur Interoperabilität durch Verwendung von Standards wie dem DID Standard normieren, sodass die Voraussetzungen für Monopolbildungen minimiert werden.

Zusammenfassung

Das bestehende System von Web2-Anwendungen ist insbesondere in Bezug auf fehlende Kontrolle der Nutzer über ihre eigenen Daten höchst unbefriedigend. Auch ist die Tatsache, dass einige Unternehmen quasi weltweit monopolistische Züge aufweisen und deren Web2-Plattformen mit den Daten und Informationen ihrer Nutzer finanzieren, mit den demokratischen Grundwerten der europäischen Union nicht vereinbar.

Diesem Missstand haben bestehende Regulierungen versucht beizukommen, indem diesen – und allen anderen – Unternehmen ein verantwortungsvoller Umgang mit den Daten und Informationen vorgeschrieben wurde. Insbesondere aufgrund der Intransparenz dieser monopolistischen Unternehmen und der hinter den Plattformen stehenden Algorithmen stellt sich Datenschutz im Web2 aber bisher als ein aussichtsloser Kampf dar.

Im Web3 wird im Gegensatz dazu wieder Augenhöhe zwischen Unternehmen und Nutzern geschaffen, indem Datenschutz direkt mit der Technologie hergestellt wird. Dabei wird den Nutzern die Kontrolle über ihre eigenen Daten zurück in die Hände gelegt. Um das zu erreichen können digitale Identitäten basierend auf DIDs und verifizierbaren, digitalen Ausweisen direkt über die eigene Wallet erstellt, verwendet und vor dem Zugriff Dritter geschützt werden.

Die Methode, mit der eIDAS2.0-Verordnung ebenfalls eine Wallet samt einem staatlichen Personenkennzeichen vorzuschreiben und dafür wieder zentrale Stellen als Verantwortliche zu etablieren, ist ein untauglicher Versuch, die Elemente von zentraler Infrastruktur mit Komponenten auszustatten, die dem Web3 nachempfunden sind, ohne dass diese tatsächlich über die Vorteile des Web3 verfügen.

In der Politik und der Verwaltung wäre es schön, würde das Bewusstsein für Web3 wachsen, um diesbezüglich sinnvolle Regelungen schaffen zu können. Dafür sollte in den Institutionen Web3-Kompetenz aufgebaut werden, um informierte und kluge Entscheidungen treffen zu können.

Die Regulierung von Identitätslösungen sollte in Zukunft nicht mehr allein auf zentrale Verantwortliche bauen, sondern zumindest gleichwertig auch dezentrale Lösungen zulassen, die Privacy-By-Design und Self-Sovereign-Identitätsmanagement durch die Nutzer selbst ermöglichen, und die Grundlage dafür schaffen, dass die Übermacht der bestehenden Web2-Monopole gebrochen wird und Nutzer wieder selbst die Hoheit über ihre Daten ausüben können. ▪

Gustav Hemmelmayr
Legal Director der BOTLabs GmbH unter anderem für das KILT Protocol

Gustav Hemmelmayr ist österreichischer Jurist mit langjähriger Erfahrung im IT-Recht und in Start-ups. Zusätzlich studierte er in den Nullerjahren Europäische Integration, in den Zehnerjahren politische Kommunikation mit Schwerpunkt auf Web2 und absolviert derzeit an der Hochschule Mittweida den Master für Blockchain und DLT. Sein Steckenpferd sind dezentrale Systeme und deren Governance.