Future Energy
Lab

BERICHT

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

04 – Rechtliche Analyse

Ein Projekt der

dena

Impressum

Herausgeber
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin

Tel.: +49 30 66 777-0
Fax: +49 30 66 777-699

E-Mail:
info@dena.de
futureenergylab@dena.de

Internet:
www.dena.de

Autoren:
Oliver Süme, fieldfisher
Dr. Johannes Baur, fieldfisher
Linda Babilon, dena
Irene Adamski, dena

Konzeption & Gestaltung:
die wegmeister gmbh

Stand:
Juli 2025

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2025): DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem. 04 – Rechtliche Analyse

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

Bundesministerium für Wirtschaft und Energie

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Energie.
Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

DIVE in aller Kürze

Warum braucht es digitale Identitäten?

Die Entwicklung digitaler Identitäten wird seit mehreren Jahren vorangetrieben. Sie sollen in unserer zunehmend digitalisierten und automatisierten Welt einen Vertrauensanker bilden. Digitale Identitäten garantieren, dass wir mit dem richtigen Gegenüber kommunizieren (digitale Identifizierung), dem wir unsere Daten auch wirklich anvertrauen wollen und dass diese Personen, Organisationen oder auch Maschinen echt sind (digitale Authentifizierung). Darüber hinaus müssen wir – vor allem in sensiblen Bereichen wie kritischen Infrastrukturen – sicherstellen können, dass die ausgetauschten Daten vollständig, korrekt und aktuell sind (digitale Verifikation). Während in der analogen Welt für diese Art der Überprüfung viele Wege und Möglichkeiten entwickelt wurden, steht dies in der digitalen Welt erst am Anfang: die EUDI-Wallet wird gerade in allen EU-Staaten auf den Weg gebracht, um natürliche Personen mit digitalen Identitäten auszustatten; eine EU-Business-Wallet für Organisationen und juristische Personen wird derzeit erarbeitet. Die Bereitstellung von digitalen Identitäten für Maschinen und Anlagen ist eine dritte und völlig neue Entwicklung, die für eine konsequente Automatisierung von Prozessen jedoch essenziell ist. Diese Maschinenidentitäten konnte das Team des DIVE-Projektes nicht nur für verschiedene Geräte und Anlagen (z.B. Photovoltaik-Anlagen, Wärmepumpen, Speicher) bereitstellen, sondern auch für aktuelle Prozesse und innovative Anwendungsfälle in die praktische Erprobung bringen.

Ein Vertrauensdreieck für mehr digitale Souveränität

DIVE verwendet ein digitales Identitätsmanagementsystem, welches auf den Prinzipien von selbst-souveränen digitalen Identitäten (SSI) aufbaut. Es geht dabei um eine Gewaltenteilung zwischen den drei Akteuren, die es für eine digitale Identifizierung, Authentifizierung und Verifizierung braucht: jemanden, der eine digitale Identität für sich beansprucht (Rolle 1, Holder), beispielsweise Name, Adresse oder Alter. Da es sich dabei aber anfangs nur um Behauptungen handelt, werden die gemachten Angaben einer vertrauenswürdigen Autorität zugesandt (Rolle 2, Issuer), mit der Bitte um Bestätigung (vergleichbar mit einem Stempel oder Siegel auf beglaubigten Dokumenten). Sind die Angaben korrekt und verifiziert, wird ein digitaler Nachweis über die Richtigkeit ausgestellt. Dieser Nachweis kann dann gegenüber Dritten (Rolle 3, Verifier) ausweisen, dass die Angaben zu einer Person, Organisation oder eben Anlage (bspw., dass die Anlage Grünstrom erzeugt) richtig, echt und aktuell sind. Man spricht hierbei von einem sogenannten Vertrauensdreieck: Holder und Verifier kennen sich nicht, aber vertrauen jeweils dem Issuer. Durch den Nachweis des Issuers können beide vertrauensvoll miteinander interagieren.

Neu bei dieser Art der Interaktion ist, dass der gesamte Vorgang digital, automatisiert und in Echtzeit erfolgen kann und dass dafür keine Inhalte ausgetauscht werden müssen, sondern eingangs nur eine Wahr-oder-Falsch-Meldung über die Vertrauenswürdigkeit der Daten. Der Vertrauensaufbau kann so datensparsam wie möglich erfolgen und alle sensiblen Daten verbleiben im größtmöglichen Umfang unter der Kontrolle und im Eigentum von Nutzern und realen Personen – die digitale Identität wird souverän selbstverwaltet.

Glaubwürdig und automatisierbar – digitale Maschinenidentitäten sind Grundlage für die Skalierung der Energiewende

Trotz der Fortschritte bei der Digitalisierung des Energiesystems fehlt bisher eine sektorenübergreifende, skalierbare Dateninfrastruktur, die eine sichere, effiziente und flexible Einbindung von Anlagen in verschiedene Anwendungsfälle (z.B. Flexibilität, granulare Herkunftsnachweise) im dezentralen Energiesystem ermöglicht. Insbesondere die Marktintegration von Kleinanlagen ist bisher mit erheblichem Aufwand verbunden. Eine effiziente Energieversorgung kann zukünftig jedoch nur gewährleistet werden, wenn die Anlagen mit ihren zugehörigen Daten lückenlos und in nahezu Echtzeit in eine digitale Dateninfrastruktur integriert sind. Dies umfasst sowohl Stammdaten (bspw. Art und

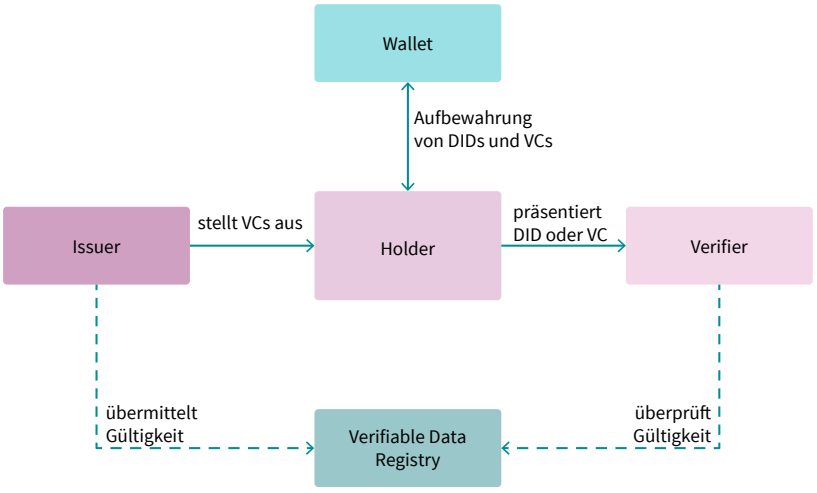


Abbildung 1: Vertrauensdreieck

Besitzer der Anlagen) als auch Bewegungsdaten (bspw. gemessene Erzeugungs- und Verbrauchsdaten) (dena 2024b). Die mangelhafte Datenerfassung und Verifizierbarkeit von Eigenschaften von kleinen und beweglichen Anlagen (bspw. E-Autos) im Energiesystem wird als „digitale Identitätslücke“ bezeichnet. Die DIVE-Basisinfrastruktur liefert einen Lösungsweg, um diese Lücke zu schließen. Im Pilotvorhaben konnten unterschiedliche Prozesse (bspw. Anmeldung einer Anlage in einem Register, Wechsel zwischen Anwendungsfällen) von der Anlage bis zum Anwendungsbereich (z.B. Grünstromnachweis) erfolgreich über digitale Identitäten durchgeführt und verwaltet werden.

Die DIVE-Basisinfrastruktur als Blaupause

DIVE zeigt einen anschlussfähigen Lösungsweg für die digitale Identitätslücke im Energiesystem: Mithilfe bereits im Markt vorhandener Komponenten und Standards sowie unter Ausnutzung bereits bestehender Strukturen und Abläufe im Energiesystem (bspw. SMGW) können sektorenübergreifende Lösungen für Endverbraucher, Netzbetreiber und Anbieter von neuen Dienstleistungen, wie virtuelle Kraftwerke oder Grünstromvermarktung, angeboten werden.

Als „DIVE-Basisinfrastruktur“ wird das im Projekt erprobte Zusammenspiel von Hardware und Software-Komponenten bezeichnet: Energiemanagementsystem (EMS), intelligentes Messsystem, Digitale Identitäten (DID), Digitale Nachweise (VCs), verifizierbares Register.

Im Ergebnis konnte DIVE zeigen, wie digitale Identitäten für Maschinen – in diesem Fall insbesondere Kleinanlagen des Energiesystems – mit relativ geringem Aufwand eingeführt werden können, um notwendige Aufgaben zur Stabilisierung und Verwaltung der Stromnetze einfacher zu machen und innovative neue Anwendungsfälle leichter zu integrieren.

Anforderungen an digitale Identitäten und die Frage der Rechtskonformität

Eine große Hürde bei der Einführung neuer Technologien ist oft die Frage von Haftung und Datenschutz. Im Energiesystem spielen zudem Cybersicherheitsanforderungen an kritische Infrastrukturen eine wichtige Rolle. Um diese Hürde abzubauen, wurde das DIVE-Projekt von Anfang an durch juristische Fachexpertise begleitet und beraten.

Während an einzelnen Stellen noch Verbesserungspotenzial für den Gesetzgeber besteht, was die Berücksichtigung dezentraler und verteilter Systeme bspw. bei Haftungsregelungen betrifft, ist hervorzuheben, dass die DIVE-Basisinfrastruktur als rechtskonforme Lösung angelegt ist, die im derzeit geltenden regulatorischen Rahmen betrieben werden kann. Es wurde eine praxistaugliche Governance-Struktur konzipiert und die Anwendbarkeit auf bekannte Anwendungsfälle (bspw. Anknüpfung ans Marktstammdatenregister, Lieferantenwechsel an der Ladesäule, Flexibilitätserbringung) geprüft.

Nächste Schritte

Das DIVE-Projekt liefert einen Vorschlag für eine Basisinfrastruktur, die die Anforderungen an Sicherheit und Leistungsfähigkeit sowie die Bedürfnisse der betrachteten energiewirtschaftlichen Anwendungsfälle erfüllt. Die einzelnen Komponenten sind durchdacht – energiewirtschaftlich, technisch, juristisch - aber müssen sich bei der Skalierung und Ausweitung im realen Umfeld unter Beweis stellen. Der Ansatz von Digitalen Identitäten als Vertrauensanker im Energiesystem dient daher als Ausgangspunkt für weitere Projekte, um die Diskussion um das digitale Identitätsökosystem im Energiesystem mit einem breiteren Stakeholderkreis fortzusetzen.

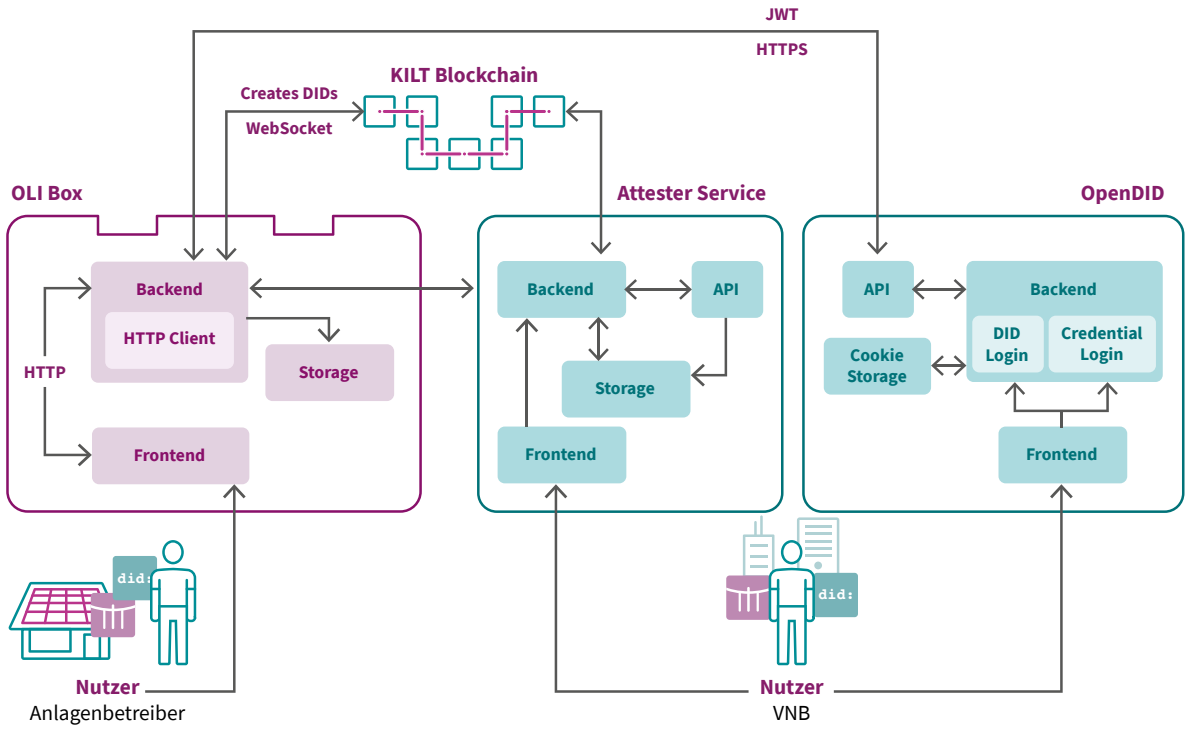


Abbildung 2: DIVE Basisinfrastruktur

Inhalt

1. Einleitung

Die frühe Integration rechtlicher Überlegungen in die technische Ausgestaltung von Digitalisierungsprojekten ist ein kritischer Erfolgsfaktor. Die technische Entwicklung sollte geltende und geplante Regulatorik nicht ignorieren, um nicht vom Gesetzgeber oder von Aufsichtsbehörden ausgebremst zu werden. Strategische Entscheidungen sollten daher in enger Abstimmung mit Rechtsexperten getroffen werden, um die richtige Balance zwischen technischer Machbarkeit und rechtlicher Zulässigkeit zu gewährleisten. Zugleich sollte aufgezeigt werden, an welchen Stellen regulatorische Bemühungen neue technische Entwicklungen noch nicht hinreichend berücksichtigen, um dem Gesetzgeber die Notwendigkeit von Anpassungen zu signalisieren. Sowohl eine technische Entwicklung an der geltenden Regulatorik vorbei als auch eine Gesetzgebung, die blind für neue Technologien ist, stellen ein Hemmnis für Innovationen dar und schaden den entwickelnden Unternehmen und damit letztlich der Gesellschaft.

Dieser Bericht hat daher das Ziel, die Demonstration der technischen Machbarkeit durch Belege zur rechtlichen Zulässigkeit des Vorhabens zu untermauern und aufzuzeigen, an welchen Stellen gesetzgeberisches Handeln vorteilhaft sein kann.

Zielgruppe dieses Berichts sind einerseits die Entwickler und Anwender der DIVE-Basisinfrastruktur, denen der Bericht einen Überblick über rechtlich relevante Herausforderungen geben soll, der durch Handlungsempfehlungen für die konkrete Umsetzung ergänzt wird. Darüber hinaus richtet sich der Bericht auch an Akteure aus Politik und Gesetzgebung und soll auf mögliches legislatives Entwicklungspotenzial aufmerksam machen, das für einen künftigen Einsatz der DIVE-Basisinfrastruktur mehr Rechtssicherheit schaffen könnte.

Den Schwerpunkt des Berichts bildet die Skizzierung einer möglichen rechtlichen Governance-Struktur für den Betrieb der DIVE-Basisinfrastruktur mit einem Vorschlag zur möglichen Ausgestaltung der Rechtsbeziehungen zwischen den beteiligten Akteuren. Dabei geht der Bericht von der im Pilotprojekt gewählten Gestaltung des Betriebs der DIVE-Basisinfrastruktur auf einer public-permissionless Blockchain aus. Sie versteht sich dabei nicht als zwingende Vorgabe für die rechtliche Gestaltung, sondern als einen Lösungsweg, neben dem auch andere Gestaltungen denkbar sind. Die Ausführungen basieren auf der Auslegung des relevanten allgemeinen deutschen Zivilrechts, insbesondere des Vertrags- und Haftungsrechts.

Im Rahmen der Bewertung der Governance-Struktur wird auf haftungsrechtliche und regulatorische Herausforderungen eingegangen. Es erfolgen eine datenschutzrechtliche Bewertung unter Heranziehung der Grundsätze der Datenschutz-Grundverordnung (DSGVO) und eine IT- und cybersicherheitsrechtliche Betrachtung, die die derzeit stattfindende Umsetzung der NIS-2-Richtlinie (zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit) und der CER-Richtlinie (EU-Richtlinie über die Resilienz kritischer Einrichtungen) in nationales Recht berücksichtigt. Ebenfalls berücksichtigt wird die aktuelle eIDAS-Verordnung 2.0 (EU-Verordnung über elektronische Identifizierung und Vertrauensdienste), soweit sie für die DIVE-Basisinfrastruktur relevante Regelungen enthält.

Der Bericht beleuchtet weiter die rechtlichen Grundlagen einer möglichen Schnittstelle zwischen der DIVE-Basisinfrastruktur und dem Marktstammdatenregister unter Berücksichtigung der hierfür relevanten Normen aus dem Energiewirtschaftsgesetz (EnWG) und der Marktstammdatenregisterverordnung (MaStRV) und geht überblicksartig auf rechtliche Besonderheiten der Anbindung der DIVE-Basisinfrastruktur an die Anwendungsfälle ein. Hinsichtlich der Anwendungsfälle fokussiert sich der Bericht auf Fragen, die allein das Identitätsmanagement der Anlagen und damit der DIVE-Basisinfrastruktur selbst sowie deren Anbindung an den Anwendungsfall betreffen. Eine Bewertung der rechtlichen Zulässigkeit der Anwendungsfälle selbst findet nicht statt. Für die Bewertung der Anbindung geht der Bericht auf die unionsrechtlichen Erneuerbare-Energien-Richtlinien und ihre nationale Umsetzung im EnWG und im Erneuerbare-Energien-Gesetz (EEG) sowie auf die Herkunfts- und Regionalnachweis-Durchführungsverordnung (HkRNDV) ein. In Bezug auf den Lieferantenwechsel werden die unionsrechtliche Verordnung über den Aufbau der Infrastruktur für alternative Kraftstoffe (AFIR) und die nationale Ladesäulenverordnung (LSV) thematisiert.

Schließlich leitet der Bericht aus den Erkenntnissen konkrete Handlungsempfehlungen für die oben genannten Akteure bei der Entwicklung und Anwendung der DIVE-Basisinfrastruktur und in Politik und Gesetzgebung ab.

2. Executive Summary

Die rechtliche Betrachtung kommt zu dem Ergebnis, dass die DIVE-Basisinfrastruktur, wie in diesem Abschlussbericht technisch und wirtschaftlich beschrieben, im derzeit geltenden regulatorischen Rahmen betrieben werden kann. An einzelnen Stellen verbleibt für den Gesetzgeber dennoch Klarstellungs- und Verbesserungsbedarf.

Die Wahl einer public-permissionless Blockchain für die DIVE-Basisinfrastruktur bringt regulatorische Herausforderungen mit sich, da das geltende Recht oftmals nicht mit Blick auf dezentrale Systeme entworfen wurde. Die identifizierten Herausforderungen lassen sich aber durch eine entsprechende Gestaltung innerhalb des Projekts lösen.

Da die DIVE-Basisinfrastruktur auf der Grundlage einer public-permissionless Blockchain ohne steuernde Zentralstelle wie eine Betreibergesellschaft funktioniert, muss ein Governance-Modell gefunden werden, das auf eine haftende Zentralstelle verzichtet. Die hier vorgeschlagene Lösung begründet den Verzicht auf die haftende Zentralstelle mit der Betrachtung der Nutzung der Blockchain-Infrastruktur durch die Akteure als die einvernehmliche Nutzung eines Gemeingutes, für dessen Ausfall eine Haftung zwar nicht übernommen, aber von den Teilnehmern auch nicht erwartet wird. Dies folgt dem Gedanken, dass Anwender der DIVE-Basisinfrastruktur die Blockchain – ähnlich wie das Internet – als eine gemeinsame Infrastruktur nutzen, auf deren Funktionsfähigkeit alle vertrauen. Zwischen den Akteuren bestehen bilaterale Rechtsverhältnisse, deren konkreter Inhalt je nach Anwendungsfall vertraglich unterschiedlich ausgestaltet sein kann. Ein zusätzliches gesetzgeberisches Tätigwerden, insbesondere hinsichtlich einer Verpflichtung der Issuer, kann aber dennoch sinnvoll sein, um eine flächendeckende Nutzung der DIVE-Basisinfrastruktur voranzutreiben.

Der Verzicht auf die haftende Zentralstelle geht für die Akteure mit einem Risiko einher, da sie sich im Falle von Fehlern der DIVE-Basisinfrastruktur nicht an eine Betreibergesellschaft wenden können. Der Tatsache der fehlenden Betreibergesellschaft müsste daher mit der Schaffung von Vertrauen bei den Akteuren in die Ausfallsicherheit der Blockchain-Technologie begegnet werden.

Weitere regulatorische Herausforderungen können sich aus dem IT- und Cybersicherheitsrecht ergeben. Dieses enthält Vorgaben für Betreiber von Einrichtungen oder kritischen Anlagen, die für die Versorgung der Bevölkerung von besonderer Bedeutung sind und deren Ausfallsicherheit daher durch Anforderungen an die Betreiber gewährleistet werden soll. Die derzeit in Umsetzung befindliche NIS-2-Richtlinie erweitert dabei den Kreis der potenziell betroffenen Unternehmen erheblich und erfasst auch Anbieter von „Vertrauensdiensten“, wozu – aufgrund der weiten Definition – grundsätzlich auch die DIVE-Basisinfrastruktur gehören könnte. Allerdings kann hier der dezentrale Aufbau der DIVE-Basisinfrastruktur sogar als Argument gegen eine Anwendbarkeit sprechen, da es keinen „Betreiber“ der Einrichtung gibt und ein Ausfall einzelner Nodes für das Funktionieren des Systems nicht von Bedeutung ist.

Datenschutzrechtlich ist der Betrieb einer public-permissionless Blockchain mit dem Konzept der DSGVO, das von zentralen Verantwortlichen ausgeht, schwer in Einklang zu bringen. Als Lösungsweg unter geltendem Recht ist daher der geplante weitgehende Verzicht auf die Nutzung personenbezogener Daten auf dem Blockchain-Layer vorzugswürdig. Da der Begriff „personenbezogene Daten“ sehr weit verstanden wird, kann ein Personenbezug für einzelne Informationen zumindest in seltenen Fällen, aber dennoch möglich sein. Rechtssicherheit schafft hier langfristig daher nur eine gesetzgeberische Klarstellung. Bislang fehlt es hier noch an nennenswerter gesetzgeberischer Aktivität. Im Rahmen der Abwägung zwischen verschiedenen technischen Gestaltungsmöglichkeiten sollte die Option einer zentralen Lösung mit klarer Zuordnung von Verantwortlichkeiten für den Registerbetrieb deshalb zumindest mitgedacht werden.

Zukünftig kann eine Symbiose der DIVE-Basisinfrastruktur mit dem Marktstammdatenregister (MaStR) Vorteile bringen, da sie die vom Gesetzgeber gewünschte staatliche Kontrolle des MaStR mit den Vorteilen der DIVE-Basisinfrastruktur verbinden könnte. Das Marktstammdatenregister und die DIVE-Basisinfrastruktur sollten dabei als gegenseitige Ergänzung betrachtet werden. Eine (gesetzliche) Erweiterung der bestehenden Schnittstellen, die es – nach Authentifizierung – ermöglichen, auch vertrauliche Informationen automatisiert aus dem MaStR auszulesen oder bestehende Informationen zu aktualisieren, könnte die Effizienz und Qualität beider Register steigern.

Für die Anbindung an die Anwendungsfälle gibt es aus dem DIVE-Projekt unmittelbar keine regulatorischen Hürden. Da die anvisierten Anwendungsfälle teils in ihrerseits stark regulierten Bereichen angesiedelt sind, sind jedoch die hierfür geltenden Regelungen bei Umsetzung der jeweiligen Anwendungsfälle gesondert zu begutachten.

3. Vorschlag einer Governance-Struktur

Im Folgenden wird ein Vorschlag für die Governance-Struktur der DIVE-Basisinfrastruktur, also die Beschreibung der rechtlichen Beziehungen zwischen den beteiligten Akteuren und ihrer inhaltlichen Ausgestaltung, dargestellt. Bevor das Konzept der Rechtsbeziehungen im Detail vorgestellt wird, sollen zunächst die Ziele und die Prämisse des vorliegenden Vorschlags erläutert werden. Schließlich wird der Bericht auch auf regulatorische Herausforderungen und mögliche Lösungen für bestehende Risiken eingehen.

3.1 Ziele und Prämisse der Governance-Struktur

Die Governance-Struktur der DIVE-Basisinfrastruktur hat zum Ziel, das System auf eine rechtlich solide Basis zu stellen, indem eine rechtskonforme Betriebsweise sichergestellt wird und Risiken für die Beteiligten minimiert werden. In der Frühphase des Projekts sind viele spezifische operative Details der Umsetzung noch offen. Die vorgestellte Governance-Struktur ist daher hinreichend abstrakt, um Entwicklungsspielräume für eine konkretere Ausgestaltung zu lassen. Für die Zwecke dieser Betrachtung müssen dennoch bereits in dieser Phase grundlegende Weichenstellungen, wie die Wahl der Blockchain-Form, die Beteiligung der Akteure der Blockchain-Infrastruktur oder die Auswahl der zu verarbeitenden Daten, rechtlich bewertet und integriert werden. Technische Erkenntnisse und regulatorische Überlegungen befruchten sich dabei bestenfalls gegenseitig. Auf diese Weise gelingt ein paralleler Aufbau von Rechtsverständnis und technischer Infrastruktur.

Die rechtliche Bewertung geht von der Prämisse aus, dass die DIVE-Basisinfrastruktur auf einer öffentlichen, zugangsfreien (public-permissionless) Blockchain betrieben wird. Diese Wahl hat das technologische Ziel, die Transparenz, Offenheit und Ausfallsicherheit des Systems zu unterstützen. Rechtlich sollte diese Wahl durch eine Governance-Struktur flankiert werden, die Haftungsrisiken für die beteiligten Akteure minimiert. Die Struktur muss zudem gewährleisten, dass alle regulatorischen Anforderungen erfüllt werden. Dies beinhaltet insbesondere Datenschutzbestimmungen und Normen zur Cybersicherheit.

3.2 Rechtlich relevante Akteure

In der Konzeption und im Betrieb eines dezentralen Blockchain-basierten Registers wie der DIVE-Basisinfrastruktur ist die Klärung der Rollen und Verantwortlichkeiten der beteiligten Akteure essenziell. Ohne klare vorherige Zuweisung von rechtlichen Rollen besteht die Möglichkeit, dass die Zuweisung dieser Rollen durch Behörden oder Gerichte vorgenommen wird und das Ergebnis weder den Interessen der Energiewende noch denen der Beteiligten und möglicherweise auch nicht den technischen Anforderungen und Umsetzungsmöglichkeiten entspricht. Dies kann beispielsweise dazu führen, dass die wirtschaftliche Kalkulation der Umsetzung durch die Beteiligten nicht mehr aufgeht und die Verfolgung dieses Projekts für sie unattraktiv wird. Das Ziel, die Energiewende voranzutreiben, könnte dadurch gefährdet werden. Die Identifizierung der relevanten Akteure und die klare Definition ihrer Rollen sind daher entscheidend, um Rechtsklarheit zu schaffen und die Einhaltung aller relevanten Gesetze und Vorschriften sicherzustellen.

Durch die klare Definition der Rollen und Verantwortlichkeiten der Akteure wird zudem Transparenz geschaffen. Dies fördert das Vertrauen aller Stakeholder, einschließlich Nutzer, Regulatoren und Partnerorganisationen, in die Integrität und Zuverlässigkeit des Registers. Im Falle von Unstimmigkeiten oder Konflikten ermöglicht die genaue Kenntnis über die Zuständigkeiten der verschiedenen Akteure eine effektive Konfliktlösung und Haftungszuschreibung. Die verschiedenen Gruppen der beteiligten Akteure werden im Folgenden näher beschrieben.

3.2.1 Anwender der DIVE-Basisinfrastruktur

Unter den Anwendern versteht man alle natürlichen und juristischen Personen, die die DIVE-Basisinfrastruktur für ihre geschäftlichen oder privaten Transaktionen nutzen. Diese Gruppe umfasst Einzelpersonen, Unternehmen und möglicherweise künftig auch staatliche Einrichtungen, die das Register zur Dokumentation und Verifizierung von Transaktionen verwenden. Im Folgenden soll ein Überblick über die möglichen Anwender der DIVE-Basisinfrastruktur gegeben werden.

Anlagenbetreiber

Die Asset-DID-Sequenz (Decentralized Identifier), die für eine Anlage während des Onboardings generiert wird, ist nur der Anlage selbst zugeordnet. Die Anlage ist als Sache jedoch nicht eigenständig rechtsfähig. Anknüpfungspunkt für Rechte ist daher der Betreiber der Anlage. Für Photovoltaik-Anlagen ist laut § 3 Nr. 2 des Erneuerbare-Energien-Gesetzes (EEG) der Anlagenbetreiber die Person oder Entität, die die Anlage im Sinne von § 3 Nr. 1 EEG zur Erzeugung von Strom nutzt. Er ist damit Adressat der Verpflichtungen nach dem EEG. Neben der Asset-DID, die sich auf eine konkrete technische Anlage bezieht, ist eine digitale User-DID denkbar, die die Identität des Anlagenbetreibers als rechtliche Person repräsentiert. Eine solche User-DID muss jedoch nicht zwingend auch Teil der DIVE-Basisinfrastruktur sein und kann auch von einem anderen DID-Anbieter stammen.[1] Sie ist daher getrennt zu betrachten. Diese Trennung erlaubt es auch, perspektivisch bestehende Identitätsmanagementsysteme zu integrieren, und fördert die Flexibilität und Interoperabilität im breiteren Kontext digitaler Identitäten. Die Interoperabilität zwischen der Asset-DID und verschiedenen User-IDs, die durch unterschiedliche DID-Anbieter verwaltet werden, könnte in Zukunft im Licht der nun umzusetzenden eIDAS-Verordnung 2.0[2] besonders relevant werden.[3] Die eIDAS-Verordnung regelt die Identifikation und die Vertrauensdienste für elektronische

1 Beispielsweise durch Verknüpfung mit der geplanten EUDI-Wallet, https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/start/

2 Verordnung (EU) 2024/1183 des Europäischen Rates und Parlaments vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1183

3 Zu den Chancen und Herausforderungen für Self-Souvereign-Identity-Systeme unter eIDAS 2.0 siehe näher Schwalm, Steffen; Albrecht, Daria; Alamillo, Ignacio (2022): eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI

Transaktionen innerhalb der Europäischen Union. Eine wichtige Neuregelung betrifft die Einführung der EUDI-Wallet (European Digital Identity Wallet, Europäische Brieftasche für die digitale Identität) durch die Mitgliedstaaten, mit der sich Bürgerinnen und Bürger für privatwirtschaftliche und Verwaltungsdienstleistungen authentifizieren können sollen. Denkbar ist, dass die Asset-DID auch mit dieser Wallet verknüpft wird. Eine solche Verknüpfung könnte bedeuten, dass Anlagenbetreiber und ihre Anlagen innerhalb des EU-Binnenmarktes einfacher und sicherer agieren können, insbesondere im Hinblick auf grenzüberschreitende Transaktionen und Kooperationen. Die Umsetzung der EUDI-Wallet in Deutschland wird derzeit vom Bundesministerium des Innern (BMI), die Bundesagentur für Sprunginnovationen (SPRIND) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) vorangetrieben.[4]

Letztverbraucher

Im Kontext des EEG ist der Letztverbraucher gemäß § 3 Nr. 33 EEG definiert als der Stromabnehmer, der elektrische Energie aus einer Entnahmestelle verbraucht. Obwohl Letztverbraucher grundsätzlich keine Anlagen betreiben, können sie eine aktive Rolle in einem möglichen DIVE-Ökosystem einnehmen. In ihrer Position als Endnutzer des Systems können sie als Verifier fungieren. In dieser Funktion könnten Letztverbraucher die Gültigkeit von Verifiable Credentials (VCs) überprüfen und sich über die Herkunft des Stroms oder den Erzeuger informieren.

Eine interessante rechtliche Dynamik entsteht, wenn Letztverbraucher zugleich als Anlagenbetreiber agieren – eine Konstellation, die im Energiesektor als „Prosumer“ (Producer-Consumer) bekannt ist. Prosumer erzeugen Energie, zum Beispiel mit Photovoltaik-Anlagen, nutzen einen Teil selbst und speisen den Überschuss ins Netz ein. So sind sie zugleich Anlagenbetreiber und Letztverbraucher.

Die Doppelfunktion als Prosumer führt zu einer komplexen rechtlichen Situation, da der Prosumer die Vorschriften sowohl für Anbieter als auch für Konsumenten von Energie einhalten muss, was unter Umständen zusätzliche regulatorische Compliance-Anforderungen mit sich bringt.[5] Es zeigt sich zudem, dass diese Doppelfunktion bislang nicht immer hinreichend regulatorisch abgebildet ist, da die Regelungen für Anlagenbetreiber oftmals größere Akteure im Blick haben.

Fahrer und Halter von Elektrofahrzeugen

Ähnlich wie Prosumer nehmen auch Fahrer und Halter von Elektrofahrzeugen bei der Nutzung der DIVE-Basisinfrastruktur eine Doppelrolle ein, da sie einerseits für ihre Fahrzeuge Verifiable Credentials generieren oder mit der Asset-DID nutzen und andererseits als auch Strom verbrauchen, also als Letztverbraucher auftreten.

Verteilnetzbetreiber (VNB)

Nach § 7 EEG befindet sich der Verteilnetzbetreiber (VNB) in einem gesetzlichen Schuldverhältnis zum Anlagenbetreiber, das durch spezifische Pflichten und Verantwortlichkeiten gekennzeichnet ist. Gemäß § 8 EEG muss der Anlagenbetreiber beim VNB ein Netzanschlussbegehren stellen, bevor er eine EEG-Anlage ans Netz anschließen darf. Dieses Begehren ist ein formalisierter Prozess, in dessen Rahmen der Anlagenbetreiber verpflichtet ist, dem VNB alle notwendigen Informationen über die Anlage und sich selbst zur Verfügung zu stellen. Im Rahmen des DIVE-Projekts ist vorgesehen, dass die VNBs eine erweiterte Rolle als Issuer für die DIDs übernehmen. Der VNB fungiert als vertrauenswürdige Instanz, die die Authentizität von Daten bestätigt und diese in VCs überführt. Durch den Abgleich der vom Anlagenbetreiber übermittelten Informationen mit den Daten in der eigenen Datenbank kann der VNB die Echtheit und Richtigkeit der Daten – soweit für ihn ersichtlich – verifizieren und somit die Erstellung sicherer und zuverlässiger VCs ermöglichen.

Messstellenbetreiber (MSB)

Die Aufgaben und Verantwortlichkeiten des Messstellenbetreibers (MSB) sind im Messstellenbetriebsgesetz (MsbG) festgelegt. Gemäß § 3 Abs. 2 MsbG ist der MSB für die ordnungsgemäße Messung von Energieverbrauchs- und Einspeisewerten verantwortlich. Diese Rolle ist entscheidend für die Genauigkeit und Integrität der Energiebilanzierung und -abrechnung. Nach § 9 MsbG schließt der MSB Messstellenverträge ab, die die Bedingungen für die Installation, den Betrieb und die Wartung von Messstellen regeln. Ein solcher Vertrag wird auch mit dem Anlagenbetreiber geschlossen, was sicherstellt, dass alle Energieflüsse, die von der Anlage ausgehen oder zu ihr hinführen, präzise erfasst werden. Diese Daten werden nach §§ 60 ff. MsbG an verschiedene Marktteilnehmer wie Energieversorger, Netzbetreiber und Behörden übermittelt.

3.2.2 Hersteller und Dienstleister

Diese Gruppe umfasst die Entitäten, die den Betrieb der DIVE-Basisinfrastruktur durch ihre Produkte und Dienstleistungen ermöglichen.

Gerätehersteller

Die Bedeutung der Gerätehersteller ergibt sich aus der Rolle ihrer Produkte, die die Teilnahme an der DIVE-Basisinfrastruktur erst ermöglichen. Durch die Bereitstellung von Krypto-Devices, die eine sichere Datenerfassung, -speicherung und -übertragung gewährleisten, leisten sie einen wichtigen Beitrag zur Umsetzung der technologischen und sicherheitstechnischen Anforderungen der DIVE-Basisinfrastruktur.

4 https://www.personalausweisportal.de/SharedDocs/kurzmeldungen/Webs/PA/DE/2024/09_eudi_wallet_sep.html

5 Zu den rechtlichen Schwierigkeiten des Markeintritts für Prosumer siehe Zerche, EnWZ 2022, 69

Dies kann dadurch erfolgen, dass der Hersteller ein (H)EMS-Krypto-Device ((Heim-)Energiemanagementsystem) anbietet, das speziell dazu dient, den Funktionsumfang einer bereits existierenden Anlage zu erweitern. Der Gerätehersteller kann alternativ zugleich der Hersteller der Anlage sein, wobei in diesem Fall der Krypto-Chip direkt in die Anlage eingebaut ist. Diese Integration bietet eine nahtlose und sichere Lösung, die es ermöglicht, dass die Anlage von Beginn an über die notwendigen Sicherheitsfeatures verfügt, um effektiv an der DIVE-Basisinfrastruktur teilzunehmen. Denkbar ist auch, dass eine technische Lösung entwickelt wird, die auf einen Krypto-Chip verzichtet.[6] Soweit auch in diesem Fall eine Integration der Softwarelösung in die Anlage erforderlich ist, wird der Gerätehersteller für die Ermöglichung dieser Implementierung relevant. Gelingt die Integration unabhängig vom Gerät, würde der Gerätehersteller als eigenständig relevanter Akteur wegfallen.

Installateure und andere IT-Dienstleister

Installateure sind für die physische Installation der erforderlichen Hardware wie Krypto-Devices zuständig. Sie oder andere IT-Dienstleister unterstützen zudem bei der digitalen Integration von Anlagen in die DIVE-Basisinfrastruktur, einschließlich der Generierung von Verifiable Credentials. Viele Anlagenbetreiber verfügen nicht über die notwendige technische Expertise, um Krypto-Devices selbst zu installieren oder ihre Anlagen eigenständig für die DIVE-Basisinfrastruktur zu registrieren. Installateure und IT-Dienstleister schließen diese Wissenslücke und ermöglichen eine professionelle und sichere Integration in das Netzwerk.

Hersteller von Zusatzsoftware

Die DIVE-Basisinfrastruktur bedarf zur praktischen Anwendung einer Reihe weiterer Zusatzsoftware, die den Nutzern und Geräten die Interaktion mit der Blockchain ermöglichen.[7] Diese Software kann den Anwendern der DIVE-Basisinfrastruktur von verschiedenen Softwareherstellern unter unterschiedlicher Lizenz angeboten werden.

3.2.3 Beteiligte der Blockchain-Infrastruktur

Diese Gruppe beinhaltet alle Akteure, die direkt an der Aufrechterhaltung und Verwaltung der Blockchain-Infrastruktur beteiligt sind. Das DIVE-Projekt nutzt die KILT Blockchain als technologische Grundlage für die Implementierung seines dezentralen Maschinen-Identitäten-Registers.[8] Prinzipiell wären hier sowohl andere Blockchain-Anbieter als auch andere technische Registerlösungen denkbar.

Bei der DIVE-Basisinfrastruktur wird der grundlegenden Prämisse einer public-permissionless Blockchain gefolgt, jedoch keine vertiefte Auseinandersetzung mit dem spezifischen Aufbau und den technischen Details einzelner konkreter Blockchain-Lösungen vorgenommen. Dieser Ansatz ermöglicht es, die rechtlichen Überlegungen allgemein und anpassungsfähig zu halten und gleichzeitig die weitere technische Entwicklung des Projekts zu unterstützen.

Node-Betreiber der Blockchain

Node-Betreiber sind verantwortlich für den Betrieb der Netzwerkknoten, die die Blockchain-Infrastruktur unterstützen und aufrechterhalten. Als Knotenpunkte im Netzwerk speichern und verarbeiten sie die Hash-Werte, die als Nachweis für Transaktionen und Datenintegrität innerhalb der DIVE-Basisinfrastruktur dienen.

Entwickler des Blockchain-Protokolls

Die zugrunde liegende Blockchain (hier die KILT Blockchain) basiert auf einem Protokoll, das im Falle von public-permissionless Blockchains in der Regel unter Open-Source-Lizenz verwendet wird. Die Entwickler dieses Protokolls übernehmen eine entscheidende Rolle bei der Bestimmung, nach welchen Regeln die DIVE-Basisinfrastruktur operieren soll. Fehler im Blockchain-Protokoll können Auswirkungen auf das Projekt als solches haben.

3.2.4 Staatliche Akteure

Staatliche Akteure sind nicht unmittelbar an der DIVE-Basisinfrastruktur und ihrem Betrieb beteiligt, können aber in ihrem Aufgabenbereich Einfluss auf bestimmte Teilbereiche des Betriebs nehmen.

Bundesnetzagentur (BNetzA)

Die Bundesnetzagentur (BNetzA) spielt eine zentrale Rolle im deutschen Energiemarkt. Unter anderem ist die sie für den Betrieb des Marktstammdatenregisters (MaStR) verantwortlich. Das MaStR dient als umfassende Datenbank, die alle wesentlichen Informationen zu Energieerzeugungsanlagen und Marktakteuren sowie weitere energiewirtschaftlich relevante Daten sammelt. Im Rahmen des DIVE-Projekts ist zwar vorgesehen, dass das MaStR parallel zur DIVE-Basisinfrastruktur betrieben wird, wobei eine gegenseitige Ergänzung anvisiert ist. Perspektivisch wäre allerdings als zusätzliche Funktion die Möglichkeit einer automatischen Aktualisierung der Daten im MaStR wünschenswert, falls während des Onboardings oder der regulären Nutzung der DIVE-Basisinfrastruktur fehlende oder fehlerhafte Daten festgestellt werden. Die BNetzA könnte in diesem Prozess eine aktive Rolle spielen, indem sie die Aktualisierung der Daten im MaStR nicht nur überwacht, sondern auch direkt unterstützt, zum Beispiel indem Schnittstellen bereitgestellt oder wenigstens ermöglicht werden. Durch eine noch engere Verzahnung zwischen dem MaStR und der DIVE-Basisinfrastruktur könnten die Datenqualität sowie die Effizienz des Prozesses der Maschinen-Identifizierung erheblich erhöht werden.

Umweltbundesamt (UBA)

Das Umweltbundesamt (UBA) ist für die Implementierung des Anwendungsfalls der Green Proofs mitverantwortlich. Dem UBA ist gesetzlich die Betreuung des Herkunftsnachweisregisters zugewiesen, das die Zuordnung von erzeugtem Strom aus erneuerbaren Quellen zu den entsprechenden Verbrauchsstellen dokumentiert. Gemäß § 47 Abs. 7 des Energiewirtschaftsgesetzes (EnWG) hat das UBA die Befugnis, die Richtigkeit von Angaben in

6 Siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“
7 Siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“
8 Siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“

den Herkunftsnachweisen zu überprüfen. Diese gesetzliche Regelung verleiht dem UBA eine Aufsichts- und Kontrollfunktion, die die Authentizität und Zuverlässigkeit der im herkömmlichen Register geführten Daten gewährleistet. Eine rechtssichere Umsetzung des Anwendungsfalls der Green Proofs durch die DIVE-Basisinfrastruktur kann daher voraussichtlich nur unter Einbeziehung des UBA erfolgen.

3.3 Konzept für die Rechtsbeziehungen zwischen den Beteiligten

Im Folgenden wird das Konzept der Rechtsbeziehungen zwischen den Beteiligten dargestellt. Dabei wird zunächst auf das Verhältnis der Blockchain-Betreiber zu den Anwendern der DIVE-Basisinfrastruktur und dann auf das Verhältnis der Anwender der DIVE-Basisinfrastruktur untereinander eingegangen.

3.3.1 Trennung des Blockchain-Betriebs von den Anwendern der DIVE-Basisinfrastruktur

Die folgende Darstellung zeigt auf, dass bei Wahl einer public-permissionless Blockchain die rechtliche Trennung des Blockchain-Betriebs von den Anwendern der DIVE-Basisinfrastruktur vorzugswürdig ist.

Vorteile der Trennungslösung

Die Wahl einer public-permissionless Blockchain für die Umsetzung des DIVE-Projekts legt nahe, für eine möglichst praktikable Gestaltung die rechtliche Trennung zwischen den Akteursgruppen der Betreiber der Blockchain-Infrastruktur und den Anwendern der DIVE-Basisinfrastruktur zu wählen. Diesem Gedanken folgend, wird die dem DIVE-Projekt zugrunde liegende Blockchain von einer Gruppe von Node-Betreibern und – je nach Blockchain-Protokoll – weiteren Akteuren aufrechterhalten, die durch ihre Beiträge die Basis der Technologie bereitstellen (siehe oben unter 3.2.2 Diese Akteure sind nur für den reinen Betrieb der Blockchain-Technologie verantwortlich, während die Anwender der DIVE-Basisinfrastruktur diese Technologie lediglich nutzen, um spezifische Funktionen, wie insbesondere die Verwaltung der Asset-DIDs, auszuführen. Das vorliegende Konzept sieht vor, dass die Anwender zwar mit der Blockchain interagieren, aber rechtlich und operativ von den Betreibern der Blockchain-Infrastruktur getrennt sind.

Ein Beweggrund für diese rechtliche Trennung ist zunächst ergebnisorientiert: Eine Verantwortung der Betreiber der Blockchain-Infrastruktur für den DIVE-Betrieb könnte Haftungsfolgen mit sich bringen, die bei einer offenen Blockchain-Lösung entweder zu fehlendem Anreiz zur Teilnahme am Blockchain-Betrieb oder zu einer mangelnden praktischen Durchsetzungsmöglichkeit von Ansprüchen gegen die Betreiber führen würden. Das liegt insbesondere daran, dass die Struktur einer public-permissionless Blockchain inhärent komplex und durch eine fluide Teilnehmerstruktur, die weltweit verteilt sein kann, charakterisiert ist. Die Beteiligten der Blockchain-Infrastruktur sind daher oft schwer greifbar, was rechtliche Herausforderungen bezüglich der Zuständigkeit und der Durchsetzbarkeit von Ansprüchen mit sich bringt.[9]

Blockchains sind zudem in der Regel nicht exklusiv für ein einzelnes Projekt wie die DIVE-Basisinfrastruktur konzipiert, sondern bieten multifunktionale Plattformen, die für verschiedene Anwendungen genutzt werden können. Diese Multifunktionalität liefert ein weiteres Argument für eine klare rechtliche Trennung, um spezifische Verantwortlichkeiten und Haftungsregelungen zu definieren. Eine direkte Verantwortung oder Haftung der Beteiligten der Blockchain-Infrastruktur für spezifische Anwendungen wie die DIVE-Basisinfrastruktur wäre praktisch schwer tragbar. Denn die Blockchain-Akteure wissen nicht, welche Anwendungen auf Basis der Blockchain konkret betrieben werden, und können dies auch nicht kontrollieren. Die Trennung sorgt dafür, dass die technischen Betreiber nicht unverhältnismäßig mit den spezifischen Anforderungen der DIVE-Anwendungen konfrontiert werden. Da sie diese nicht kennen, würden sich daraus unkalkulierbare Risiken für sie ergeben. Dieser Ansatz fördert zudem eine breitere Teilnahme am Betrieb der Blockchain-Infrastruktur. Dies heißt nicht, dass Blockchain-Akteure im rechtsfreien Raum agieren. Auch wenn es bei der Trennungslösung keine vertragliche Haftung gibt, verbleibt die Möglichkeit einer deliktischen Haftung nach §§ 823 ff. Bürgerliches Gesetzbuch (BGB) unter der Voraussetzung einer vorsätzlichen oder fahrlässigen Verletzung geschützter Rechtsgüter.

Eine Trennung hat zudem den Vorteil, dass die eigentliche Blockchain-Governance, also die Regeln des jeweiligen Blockchain-Protokolls, für den technischen Betrieb der DIVE-Basisinfrastruktur generell nebensächlich sind und dies somit auch rechtlich abgebildet wäre. Durch die Trennung ist es für die Beteiligten der DIVE-Basisinfrastruktur egal, nach welchen spezifischen Regeln die darunterliegende Blockchain funktioniert, womit sie zur Modularisierung und Technologieoffenheit beiträgt. Details des Blockchain-Protokolls sind daher auch nicht Gegenstand der vorliegenden Betrachtung der Governance der DIVE-Basisinfrastruktur.

Rechtfertigung durch den Gedanken der DIVE-Basisinfrastruktur als Gemeingut

Die rechtliche Trennung zwischen dem Betrieb der Blockchain und den Anwendern der DIVE-Basisinfrastruktur ist nicht selbstverständlich und erfordert eine rechtliche Begründung. Vergleicht man die DIVE-Basisinfrastruktur auf Grundlage einer Blockchain mit einer Multi-Layer-Softwarearchitektur könnte die Forderung nach einer Haftung der Betreiber des Blockchain-Layers auch für Fehler beim Betrieb der DIVE-Basisinfrastruktur aufkommen, wenn diese aus Fehlern der Blockchain resultieren.[10] Bei einer Multi-Layer-Softwarearchitektur besteht nämlich durchaus eine Haftung der Betreiber eines Layers für Fehler

9 So wird eine rechtliche Beziehung zwischen den Nodes einer Blockchain weitgehend abgelehnt, vgl. Schwintowski/Klausmann/Kadgien, NJOZ 2018, 1401 (1404); Omlor, ZRP 2018, 85 (86); Spindler/Bille, WM 2014, 1357 (1360)

10 Siehe zur Einordnung von vergleichbaren Cloud-Lösungen auch Redeker in Redeker, IT-Recht, Rn. 1278.

dieses Layers, auch wenn sich dieser Fehler auf darüberliegende Layer auswirkt.[11] Auch im DIVE-Projekt bestehen ein Vertrauen und eine Abhängigkeit der Anwender der DIVE-Basisinfrastruktur in Bezug auf die Funktionsfähigkeit des Blockchain-Layers. Damit könnte auch hier grundsätzlich ein Interesse an einer Haftung der Betreiber der Blockchain-Infrastruktur bestehen.

Um dennoch das oben formulierte Ziel einer Trennung der Verantwortlichkeiten zu erreichen, könnte die Nutzung der Daten in der public-permissionless Blockchain durch die Anwender der DIVE-Basisinfrastruktur allerdings auch wie die Nutzung eines Gemeingutes verstanden werden.[12] Diese Sichtweise könnte helfen, die fehlende Verantwortung und Haftung der Blockchain-Betreiber zu begründen und realistische Erwartungen der Anwender der DIVE-Basisinfrastruktur hinsichtlich der Nutzung und des Risikomanagements zu etablieren.

Ein „Gemeingut" ist eine öffentlich verfügbare Ressource, wie zum Beispiel Luft oder Licht, die allen zur freien Verfügung steht.[13] Die Nutzung eines solchen Gutes erfolgt auf eigene Gefahr, ohne dass eine spezifische Haftung für oder ein Leistungsanspruch gegen bestimmte Personen für die Bereitstellung und Aufrechterhaltung bestehen. Jeder Nutzer akzeptiert die inhärenten Risiken und Vorteile, die mit der Nutzung eines Gemeingutes verbunden sind. Im digitalen Umfeld kann zum Verständnis dieses Konzepts auch der Vergleich mit der Nutzung des Internetprotokolls (IP) helfen. Das Internet wird von allen Anschlussinhabern genutzt. Darauf basierend werden Geschäftsbeziehungen aufgebaut, ohne dass die Nutzer individuelle Verträge mit den „Betreibern des Internets" schließen, die als solche auch schwer identifizierbar oder greifbar wären. Zwar bestehen Verträge mit Zugangsanbietern. Die Regeln, nach denen Informationen über das Internet übertragen werden, finden sich jedoch in Protokollen, auf deren Einhaltung alle vertrauen. Das Risiko eines (zeitweisen) Ausfalls dieser Übertragung oder von Fehlern in der Datenübertragung tragen die Vertragspartner gemeinsam, wenn sie Dienstleistungen anbieten oder nutzen, die nur mit dem Internet funktionieren.

Vertragliche Ansprüche bestehen gegenüber einzelnen Anbietern nur bezüglich der von ihnen konkret erbrachten Leistungen. So muss der Internetzugangsprovider nach § 58 Telekommunikationsgesetz (TKG) für Störungen seiner technischen Infrastruktur einstehen. Der Begriff der „Störung" wird dabei aber als ungewollte Veränderung der vom Anbieter genutzten technischen Einrichtungen verstanden.[14] Liegt der Fehler nicht in der genutzten technischen Einrichtung, sondern im verwendeten Protokoll für die Kommunikation, hat dies der Provider nicht zu verantworten. Anbieter von Zugangssoftware wie beispielsweise Browsern schulden nur die objektive Eignung für die vertraglich vorausgesetzte Verwendung, wobei das Verwendungsrisiko grundsätzlich den Nutzer trifft.[15] Der Anbieter der Zugangssoftware ist daher nicht verantwortlich, wenn die Software keine erfolgreiche Verbindung zum aufgerufenen Webserver herstellen kann, wenn der Grund hierfür nicht in Fehlern der Zugangssoftware selbst liegt. Auch die Anbieter von internetbasierten Diensten haften für diese Fälle nicht. Beim Angebot von Software as a Service (SaaS), wie beispielsweise einem Cloud-Dienst, schuldet der Anbieter nach dem Service Agreement in der Regel eine Verfügbarkeit seiner Dienste, oftmals abgestuft nach näheren Vorgaben in einem Service Level Agreement.[16] Diese Verfügbarkeitsverpflichtung beschränkt sich jedoch regelmäßig auf die objektive Abrufbarkeit der Dienste und setzt eine funktionierende Internetverbindung zum SaaS-Anbieter voraus. Die Verantwortung für Verbindungsstörungen, die nicht im Herrschaftsbereich des SaaS-Anbieters liegen, übernimmt dieser nicht. Vertragsschlüsse setzen bei internetbasierten Diensten die Funktionsfähigkeit des Internetprotokolls damit stillschweigend voraus. Bei Problemen oder Ausfällen wird dies als allgemeines Betriebsrisiko betrachtet. Zu einer vertraglichen Haftung einzelner Beteiligter in der Übertragungskette kommt es regelmäßig nicht.

Diese Idee ließe sich auf den DIVE-Betrieb übertragen. Anwender der DIVE-Basisinfrastruktur nutzen die Blockchain – ähnlich wie das Internet – als eine gemeinsame Infrastruktur, auf deren Funktionsfähigkeit alle vertrauen. Dieses Vertrauen ist eine grundlegende Voraussetzung für die Nutzung der DIVE-Basisinfrastruktur. Den Teilnehmern ist bewusst, dass der Einsatz der Blockchain Risiken mit sich bringen kann, die sie jedoch gemeinsam tragen. Sollte es zu Fehlern auf der Blockchain kommen, wären sie wie höhere Gewalt zu werten. Jeder Teilnehmer akzeptiert das Risiko und die Unvorhersehbarkeit, die mit der Nutzung einer public-permissionless Blockchain verbunden sind. Die Anwender haben zwar Vertragsverhältnisse mit den Anbietern von Zusatzsoftware,[17] diese sind jedoch nur für die Funktionsfähigkeit der jeweiligen Software verantwortlich, nicht für Fehler des Blockchain-Protokolls.

Dieses Risiko könnte für die Anwender der DIVE-Basisinfrastruktur auch deshalb akzeptabel sein, weil auf der Blockchain selbst keine geschützten oder sensiblen Daten liegen, sondern die Blockchain lediglich als Speicherort für Hash-Werte zum Nachweis dient.[18] Dadurch werden das Risiko eines Datenmissbrauchs und damit auch das Bedürfnis einer Haftung der Blockchain-Betreiber erheblich reduziert.

Betrachtet man die Nutzung der Blockchain wie die Nutzung eines Gemeingutes, könnte dies eine nachvollziehbare

11 Vgl. zum Fall des ähnlich gelagerten Cloud-Computings Wicker, MMR 2014, 715 (716 ff.)

12 Siehe hierzu auch die Ausführungen zur DLT (Distributed Ledger Technology) als digitale Infrastruktur bei Fridgen et al. (Fraunhofer FIT) (2019): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, S. 80 f., abrufbar unter: https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1106/wi-1106.pdf. Auch für Kryptowährungen wurde schon früh die These formuliert, dass es sich um „gemeinfreie Güter" handelt, vgl. Engelhardt/Klein, MMR 2014, 355 (357)

13 Siehe auch Remer in Gramlich/Gluchowski/Horsch/Schäfer/Waschbusch, Gabler Banklexikon zum „Gemeingut", abrufbar unter https://www.gabler-banklexikon.de/definition/gemeingut-70740/version-339783

14 Bezüglich des gleich verwendeten Begriffs in § 100 Abs. 1 TKG a.F.: BT-Drs. 16/11967, 17; BGH NJW 2011, 1509 (1511); LG Göttingen K&R 2023, 763 (765); Kiparski CR 2020, 818 (823); Scheurle/Mayen/Kannenberg/Müller § 100 Rn. 9

15 Borges/Hilber (2023), BeckOK IT-Recht, 15. Ed. 1.4.2023, BGB § 434 Rn. 6

16 Heydn, MMR 2020, 435 (437)

17 Siehe hierzu oben unter 3.2.2(c)

18 Siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur"

Begründung für die fehlende Haftung der Blockchain-Betreiber liefern und ein Verständnis für die gemeinsamen Risiken, die mit der Nutzung der Blockchain-Technologie verbunden sind, schaffen. So wird die Blockchain zu einer gemeinsam geteilten Ressource, die das Fundament für die verschiedenen Anwendungen der DIVE-Basisinfrastruktur bildet. Voraussetzung für ein Gelingen ist daher die Schaffung des Vertrauens in die Technologie, wie es heute beim Internetprotokoll besteht.

3.3.2 Beschreibung der Rechtsbeziehungen zwischen den Anwendern der DIVE-Basisinfrastruktur

Während nach dem hier vorgeschlagenen Konzept zwischen den Blockchain-Betreibern und den Anwendern der DIVE-Basisinfrastruktur keine direkte rechtliche Beziehung besteht, kann es zwischen den Anwendern untereinander durchaus wichtige rechtliche Verbindungen geben. Dabei kann man zwischen den Leistungsbeziehungen zwischen den Anwendern der DIVE-Basisinfrastruktur und den Beziehungen von Anwendern der DIVE-Basisinfrastruktur und Dritten unterscheiden.

Rechtsbeziehungen zwischen den Anwendern der DIVE-Basisinfrastruktur

Die Rechtsbeziehungen zwischen den Anwendern der DIVE-Basisinfrastruktur sind durch die Dreiecksbeziehung zwischen Holder, Issuer und Verifier geprägt, wobei die rechtliche Verbindung dieser Parteien je nach Anwendungsfall teilweise unterschiedlich ausgestaltet sein kann.

i. Verhältnis zwischen Holder und Issuer

Kernelement des Verhältnisses zwischen Holder und Issuer ist die Ausstellung des Verifiable Credentials (VC) durch den Issuer für den Holder.[19] Da der Holder auf sie angewiesen ist, muss rechtlich sichergestellt werden, dass der Issuer die Ausstellung in einer Weise vornimmt, die dem Holder die Nutzung des VC im Rechtsverkehr ermöglicht. Für die Ausgestaltung dieser Verpflichtung sind zwei Optionen denkbar:

A. Gesetzliche Verpflichtung zur Generierung von Verifiable Credentials

Es wäre zunächst denkbar, für die Issuer gesetzliche Verpflichtungen zur Ausstellung von Verifiable Credentials zu schaffen. Im Falle der Verteilnetzbetreiber (VNBs) wäre es beispielsweise möglich, das gesetzliche Schuldverhältnis nach § 7 EEG um die Verpflichtung zu erweitern, VCs für Anlagenbetreiber auszustellen. Die VNBs würden dann als Issuer die Ausstellung der VCs als Teil ihrer gesetzlichen Verpflichtungen vornehmen. Vorteil einer solchen Lösung wäre, dass eine flächendeckende Anwendung der DIVE-Basisinfrastruktur leichter sichergestellt wäre, da durch die verpflichtende Attestierung jeder Anlagenbetreiber einen Anspruch auf die Generierung eines Verifiable Credentials erhält. Für viele Anwendungsfälle, die auf der DIVE-Basisinfrastruktur aufbauen könnten, ist die flächendeckende Nutzbarkeit von großem Vorteil, wenn nicht sogar Voraussetzung für einen wirtschaftlich sinnvollen Einsatz. Eine gesetzliche Verpflichtung zur Ausstellung der VCs würde mittelbar die Entwicklung und Verbreitung innovativer Anwendungsfälle und damit die Energiewende an sich fördern – bei verhältnismäßig geringem Aufwand für die VNBs und andere attestierende Akteure. Besteht eine gesetzliche Verpflichtung, eröffnet dies die Möglichkeit, bereitgestellte Software und andere technologische Ergebnisse von Anbietern von Maschinen-Identitäten, wie zum Beispiel des DIVE-Konsortiums, sowie darauf aufbauende Anwendungsfälle ausgiebig zu testen und weiterzuentwickeln.

Eine gesetzliche Verpflichtung zur Ausstellung von Credentials wird anspruchsvoller, wenn im Einzelfall auch andere Stellen als der VNB die Rolle des Issuers übernehmen sollen. So werden beispielsweise im Anwendungsfall der Flexibilitätserbringung auch Installateure und Hersteller als mögliche Issuer vorgeschlagen.[20] Während für Hersteller eine gesetzliche Verpflichtung noch denkbar ist, scheint dies für Installateure eher schwieriger umsetzbar. Falls eine gesetzliche Verpflichtung zur Ausstellung von Credentials anvisiert wird, kann es daher ratsam sein, sie grundsätzlich bei einer Stelle zu bündeln. Wählt man den VNB als zentrale Stelle für die Ausstellung der Credentials, schließt dies nicht aus, dass für einzelne Anwendungsfälle eine Beauftragung anderer Stellen durch den VNB erfolgt oder eine zusätzliche gesetzliche Verpflichtung dritter Stellen für den Anwendungsfall besteht.

Eine gesetzliche Verpflichtung sollte die Interoperabilität mit anderen IDs, insbesondere der EUDI-Wallet, im Auge behalten. Die gesetzliche Verpflichtung ist bestenfalls so zu gestalten, dass eine Verknüpfung der Asset-DID mit anderen DIDs möglich ist. Technische Spezifikationen zur EUDI-Wallet können dabei einen Einfluss haben oder als Vorlage dienen.

Eine gesetzliche Verpflichtung macht eine Gesetzesänderung erforderlich. Auch wenn die Verpflichtung aus den oben genannten Gründen Vorteile hat, kann der Gesetzgebungsprozess Zeit kosten. Ein Warten auf eine gesetzliche Regelung kann zur Folge haben, dass wichtige Innovationen zu spät kommen. Es ist

19 Siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“

20 Siehe Berichtsteil „Mehrwerte für die energiewirtschaftlichen Anwendungsfälle“

daher zu überlegen, ob kurzfristig auch eine vertragliche Verpflichtung eine gangbare Alternative sein kann.

B. Vertragliche Verpflichtung zur Generierung von Verifiable Credentials

Eine gesetzliche Verpflichtung bedarf zunächst einer Gesetzesänderung. Solange eine solche nicht vorliegt, sind die Parteien auf vertragliche Beziehungen angewiesen, wenn sie sich zur Ausstellung von Verifiable Credentials verpflichten wollen. Da das VC vom Issuer für den Holder ausgestellt wird, liegt es nahe, die Pflicht zur Ausstellung in einen Vertrag zwischen Holder und Issuer aufzunehmen. In den meisten Fällen wird ein solcher Vertrag zwischen Holder und Issuer bereits bestehen. Der VNB, der meist als Issuer auftritt, hat üblicherweise bereits einen Nutzungsvertrag mit dem Anlagenbetreiber, der als Holder auftritt. Dieser Vertrag könnte um die Verpflichtung zur Ausstellung von VCs erweitert werden. Auch Stromlieferanten, die im Anwendungsfall „Lieferantenwechsel an Ladesäulen" als Issuer fungieren, haben bereits ein Vertragsverhältnis mit den Haltern oder Fahrern von Elektrofahrzeugen, das entsprechend um die Ausstellung von Verifiable Credentials erweitert werden könnte. Diese Verträge könnten auch Regelungen zu Fristen und zur Erneuerung der VCs enthalten.

Will man auch Hersteller oder Installateure als Issuer einbinden, müssten auch hierfür entsprechende Verträge vorgesehen werden. Der Installateur könnte die Ausstellung des Credentials als Teil seines Dienst- oder Werkvertrags erbringen. Der Hersteller könnte mit Anlagenbetreibern einen entsprechenden zusätzlichen Dienst- oder Werkvertrag abschließen.

Vorteil einer vertraglichen Regelung ist, dass sie den Parteien große Gestaltungsfreiheit einräumt. Es besteht die Möglichkeit, die Umsetzung zunächst mit einer Gruppe von Holdern und Issuern zu testen. Es sollte festgehalten werden, welche technologische Grundlage für die DIVE-Basisinfrastruktur genutzt wird (beispielsweise die Nutzung der KILT Blockchain) und wie die Ausstellung eines VC abläuft. Die vertragliche Freiheit räumt den Parteien auch die Möglichkeit ein, Testzeiträume zu vereinbaren und spätere Anpassungen vorzunehmen. Kurzfristig kann die vertragliche Lösung daher eine gute Alternative sein, um die Technologie zu testen und ihre Umsetzbarkeit unter Beweis zu stellen.

ii. Verhältnis zwischen Holder und Verifier

Der Holder, beispielsweise der Anlagenbetreiber, nimmt mit seiner Anlage an Anwendungsfällen teil und interagiert dabei mit Dritten, unter anderem den Verifiern. Diesen gegenüber weist er seine Anlage mit der Asset-DID und dem VC aus. Auch Holder und Verifier vereinbaren daher, die DIVE-Basisinfrastruktur für den Identifikationsnachweis zu nutzen. Auch wenn das Rechtsverhältnis zwischen Holder und Verifier vom jeweiligen Anwendungsfall abhängt, besteht in aller Regel bereits ein vertragliches Verhältnis zwischen den Parteien, wie beispielsweise ein Stromlieferungsvertrag. Dieser Vertrag kann um eine Vereinbarung zur Nutzung der DIVE-Basisinfrastruktur erweitert werden. Im Vergleich zum übrigen Vertragsinhalt könnte die Regelung dieser Verpflichtung vergleichsweise knapp gehalten werden, sodass kein erheblicher Mehraufwand entsteht. Inhalt dieser Zusatzvereinbarung wäre die Vereinbarung, für die Identifikation der Anlage ein digitales Identitätsmanagementsystem, wie beispielsweise die DIVE-Basisinfrastruktur, zu nutzen. Es gibt dabei mehrere Möglichkeiten, wie die Identifikation über die DIVE-Basisinfrastruktur vertraglich konkret geregelt werden könnte.

A. Identifikation als Verpflichtung des Holders

Eine Option wäre es, dem Holder, also in der Regel dem Anlagenbetreiber, die vertragliche Pflicht aufzuerlegen, seine Anlage erfolgreich mittels der DIVE-Basisinfrastruktur zu identifizieren. Für den Verifier, also den Vertragspartner, hätte dies den Vorteil, dass er das Risiko von Fehlern der DIVE-Basisinfrastruktur oder der konkreten Asset-DID nicht zu tragen hätte. Allerdings könnte diese Lösung zu einer hohen Belastung für den Holder werden, da er verpflichtet sein könnte, Fehler bei oder Probleme mit der Asset-DID oder dem VC zu beheben oder die Identität der Anlage auf andere Weise nachzuweisen. Beides könnte für den Holder schwer bis gar nicht erfüllbar sein.

B. Identifikation als aufschiebende Bedingung

Eine andere Lösung könnte daher sein, dass die Parteien eine erfolgreiche Identifikation der Anlage über die DIVE-Basisinfrastruktur zur aufschiebenden Bedingung für den Vertragsschluss machen. Der Vertrag kommt erst dann zustande, wenn die Asset-DID und das VC vom Verifier akzeptiert wurden. Diese Option könnte in vielen Fällen vorzugswürdig sein, da sie sicherstellt, dass alle vertraglichen Verpflichtungen erst nach erfolgreicher Verifizierung beginnen, die Parteien also keine Verpflichtungen eingehen, falls die Identifikation über die DIVE-Basisinfrastruktur fehlschlägt. Dies würde auch zum oben beschriebenen Konzept passen, dass die Parteien auf eine Haftung der Blockchain-Betreiber verzichten, und dazu

führen, dass weniger Vertrauen in die teils noch unbekannte Blockchain-Technologie notwendig ist.

iii. Verhältnis zwischen Verifier und Issuer

Zwischen Verifier und Issuer besteht meist kein gesondertes Vertragsverhältnis. Eine unmittelbare vertragliche Haftung kommt daher regelmäßig nicht in Betracht. Es ist dennoch festzustellen, dass der Verifier auf die ordnungsgemäße Prüfung und Ausstellung der Verifiable Credentials durch den Issuer vertraut. Es spricht daher einiges für eine Vertrauenshaftung nach § 311 Abs. 3 BGB, wenn der Verifier auf die Arbeit des Issuers vertraut und dieser einen Fehler macht. Nach § 311 Abs. 3 S. 2 BGB ist eine sogenannte „Sachwalterhaftung" dann anzunehmen, wenn eine Person, die nicht selbst Vertragspartei wird, in besonderem Maße Vertrauen für sich in Anspruch nimmt und dadurch die Vertragsverhandlungen oder den Vertragsschluss erheblich beeinflusst. Hierbei kommt zudem die besondere Form einer „Expertenhaftung" in Betracht, wenn ein Dritter, auf dessen besondere Expertise ein Vertragspartner vertraut, bestimmte Tatsachen, die Grundlage des Vertrags sind, attestiert.[21] Bezüglich der Ausstellung der Verifiable Credentials lässt sich dies für den Issuer annehmen, da dieser eine Überprüfung der Daten vornehmen soll. Folge ist ein Schuldverhältnis mit Pflichten nach § 241 Abs. 2 BGB, also die Haftung für die Verletzung von Nebenpflichten. Verletzt der Issuer diese Pflichten nachweisbar, sind Schadensersatzansprüche des Verifiers gegen den Issuer möglich, wenn dieser VCs fehlerhaft ausstellt.

Bilaterale Rechtsbeziehungen bei Zusatzleistungen

Auch Hersteller und Dienstleister leisten einen essenziellen Beitrag zum Betrieb der DIVE-Basisinfrastruktur. Da sie aber mit dem Betrieb der DIVE-Basisinfrastruktur unmittelbar nichts zu tun haben, ist eine Verantwortung für den DIVE-Betrieb insoweit eher fernliegend. Etwas anderes gilt nur dann, wenn Hersteller oder Installateure in Einzelfällen die Rolle des Issuers übernehmen (siehe dazu oben unter 3.2.2(i)(A)(b)). Die Leistungen der Hersteller und Dienstleister erfolgen stattdessen in Erfüllung eigenständiger bilateraler Verträge mit den Anwendern der DIVE-Basisinfrastruktur. Die Art dieser Verträge unterscheidet sich jedoch je nach der Art der konkreten Leistungserbringung.

i. Verträge mit Herstellern und Händlern

Hersteller und Händler schließen in der Regel Kaufverträge über Anlagen mit Krypto-Chip oder eigenständige Krypto-Devices für die Aufrüstung bestehender Anlagen mit den Anlagenbetreibern, in diesem Fall mit Anwendern der DIVE-Basisinfrastruktur.

Die Hardwarehersteller und Händler schulden dabei die technische Funktionsfähigkeit ihrer Produkte. Sie haften jedoch nicht unmittelbar für den Betrieb der DIVE-Basisinfrastruktur. Ihre Haftung beschränkt sich auf Mängelhaftung im Rahmen des Kaufvertrags. Sollten Mängel am Krypto-Device auftreten, die die Teilnahme an der DIVE-Basisinfrastruktur zeitweise verhindern, könnten grundsätzlich Schadensersatzansprüche durch den Vertragspartner geltend gemacht werden, wobei der betroffene Anwender der DIVE-Basisinfrastruktur den Eintritt des Schadens bei sich nachweisen muss.

ii. Verträge mit Softwareherstellern

Ähnliches gilt für Anbieter von Software, die für den Zugang zur, die Einspeicherung von Daten in die und das Auslesen von Daten aus der DIVE-Basisinfrastruktur verwendet wird. Auch hier schulden die Softwarehersteller lediglich die abstrakte Funktionsfähigkeit der Software. Wird Software gezielt für den Einsatz in der DIVE-Basisinfrastruktur beworben und hierfür auch bezahlt, werden die Anwender der DIVE-Basisinfrastruktur in der Regel einen Anspruch darauf haben, dass die Software die versprochene Funktion, also auch die Kommunikation mit der DIVE-Basisinfrastruktur, erfüllen kann. Auch hier sind Mängelansprüche denkbar, wenn die Software zeitweise nicht in der Lage ist, den Zugang zur oder die Kommunikation mit der DIVE-Basisinfrastruktur zu gewährleisten und dem Anwender dadurch Schäden entstehen.

Wird Software zum Zugang zur DIVE-Basisinfrastruktur unter Open-Source-Lizenz kostenlos zur Verfügung gestellt, ist eine Haftung der Entwickler nur eingeschränkt anzunehmen. Da es sich hier oft um eine Schenkung handeln dürfte[22] und die Herausgeber nach § 521 BGB dann nur für Vorsatz und grobe Fahrlässigkeit haften, wird es praktisch nur selten zu Ansprüchen gegen die Entwickler kommen.[23] Dies dürfte jedoch auch für die Anwender der DIVE-Basisinfrastruktur tragbar sein, solange alternative Angebote für den Zugang zu ihr zur Verfügung stehen.

iii. Verträge mit Dienstleistern

Dienstleister erbringen Leistungen, die sich auf die Installation und Anmeldung der Hardware in der DIVE-Basisinfrastruktur beziehen. Diese Leistungen werden in der Regel durch Dienst- oder Werkverträge mit den Anwendern der DIVE-Basisinfrastruktur, insbesondere den Anlagenbetreibern, geregelt. Auch diese Verträge sind nur bilateral und betreffen die konkrete Leistung der Installation oder Einrichtung der Anlage in der DIVE-Basisinfrastruktur. Dienstleister haften nicht für den Betrieb der DIVE-Basisinfrastruktur selbst, sondern nur für die ordnungsgemäße Erbringung ihrer spezifischen Leistungen. Sollte es zu einer fehlerhaften Installation oder Einrichtung kommen, können jedoch auch hier grundsätzlich Schadensersatzansprüche geltend gemacht werden, sofern durch die mangelhafte Leistung die Teilnahme an der DIVE-Basisinfrastruktur beeinträchtigt wird, den Anwendern ein Schaden entsteht und den Dienstleistern ein Verschulden vorzuwerfen ist.

21 MüKoBGB/Emmerich, 9. Aufl. 2022, BGB § 311 Rn. 216

22 Redeker in Redeker, IT-Recht, Rn. 623; Auer-Reinsdorff/Conrad/Auer-Reinsdorff/Kast, § 9 Rn. 36

23 Raue, NJW 2017, 1841 (1843)

3.4 Haftungsrechtliche und regulatorische Herausforderungen

Die oben dargestellte Trennung des Blockchain-Betriebs von den Anwendern der DIVE-Basisinfrastruktur und der Verzicht auf eine verantwortliche Zentralstelle bringt haftungsrechtliche und regulatorische Herausforderungen mit sich, die im Folgenden beschrieben und für die verschiedene Lösungswege aufgezeigt werden. Dabei wird von dem oben beschriebenen Aufbau der Infrastruktur auf Basis einer offenen Blockchain ausgegangen. Alternative Architekturansätze, für die die Schaffung einer Zentralstelle, beispielsweise in Gestalt einer zentralen Betreibergesellschaft, eine geeignete Lösung sein könnte, werden mitgedacht, weswegen dieser Ansatz ebenfalls kurz skizziert wird.

3.4.1 Fehlende Zentralstelle als Haftungs- und Investitionsrisiko

Bei einer Behandlung der dezentralen Architektur der DIVE-Basisinfrastruktur als Gemeingut bestehen keine Haftungsansprüche gegen einen Betreiber. In der Folge könnten Investitionen in eine solche Infrastruktur ausbleiben, da das Risiko als zu hoch eingeschätzt wird. Das Vertrauen muss daher durch Aufklärung und Überzeugung in die Sicherheit der Technologie hergestellt werden.

Eine klare Zuordnung der Verantwortlichkeit für den Blockchain-Betrieb könnte diese Probleme lösen. Dabei ist aber festzuhalten, dass eine solche Lösung, beispielsweise durch die Einrichtung einer Betreibergesellschaft oder einer ähnlichen zentralen Instanz, dem Grundkonzept der public-permissionless Blockchain, die auf Dezentralität und Unabhängigkeit aufbaut, zuwiderlaufen würde. Eine Blockchain, die zentral verwaltet wird, beispielsweise eine private-permissioned Blockchain mit PoA-Verfahren (Proof of Authority), ist eben nicht mehr das dezentrale und führungslose Register, das ohne Intermediär auskommen möchte. Rechtlich besteht auch zunächst kein zwingendes Erfordernis für die Schaffung einer gesonderten gesellschaftsrechtlichen oder vertraglichen Basis für den Blockchain-Betrieb. Den Parteien steht es grundsätzlich frei, auf vertragliche Vereinbarungen bewusst zu verzichten. Als Schutzmechanismus bleiben deliktische Ansprüche, die jedoch ein nachweisbares Verschulden von einzelnen Akteuren erfordern. In Fällen, in denen Akteure den Betrieb jedoch vorsätzlich oder fahrlässig beeinträchtigen, könnten unter Umständen Haftungsansprüche entstehen. Dies bedeutet für Anwender und Investoren zwar ein gewisses Maß an rechtlicher Absicherung, jedoch ist dies gegenüber konventionellen Softwarelösungen, wie beispielsweise Cloud-Infrastrukturen, geringer.

Für eine erfolgreiche Durchdringung des Marktes und Etablierung der Technologie müssen gegenüber diesem (potenziell vorübergehenden) Nachteil die Vorteile einer Blockchain-Lösung sowie das Vertrauen in die Funktionalität der Lösung schwerer wiegen. Eine Lösung ohne die Schaffung einer vertraglich verantwortlichen Stelle wertet das Vertrauen in die dezentrale Technologie selbst höher als das Vertrauen in einen bestimmten Vertragspartner. Dies erfordert – gerade in der Anfangsphase – jedoch ein tiefes Verständnis der Blockchain-Technologie seitens der Akteure und gegebenenfalls wesentliche Aufklärungs- und Überzeugungsarbeit. Die Teilnehmer der Anwendungsfälle müssen die zugrunde liegende Blockchain so gut verstehen, dass sie von deren Ausfallsicherheit und Robustheit überzeugt und daher bereit sind, auf einen haftbaren Vertragspartner zu verzichten. Mit anderen Worten: Das Risiko und die Folgen eines möglichen Ausfalls der DIVE-Basisinfrastruktur müssen als so gering eingestuft werden, dass die Vorteile bei Teilnahme am Anwendungsfall überwiegen.

Im weiteren Verlauf können dafür auch (große) Vorbilder in der Praxis, die auf die Technologie setzen, vertrauensstiftend sein. Sobald sich zeigt, dass die Technologie funktioniert, tritt das notwendige technologische Verständnis möglicherweise in den Hintergrund und die Nutzung wird – wie beim Internet – zu einer Selbstverständlichkeit. Es kann daher lohnenswert sein, einzelne große Akteure für Testprojekte zu gewinnen, die die Nutzung der DIVE-Basisinfrastruktur auf der Grundlage einer Blockchain vorleben.

Ein wesentliches Argument für den Verzicht auf einen Vertragspartner ist, dass keine Klardaten in der Blockchain gespeichert werden. Ein Ausfall der DIVE-Basisinfrastruktur würde die Teilnahme an den jeweiligen Anwendungsfällen zeitweise erschweren oder unmöglich machen, jedoch nicht unbedingt zu erheblichen wirtschaftlichen Verlusten führen. Um dies sicherzustellen, sollten Anwendungsfälle die Möglichkeit eines Ausfalls der DIVE-Basisinfrastruktur aber einkalkulieren und über Notfallmaßnahmen nachdenken, um dieses Risiko weiter zu senken.

3.4.2 IT- und Cybersicherheitsrecht

Beim Betrieb der DIVE-Basisinfrastruktur auf Basis einer Blockchain ohne zentralen Betreiber sind auch IT- und cybersicherheitsrechtliche Fragen zu beachten. Dabei ist zu erörtern, inwiefern die Bestimmungen des IT- und Cybersicherheitsrechts auf den Betrieb der DIVE-Basisinfrastruktur Anwendung finden und inwiefern sich daraus ergebende Pflichten erfüllt werden könnten. Die dezentrale Struktur des Betriebs schafft dabei einerseits rechtliche Probleme, könnte jedoch gleichzeitig auch als Lösung der IT- und cybersicherheitsrechtlichen Bedenken gesehen werden.

Die dezentrale Verteilung der Angriffsflächen der DIVE-Basisinfrastruktur eröffnet Raum für das Argument, dass keine sicherheitsrelevante Anlage oder Einrichtung vorliegt und die Vorschriften des IT- und Cybersicherheitsrechts daher keine Anwendung finden. Wählt man dagegen doch den Weg einer zentralen Betreibergesellschaft, muss man sich mit den sicherheitsrechtlichen Vorschriften auseinandersetzen. Die Zentralstelle müsste dann zumindest die Verpflichtungen für „wichtige Einrichtungen“ nach der NIS-2-Richtlinie und bei wachsender Größe potenziell auch die Pflichten für Betreiber kritischer Anlagen nach dem Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITISDachG) erfüllen.

Rechtsgrundlagen und Adressaten des IT- und Cybersicherheitsrechts

Auf europäischer Ebene gab es zuletzt zwei wichtige Richtlinien zur Regulierung Kritischer Infrastrukturen (KRITIS): Mit der NIS-2-Richtlinie[24] soll die Cybersicherheit in insgesamt 18 Sektoren sichergestellt werden. Der Fokus liegt hier auf der Prävention von Gefahren durch mangelnde Cybersicherheit und Informationstechnik. Parallel dazu soll durch die CER-Richtlinie[25] die physische Resilienz der kritischen Einrichtungen sichergestellt werden. Hier geht es um die Ausfallsicherheit auch im Falle eines Angriffs. Die Richtlinien haben damit parallel laufende Ziele. Ihre Umsetzung in nationales Recht war bis zum 17. Oktober 2024 vorgeschrieben, ist jedoch verzögert.

In Deutschland fand die letzte Aktualisierung der Regelungen zu Kritischen Infrastrukturen im Mai 2021 mit dem IT-Sicherheitsgesetz 2.0 statt. Demnach finden sich die wesentlichen Regelungen im BSI-Gesetz und die Konkretisierung in der KRITIS-Verordnung des Bundesinnenministeriums.

Für die Umsetzung der neuen Vorgaben der europäischen Richtlinien liegen derzeit Entwürfe für zwei Gesetze vor: Die Umsetzung der NIS-2-Richtlinie ist mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) geplant. Es wird die Regelungen des BSI-Gesetzes voraussichtlich erweitern. Für das NIS2UmsuCG wurde ein Regierungsentwurf am 2. Oktober 2024 verabschiedet.[26] Die Umsetzung der CER-Richtlinie ist mit dem KRITIS-DachG geplant. Der Referentenentwurf vom 21. Dezember 2023[27] sieht vor, dass die Bundesregierung bis zum 17. Januar 2026 eine Strategie zur Verbesserung der Resilienz Kritischer Infrastrukturen verabschieden soll.

i. Betreiber kritischer Anlagen und Vertrauensdiensteanbieter als Adressaten

Die Begriffsdefinitionen weichen in den genannten Gesetzen in der Formulierung leicht ab, in ihrem Kerngehalt sind sie jedoch identisch:

- **Betreiber kritischer Anlagen** ist „eine natürliche oder juristische Person oder eine rechtlich unselbständige [sic] Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt“[28], wobei

- eine **Anlage** „eine Betriebsstätte, sonstige ortsfeste Installation, Maschine, Gerät und sonstige ortsveränderliche technische Installation“[29] und

- eine **Kritische Anlage** „eine Anlage, die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“[30].

Die Gesetze nennen jeweils eine Reihe von Sektoren, für die die Einordnung als Kritische Infrastruktur in Betracht kommt. Übereinstimmend ist dabei der Bereich Informationstechnik und Telekommunikation genannt. Zu den genannten Anbietern zählen ausdrücklich auch Vertrauensdiensteanbieter nach Art. 3 Nr. 19 eIDAS-VO[31]. Kritische Infrastruktur sind diese nur, wenn sie bestimmte Schwellenwerte hinsichtlich ihrer Nutzerzahlen erreichen. Diese müssen noch durch Rechtsverordnung des Innenministeriums festgelegt werden. Der aktuelle Entwurf des KRITIS-Dachgesetzes sieht einen Regelschwellenwert von 500.000 zu versorgenden Einwohnerinnen und Einwohnern vor. Zu beachten ist jedoch, dass Vertrauensdiensteanbieter auch dann, wenn sie keine „kritische Anlage“ betreiben, nach § 28 Abs. 2 Nr. 1 BSIG-E als „wichtige Einrichtung“ eingeordnet werden, unabhängig davon, wie groß das Unternehmen des Diensteanbieters ist. Auch von Betreibern wichtiger Einrichtungen sind Maßnahmen zur Cybersicherheit zu treffen.

ii. Pflichten der Adressaten

Betreiber Kritischer Infrastrukturen sind verpflichtet, die Anlage zu registrieren und Mindeststandards hinsichtlich der technischen und organisatorischen Sicherheit einzuhalten und dies gegenüber der zuständigen Behörde (derzeit BSI) nachzuweisen.[32] Betreiber sind zur Kooperation mit dem BSI verpflichtet. Das BSI kann Überprüfungen bei den Betreibern der Kritischen Infrastrukturen durchführen.

Der Pflichtenkatalog von „wichtigen Einrichtungen“, die keine kritische Anlage betreiben, ist eingeschränkter. Auch hier sind jedoch technische und organisatorische Sicherheitsmaßnahmen nachzuweisen.

Anwendbarkeit auf die DIVE-Basisinfrastruktur

Voraussetzung für eine Anwendbarkeit der Vorschriften ist, dass mit der DIVE-Basisinfrastruktur eine „wichtige Einrichtung“ oder „kritische Anlage“ betrieben wird, die die erforderlichen Grenzwerte erreicht und deren Ausfall zu einer Gefährdung für wirtschaftliche Tätigkeiten führen würde.

Solange mit der DIVE-Basisinfrastruktur keine größere Marktdurchsetzung erreicht wird, sind die strengen Vorschriften für kritische Anlagen nicht relevant. Da die DIVE-Basisinfrastruktur

24 Richtlinie (EU) 2022/2555, abrufbar unter https://eur-lex.europa.eu/eli/dir/2022/2555
25 Richtlinie (EU) 2022/2557, abrufbar unter https://eur-lex.europa.eu/eli/dir/2022/2557/oj
26 https://dserver.bundestag.de/btd/20/131/2013184.pdf
27 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html
28 So in § 2 Nr. 1 des Referentenwurfs zum KRITISDachG vom 21.12.2023
29 So in § 2 Nr. 2 des Referentenwurfs zum KRITISDachG vom 21.12.2023
30 So in § 2 Nr. 3 und 4 des Referentenwurfs zum KRITISDachG vom 21.12.2023
31 Verordnung (EU) Nr. 910/2014, abrufbar unter: http://data.europa.eu/eli/reg/2014/910/oj
32 Derzeit geregelt in § 8a Abs. 3 BSI-Gesetz

jedoch längerfristig eine flächendeckende Verbreitung anstrebt, ist zumindest in der Gesamtheit der Teilnehmer mit einem Erreichen des Regelschwellenwertes zu rechnen. Für eine Einordnung als wichtige Einrichtung in Form eines Vertrauensdiensteanbieters wäre das Erreichen der Grenzwerte nicht erforderlich, sodass hier die Voraussetzungen von Beginn an gelten würden. Es müsste dann jedoch sowohl eine kritische Anlage bzw. wichtige Einrichtung als auch ein Betreiber dieser Anlage oder Einrichtung identifizierbar sein.

i. DIVE-Basisinfrastruktur als kritische Anlage oder wichtige Einrichtung

Es ist zwar möglich, bei der DIVE-Basisinfrastruktur eine Anlage oder Einrichtung auszumachen. Zumindest für die Anlagen ist es jedoch schwierig, eine einzelne Anlage als „kritisch“ einzustufen.

Eine detaillierte Aufzählung der kritischen Anlagen wird der noch kommenden Verordnung durch das Innenministerium vorbehalten bleiben. Bereits nach geltender Rechtslage zählen aber „Anlagen zur Erbringung von Vertrauensdiensten“ zu den kritischen Anlagen. Auch die NIS-2-Richtlinie zählt Vertrauensdiensteanbieter ausdrücklich zu den Adressaten und fordert hierfür auch kein Erreichen von Schwellenwerten. Der Begriff der **Vertrauensdienste** ist in der eIDAS-VO geregelt und erfasst unter anderem alle Dienste zur „Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln“ sowie zur „Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten“. Die eIDAS-VO ist technologieneutral[33] und erfasst grundsätzlich auch Vertrauensdienste, die auf Blockchain-Basis aufgebaut sind. Es spricht daher viel dafür, dass die DIVE-Basisinfrastruktur einen solchen Dienst darstellt, da sie die Erstellung, Überprüfung und Validierung von Zertifikaten maßgeblich ermöglicht. Auch wenn Signaturen, Siegel und Zertifikate nicht auf der Blockchain direkt aufbewahrt werden, ist ihr weiterer Einsatz vom Betrieb der DIVE-Basisinfrastruktur abhängig.

Wenn man die DIVE-Basisinfrastruktur als einen solchen Dienst begreift, so müsste es auch eine „Anlage“ oder „Einrichtung“ geben, die diesen Dienst bereitstellt. Ermöglicht wird die Erstellung, Überprüfung und Validierung der Zertifikate durch das zugrunde liegende Protokoll (im DIVE-Projekt das KILT-Protokoll) und die dezentrale Speicherung der Registereinträge durch die Nodes. Als Anlage oder Einrichtung kämen im dezentralen Blockchain-System daher nur die einzelnen Speichergeräte der Nodes in Betracht, die eine Kopie der Blockchain halten. Man könnte annehmen, dass sie jeweils eine kritische Anlage oder wichtige Einrichtung darstellen. Gegen das Vorhandensein einer kritischen Anlage kann man bereits hier Zweifel anmelden und argumentieren, dass der Ausfall eines Nodes gerade nicht zur geforderten Beeinträchtigung führen würde. Folglich läge eine kritische Anlage wohl nur dann vor, wenn man die Anlagen der Nodes als einen Verbund betrachten würde, der von einem Betreiber kontrolliert wird. Diese tatsächliche Einflussnahme durch eine Zentralstelle ist jedoch ausdrücklich nicht vorgesehen.

Anders kann dies bei der „wichtigen Einrichtung“ aussehen, da hier der Vertrauensdiensteanbieter unabhängig vom Betrieb einer kritischen Anlage erfasst ist. Auch hier müsste jedoch ein Betreiber als Anbieter des Vertrauensdienstes auftreten.

ii. DIVE-Basisinfrastruktur ohne Betreiber der Anlage oder Einrichtung

Selbst wenn man eine kritische Anlage oder das Vorhandensein einer wichtigen Einrichtung annimmt, lässt sich hierfür in der DIVE-Basisinfrastruktur kein Betreiber ausmachen. Die Definition fordert einen „bestimmenden“ Einfluss auf die Anlage. Einen solchen gibt es im Blockchain-System faktisch nicht. Denkbar wäre es, die Stelle, die das Blockchain-Protokoll entwickelt hat, als bestimmend zu betrachten, da die Nodes den Regeln dieses Protokolls bei der Verarbeitung folgen. Allerdings besteht keine tatsächliche und rechtliche Einwirkungsmöglichkeit. Auch eine wirtschaftliche Abhängigkeit von den Erstellern des Protokolls besteht nicht, da diese nicht für die Bezahlung der Nodes verantwortlich sind. Einen Betreiber im Sinne der KRITIS-Gesetze wird es daher nicht geben. Gleiches wird wohl für den Anbieter des Vertrauensdienstes gelten. Zwar könnte man den Issuer jeweils als solchen betrachten, wobei der Vertrauensdienst dann auf die Tätigkeit im Einflussbereich des Issuers beschränkt bleiben dürfte. Der Anbieter eines Vertrauensdienstes, der die ganze DIVE-Basisinfrastruktur erfasst, ist dagegen unmittelbar nicht erkennbar.

iii. Verteilter Betrieb als Argument gegen die Anwendbarkeit

Die Anwendbarkeit von IT- und cybersicherheitsrechtlichen Vorschriften auf potenziell kritische Anlagen, die dezentral betrieben werden, ist derzeit nicht abschließend geklärt. Es lässt sich jedoch vertreten, dass der Umstand, dass es keinen einzelnen Betreiber gibt, der die notwendigen Grenzwerte erreicht oder als Anbieter eines Vertrauensdienstes identifizierbar wäre, eine Anwendung der Vorschriften ausschließt. Dieses Ergebnis könnte durchaus dem gesetzgeberischen Willen entsprechen. Denn da das Risiko in der Blockchain verteilt ist, gibt es gerade keine Kritische Infrastruktur und auch keinen Betreiber einer wichtigen Einrichtung. Keiner der Nodes ist für sich gesehen „wichtig“ genug, als dass die strengen Vorschriften des IT- und Cybersicherheitsrechts Anwendung finden müssten. Eine schützenswerte Schwachstelle gibt es nicht. Ein „Betreiber“ müsste daher auch gar nicht zwingend gefunden werden.

33 Siehe Erwägungsgrund Nr. 26 und 27 eIDAS-VO

Diese Argumentation soll jedoch nicht den Blick auf ein bestehendes Restrisiko versperren. Der Gesetzgeber macht durch die ausdrückliche Nennung von Vertrauensdiensten als wichtige Einrichtung deutlich, dass der Schutz dieser Systeme von besonderer Bedeutung ist. Es ist nicht ausgeschlossen, dass sich das BSI, das nach dem aktuellen Entwurf des NIS2UmsuCG für die Aufsicht zuständig sein wird, mit dem oben skizzierten Ergebnis nicht zufriedengibt und die gesetzlich geforderte Absicherung durchsetzen will. Die weitere regulatorische Entwicklung bezüglich dezentraler Systeme unter den maßgeblichen Vorschriften des IT- und Cybersicherheitsrechts sollte daher eng verfolgt werden. Denkbar ist auch ein proaktiver Austausch mit den zuständigen Behörden zu dieser Frage. In jedem Fall wäre eine gesetzgeberische Klarstellung dazu, ob die hier beschriebenen dezentralen Systeme von den Vorschriften des Cybersicherheitsrechts ausgenommen sind, wünschenswert.

3.4.3 Datenschutzrecht

Das geltende Datenschutzrecht schafft für die Umsetzung von Projekten auf einer öffentlichen Blockchain Hürden. Diese Hürden können durch weitgehenden Verzicht auf die Speicherung von personenbezogenen Daten auf dem Blockchain-Layer abgebaut werden. Langfristige Sicherheit für die Umsetzung kann jedoch nur eine gesetzgeberische Klarstellung zu Verantwortlichkeiten und Löschansprüchen auf der Blockchain geben. Bis dahin sind verbleibende Risiken entweder in Kauf zu nehmen oder durch Wahl einer zentralen Lösung zu vermeiden.

Rechtsgrundlagen

Die zentralen Rechtsvorschriften für die Zulässigkeit der Verarbeitung personenbezogener Daten innerhalb der Europäischen Union finden sich in der EU-Datenschutz-Grundverordnung (DSGVO). Sie verfolgt das Ziel der Vollharmonisierung und verdrängt grundsätzlich alle nationalen Vorschriften zum Datenschutz. Ausnahmen sind durch sogenannte Öffnungsklauseln vorgesehen. Soweit hierdurch zugelassen, gilt daher auf nationaler Ebene ergänzend das Bundesdatenschutzgesetz (BDSG).

Die DSGVO legt ihre Verpflichtungen grundsätzlich dem für die Datenverarbeitung „Verantwortlichen“ auf, wobei dieser Begriff in Art. 4 Nr. 7 DSGVO näher definiert wird. Für die Verarbeitung personenbezogener Daten gilt ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Personenbezogene Daten dürfen demnach nur bei Vorliegen einer Rechtsgrundlage verarbeitet werden.

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Die Blockchain-Lösung im Konflikt mit dem Datenschutzrecht

Das geltende Datenschutzrecht stellt unveränderliche dezentrale Systeme wie Blockchain-Register vor wesentliche rechtliche Herausforderungen. Dies liegt zum einen an der Tatsache, dass die DSGVO von einem zentralen Verantwortlichen ausgeht, zum anderen an der Unveränderlichkeit von Blockchain-Einträgen selbst.

i. Dezentrales Register und zentrale Verantwortlichkeit

Während der Blockchain-Layer der DIVE-Basisinfrastruktur eine Verteilung der Verantwortlichkeit auf eine Vielzahl von Stellen anstrebt, geht die DSGVO im Grundsatz von einem zentralen Verantwortlichen aus. Adressat der Pflichten aus der DSGVO ist grundsätzlich der für die Verarbeitung der Daten Verantwortliche.[34] Für den von der Datenverarbeitung Betroffenen ist der Verantwortliche Anspruchsgegner zur Erfüllung der datenschutzrechtlichen Pflichten. Für Verstöße ist grundsätzlich der Verantwortliche haftbar. Aus diesen Gründen ist die Feststellung des Verantwortlichen von besonderer Bedeutung. Dabei ist neben der alleinigen Verantwortlichkeit einer Stelle auch eine gemeinsame Verantwortlichkeit mehrerer Stellen nach Art. 26 DSGVO möglich. Der Verantwortliche kann sich zudem Auftragsverarbeitern (Art. 28 DSGVO), die nach Weisung des Verantwortlichen tätig werden, bedienen.

Nach Art. 4 Nr. 7 DSGVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für die Frage, wer „entscheidet“, kommt es darauf an, wer tatsächlichen Einfluss auf die Entscheidung nimmt. Einer formalen rechtlichen Benennung eines Entscheidungsträgers kommt dabei nur Indizwirkung zu.[35] Mit der Entscheidung über den Zweck ist diejenige über das erwartete oder geplante Ergebnis der Verarbeitung gemeint, die Entscheidung über die Mittel ist diejenige über die Art und Weise, wie dieses Ergebnis erreicht wird.[36] Der Begriff des Mittels umfasst dabei unter anderem die Entscheidung über die technischen Methoden und den Umfang der Verarbeitung, die Zugangsberechtigung zu den Daten oder die Löschfristen.[37]

34 Sydow/Marsch/Raschauer, Art. 4 Rn. 114

35 Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 00264/10/DE., S. 15

36 Ebd., S. 16

37 Ebd., S. 17

Regelmäßig kommt es bei der Führung eines dezentralen Registers zu mehreren Verarbeitungsvorgängen. Relevant sind insbesondere das Einpflegen neuer Daten ins Register, das Auslesen bestehender Daten und die fortdauernde Speicherung der Daten im Register. Bezüglich des Einpflegens und Auslesens von Daten wird man feststellen können, dass regelmäßig allein die jeweils einpflegende oder auslesende Stelle über die Zwecke und Mittel der Verarbeitungsvorgänge entscheidet. Im Falle des DIVE-Projekts wären dies jeweils Holder, Issuer und Verifier. Eine Herausforderung kann dagegen die Bestimmung des Verantwortlichen für diejenigen Datenverarbeitungen sein, die von den Teilnehmern des dezentralen Netzwerks zur Erstellung und Fortführung der dezentralen Datenbank vorgenommen werden.[38]

Entscheidet man sich, wie im DIVE-Projekt, dafür, Daten auf einer permissionless DLT-Infrastruktur (Distributed Ledger Technology) zu verarbeiten, so wird man unmittelbar keine Zentralinstanz als Kontrollstelle bei einer stattfindenden personenbezogenen Datenverarbeitung identifizieren können. In der rechtswissenschaftlichen Literatur überwiegt die Auffassung, dass hier sämtliche Nodes, also alle, die eine Kopie der dezentralen Datenbank öffentlich bereithalten, als Verantwortliche anzusehen sind.[39]

Dafür spricht, dass die Nodes die Transaktionen im Netzwerk weitergeben und neue Daten in die eigene Kopie des Registers nach den Regeln des Systems einpflegen. Die Nodes üben damit die Schlüsselrolle bei der Verarbeitung der Daten in der Blockchain aus. Die Nodes werden hierzu von keiner anderen Stelle unmittelbar angewiesen. Vielmehr entscheiden sie selbstbestimmt, ob sie die Daten auf ihren Geräten nach den Regeln der von ihnen genutzten Software verarbeiten möchten. Jeder Node hätte grundsätzlich auch die Möglichkeit, die Daten gar nicht oder nach den Regeln eines anderen Protokolls zu verarbeiten. Es wird daher argumentiert, dass jeder Node mit der Wahl, seine Rechengeräte nach den Regeln eines bestimmten Blockchain-Protokolls arbeiten zu lassen, über die Zwecke und Mittel der bei ihm stattfindenden Datenverarbeitungen entscheidet und damit die Voraussetzungen des datenschutzrechtlich Verantwortlichen für die Speicherung auf seinem Node erfüllt.

Es sprechen gute Gründe dafür, dass die Nodes auf einer permissionless DLT-Plattform dabei nicht als gemeinsame Verantwortliche nach Art. 26 DSGVO handeln. Eine gemeinsame Verantwortlichkeit würde nämlich erfordern, dass die Entscheidung über Zwecke und Mittel der Datenverarbeitung von allen Nodes gemeinsam getroffen wird. Tatsächlich kommt es auf einer permissionless DLT-Plattform aber regelmäßig nicht zu einer Absprache zwischen den Nodes. Jeder entscheidet autonom über die Art und Weise, wie er seine datenverarbeitenden Geräte einsetzt und nach welchem Blockchain-Protokoll er diese Daten verarbeiten lässt. Eine Einordnung der Nodes als Auftragsverarbeiter würde erfordern, dass eine andere Stelle den Nodes Weisungen für die Verarbeitung erteilt. Dies ist jedoch nicht ersichtlich. Zwar gibt das Blockchain-Protokoll den Nodes die Regeln der Verarbeitung faktisch vor, sie werden jedoch von keiner Stelle zur Nutzung dieses Protokolls beauftragt.

Ein entscheidender Einfluss der Entwickler des Blockchain-Protokolls ist dennoch erkennbar. Neben den Nodes könnte man daher auch sie als (gemeinsam) Verantwortliche für die Datenverarbeitung ansehen. Die Entwickler entscheiden mittelbar durch die Regeln des Protokolls, nach welchen Regeln die Nodes, die sich für eine Teilnahme entscheiden, die Daten verarbeiten. Beide Argumentationen führen aber zu unbefriedigenden Ergebnissen. Die Ersteller des Blockchain-Protokolls können nicht beeinflussen, durch wen und wo es eingesetzt wird und personenbezogene Daten verarbeitet werden. Die Nodes könnten lediglich auf die Verarbeitung ihrer eigenen Systeme einwirken, würden dadurch aber für die von Datenschutzverletzungen betroffenen Personen wenig bewirken können. Weder Nodes noch Protokoll-Entwickler könnten als Verantwortliche die datenschutzrechtlichen Pflichten (siehe sogleich) wirksam erfüllen.

ii. Immutabilität und Lösch- und Berichtigungsansprüche

Eine weitere große datenschutzrechtliche Herausforderung für den Einsatz von DLT für die Registerführung stellt ihre technisch bedingte Immutabilität, also die grundsätzliche Unveränderbarkeit der Registerinhalte, vor dem Hintergrund der Betroffenenrechte auf Berichtigung und Löschung dar.

Die betroffene Person hat nach Art. 16 S. 1 DSGVO das Recht, dass sie betreffende unrichtige personenbezogene Daten unverzüglich berichtigt werden. Zudem hat sie das Recht, dass die Daten auf ihren Wunsch unverzüglich gelöscht werden, soweit hierfür ein in Art. 17 Abs. 1 DSGVO aufgezählter Löschungsgrund vorliegt. Demnach kann eine Löschung verpflichtend sein, wenn die Daten für die Zwecke ihrer Erhebung nicht mehr erforderlich sind, die betroffene Person eine von ihr gegebene Einwilligung zur Verarbeitung der Daten widerruft und keine andere Rechtsgrundlage für die Verarbeitung mehr besteht, die betroffene Person rechtmäßig von ihrem Widerspruchsrecht gegen die Verarbeitung der Daten Gebrauch macht, die Datenverarbeitung unrechtmäßig erfolgte oder die Löschung der Daten zur Erfüllung einer rechtlichen Verpflichtung aus dem Unionsrecht

38 Hierzu auch Wimmer, EnWZ 2020, 387 (391);

39 Martini/Weinzierl, NVwZ 2017, 1251 (1253 f.); Bitkom, Blockchain und Datenschutz – Faktenpapier, S. 28 f. Andere – Schrey/Thalhofer, NJW 2017, 1431 (1433 f.); Bechtolf/Vogt, ZD 2018, 66 (69) – gehen davon aus, dass alle „Teilnehmer" des Netzwerks Verantwortliche sind, wobei der Begriff hier synonym zum Begriff „Node" verwendet wird, womit letztlich die gleiche Ansicht vertreten wird.

oder dem Recht der Mitgliedstaaten, der der Verantwortliche unterliegt, erforderlich ist.

Diesen Verpflichtungen könnte beim Betrieb der DIVE-Basisinfrastruktur nicht ohne Weiteres nachgekommen werden. Auf einer DLT-Plattform ist eine nachträgliche Änderung des Inhalts des dezentralen Registers ausgeschlossen. Dies ist notwendig, um Manipulationen zu verhindern und damit der dezentrale Betrieb des Registers überhaupt erst ermöglicht wird. Es leuchtet damit unmittelbar ein, dass bei Speicherung von personenbezogenen Daten in diesem Register die Rechte des Betroffenen auf Löschung oder Berichtigung nicht erfüllt werden können.

Das DIVE-Projekt mit minimal erforderlichen personenbezogenen Daten

Aus den oben genannten Gründen ist die Speicherung von personenbezogenen Daten auf dem Blockchain-Layer im DIVE-Projekt mit rechtlichen Risiken verbunden. Will man das Projekt auf einer public-permissionless Blockchain aufbauen, sollte daher auf die Speicherung personenbezogener Daten nach Möglichkeit verzichtet werden. Aufgrund der teils weit verstandenen Definition des Begriffs „personenbezogene Daten“ ist ein gänzlicher Verzicht auf einen Personenbezug aber praktisch kaum umsetzbar. Das DIVE-Projekt wählt jedoch einen Ansatz, der den Umfang der personenbezogenen Informationen auf dem Blockchain-Layer auf das absolut erforderliche Minimum beschränkt und damit die datenschutzrechtlichen Risiken weitestmöglich reduziert.

Der Begriff der personenbezogenen Daten bezieht sich auf Informationen, die einer natürlichen Person zugeordnet werden können. Dabei genügt es bereits, wenn der jeweilige Betrachter weiß, dass eine bestimmte Information einer natürlichen Person zugeordnet werden kann. Hierbei darf nicht nur der reine Datensatz auf der Blockchain, sondern es müssen auch alle Informationen, die dem Betrachter (auch off-chain) zur Verfügung stehen, berücksichtigt werden.

Daten sind erst dann anonym und somit nicht mehr personenbezogen, wenn es realistisch ausgeschlossen ist, dass die Verbindung zwischen Information und Person hergestellt werden kann – selbst unter Zuhilfenahme aller verfügbaren Zusatzinformationen.

Die Einträge auf dem Blockchain-Layer sind verhasht. Isoliert betrachtet kann ihnen keiner eine Information über eine Person entnehmen. Es ließe sich daher argumentieren, dass sie für die meisten Betrachter anonyme Daten darstellen, solange sie keine Zusatzinformationen haben. Für diese Betrachter wären die Einträge auf der Blockchain dann keine personenbezogenen Daten.[40] Diese Argumentation ist jedoch umstritten. Es wird ebenso vertreten, dass es für personenbezogene Daten ausreicht, dass irgendeine Person den Personenbezug herstellen kann.

Bezieht man auch Zusatzwissen mit ein, das Betrachtern neben den Einträgen auf dem Blockchain-Layer zur Verfügung steht, kann sich ein anderes Bild ergeben: Kennt der Betrachter die Anlage und ihren menschlichen Betreiber und verfügt über die DID der Anlage und ein VC, kann er den Informationen auf dem Blockchain-Layer die Information über eine Statusänderung entnehmen. Auch wenn der Informationsgehalt auf dem Blockchain-Layer damit sehr begrenzt ist, genügt dies nach strenger Ansicht, um von einem personenbezogenen Datum auszugehen. Für alle, die aufgrund des notwendigen Zusatzwissens wissen, dass die verhashte Eintragung auf dem Blockchain-Layer zu einem Gerät einer bestimmten Person gehört, wird das Datum somit personenbezogen.

Das gilt für alle Personen, denen die Verbindung zwischen DID und Person bekannt ist, etwa Verifier, Issuer oder andere, denen Informationen zur Überprüfung mitgeteilt wurden. Es lässt sich zudem nicht kontrollieren, ob Anlagenbetreiber ihre DID veröffentlichen. Wenn dies geschieht, werden die Daten auf dem Blockchain-Layer für jeden Empfänger zu personenbezogenen Daten.

Bei geltender Rechtslage ist der Einsatz der Blockchain im DIVE-Projekt zumindest in einer Pilotphase dennoch mit einem risikobasierten Ansatz möglich. Dieser Ansatz nimmt in Kauf, dass eine zweifelsfrei datenschutzkonforme Lösung nicht gefunden werden kann, rechtfertigt dies jedoch mit den geringen Risiken, die sich aus datenschutzrechtlicher Sicht ergeben.

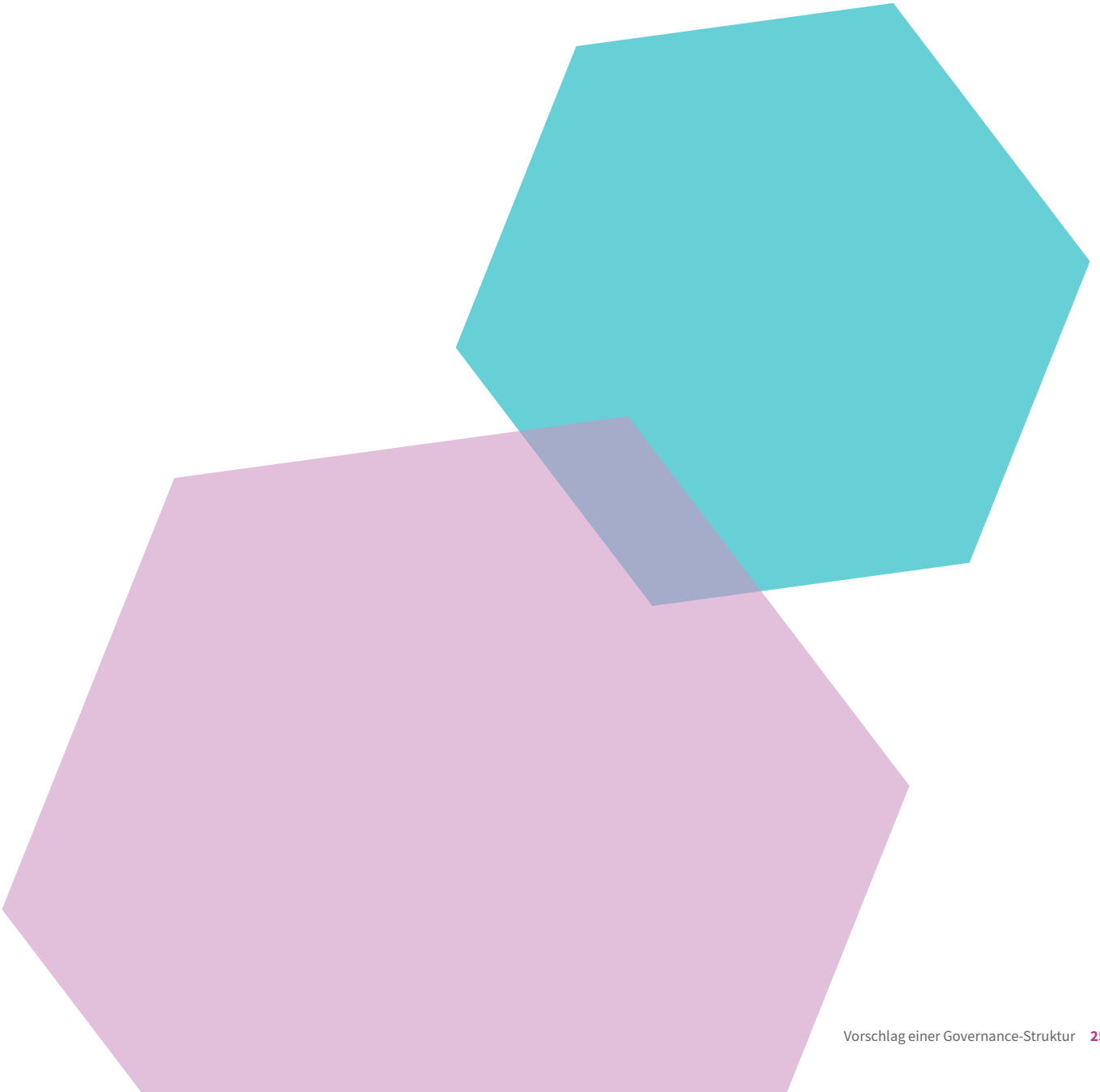
Das geringe Risiko ergibt sich vorliegend aus der Kombination aus einem sehr geringen Informationsgehalt der auf der Blockchain abgelegten Daten, der Komplexität der Herstellung des konkreten Personenbezugs und der Eigenverantwortung der Anlagenbetreiber beim Veröffentlichen von DIDs.

Ein für den Betroffenen relevanter Personenbezug kann sich in der Regel nur durch die aktive Veröffentlichung der DID durch die Nutzer oder Dritte ergeben. Solange die Nutzer ihre DIDs vertraulich behandeln, bleibt der Personenbezug verborgen. Es ist daher vergleichsweise unwahrscheinlich, dass der Personenbezug von einzelnen Einträgen öffentlich wird.

Selbst wenn dies geschieht, ist der Informationswert der so veröffentlichten Daten äußerst gering. Die Informationen betreffen ausschließlich die Interaktion einer Anlage, während der Inhalt der Verifiable Credentials nicht auf der Blockchain sichtbar ist. Im Extremfall kann sich die Information auch nur auf die Tatsache einer Eintragung durch ein Gerät auf der Blockchain beschränken. Die auf der Blockchain gespeicherten Daten sind keine sensiblen Daten. Es handelt sich lediglich um Hash-Werte, die als Nachweis dienen. Unmittelbar personenbezogene Daten über den Anlagenbetreiber oder die Anlage selbst finden sich nicht.

40 So wenn man von einem „relativen Personenbezug“ ausgeht, vgl. EuG, Urteil vom 26.04.2023 – T-557/20, Rn. 99 mit Verweis auf EuGH, Urteil vom 19.10.2016 – C-582/14, Rn. 46

Trotz der geringen Risiken wäre eine gesetzgeberische Klarstellung wünschenswert. Der Blockchain-Einsatz und die datenschutzrechtlichen Bestimmungen bleiben regulatorisch ein ungelöstes Problem. Eine klare gesetzliche Regelung könnte helfen, Unsicherheiten zu beseitigen und den rechtlichen Rahmen für den Einsatz von Blockchain-Technologien zu stärken. Eine solche Klarstellung würde nicht nur das Vertrauen der Nutzer in die Technologie, sondern auch die Rechtssicherheit für alle Beteiligten erhöhen. Alternativ kann auch hier eine vorherige Konsultation mit der oder den zuständigen Aufsichtsbehörden Klarheit schaffen.



4. Anknüpfungsmöglichkeiten der DIVE-Basisinfrastruktur an das Marktstammdaten-register

Die DIVE-Basisinfrastruktur und das Marktstammdatenregister können als gegenseitige Ergänzung betrachtet werden. Eine Erweiterung der bestehenden Schnittstellen könnte die Effizienz und Qualität beider Register steigern.

4.1 Rechtsgrundlagen des Marktstammdatenregisters (MaStR)

Das MaStR ist eine zentrale Datenbank, die umfassende Informationen über sämtliche Akteure und Anlagen im deutschen Energiemarkt sammelt und verwaltet. Es dient als zentrales Verzeichnis, das alle relevanten Daten über Strom- und Gasversorgungsanlagen sowie die Betreiber dieser Anlagen speichert. Das Ziel des MaStR ist es, die Transparenz und Effizienz im Energiemarkt zu erhöhen, indem es eine zentrale und leicht zugängliche Quelle für stammdatenrelevante Informationen bietet.

Die gesetzlichen Regelungen zum Marktstammdatenregister finden sich in § 111e und f Energiewirtschaftsgesetz (EnWG) und der aufgrund § 111e EnWG erlassenen Marktstammdatenregisterverordnung (MaStRV), die die gesetzlichen Vorgaben des EnWG konkretisiert.[41] Die MaStRV regelt detailliert die Anforderungen an die Registrierung und die zu meldenden Daten sowie die technischen und administrativen Details des Betriebs des MaStR. Das MaStR wird von der Bundesnetzagentur (BNetzA) betrieben, die für die Verwaltung und Sicherstellung der Datenintegrität verantwortlich ist.

4.2 Die DIVE-Basisinfrastruktur als sinnvolle Ergänzung des MaStR

Die DIVE-Basisinfrastruktur und das MaStR stehen nicht in Konkurrenz zueinander, sondern können in einer symbiotischen Beziehung koexistieren. Durch die Kombination der zentralen Verwaltungsfunktionen des MaStR mit den dezentralen Sicherheits- und Verifizierungsmöglichkeiten der DIVE-Basisinfrastruktur könnte ein robustes und transparentes Gesamtsystem entstehen.

Die Blockchain-basierte DIVE-Basisinfrastruktur und das MaStR verfolgen beide das Ziel, Transparenz im Energiemarkt zu schaffen. Die DIVE-Basisinfrastruktur soll Vertragspartnern unkompliziert Klarheit über die Identität von Anlagen und Anlagenbetreibern geben, während das MaStR die Registrierung und Nachverfolgbarkeit aller relevanten Energieanlagen und ihrer Betreiber sicherstellt. Beide Systeme tragen somit zur Integrität und Verlässlichkeit des Energiemarktes bei.

Sowohl die DIVE-Basisinfrastruktur als auch das MaStR sind darauf ausgelegt, Stammdaten über Energieanlagen und ihre Betreiber zu sammeln und zu verwalten. Beide Systeme sollen als verlässliche Quellen für stammdatenrelevante Informationen dienen, die für Marktteilnehmer und Regulierungsbehörden von großer Bedeutung sind. Beide Systeme unterstützen die Marktteilnehmer dabei, ihre gesetzlichen Meldepflichten zu erfüllen und die Richtigkeit ihrer Daten sicherzustellen. Die DIVE-Basisinfrastruktur ermöglicht darüber hinaus eine schnelle und flexible Verifizierung von Identitäten und Anlagen im Geschäftsverkehr.

Ein Datenaustausch zwischen der DIVE-Basisinfrastruktur und dem Marktstammdatenregister könnte sicherstellen, dass die Informationen in beiden Systemen konsistent und aktuell sind. Auch wenn das MaStR den Anspruch hat, verlässliche Informationen zu liefern, kann es dort auch zu fehlerhaften Einträgen kommen. Wird ein solcher fehlerhafter Eintrag beim Abgleich erkannt, könnte eine Steigerung der Datenqualität durch die DIVE-Basisinfrastruktur auch dem MaStR zugutekommen. Dies könnte durch Schnittstellen realisiert werden, die einen nahtlosen Datenaustausch ermöglichen. Während das MaStR als zentrales Register für die staatliche Kontrolle und Regulierung eine wichtige Rolle spielt, bietet die DIVE-Basisinfrastruktur ein flexibles und schnelles System für die unmittelbare Nutzung im Geschäftsverkehr. Der Zugriff auf die DIVE-Basisinfrastruktur ist einfacher und bietet eine größere Anschlussfähigkeit als das vergleichsweise starre MaStR, was die Effizienz und Geschwindigkeit von Geschäftsabwicklungen erhöht.

Das MaStR stellt weiterhin sicher, dass alle gesetzlichen Anforderungen an die Registrierung und Nachverfolgbarkeit von Energieanlagen erfüllt werden. Die DIVE-Basisinfrastruktur ergänzt dies durch die Bereitstellung einer leicht zugänglichen Plattform für die Verifizierung von Identitäten und Anlagen. Diese komplementären Eigenschaften könnten dazu beitragen, die Gesamtzuverlässigkeit und Transparenz im Energiemarkt zu erhöhen.

Rechtlich ist daher von Bedeutung, inwiefern ein Austausch der Daten zwischen dem MaStR und der DIVE-Basisinfrastruktur bereits de lege lata (also nach derzeit geltendem Recht) realisiert werden kann und welche Schnittstellen eine Anpassung der rechtlichen Regelungen erforderlich machen würden. Relevant sind dabei insbesondere der Abruf von Daten aus dem MaStR zum Ausfüllen der VCs und eine Aktualisierung von Daten im MaStR aufgrund fehlender oder fehlerhafter Informationen.

4.3 Abruf von Daten aus dem Marktstammdatenregister zum Vorausfüllen der VCs

Eine ausdrückliche gesetzliche Pflicht zur Gewährung des Zugangs zu Daten im MaStR findet sich nur für Behörden in § 111e Abs. 4 EnWG. Allerdings sieht § 111f Nr. 8 EnWG die Möglichkeit vor, durch die MaStRV einen automatisierten Abruf von Daten auch durch Anlagenbetreiber und freiwillig registrierte Personen vorzuschreiben. Derzeit besteht eine solche Schnittstelle für den Abruf nur für nicht vertrauliche Informationen. Weitere Informationen über die Anlage sind für den Anlagenbetreiber zwar abrufbar. Die BNetzA ist aber bislang nicht zur Einrichtung einer geeigneten Schnittstelle zur automatischen Auslesung verpflichtet.

41 Es liegt derzeit ein Referentenentwurf vom 28.08.2024 für eine Verordnung zur Änderung der MaStRV vor. Die vorgeschlagenen Änderungen haben auf die hier behandelten Themen jedoch keine Auswirkungen.

Ein Installateur oder andere Dienstleister könnten im Rahmen des Registrierungsprozesses die Erstellung von VCs für den Anlagenbetreiber und die zu registrierende Anlage unterstützen. Dabei könnten anhand von Stammdaten, die der Anlagenbetreiber bereitstellt, und einer Kennziffer der zu registrierenden Einheit Informationen aus dem MaStR abgerufen und die VCs mit diesen Daten vorausgefüllt werden.

Nicht vertrauliche Informationen aus dem MaStR können über einen Webdienst abgerufen werden. Hierüber werden jedoch nicht immer alle notwendigen Informationen für die Generierung der VCs abrufbar sein. Nach § 15 MaStRV sind die Daten im MaStR grundsätzlich öffentlich zugänglich. Die BNetzA stellt einen Webdienst bereit, mit dem die öffentlich zugänglichen Informationen aus dem MaStR automatisiert abgerufen werden können. Soweit die technischen Voraussetzungen bestehen, können daher die öffentlich zugänglichen Informationen vom Anlagenbetreiber, Installateur oder Dienstleister ausgelesen werden. Es sind jedoch nicht alle Inhalte des MaStR öffentlich zugänglich. § 15 MaStRV sieht für einige Inhalte des MaStR eine Vertraulichkeit vor. Folglich sind alle Eintragungen des MaStR, die mit einem „V“ gekennzeichnet sind, nicht öffentlich abrufbar. Dies betrifft unter anderem alle Nutzerinformationen von Marktakteuren, die natürliche Personen sind, und Standortinformationen von Anlagen unter 30 Kilowatt sowie Daten, die Betriebs- oder Geschäftsgeheimnisse betreffen. Anlagenbetreiber können zudem nach § 15 Abs. 1 S. 2 MaStRV verlangen, dass mehrere Einheiten, die von ihnen betrieben werden, zusammengefasst werden. Soweit dies geschieht, sind die öffentlich abrufbaren Daten nicht mehr zwingend anlagenscharf.

Der Abruf der übrigen Informationen aus dem MaStR zu einem bestimmten Marktakteur und den auf seinen Namen registrierten Einheiten ist derzeit vollumfänglich nur dem jeweiligen Marktakteur selbst möglich. Dies bedeutet, dass der Abruf durch den Marktakteur (hier dem Anlagenbetreiber) oder in dessen Auftrag mit seinen Zugangsdaten erfolgen muss. Dabei wäre grundsätzlich denkbar, dass der Installateur oder Dienstleister diese Aufgabe übernimmt. Nach § 17 Abs. 2 MaStRV ist es Marktakteuren möglich, die über sie gespeicherten Inhalte des MaStR mit anderen Marktakteuren zu teilen. Die Verordnung sieht jedoch nicht vor, wie der Abruf und eine Verteilung technisch ausgestaltet sind. Der BNetzA ist dabei derzeit nicht rechtlich vorgeschrieben, dass dem Marktakteur (oder dem Installateur oder Dienstleister als dessen Stellvertreter) hierfür eine technische Schnittstelle bereitgestellt wird, über die neben den öffentlich zugänglichen Informationen auch die vertraulichen Informationen abgerufen werden können.

4.4 Änderungen von Daten im Marktstammdatenregister

Für den Fall, dass eine Anlage noch nicht im MaStR eingetragen ist oder die Daten nicht aktuell sind, wäre es wünschenswert, wenn der Anlagenbetreiber, Installateur oder Dienstleister automatisiert eine Anpassung der Daten im MaStR auslösen könnte. Für dieses Vorhaben wäre allerdings eine Anpassung der MaStRV erforderlich. Eine Anpassung von Eintragungen im MaStR kann derzeit nur über das Webportal oder – im Falle von Marktakteuren, die natürliche Personen sind – schriftlich gegenüber der BNetzA beantragt werden.

Das Registrierungsverfahren ist in § 8 MaStRV geregelt. Nach § 8 Abs. 1 MaStRV muss für jede Registrierung das Webportal verwendet werden. Zudem dürfen natürliche Personen der BNetzA die erforderlichen Informationen auch schriftlich übermitteln. Es ist hier jedoch keine Möglichkeit zur automatisierten Anpassung der Eintragungen über eine Schnittstelle vorgesehen. Diese Regelungen gelten gleichermaßen für die Registrierung von Änderungen nach § 7 MaStRV.

4.5 Folgen für eine künftige Interaktion zwischen MaStR und DIVE-Basisinfrastruktur

Um eine engere Integration und effizientere Nutzung der Daten zwischen dem MaStR und der DIVE-Basisinfrastruktur zu ermöglichen, wäre eine Anpassung der MaStRV wünschenswert. Im Rahmen dieser Anpassung könnten folgende Regelungen aufgenommen werden:

Verpflichtung zur Schaffung einer Schnittstelle für vertrauliche Informationen: Die BNetzA könnte sich selbst verpflichten, eine Schnittstelle zu schaffen, die es ermöglicht, vertrauliche Informationen automatisiert aus dem MaStR in die DIVE-Basisinfrastruktur zu übernehmen. Die Nutzung dieser Schnittstelle könnte voraussetzen, dass sich Anlagenbetreiber durch DIDs oder Credentials ausweisen und somit ihre Daten sicher in die DIVE-Basisinfrastruktur übertragen.

Verpflichtung zur Schaffung einer Schnittstelle zur Datenaktualisierung: Die BNetzA könnte sich ebenfalls verpflichten, eine Schnittstelle zur Aktualisierung von Daten im MaStR zu schaffen, die auf Initiative des Anlagenbetreibers genutzt werden kann. Auch hier sollte die Authentifizierung vor der Datenübermittlung über DIDs oder Credentials erfolgen, um sicherzustellen, dass nur autorisierte Betreiber Änderungen an den Daten vornehmen können.

Durch diese Anpassungen würde die Interoperabilität zwischen dem Marktstammdatenregister und der DIVE-Basisinfrastruktur verbessert, was zu einer höheren Datenqualität und Effizienz, insbesondere im Anmeldeprozess, beitragen würde. Gleichzeitig könnte dies die administrative Last für die Anlagenbetreiber reduzieren und die Transparenz und Nachvollziehbarkeit der Daten erhöhen.

5. Regulatorische Besonderheiten aus den Anwendungsfällen

Das DIVE-Projekt soll insbesondere auch die Umsetzbarkeit der Anbindung an konkrete Anwendungsfälle demonstrieren. Auch hierbei ist zu untersuchen, ob der Anbindung der DIVE-Basisinfrastruktur an die Anwendungsfälle rechtliche Hürden entgegenstehen. Diese Untersuchung ist im Detail durchaus komplex, da die verschiedenen Anwendungsfälle, die im Rahmen des DIVE-Projekts betrachtet werden, teils hochregulierte Rechtsgebiete betreffen, wie beispielsweise die Regelungen zu Flexibilitätsmärkten und Herkunftsnachweisen. Jeder dieser Anwendungsfälle beinhaltet spezifische rechtliche Anforderungen, die für sich eine detaillierte und individuelle Prüfung erfordern. Die rechtliche Umsetzung der einzelnen Anwendungsfälle umfasst dabei viele Details, die die DIVE-Basisinfrastruktur weder direkt betreffen noch in diesem Projekt konkret beantwortet werden sollen. Die DIVE-Basisinfrastruktur versteht sich insofern als Enabler der Anwendungsfälle, lässt ihnen jedoch einen breiten Umsetzungsspielraum. Der vorliegende Bericht konzentriert sich daher auf die Frage, ob der Einsatz der DIVE-Basisinfrastruktur für den jeweiligen Anwendungsfall rechtlich abstrakt denkbar ist und keine offensichtlichen Hindernisse erkennbar sind, die dem Einsatz der DIVE-Basisinfrastruktur für den Anwendungsfall grundsätzlich im Wege stehen.

Die Anwendungsfälle, die in diesem Rahmen betrachtet werden sollen, sind die Verwendung der DIVE-Basisinfrastruktur für digitale Herkunftsnachweise, die Flexibilitätserbringung und den Lieferantenwechsel. Bei diesen zeigt sich, dass die Anbindung der DIVE-Basisinfrastruktur an die einzelnen Anwendungsfälle grundsätzlich rechtlich umsetzbar wäre. Je nach Anwendungsfall sind jedoch Gesetzesanpassungen notwendig, bei deren Umsetzung der Einsatz der DIVE-Basisinfrastruktur zur Identifikation der Anlagen jeweils mitgedacht werden sollte.

5.1 Anwendungsfall Herkunftsnachweise

Da Herkunftsnachweise (HKN) einen streng regulierten Markt betreffen, wären digitale Herkunftsnachweise, die von der DIVE-Basisinfrastruktur ergänzt werden könnten, nur mit regulatorischer Anpassung denkbar. Im Rahmen dieser Anpassung wäre es sinnvoll, den Einsatz von Identitätslösungen wie der DIVE-Basisinfrastruktur einzuplanen und entsprechende Regelungen für die Anbindung zu schaffen.

Herkunftsnachweise für Strom aus erneuerbaren Energien sind auf europäischer Ebene insbesondere durch die Richtlinie 2009/28/EG (Erneuerbare-Energien-Richtlinie) und ihre Nachfolgerichtlinie 2018/2001 (Erneuerbare-Energien-Richtlinie II) geregelt. Diese Richtlinien verpflichten die Mitgliedstaaten, Systeme zur Ausstellung, Übertragung und Entwertung von Herkunftsnachweisen einzurichten, die den HKN für den Erzeuger von Strom aus erneuerbaren Quellen dokumentieren. In Deutschland sind die Regelungen zu Herkunftsnachweisen im Erneuerbare-Energien-Gesetz (EEG) und im Energiewirtschaftsgesetz (EnWG) umgesetzt. Das Umweltbundesamt (UBA) betreibt das Herkunftsnachweisregister (HKNR) gemäß § 79 Abs. 3 EEG. Das HKNR ist die zentrale Plattform zur Ausstellung, Übertragung und Entwertung von HKN für Strom aus erneuerbaren Energien in Deutschland. Anlagenbetreiber können nach § 79 Abs. 1 Nr. 1 EEG die Ausstellung von Herkunftsnachweisen für Strom aus erneuerbaren Energien beim UBA beantragen. Dies gilt allerdings nur dann, wenn der Anlagenbetreiber keine Zahlungen für die Einspeisevergütung nach § 19 EEG oder Zahlungen für Flexibilität nach § 50 EEG in Anspruch nimmt.

Das UBA hat auf Basis des EEG im Einvernehmen mit dem damaligen Bundesministerium für Wirtschaft und Energie und dem Bundesministerium der Justiz und für Verbraucherschutz die Herkunfts- und Regionalnachweis-Durchführungsverordnung (HkRNDV) erlassen. Nach § 21 HkRNDV können Anlagenbetreiber ihre Anlage im Herkunftsnachweisregister anmelden und haben dafür dem UBA eine Reihe von Daten zur Anlage und zum Anlagenbetreiber zur Verfügung zu stellen.

Relevant werden Herkunftsnachweise beim Stromhandel. Die §§ 42 und 47 EnWG enthalten hierzu Regelungen zum Umgang mit HKN, einschließlich der Verpflichtungen der Marktteilnehmer zur Transparenz und Dokumentation. Stromlieferanten müssen daher kennzeichnen, woher der Strom stammt, und wenn Strom aus erneuerbaren Energien angeboten wird, müssen die Herkunftsnachweise bei Lieferung an Letztverbraucher entwertet werden.

Die DIVE-Basisinfrastruktur könnte eine sinnvolle Ergänzung für Herkunftsnachweise sein, indem sie die notwendige Sicherheit hinsichtlich der Identität der Erneuerbare-Energien-Erzeugungsanlagen liefert. Die bisherigen Regelungen zu HKN stellen nicht per se ein Hindernis für den Einsatz der DIVE-Basisinfrastruktur zur Identifikation der Anlagen dar. Während die Möglichkeit einer digitalen Anlagen-Identität in den bestehenden Regelungen zwar nicht ausdrücklich vorgesehen ist, steht es den Akteuren jedoch grundsätzlich frei, sich auch mittels DIVE-Basisinfrastruktur auszuweisen.

Interessant wird dies jedoch erst dann, wenn digitale Anlagen-Identitäten auch mit einem digitalen – gegebenenfalls auch dezentralen – Herkunftsnachweis verknüpft sind. Diese Verknüpfung gestaltet sich regulatorisch derzeit noch schwierig. Es müssten zunächst die möglichen Grundlagen für einen digitalen Herkunftsnachweis geschaffen werden. Die bisherigen regulatorischen Vorgaben sind hier starr und schreiben das bestehende System mit dem UBA als zentralen Akteur und dem zentral geführten HKNR detailliert vor. Dies beginnt bereits auf EU-Ebene mit einer deutlichen Verpflichtung zur staatlichen Kontrolle und einer Kompetenzbündelung bei einer staatlichen Stelle wie dem UBA.

Will man hier eine digitale Möglichkeit einführen, die sinnvoll mit dem DIVE-Projekt verknüpft ist, müssten zunächst rechtliche Grundlagen für digitale Herkunftsnachweise geschaffen werden, wobei dies sinnvollerweise auf EU-Ebene erfolgen sollte. In diesem Zuge könnten auch Regelungen zur Integration mit digitalen Maschinen-Identitäten aufgenommen werden, um Rechtsklarheit für die Verknüpfung zu schaffen. Eine grundsätzliche Abkehr

vom Prinzip der staatlichen Kontrolle wird sich hier wohl nicht durchsetzen lassen. Auf nationaler Ebene könnte dies bedeuten, dass die Ausstellung eines VC für die Anlage durch das UBA analog zum Anmeldeprozess nach der HkRNDV erfolgt. Das UBA würde dann als (zusätzlicher) Issuer auftreten. Dieser Prozess sollte dann durch gesonderte gesetzliche Bestimmungen geregelt werden.

Solange eine solche Gesetzesänderung noch nicht absehbar ist, könnte ein paralleles System aus digitalen Herkunftsnachweisen denkbar sein, möglicherweise auch zunächst zur Erprobung. Auf solche digitalen HKN sind die bestehenden Regelungen zu Herkunftsnachweisen nicht direkt anwendbar und stehen daher auch nicht im Weg. Ein Nachteil des Entstehens von parallelen Systemen besteht jedoch darin, dass diese digitalen HKN nicht die staatliche Anerkennung hätten und im Rechtsverkehr nicht die notwendige Legitimation besäßen. Dennoch könnte ein solches System als Pilotprojekt sinnvoll sein, um die Vorteile und die Machbarkeit des Einsatzes der DIVE-Basisinfrastruktur für Herkunftsnachweise zu demonstrieren und die Grundlage für zukünftige gesetzliche Anpassungen zu schaffen.

5.2 Anwendungsfall Flexibilitätserbringung

Die Regulierung des Stromhandels ist derzeit noch stark an großen Akteuren orientiert. Für Flexibilitätslösungen zeigen sich erste Ansätze, die aber immer noch einen wesentlichen Grad an Zentralisierung vorsehen. Da die Details der Anlagenidentifikation im bestehenden System nicht abschließend geregelt sind, bleibt Spielraum für einen Einsatz der DIVE-Basisinfrastruktur im bestehenden System. Für absolute Rechtssicherheit bei der flexibleren Einbindung von Kleinanlagen müssten jedoch weitere Regelungen getroffen werden. Diese künftigen Regulierungsansätze zum Ausbau von Flexibilitätsmärkten sollten dann Lösungen wie die DIVE-Basisinfrastruktur mitdenken und die Möglichkeit der digitalen Identifikation der Anlagen vorsehen.

Auf europäischer Ebene ist der grobe rechtliche Rahmen für die Akteure des Strommarktes hauptsächlich durch die Verordnung (EU) 2019/943 über den Elektrizitätsbinnenmarkt und die Richtlinie (EU) 2019/944 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt geregelt. Wichtige Grundsteine für die Anbindung von Betreibern von Erneuerbare-Energien-Anlagen liefern die Richtlinie 2009/28/EG (Erneuerbare-Energien-Richtlinie) und ihre Nachfolgerichtlinie 2018/2001 (Erneuerbare-Energien-Richtlinie II), novelliert durch die Richtlinie 2023/2413 (Erneuerbare-Energien-Richtlinie III), die die Mitgliedstaaten unter anderem dazu verpflichten, Erneuerbare-Energie-Gemeinschaften zu fördern. Auf nationaler Ebene sind die Verpflichtungen zur Anbindung von Erneuerbare-Energien-Anlagen durch die Netzbetreiber in den §§ 8 ff. EEG geregelt. Für steuerbare Netzanschlüsse enthält das EnWG ebenfalls Vorgaben für Verteilnetzbetreiber, die eine netzorientierte Steuerung der Anlagen ermöglichen sollen.

Die bisherige Regulierung zu Flexibilitätsmärkten enthält keine detaillierten Regelungen, die spezifische Vorgaben für die Identifikation von einzelnen Anlagen in Echtzeit machen, wie es ein Flexibilitätsmarkt für Kleinanlagen perspektivisch benötigen würde. Neue Arten von Flexibilitätsmärkten, bei denen Anlagen sich gegenüber Aggregatoren in Echtzeit identifizieren können, sind in der bestehenden Regulierung noch nicht ausdrücklich vorgesehen. Es spricht aber zunächst nichts dagegen, dass die Marktakteure zur Durchführung und Abwicklung bereits bestehender Flexibilitätsmärkte zur Identifikation der Anlagen auf dezentrale Register wie die DIVE-Basisinfrastruktur setzen.

Flexibilitätsmärkte sind jedoch ein insgesamt regulatorisch dynamisches Feld, dessen weitere Entwicklung beobachtet werden muss. Als Empfehlung bleibt, dass im Rahmen einer möglichen weiteren Öffnung von Flexibilitätsmärkten die dezentrale Identifikationsmöglichkeit von Anlagen mitgedacht werden sollte. Künftige Gesetzesänderungen sollten daher technologieoffen gestaltet sein und auch die Möglichkeit eines dezentralen Registers wie der DIVE-Basisinfrastruktur berücksichtigen, um die Identifikation und Verifizierung von Anlagen zu ermöglichen.

5.3 Anwendungsfall Lieferantenwechsel

Für den Lieferantenwechsel sind die Details der Vertragsabwicklung zwischen den Betreibern von Ladepunkten, Stromanbietern und Letztverbrauchern nicht so detailliert geregelt, dass ein Einsatz der DIVE-Basisinfrastruktur zur Vertragsabwicklung nicht möglich wäre. Den Parteien stünde es hier grundsätzlich frei, entsprechende Vereinbarungen zu treffen, bei denen der Betreiber der Ladesäule auf ein vom Stromanbieter ausgestelltes VC vertraut, das den ladenden Kunden als Stromkunden des jeweiligen Anbieters ausweist.[42]

Auf europäischer Ebene bildet die Verordnung (EU) 2023/1804 über den Aufbau der Infrastruktur für alternative Kraftstoffe und zur Aufhebung der Richtlinie 2014/94/EU (AFIR) die Grundlage für den Betrieb von Ladesäuleninfrastrukturen. Diese Verordnung zielt darauf ab, die Infrastruktur für alternative Kraftstoffe, insbesondere Elektrofahrzeuge, auszubauen und zu verbessern. Sie enthält spezifische Verpflichtungen für Betreiber von Ladepunkten, Mobilitätsdienstleister und E-Roaming-Plattformen. Sie sieht vor, dass Betreiber von Ladepunkten E-Roaming anbieten können und über E-Roaming-Plattformen die Abrechnung mit dem gewünschten Mobilitätsdienstleister des Letztverbrauchers ermöglichen. Die Regelungen der Verordnung enthalten jedoch bislang keine Pflicht für die Betreiber von Ladepunkten, E-Roaming anzubieten. Es bleibt den Betreibern überlassen, ob sie diese Option implementieren.

Auf nationaler Ebene wird die AFIR durch die Ladesäulenverordnung (LSV) konkretisiert. Diese Verordnung schafft spezifische Anforderungen und Standards für die Installation und den Betrieb von Ladesäulen in Deutschland. Besonders wichtig sind die Transparenzpflichten, die festgelegt wurden, um sicherzustellen,

42 Im Ergebnis sehen auch Overkamp/Schings, EnWZ 2019, 3 (7 f.) grundsätzlich keine rechtlichen Hindernisse für den Einsatz der Blockchain für öffentliche Ladeinfrastrukturen.

dass Nutzer klare und verständliche Informationen über die Nutzung und die Kosten der Ladeinfrastruktur erhalten. Die LSV schreibt etwa vor, dass Betreiber von Ladesäulen die Nutzer über die Kostenstruktur und die verfügbaren Zahlungsmethoden informieren müssen. Diese Transparenzpflichten sollen den Wettbewerb fördern und den Verbrauchern die Auswahl des besten Angebots ermöglichen.

Die Möglichkeit, beispielsweise den eigenen Stromlieferanten an die Ladesäule „mitzunehmen", ist über das bestehende E-Roaming hinaus bislang nicht konkret geregelt. Die bestehenden Regelungen zu E-Roaming stehen einer solchen Nutzung jedoch nicht grundsätzlich entgegen. Das bedeutet, dass Betreiber von Ladepunkten diese Möglichkeit mithilfe der DIVE-Basisinfrastruktur grundsätzlich anbieten könnten, wobei der Anwendungsfall selbst einer rechtlichen Überprüfung bedarf.

Die beteiligten Akteure sind in ihrer Vertragsgestaltung grundsätzlich offen. Die Beteiligten könnten vereinbaren, den Nachweis der Identität und der Berechtigung des Fahrzeugs sowie des Vorhandenseins eines Vertrags mit dem Stromlieferanten über die DIVE-Basisinfrastruktur zu erbringen. Es müssten entsprechende Verträge zwischen dem Betreiber der Ladesäule, dem Letztverbraucher und dem Stromlieferanten geschlossen werden. Der Betreiber würde dann die Abrechnung mit dem Stromlieferanten durchführen, ähnlich wie es derzeit beim E-Roaming praktiziert wird. Das Vorzeigen eines Verifiable Credentials und der Nachweis über den Vertrag zwischen dem Letztverbraucher und dem Stromlieferanten wären hierbei grundsätzlich denkbar.

6. Zusammenfassung und Handlungsempfehlungen

Aus dem rechtlichen Bericht lässt sich auf einige konkrete Handlungsempfehlungen schließen. Diese Empfehlungen richten sich an unterschiedliche Adressaten, die in verschiedener Form Einfluss auf die weitere Entwicklung von dezentralen Maschinen-Identitäten nehmen können.

6.1 Empfehlungen an die Entwickler und Anwender der DIVE-Basisinfrastruktur

Eine erste Gruppe von Adressaten sind die Entwickler und Anwender einer Basisinfrastruktur für digitale Maschinen-Identitäten. Damit sind nicht nur diejenigen gemeint, die an der konkreten DIVE-Basisinfrastruktur beteiligt sind, sondern alle Entwickler und Anwender, die dieses oder ein vergleichbares Projekt realisieren wollen. Die Entwickler stellen durch ihre Entscheidungen zum technischen Design der Lösung wichtige Weichen für die Funktionen einer solchen Lösung. Anwender nehmen durch ihre Entscheidung, wie sie die Lösung konkret einsetzen, ebenfalls Einfluss. Beides kann rechtliche Implikationen haben. Für Entwickler und Anwender lassen sich folgende Handlungsempfehlungen ableiten:

- **Fokus auf Dezentralität und Minimierung der Angriffsflächen setzen**

Wie die Auseinandersetzung mit den Vorgaben des Cybersicherheitsrechts zeigt, kann die Wahl einer Blockchain-Lösung durchaus Vorteile haben, da durch die dezentrale Architektur Angriffsflächen diversifiziert werden. Dies kann dazu führen, dass die Bestandteile der DIVE-Basisinfrastruktur für sich genommen nicht als kritische Anlage oder wichtige Einrichtung eingestuft werden. Da eine solche Einordnung bei der Suche nach einem verantwortlichen Betreiber zu unliebsamen Ergebnissen führen dürfte, ist zu empfehlen, die dezentrale Struktur konsequent zu verfolgen. Wenn die Entscheidung für eine offene Blockchain-Lösung gefallen ist, sollten der dezentrale Gedanke und der Verzicht auf die Schaffung zentraler Angriffspunkte konsequent umgesetzt werden.

- **Daten minimieren und weitgehend auf personenbezogene Daten auf dem Blockchain-Layer verzichten**

Die Untersuchung zu den Vorgaben des Datenschutzrechts hat gezeigt, dass die Verarbeitung personenbezogener Daten in einer public-permissionless Blockchain derzeit nicht rechtssicher umsetzbar ist. Um auch hier nicht Gefahr zu laufen, dass einzelne Akteure der Blockchain für die stattfindenden Datenverarbeitungen zur Verantwortung gezogen werden, sollte auf personenbezogene Daten auf dem Blockchain-Layer verzichtet werden. Das Pilotprojekt setzt diese Vorgabe bereits gut um, indem lediglich Hash-Werte der DIDs ohne unmittelbaren Personenbezug hinterlegt werden. Dieses Prinzip muss auch konsequent in der weiteren Entwicklung und Anwendung der DIVE-Basisinfrastruktur beachtet werden. Bereits durch technische Vorkehrungen sollte verhindert werden, dass einzelne Anwender – wenn auch versehentlich – personenbezogene Daten auf dem Blockchain-Layer ablegen können.

6.2 Empfehlungen für die Vermarktung von Identitätslösungen auf Blockchain-Basis

Eine weitere Gruppe von Adressaten sind die Vermarkter der dezentralen Identitätslösung. Für sie lässt sich folgende Handlungsempfehlung formulieren:

- **Vertrauen und Verständnis für die Blockchain-Technologie schaffen**

Die Ausführungen zum Haftungsrecht haben gezeigt, dass das Fehlen einer haftenden Zentralstelle für den Blockchain-Betrieb durch ein Vertrauen in die Sicherheit der Blockchain-Technologie ausgeglichen werden muss. Dies verlangt von denjenigen, die die DIVE-Basisinfrastruktur als wirtschaftlich gewinnbringende Lösung verkaufen wollen, unter Umständen Überzeugungsarbeit hinsichtlich der Ausfallsicherheit der Technologie. Während die Kommunikation über das Internet heute weitgehend als selbstverständlich angesehen und das Risiko eines Ausfalls aufgrund seiner geringen Wahrscheinlichkeit hingenommen wird, ist das bei der Verwendung der Blockchain-Technologie noch nicht zwingend der Fall. Viele wichtige Stakeholder könnten Vorbehalte gegen die Technologie haben. Um sie davon zu überzeugen, dass der Verzicht auf eine haftende Betreibergesellschaft für die DIVE-Basisinfrastruktur ein wirtschaftlich hinnehmbares Risiko darstellt, muss Aufklärung hinsichtlich der Funktionsweise und Sicherheit der Blockchain geschaffen werden.

6.3 Empfehlungen an Politik und Gesetzgebung

Nicht alle identifizierten Risiken lassen sich allein durch die technische Gestaltung und durch Aufklärung lösen. An einzelnen Stellen verbleiben regulatorische Unsicherheiten, die durch entsprechende gesetzliche Regelungen beseitigt werden sollten. Eine weitere Gruppe von Adressaten sind daher Akteure in Politik und Gesetzgebung, die nach unserer Einschätzung in folgenden Bereichen gesetzliche Anpassungen erwägen sollten:

- **Cybersicherheitsrecht und dezentrale Systeme in Einklang bringen**

Im bestehenden Cybersicherheitsrecht fehlt derzeit noch eine klare Einordnung zur Regelung dezentraler Systeme. Die in diesem Bericht vorgenommene Einordung ist keinesfalls zwingend. Es wäre daher wünschenswert, wenn gesetzlich klargestellt werden würde, unter welchen Bedingungen dezentrale Systeme, die in ihrer Gesamtheit die Funktion einer potenziell kritischen Anlage oder wichtigen Einrichtung erfüllen, vom Anwendungsbereich der Cybersicherheitsvorschriften ausgenommen sind oder wer in einem solchen Fall als Betreiber zu gelten hat und die entsprechenden Pflichten erfüllen müsste.

- **Dezentrale Systeme im Datenschutzrecht besser abbilden**

Trotz aller Bemühungen um den Verzicht auf personenbezogene Daten auf dem Blockchain-Layer zeigt der Bericht, dass ein Personenbezug nicht immer vollständig vermieden werden kann. Die Folgen der Existenz personenbezogener Daten in einer öffentlichen Blockchain sind bis heute nicht zufriedenstellend geklärt. Das geltende Datenschutzrecht scheint auf dezentrale,

unveränderliche Systeme wie die Blockchain nicht vorbereitet zu sein. Künftige Anpassungen im Datenschutzrecht könnten daher auch das Thema der Distributed-Ledger-Technologie angehen und Lösungsansätze hierfür entwickeln. Dauerhaft werden sich Blockchain-Lösungen nur bei hinreichender Rechtssicherheit im Datenschutzrecht realisieren lassen. Auch wenn das Thema in der Literatur bereits diskutiert wurde, scheint eine zufriedenstellende Lösung – zumindest für public-permissionless Blockchains – noch nicht gefunden. Von gesetzgeberischer Seite war bisher keine Bewegung zu verzeichnen, was – abgesehen von Kryptowährungen – bislang noch am Mangel vorzeigbarer erfolgreicher Projekte liegen könnte. Zeigen Projekte wie DIVE, dass offene Blockchain-Systeme einen echten Mehrwert bringen können, sollte auch der politische Druck entstehen, sich des Themas Datenschutz bei dezentralen Systemen anzunehmen und tragfähige Lösungen zu erarbeiten.

- **Voraussetzungen für Schnittstellen mit dem Marktstammdatenregister schaffen**

Der Bericht hat die möglichen positiven Synergieeffekte zwischen dem Marktstammdatenregister und der DIVE-Basisinfrastruktur aufgezeigt. Die Bundesnetzagentur könnte im Verordnungswege die bereits bestehenden Schnittstellen weiter ausbauen und sich selbst zur Schaffung einer Schnittstelle zwischen MaStR und der DIVE-Basisinfrastruktur verpflichten. Soweit sich hierfür nicht genügend Kräfte mobilisieren lassen, könnte auch eine eindeutige gesetzliche Vorgabe zur Öffnung des MaStR zum Datenabgleich mit einem Register wie der DIVE-Basisinfrastruktur empfehlenswert sein.

- **DIVE-Basisinfrastruktur bei der Regulierung von Anwendungsfällen mitdenken**

Die Anwendungsfälle, für die die DIVE-Basisinfrastruktur vorgesehen ist, stecken teilweise selbst noch in der Entwicklungsphase und bedürfen gesonderter regulatorischer Anpassungen. Betrachtet man die DIVE-Basisinfrastruktur als Enabler dieser Anwendungsfälle, sollte eine Regulierung der Anwendungsfälle die Anbindung an die DIVE-Basisinfrastruktur mitdenken und die gegebenenfalls erforderlichen Regelungen schaffen, die eine Schnittstelle zwischen Anwendungsfall und der DIVE-Basisinfrastruktur benötigt.

Literaturverzeichnis

Auer-Reinsdorff/Conrad: Handbuch IT- und Datenschutzrecht, 3. Auflage 2019.

Bechtolf/Vogt: Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66-71.

Bitkom e. V.: Blockchain und Datenschutz – Faktenpapier, 2017, abrufbar unter https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf.

Borges/Hilber, Beck'scher Online-Kommentar, IT-Recht, 15. Auflage 2023.

Engelhardt/Klein: Bitcoins – Geschäfte mit Geld, das keines ist – Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355-360.

Fridgen/Guggenberger/Hoeren/Prinz/Urbach et al.: Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, Fraunhofer FIT, 2019, abrufbar unter: https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1106/wi-1106.pdf.

Gramlich/Gluchowksi/Horsch/Schäfer/Waschbusch: Gabler Banklexikon: Bank – Börse – Finanzierung, 2018.

Heydn: Software as a Service (SaaS): Probleme und Vertragsgestaltung, MMR 2020, 435-440.

Kiparski: Die TKG-Novelle 2021, CR 2020, 818-827.

Martini/Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251-1259.

Omlor: Blockchain-basierte Zahlungsmittel, ZRP 2018, 85-89.

Overkamp/Schings: Blockchain im Strom- und Verkehrssektor, EnWZ 2019, 3-8.

Raue: Haftung für unsichere Software, NJW 2017, 1841-1846.

Redeker: IT-Recht, 8. Auflage, München 2023.

Säcker/Rixecker/Oetker/Limperg: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 3, 9. Auflage, 2022 (zitiert als „MüKo/Bearbeiter").

Scheurle, Klaus-Dieter/Mayen, Thomas: Telekommunikationsgesetz Kommentar, 3. Auflage 2018.

Schrey/Thalhofer: Rechtliche Aspekte der Blockchain, NJW 2017, 1431-1436.

Schwalm, Steffen; Albrecht, Daria; Alamillo, Ignacio (2022): eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. Open Identity Summit 2022, S. 63-74, Regular Research Papers 2022.

Schwintowski/Klausmann/Kadgien: Das Verhältnis von Blockchain-Governance und Gesellschaftsrecht, NJOZ 2018, 1401-1406.

Spindler/Bille: Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014,1357-1369.

Sydow/Marsch/Raschauer: DS-GVO, BDSG, Handkommentar, 3. Auflage 2022.

Wicker: Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? – Relevante Haftungsfragen in der Cloud, Cloud, MMR 2014, 715-718.

Wimmer: Smart Meter, Plattform und Blockchain, EnWZ, 2020, 387.

Zerche: Aus Produzent und Konsument mach Prosument: Die Potenziale einer neuen Marktrolle, EnWZ 2022, 69-72.

Abkürzungen

AFIR	Verordnung über den Aufbau der Infrastruktur für alternative Kraftstoffe (Alternative Fuels Infrastructure Regulation)
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMI	Bundesministerium des Innern
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CER-Richtlinie	EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience)
DID	Decentralized Identifier, eine Sequenz von Zahlen und Buchstaben; je nach Kontext wird auf den Identifier als Konzept oder die DID-Sequenz als Datum referiert
DLT	Distributed Ledger Technology
DSGVO	Datenschutz-Grundverordnung
EEG	Erneuerbare-Energien-Gesetz (Gesetz für den Ausbau erneuerbarer Energien)
eIDAS-VO	EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (Electronic Identification, Authentication and Trust Services)
EnWG	Energiewirtschaftsgesetz
EUDI-Wallet	Europäische Brieftasche für die digitale Identität (European Digital Identity Wallet)
HKN	Herkunftsnachweis
HKNR	Herkunftsnachweisregister
HkRNDV	Herkunfts- und Regionalnachweis-Durchführungsverordnung
KRITIS	Kritische Infrastrukturen
KRITISDachG	Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen
LSV	Ladesäulenverordnung
MaStR	Marktstammdatenregister
MaStRV	Marktstammdatenregisterverordnung

MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
NIS-2-Richtlinie	Zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit
NIS2UmsuCG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
SaaS	Software as a Service
SPRIND	Bundesagentur für Sprunginnovationen
TKG	Telekommunikationsgesetz
UBA	Umweltbundesamt
VC	Verifiable Credential
VNB	Verteilnetzbetreiber

Glossar

Begriff	Definition
Aggregator (digitaler)	Aggregatoren sind Einheiten, die mehrere einzelne Einheiten, zum Beispiel Verbrauchseinheiten wie (Wohn-)Gebäude mit einzelnen Haushalten oder Unternehmen und Erzeugungseinheiten wie Photovoltaik-Anlagen auf Hausdächern, zusammenfassen und steuern. Die aus der Aggregation resultierende Flexibilität wird gebündelt und an die nächste Ebene, beispielsweise Netzbetreiber, weitergegeben.
Anlage (technische) **Weitere Bezeichnungen: Technische Einheit, DIVE-Gerät**	Eine technische Anlage im Kontext von DIVE sind Assets wie Photovoltaik-Anlagen bzw. Wechselrichter, Batteriespeicher und deren Steuerelektronik, Wallboxen sowie Wärmepumpen.
AS4-Standard	Die Marktkommunikation muss seit dem 1. April 2024 über den Übertragungsweg AS4 (Applicability Statement 4) durchgeführt werden. Abgesichert mit TLS (Transport Layer Security) unter Nutzung der Smart Meter Public Key Infrastructure (SM-PKI) wird die Sicherheit der Übertragung erhöht.
Attester	Siehe Issuer.
Bewegungsdaten (dynamische Daten)	Die Bewegungsdaten einer Anlage sind das dynamische Pendant zu den Stammdaten. Sie enthalten Informationen wie die derzeitige Produktion bzw. den Verbrauch der Anlage, Daten zu einem Ladevorgang eines E-Autos oder auch die Telemetrie. Bewegungsdaten sind zum Beispiel Messdaten von Anlagen und weisen einen hohen Datendurchsatz auf, da sie die zeitliche Veränderung von Zuständen darstellen und somit kontinuierlich aktualisiert werden. Im Energiesystem ist die zeitnahe Verfügbarkeit von Bewegungsdaten von besonderer Bedeutung, vor allem durch die Volatilität der erneuerbaren Energien, die steigende Anzahl von Elektrofahrzeugen und die Zunahme steuerbarer Lasten.
Collator	Collators sind eine spezifische Art von Node, die Transaktionen sammeln und sie zu Blöcken bündeln.

Datenraum (Data Space)	Datenräume ermöglichen den souveränen und selbstbestimmten Austausch von Daten über organisatorische Grenzen hinweg. Um Datensicherheit, Datensouveränität, Interoperabilität, Portabilität und Vertrauen zwischen den Akteuren zu gewährleisten, wird ein föderalistischer Ansatz mit definierten Standards, Technologien und Governance-Modellen genutzt.
Decentralized Identifier (DID)	DIDs sind eine neue Art von Identifikatoren, die eine überprüfbare, dezentralisierte digitale Identität ermöglichen. Eine DID bezieht sich auf ein beliebiges Subjekt (z. B. eine Person, eine Organisation, eine Sache, ein Datenmodell, eine abstrakte Entität usw.). Im Gegensatz zu typischen, föderierten Identifikatoren sind DIDs so konzipiert, dass sie von zentralen Registern, Identitätsanbietern und Zertifizierungsstellen entkoppelt werden können. (Quelle: https://www.w3.org/TR/did-core/)
Digitale Identitäten	Digitale Identitäten im Energiesektor beziehen sich auf eindeutige digitale Repräsentationen von Energieanlagen oder Akteuren und ermöglichen eine sichere und effiziente Durchführung von Transaktionen und Interaktionen im digitalen Energiemarkt. Sie umfassen wesentliche Stammdaten wie Eigentumsverhältnisse, Standort, Kapazität und technische Spezifikationen.
DIVE-Basisinfrastruktur	Die im Projekt DIVE pilotierte Basisinfrastruktur bietet die Funktionalitäten zur Nutzung in neuen Anwendungsfällen und bei bestehenden Akteuren im Energiesystem, wie die Anlagenregistrierung oder die Einhaltung von Marktregeln.
EMS	siehe (H)EMS.
Energy Communities (dt. Energiegemeinschaften)	Bei Energy Communities schließen sich mehrere Akteure (z. B. Bürgerinnen und Bürger sowie Kommunen und KMUs) zusammen, betreiben eigene Anlagen zur Erzeugung erneuerbarer Energien, verbrauchen die erzeugte Energie gegebenenfalls direkt selbst, vermarkten sie oder bieten weitere Energiedienstleistungen an. Für den Aufbau von Energy Communities ist die räumliche Nähe häufig entscheidend.
Flexumer	Kofferwort aus „Flexibilität“ und „Prosumer“. Es beschreibt das Konzept, dass Akteure oder Anlagen im Energiesektor ihre Erzeugungs- wie auch Verbrauchskapazitäten flexibel nutzen und nach bestimmten Parametern optimieren können (sollen).
Hardware Secure Module (HSM, Krypto-Chip)	Ein Hardware Secure Module (HSM) ist ein Hardwaremodul, das bestimme kryptografische Operationen oder Funktionen (bzw. Primitiven) in einem System umsetzt. Die Funktionen beinhalten zum Beispiel das Erstellen von Schlüsselpaaren mit hoher Entropie, das sichere Verwahren der Keys und das Signieren von Daten mithilfe des Private Key. Die Features könnten prinzipiell auch ausschließlich mit Software umgesetzt werden, ein HSM ermöglicht durch das strikte Abtrennen der Sub-Systeme innerhalb des Betriebssystems allerdings eine deutliche Steigerung der Sicherheit bezüglich verschiedener Angriffsvektoren.
(H)EMS	Ein (Heim-)Energiemanagementsystem stellt den lokalen Datenaustausch für den optimierten Einsatz und die Visualisierung von Energieanlagen und Verbrauchern in Ein- und Mehrfamilienhäusern, Liegenschaften und Gewerben sicher.
Holder	Ein Holder (auch Claimer) ist eine Person oder eine Entität, die die Kontrolle über seine bzw. ihre eigenen digitalen Identitätsdaten besitzt und diese verwaltet. Holder speichern und verwenden Verifiable Credentials in einer Digital Wallet, um ihre Identität oder bestimmte Attribute davon gegenüber Dritten zu authentifizieren und zu verifizieren.

Intelligentes Messsystem (iMSys)	siehe Moderne Messeinrichtung.
Issuer	Ein Issuer (auch Attester) ist eine vertrauenswürdige Instanz oder Autorität, die Verifiable Credentials ausstellt. Die VCs werden vom Issuer kryptografisch signiert, was nicht nur die Integrität der Daten sicherstellt, sondern es auch dem Verifier ermöglicht, zu erkennen, von wem sie ausgestellt wurden.
Kritische Infrastruktur (KRITIS)	Als Kritische Infrastrukturen (KRITIS) werden Einrichtungen und Organisationen bezeichnet, die für das staatliche Gemeinwesen wichtig sind. Dazu gehören beispielsweise die Bereiche Energie und Gesundheit. Der Ausfall Kritischer Infrastrukturen kann unter anderem zu Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit und volkswirtschaftlichen Schäden führen.
Moderne Messeinrichtung (mME) / Intelligentes Messsystem (iMSys)	Die moderne Messeinrichtung (oftmals auch „digitaler Stromzähler“ genannt) ist der in Deutschland vorgeschriebene Stromzähler und ersetzt den Ferraris-Zähler. Die mME hält neben einem Display zur Anzeige verschiedener Informationen auch weitere Schnittstellen bereit. Erst in Verbindung mit einem Smart Meter Gateway (SMGW) kann eine mME energiewirtschaftlich relevante Daten übertragen und wird damit zu einem intelligenten Messsystem (iMSys).
Netzbetreiber	Die Netzbetreiber sind für den sicheren Netzbetrieb verantwortlich. Dabei wird zwischen Übertragungs- und Verteilnetzbetreibern unterschieden.
Node (Knoten)	Eine Infrastruktur-Einheit in einem verteilten System. Der Node bündelt verschiedene Transaktionen zu einem Block, der kryptografisch verschlüsselt und dann in das bestehende System integriert wird. Die Anzahl, Rechenleistung und Art von Nodes entscheiden über die Sicherheit, Latenz und Art eines dezentralen Systems (in der Regel ein DLT- oder Blockchain-System).
openEMS	openEMS ist eine modulare und auf Open-Source-Komponenten basierende Software für EMS-Anwendungen. Neben der openEMS Association e. V. wird es von freien Softwareentwicklern kontinuierlich weiterentwickelt und stellt einen Ausgangspunkt für Eigenentwicklungen dar.
Prosumer	Als Prosumer werden in der Energiewirtschaft Akteure oder Anlagen bezeichnet, die sowohl als Erzeugungs- wie auch als Verbrauchseinheit agieren können. Das Wort setzt sich zusammen aus „Produzent/Producer“ und „Konsument/Consumer“.
Public Key Infrastructure (PKI) / Smart Meter PKI (SM-PKI)	Eine Public Key Infrastructure (PKI) ist notwendig, um die korrekte asymmetrische Verschlüsselung von Nachrichten sicherzustellen. Hierbei gibt es verschiedene Umsetzungsarten. Die Smart Meter PKI (SM-PKI) ist die eigene PKI für Smart-Meter-Anwendungen in Deutschland und besitzt ein Wurzelzertifikat (Root) als Vertrauensanker, das vom BSI beaufsichtigt wird. Mit dem Wurzelzertifikat können weitere, zum Ausstellen neuer Zertifikate berechtigte Entitäten, sogenannte Sub-CAs (Sub Certification Authorities) definiert werden. Mit der SM-PKI wird auf diese Weise Vertrauen durch ein Rollenmodell vom Root über die Sub-CAs bis zu den Marktteilnehmern hergestellt.
Public-permissionless Blockchain	Eine Public-permissionless Blockchain ist eine öffentlich zugängliche, dezentrale Blockchain, bei der jeder ohne Erlaubnis teilnehmen kann.

Redispatch	Unter Redispatch versteht man die Anpassung des Kraftwerkseinsatzes durch die Netzbetreiber, um Netzengpässe zu vermeiden. Dazu werden Erzeugungseinheiten vor dem Engpass gedrosselt und Erzeugungseinheiten hinter dem Engpass hochgefahren. Mit Redispatch 3.0 sollen auch Flexibilitätspotenziale von (Kleinst-)Anlagen (< 100 Kilowatt) wie zum Beispiel Elektrofahrzeugen zur Vermeidung von Netzengpässen berücksichtigt werden.
Sektorenkopplung	Sektorenkopplung beschreibt das Zusammenspiel der verschiedenen Sektoren des Energiesystems. Denn nur wenn die verschiedenen Sektoren (wie Strom, Wärme und Mobilität) integriert betrachtet werden, kann der Strom aus erneuerbaren Energien optimal genutzt werden.
Self-Sovereign Identity (SSI) (selbstbestimmte oder selbstsouveräne Identität)	Eine Self-Sovereign Identity (SSI) erlaubt es einer Person, Organisation oder Anlage, eine digitale Identität zu erzeugen und vollständig zu kontrollieren, ohne dass es der Erlaubnis eines Vermittlers oder einer zentralen Stelle bedarf. Zudem erlaubt sie die Kontrolle darüber, wie die persönlichen Daten geteilt und verwendet werden.
Shoveler	Als Shoveler wird eine IT-Werkzeug-Komponente bezeichnet. Mithilfe eines Shovelers wird die Migration von Daten von einem lokalen System in eine Cloud-Umgebung vereinfacht.
Smart Meter Gateway (SMGW)	Das Smart Meter Gateway (SMGW) ist eine besonders gesicherte Schnittstelle für die Datenkommunikation von modernen Messeinrichtungen. Es verbindet Verbraucherinnen und Verbraucher sowie Erzeugerinnen und Erzeuger von Strom mit den Betreibern der Stromnetze und Versorgungsunternehmen. Das Smart Meter Gateway ermöglicht eine datenschutz- und datensicherheitskonforme Einbindung von Zählern in das intelligente Stromnetz.
Stammdaten	Stammdaten bilden häufig die Grundlage für verschiedene Marktprozesse in der Energiewirtschaft. Daher sind die Vollständigkeit und Richtigkeit für die Marktkoordination und -kommunikation unerlässlich. Mit Stammdaten sind im Energiekontext (größtenteils) statische Informationen über technische Anlagen oder Marktrollen gemeint. Dazu gehören unter anderem Datenpunkte wie die Kennungen (ID) in den verschiedenen Systemen (EEG-Nummer, Seriennummer des Herstellers etc.), die installierte Kapazität, der Installationsort sowie der Betreiber und seine ID. Die Liste lässt sich je nach Anlagentyp beliebig lang fortsetzen und ist schwierig abzuschließen. Die Informationen im Marktstammdatenregister stellen ein Beispiel für Stammdaten dar.
Tarifanwendungsfall (TAF)	Tarifanwendungsfälle sind insgesamt 14 vordefinierte Prozedere und Funktionen, die in einem Smart Meter Gateway standardisiert aktiviert und abgebildet werden können. Ein einfaches Beispiel hierfür ist der TAF 7, der das SMGW dazu veranlasst, im Zusammenspiel mit der modernen Messeinrichtung (mME) 15-minütlich Messwerte an einen externen Marktteilnehmer zu übertragen.
Trust-Framework	Ein Trust-Framework beschreibt in der IT ein offizielles Rahmenwerk, das die Handhabung und Anerkennung von Zertifikaten und Formaten zwischen Akteuren regelt. Neben der Harmonisierung bei der Zusammenarbeit stehen in Trust-Frameworks die Ziele Interoperabilität und Datensouveränität im Vordergrund.
Übertragungsnetzbetreiber	Übertragungsnetzbetreiber sind für die Übertragungsnetze, das heißt für die Höchstspannungsleitungen, zuständig, verantwortlich. Sie sorgen für die Sicherheit und Stabilität des Netzes innerhalb einer Regelzone. Die vier Regelzonen in Deutschland verteilen sich auf die vier Übertragungsnetzbetreiber 50Hertz, Amprion, TenneT und TransnetBW.

Validator	Bestimmte Art von Nodes (Knoten) in dezentralen Systemen, die für die kryptografische Prüfung von verschlüsselten Transaktionsblöcken verantwortlich sind.
Verifiable Credentials (VCs)	Verifiable Credentials (VCs) sind ein offener Standard für digitale Ausweise. Sie können Informationen darstellen, die in physischen Ausweisen wie einem Reisepass oder Führerschein enthalten sind, aber auch neue Dinge, die keine physische Entsprechung haben, wie die Inhaberschaft eines Bankkontos. Sie haben zahlreiche Vorteile gegenüber physischen Ausweisen, insbesondere die Tatsache, dass sie digital signiert sind, was sie fälschungssicher und sofort überprüfbar macht. (Quelle: https://en.wikipedia.org/wiki/Verifiable_credentials)
Verifier	Ein Verifier fragt beim Holder die für den Anwendungsfall notwendigen Informationen in Form einer Verifiable Presentation an. Im Rahmen der Präsentation wird kryptografisch bewiesen, dass die zur Verfügung gestellten Informationen gültig sind und weder modifiziert noch vom Issuer widerrufen wurden.
Verteilnetzbetreiber	Die Verteilnetzbetreiber sind für die Nieder-, Mittel- und Hochspannungsnetze zuständig. Sie sind verantwortlich für den Transport und die Verteilung von Strom oder Gas sowie für den Betrieb, die Wartung und den Ausbau des eigenen Netzes in einem bestimmten Gebiet und gegebenenfalls der Verbindungsleitungen zu anderen Netzen. In Deutschland gibt es derzeit über 850 Verteilnetzbetreiber.
Wallet	Eine Wallet ist eine digitale Brieftasche, in der beispielsweise Bezahlkarten, Tickets oder auch Identitätsnachweise abgelegt werden können. In DIVE wurde die Krypto-Wallet Sporran eingesetzt (siehe DIVE-Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“). Eine (Krypto-)Wallet ist eine digitale „Geldbörse“, die zur Aufbewahrung, zum Senden und zum Empfangen von Kryptowährung verwendet wird. Dabei speichert die Wallet nicht die Kryptowährungen selbst, sondern die Schlüssel, die den Zugriff auf die Kryptowährungen ermöglichen.
Zero-Knowledge Proof (ZKP)	Mit einem „Null-Wissen-Beweis“ kann nachgewiesen werden, von einem Geheimnis Kenntnis zu haben, ohne das Geheimnis selbst zu offenbaren. Einsatzgebiete finden sich beispielsweise in der Kryptografie und bei der Authentifizierung.

Ein Projekt der

dena

www.dena.de

future-energy-lab.de