Future Energy
Lab

STUDIE

Der Einsatz von Web3 in der Energiebranche

Bausteine und Grundlagen erklären, Potenziale und Einsatzmöglichkeiten aufzeigen

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
Internet: www.dena.de, www.future-energy-lab.de

Autorinnen und Autoren:
Christina Leinauer, Fraunhofer-Institut für Angewandte Informationstechnik FIT
Charukeshi Mayuresh Joglekar, Fraunhofer-Institut für Angewandte Informationstechnik FIT
Felix Paetzold, Fraunhofer-Institut für Angewandte Informationstechnik FIT
Tobias Ströher, Fraunhofer-Institut für Angewandte Informationstechnik FIT
Jens Strüker, Fraunhofer-Institut für Angewandte Informationstechnik FIT
Robin Patrick Williams, Fraunhofer-Institut für Angewandte Informationstechnik FIT
Nikolaus Wirtz, Fraunhofer-Institut für Angewandte Informationstechnik FIT

Redaktion:
Irene Adamski, dena
Bianca Biermann, dena
Jasmin Wagner, dena

Stand:
12/2025

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2025): Der Einsatz von Web3 in der Energiebranche – Bausteine und Grundlagen erklären, Potenziale und Einsatzmöglichkeiten aufzeigen

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.

Inhalt

1 Einleitung

Die deutsche Energiewende erfordert als Transformation hin zu einem nachhaltigen Energiesektor die Dekarbonisierung der Energiequellen und damit insbesondere die Abkehr von fossilen Kraftwerken als Haupterzeugungsanlagen im deutschen Stromnetz. Mit der fortschreitenden Transformation steigt auch die Anzahl kleiner, dezentral verteilter Erzeugungsanlagen, die Strom aus erneuerbaren Quellen zur Verfügung stellen (*Dezentralisierung*). Diese Entwicklung führt von einer Zentrierung auf ursprünglich wenige Hundert Erzeugungsanlagen in Nähe der Verbrauchszentren zu einer zunehmenden physischen Verteilung von Millionen von Energieerzeugungsanlagen über das gesamte Stromnetz hinweg. Parallel verlagert sich der Betrieb von Erzeugungsanlagen von Energieunternehmen auf immer mehr Privatpersonen, Genossenschaften und Unternehmen aus allen Branchen. Die Dezentralisierung der Struktur der Energieversorgung erfolgt somit nicht nur auf der physikalischen, sondern auch auf der gesellschaftlichen und wirtschaftlichen Ebene.

Die strukturellen Veränderungen durch die Energiewende gehen mit neuen technischen Herausforderungen einher. So sind erneuerbare Energieformen wie Wind- und Solarenergie naturgemäß volatil, was eine geringere Steuerbarkeit der Erzeugungsanlagen mit sich bringt. Die daraus folgenden Schwankungen in der Erzeugung stellen sowohl die Sicherung der Netzstabilität als auch die Vermarktung des Stroms vor neue Herausforderungen (Lund et al., 2015). Vor diesem Hintergrund ergeben sich nicht nur neue Anforderungen, sondern es eröffnen sich auch Chancen für die Einbindung von Endverbraucherinnen und Endverbrauchern: Als sogenannte *Prosumer* können sie aktiv am Energiesystem partizipieren, indem sie ihre Energieflexibilität einbringen, beispielsweise durch die zeitlich variable Einspeisung selbst erzeugter und gespeicherter Energie in das Stromnetz oder die Anpassung des eigenen Verbrauchsverhaltens. Um Schwankungen auf der Erzeugungs- und der Nachfrageseite auszugleichen, muss daher die vorhandene Energieflexibilität der dezentral verteilten Marktakteure systemisch nutzbar gemacht werden. Insbesondere die Identifikation, Koordination und Steuerung der Marktakteure und ihrer Anlagen in ihren unterschiedlichen Rollen im Energiesystem (z. B. Erzeugung, Verbrauch oder beides) stellen jedoch eine enorme Herausforderung dar (Bari et al., 2014; Tristán et al., 2020). Entsprechend werden innovative Konzepte in Verbindung mit digitalen Technologien benötigt, um neue Marktakteure und ihre Erzeugungs- und Verbrauchsanlagen netzdienlich und marktdienlich in das Energiesystem zu integrieren und eine zuverlässige Energieversorgung sicherzustellen (Deutsche Energie-Agentur, 2024c).

Diese digitalen Technologien schaffen zugleich die Grundlage für die Automatisierung der erforderlichen Prozesse und Lösungen. Eine zentrale Voraussetzung für eine automatisierte Integration in bestehende Netz- und Marktstrukturen ist ein effizienter Prozess der Anmeldung von Anlagen und Marktakteuren bei entsprechenden Anwendungen. Zu den Anlagen gehören mit einer fortschreitenden Energiewende insbesondere eine Vielzahl kleiner Erneuerbare-Energien-Anlagen wie Photovoltaik-Dachanlagen oder Heimspeicher sowie elektrisch betriebene Fahrzeuge und Wärmepumpen. Damit Marktakteure wie Prosumer, die entsprechende Anlagen besitzen und betreiben, durch flexible Verbrauchssteuerung sowie durch direkte Vermarktung der selbst erzeugten Energie zur Stabilität und Effizienz des Energiesystems beitragen können, müssen sie koordiniert und gesteuert werden. Für diese Koordination und Steuerung ist neben dem Austausch der Stammdaten zur Identifikation von Anlagen zwischen den verschiedenen Marktakteuren auch ein Austausch von sogenannten Bewegungsdaten (z. B. Stromerzeugungs- bzw. Verbrauchsdaten) über die Zeit erforderlich – etwa zwischen Anlagenbetreibern, Netzbetreibern, Aggregatoren und weiteren Marktakteuren (Gerard et al., 2018).

Da Teile des Energiesystem als Kritische Infrastruktur (KRITIS) eingestuft ist, muss der Datenaustausch zwischen Marktakteuren besonders sicher und zuverlässig erfolgen (Li et al., 2025). Eine „sichere Übermittlung und Verarbeitung von Daten“ meint dabei insbesondere den Schutz vor Zugriffen Unberechtigter und Manipulation von Daten, während sich „Zuverlässigkeit“ auf die ausfallsichere Bereitstellung von Daten bezieht. Darüber hinaus ist die Bereitstellung von verlässlichen Informationen nicht nur für die Koordination und Steuerung der Erzeugungsanlagen essenziell. Für die Umsetzung eines nachhaltigen Energiesystems und die Förderung einer zunehmenden Dekarbonisierung werden auch Nachweise zur Stromherkunft und CO_2-Intensität benötigt. Sie bilden die Basis, um sowohl informierte Verbrauchsentscheidungen als auch regulatorische und marktbezogene Steuerungsprozesse zu ermöglichen (Abad & Dodds, 2020; Holzapfel et al., 2024).

Tabelle 1: Definition und Beispiele für Web3-Technologien

Web3-Technologien
Sogenannte Web3-Technologien können ein dezentral organisiertes und nutzerzentriertes Internet realisieren, oft basierend auf einem direkten, bilateralen und souveränen Austausch von Daten oder digitalen Vermögenswerten ohne Intermediär. Bekannte und verbreitete Web3-Technologien sind: • Distributed-Ledger-Technologien (z. B. Blockchain), • dezentrale Speichersysteme (z. B. InterPlanetary File System), • dezentrales Identitätsmanagement (z. B. selbstsouveräne Identitäten) und • Datenräume. Für weitere Ausführungen zu Web3-Technologien siehe Kapitel 2.

Digitale Technologien spielen in der Energiewende eine Schüsselrolle: Sie ermöglichen die ökonomisch effiziente und schnelle Erfassung, Verarbeitung und Nutzung von sehr kleinen bis sehr großen Datenmengen – etwa von Erneuerbare-Energien-Anlagen, Smart Metern, Ladesystemen oder Marktplattformen – zur intelligenten Koordination und Steuerung des Energiesystems und der dazugehörigen Akteure. Dezentralisierung ist dabei nicht nur im Energiesektor von wachsender Bedeutung, sondern spielt auch eine wesentliche Rolle bei der Weiterentwicklung von technologischen Konzepten. Innovative Ansätze der Dezentralisierung tragen maßgeblich zur Weiterentwicklung des Internets bei. Das ist insbesondere bei der derzeitigen Entwicklungsstufe des Internets (sogenanntes Web3) und den damit verbundenen Technologien (sogenannte Web3-Technologien, vgl. Tabelle 1) erkennbar.

Web3-Technologien versprechen zur Transformation des Energiesystems beizutragen, indem sie Prinzipien wie Dezentralisierung, Transparenz und Benutzerkontrolle im digitalen Raum mit der strukturellen Dezentralisierung von Energieinfrastrukturen verknüpfen. Der Einsatz von Web3-Technologien kann beispielsweise ermöglichen, dass der Austausch von Daten und Transaktionen selbstbestimmt (souverän) und sicher durch die Nutzerinnen und Nutzer erfolgt (vgl. Tabelle 2) und somit die Notwendigkeit von Intermediären reduziert wird.[1] Das kann nicht nur ein zentraler Baustein für die effiziente Koordination und Steuerung im Energiesystem sein, sondern auch eine wichtige Voraussetzung für die Partizipation von (neuen) Marktakteuren wie Unternehmen und Endverbraucherinnen und -verbrauchern. Neben souveränem Datenaustausch lassen sich mithilfe von Web3-Technologien auch neue Mechanismen der Koordination, Beteiligung und Vertrauensbildung zwischen den verschiedenen Akteuren im Energiesystem implementieren. Beispielsweise kann die

[1] Weitere Erläuterungen zur Problematik von Intermediären finden Sie in Kapitel 2 (Entwicklungsstufe Web2.0).

Blockchain-Technologie es dezentralen Energieerzeugern wie Haushalten mit Solaranlagen ermöglichen, ihren potenziellen Energieüberschuss effizient durch Peer-to-Peer-Energiehandel direkt an andere Verbraucherinnen und Verbraucher zu verkaufen. Welches Potential in Peer-to-Peer Märkten steckt zeigt die Studie „Das dezentralisierte Energiesystem im Jahr 2030“ (Deutsche Energie-Agentur, 2023b).

Tabelle 2: Definition von Datensouveränität

Datensouveränität
Datensouveränität bezeichnet die Hoheit des Dateneigentümers über seine eigenen Daten und somit die Fähigkeit, selbst zu bestimmen, wer, wann, zu welchem Zweck und unter welchen Bedingungen auf die Daten zugreifen und sie nutzen darf. Souveräner Datenaustausch ist dabei ein Datenaustausch unter technisch und vertraglich geregelten Bedingungen, bei denen die Datensouveränität des Dateneigentümers gewahrt bleibt (Ernstberger et al., 2023; von Scherenberg et al., 2024).

Die Integration von Web3-Technologien kann vielfältige Vorteile bieten, sowohl im Hinblick auf Netzstabilität (*netzdienlich*) und Marktmechanismen (*marktdienlich*) als auch in Bezug auf den Datenschutz der Verbraucherinnen und Verbraucher sowie die volkswirtschaftliche Wohlfahrt (Hussain et al., 2025; Liu & Li, 2021; Tariq & Amin, 2025). Diesbezüglich kann der Einsatz von Web3-Technologien bestehende komplexe Prozesse im Energiesystem vereinfachen und die dazugehörigen Kosten reduzieren. Ein Beispiel hierfür ist die Automatisierung der Anmeldung, Erfassung oder Vermarktung und Nutzung von Energieflexibilitäten von Kleinstanlagen. Dezentrales Identitätsmanagement und digitale Identitäten für Anlagen versprechen, die Identifizierung und Authentifizierung von Anlagen für unterschiedliche Anwendungen effizienter zu gestalten und einen Rollenwechsel der Anlage zu ermöglichen (Deutsche Energie-Agentur, 2022a). Das Future Energy Lab der dena hat mit „DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem“ und „Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem“ hierzu bereits wegweisende Studien durchgeführt (Deutsche Energie-Agentur, 2025b); Deutsche Energie-Agentur, 2022c). In Bezug auf die Integration neuer Marktakteure können Konzepte der Datenökonomie bestehende Prozesse effizienter gestalten und Potenzial für neue Anwendungen und Geschäftsmodelle heben (Deutsche Energie-Agentur, 2022b).

Diese Integration kann zum Beispiel durch föderierte und offene Infrastrukturen wie Datenräume gelingen. Derzeit liegen die meisten energiewirtschaftlich relevanten Daten bei Netzbetreibern oder spezifischen Marktakteuren (Netztransparenz.de, 2025). Der kontrollierte Austausch von Daten über Zugriffsrechte, Speicherorte und Nutzungszwecke ist für die ursprünglichen Datenbereitsteller jedoch häufig eingeschränkt – insbesondere bei fehlender Transparenz oder unklaren Governance-Strukturen. Ein Datenraum[2] hingegen bildet eine Infrastruktur für den souveränen Datenaustausch basierend auf einem technischen und rechtlichen Rahmen, auf den sich die Gruppe der Teilnehmerinnen und Teilnehmer geeinigt hat (beispielsweise in Bezug auf Zugriffsrechte, Speicherfristen, physische Speicherorte etc.). Die Integration von Datenräumen im Stromsystem kann daher dazu beitragen, sowohl Interoperabilität als auch geeignete Governance-Strukturen zu fördern sowie den stark wachsenden Datenaustausch zu realisieren. Dadurch könnten Marktakteure im Energiesystem einen vereinfachten, aber sicheren Zugang zu Daten erhalten und gleichzeitig kann die Datensouveränität der beteiligten Akteure gestärkt werden. Unter anderem zu diesen Fragestellungen betreut die dena derzeit den „Use Case Energie“ im Rahmen des Aufbaus eines Dateninstituts im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWE) (Deutsche Energie-Agentur, 2025c). Weiterhin ist das

[2] Weitere Erläuterungen zu Datenräumen finden Sie in Kapitel 2.4.

Projekt „energy data – X“ als wesentliches Projekt zu diesen Fragstellungen zu nennen (energy data-X, 2025). Web3-Technologien können somit ein zentraler Baustein für die effiziente Bereitstellung und den Austausch von Daten für neue, innovative Dienstleistungen sein, die wiederum dazu beitragen, dass die Vielzahl an Erzeugungsanlagen, Speichern und Verbrauchern im Energiesystem integriert werden.

Durch die Dezentralisierung der Erzeugungs- und Verbrauchsstrukturen kann die Resilienz des Energiesystems potenziell erhöht werden, da sogenannte *Single Points of Failure* wie große Erzeugungsanlagen im System reduziert werden. Durch die digitale Vernetzung einer Vielzahl dezentraler Erzeugungs- und Verbrauchsanlagen wandelt sich das bislang stark zentral organisierte Energiesystem zu einem offenen, datengetriebenen System. Damit steigt die Abhängigkeit von digitalen Infrastrukturen und Steuerungslösungen, die etwa für den Ausgleich von Schwankungen zwischen Erzeugung und Nachfrage unverzichtbar sind. Anstelle von zentralen Dateninfrastrukturen werden bei Web3 verteilte und redundante Infrastrukturen angestrebt. Diese dezentrale Architektur kann die Resilienz des Gesamtsystems konkret gegen Ausfälle und Angriffe erhöhen, indem sie nicht nur *Single Points of Failure* reduziert, sondern auch die Datenintegrität und die Authentifizierung von Identitäten durch beispielsweise nachvollziehbare Protokolle gewährleistet.

Es ist aber ebenfalls zu beachten, dass auch das Risiko einer *Rezentralisierung* besteht, in der die Verbreitung von Web3-Technologien auch neue, zentrale Intermediäre wie große Betreiber dezentraler Plattformen oder Wallet-Anbieter hervorbringen kann. Ebenso muss bei einer Dezentralisierung der digitalen Infrastruktur im Energiesystem auch berücksichtigt werden, dass es einen Trade-off zwischen dem entstehenden Nutzen und den Kosten für den Aufbau und das Management komplexer, dezentraler Infrastrukturen gibt. Da es sich beim Energiesystem um Kritische Infrastruktur handelt, kann es für zentrale Akteure im Energiesystem erstrebenswert sein, dass bestimmte Funktionen – wie die Überwachung und Wiederherstellung des Netzes – zentral von wenigen Akteuren übernommen werden. Die Zentralisierung hat dann zum Ziel, die mit der Komplexität eines dezentral organisierten Energiesystems einhergehenden Herausforderungen zu minimieren und eine zeitnahe Koordination in kritischen Zeiträumen zu gewährleisten.

Die vorliegende Studie analysiert die mögliche Rolle verschiedener Web3-Technologien in der Energiewirtschaft und skizziert zukünftige Anwendungen. In diesem Kontext wird untersucht, wie diese Technologien zu einer erfolgreichen Energiewende beitragen können, die eine klimaneutrale Energiewirtschaft, Netzstabilität und ökonomische Nachhaltigkeit realisiert. Ein zentraler Bestandteil der Studie ist die Analyse der aktuellen Entwicklungen relevanter Web3-Technologien sowie ihrer Stärken, Schwächen, Chancen und Risiken (SWOT-Analyse) für unterschiedliche Anwendungsfälle im Energiesystem. Basierend auf diesen Erkenntnissen werden in der Studie gezielte Handlungsempfehlungen entwickelt, um die Stärken und Chancen optimal zu nutzen und sich gleichzeitig gegen die Schwächen und Risiken abzusichern.

2 Komponenten und Technologien des Web3

Bereits zum Ende der 1960er Jahre und primär für den Zweck der militärischen Kommunikation und dann des wissenschaftlichen Austauschs entstanden die ersten Vorläufer des Internets (z. B. ARPANET) und damit eine erste Vernetzung von Computern (Lukasik, 2010). Mit dem Aufkommen des World Wide Web in den 1990er Jahren begannen das exponentielle Wachstum des Internets hin zu einem globalen Netzwerk und die Weiterentwicklung der ursprünglichen Kommunikationsfunktion.

Die erste Entwicklungsstufe, häufig als **Web1.0** bezeichnet, war durch eine zentrale Server-Architektur (*Hub and Spoke*) geprägt (Nath et al., 2014). Darin konnten Nutzerinnen und Nutzer erstmals Informationen mit einer globalen Reichweite veröffentlichen und abrufen, allerdings ohne direkte Interaktionsmöglichkeiten (das heißt in der Regel monodirektional, *few-to-many*). Das Web1.0 zeichnete sich hauptsächlich durch die Bereitstellung *statischer* Inhalte und den Fokus auf die Lesefunktion aus (*read-only*, vgl. Abbildung 1). Die Inhalte waren weitgehend einfache, textbasierte Dokumente, ergänzt durch Hyperlinks zur Navigation (*Web of Documents*). Unternehmen nutzten das Web in dieser Phase vor allem, um digitale Kataloge oder Broschüren bereitzustellen, die passiv konsumiert wurden (Aghaei et al., 2012). Die geringe Informationsdichte, eingeschränkte Such- und Navigationsmöglichkeiten sowie die niedrige Portabilität der Inhalte weisen auf den begrenzten Funktionsumfang des Web1.0 hin (Nath et al., 2014).

Dynamische Inhalte, also Webinhalte, die sich in Echtzeit oder basierend auf den Interaktionen der Nutzerinnen und Nutzer verändern, sowie personalisierte Erfahrungen waren im Web1.0 noch kaum realisiert. Dies erfolgte mit dem Übergang in die nächste Entwicklungsstufe des Internets, das sogenannte **Web2.0**, beginnend in den späten 1990er Jahren. Die Etablierung interaktiver Möglichkeiten führte zu nutzergenerierten Inhalten und ermöglichte kollaborative Webanwendungen und damit einen signifikanten Wandel in der Nutzung des Internets (vgl. Abbildung 1). Das Web2.0 wird daher im Gegensatz zum Web1.0 oft durch die Eigenschaft *read and write* charakterisiert, da es nicht nur das Lesen, sondern auch das Schreiben, Bearbeiten und Teilen von Inhalten durch die Nutzerinnen und Nutzer erlaubt (Aghaei et al., 2012; Murugesan, 2007).

Auf Basis dieser interaktiven Funktionen entstanden im Web2.0 digitale Plattformen wie GitHub und Facebook oder Streaming-Dienste, die als Intermediäre zwischen den Interaktionen der Nutzerinnen und Nutzer, Datenflüssen und Services fungierten und dadurch wirtschaftlich erfolgreich wurden (das heißt in der Regel bidirektionale Inhaltsübermittlung über einen zentralen Intermediär, *many-to-many (centralized)*). Insbesondere soziale Netzwerke entwickelten sich zu zentralen Echtzeit-Kanälen für Informationen und Kommunikation, weshalb das Web2.0 auch als *People-centric / Participative Web* bezeichnet wird (Murugesan, 2007; Kenchakkanavar, 2015). Interoperabilität sowie eine kollaborative und plattformbasierte Inhaltsproduktion wurden zudem durch nutzerfreundliche grafische Oberflächen (Graphical User Interface, GUI) und technische Konzepte wie Application Programming Interface (API) oder Single Sign-On (SSO) sowie die dazugehörigen Standards (z. B. REST, OAuth) gefördert. Dominante Plattformen boten dadurch zwar Komfort, erzeugten aber gleichzeitig eine starke Abhängigkeit der Nutzerinnen und Nutzer von den Plattformbetreibern. Die zunehmende Nutzung der angebotenen Plattformen und ihrer Lösungen führte – begünstigt durch starke Netzwerkeffekte und ökonomische Skaleneffekte im Plattformbetrieb – zu Monopolbildung und Machtkonzentration bei einzelnen großen Tech-Konzernen und damit auch zu einer zunehmenden Zentralisierung von Inhaltsentwicklung und -austausch über diese Plattformen (Cusumano et al., 2019). Da das Web2.0 den derzeit vorherrschenden Entwicklungsstand des Internets beschreibt, bestimmten und bestimmen die Plattformbetreiber durch die Gestaltung ihrer digitalen Schnittstellen, welche Inhalte sichtbar,

zugänglich oder teilbar sind, und legen damit fest, welche Handlungsoptionen Nutzerinnen und Nutzern überhaupt zur Verfügung stehen (sogenanntes „*Gatekeeping*“, Kelkar, 2018; Flyverbom et al., 2019). So können marktbeherrschende Plattformen von den Nutzerinnen und Nutzern verlangen, den eigenen Plattform-Richtlinien für die Nutzung und den Schutz ihrer Daten zuzustimmen. Durch die Zustimmung zu diesen Richtlinien können Plattformbetreiber die Nutzerdaten für die Entwicklung neuer Services verwenden (Marty & Warin, 2020; Su & Tang, 2023; Wan et al., 2024). Dies ermöglicht es insbesondere marktbeherrschenden Plattformen, durch Erkenntnisse aus Nutzerdaten ihres Hauptmarktes (das heißt des Plattformbetriebs) Vorteile in anderen Märkten zu erzielen, wo diese Nutzerdaten wiederum verwertet werden können (Krämer & Shekhar, 2025). Während das Web2.0 den Nutzerinnen und Nutzern mehr Möglichkeiten zur Interaktion und mehr Komfort bietet, verbleibt die Kontrolle über die erzeugten Inhalte daher meist bei den Plattformbetreibern. In der Folge hat sich in Europa politisch der Wunsch nach besseren Wettbewerbskonditionen und digitaler Souveränität entwickelt, insbesondere in Form eines neuen Bedarfs an Selbstbestimmung über die Daten der Nutzerschaft (*Datensouveränität*, vgl. Tabelle 2; Ernstberger et al., 2023; Floridi, 2020).

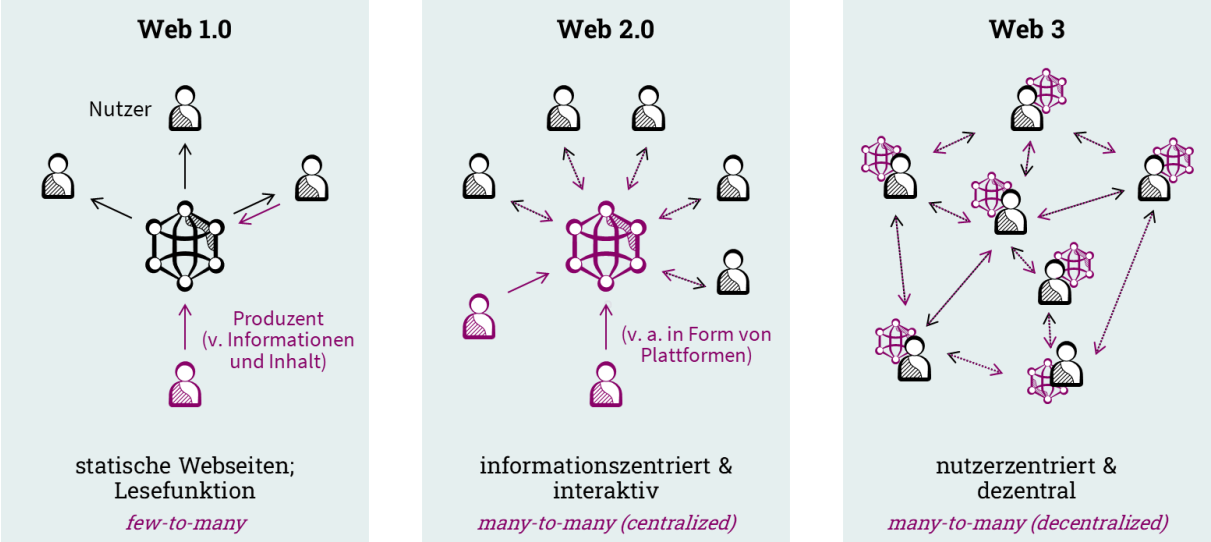

Abbildung 1: Entwicklung Web1.0 – Web2.0 – Web3

Aktuelle Entwicklungen des Internets hin zum sogenannten **Web3** versprechen einen Paradigmenwechsel. Ausgehend von einem statischen, konsumorientierten Web1.0 und einem dynamischen, plattformorientierten Web2.0 zielt die aktuelle Weiterentwicklung darauf ab, ein *dezentrales* Web-Ökosystem zu schaffen. Es ist wichtig, zu betonen, dass es sich bei den Entwicklungsschritten des Internets hin zum Web3 um technologische und gesellschaftliche Trends handelt, die sich derzeit dynamisch weiterentwickeln. Das Web3 ist in seinen Ausprägungen noch nicht abschließend entwickelt und damit nicht einheitlich definierbar.

In diesem Zusammenhang ist auch die Unterscheidung zwischen **Web3** und **Web3.0** relevant: Das Web3 beruht vor allem auf Technologien für eine dezentrale Datenorganisation und wird meist als Sammelbegriff für dezentrale Entwicklungstrends verwendet. Definitionen des Web3 fokussieren sich oft auf die grundsätzliche Transformation hin zum Zielbild eines dezentralen Web-Ökosystems (*many-to-many (decentralized)*), das vor allem durch neu entstandene und neu entwickelte Technologien wie beispielsweise Blockchain – sogenannte **Web3-Technologien** – und dezentrale autonome Organisationen (Decentralized Autonomous

Organizations, DAOs)[3] ermöglicht wird (Bambacht & Pouwelse, 2022; Kovacova et al., 2022). Dadurch sollen bestimmte Eigenschaften wie Datensouveränität – und damit die Fähigkeit von Nutzerinnen und Nutzern, die Kontrolle über ihre Daten auszuüben –, Transparenz und die Sicherstellung von digitalem Eigentum realisiert werden (Beck, 2022; Cao, 2022; Wan et al., 2024): Nutzerinnen und Nutzer sollen im Web3 nicht nur Inhalte konsumieren und generieren, sondern auch selbstbestimmt über ihre Inhalte (z. B. ihre erzeugten Daten, ihre Identität und ihre digitalen Vermögenswerte) verfügen können (Bambacht & Pouwelse, 2022). Im Gegensatz dazu bezeichnet Web3.0 die Entwicklung eines intelligenten, maschinenlesbaren Webs (*semantisches Web* oder *Web of Data*), bei dem Daten strukturiert miteinander verknüpft sind und dadurch effizienter gefunden und integriert sowie automatisiert genutzt werden können (Aghaei et al., 2012; Patel, 2013;). Web3.0 verfolgt das Ziel, Inhalte kontextbezogen bereitzustellen und so die Interaktion mit dem Web zu verbessern, und strebt somit als Konzept primär semantische Standards an (unter anderem entwickelt durch das World Wide Web Consortium (W3C)). Die Konzepte des Web3 und Web3.0 weisen je nach Definition einige Überschneidungen auf, unter anderem in Bezug auf ihr Zielbild (z. B. die Nutzerzentrierung und Förderung der Datensouveränität).

Die Entwicklung hin zu einem Web3 ist noch kein abgeschlossener Vorgang. Die zunehmende Integration von Elementen des Web3 in die bestehenden Strukturen des Web2.0 lassen jedoch einen signifikanten Wandel in der Architektur des Internets erkennen. Dies zeigt sich insbesondere an den Eigenschaften, die oft im Fokus der Entwicklung von Web3-Technologien stehen. Im Folgenden werden daher verschiedene Web3-Technologien anhand ausgewählter Eigenschaften vorgestellt. Insbesondere die **Datensouveränität** und die Wahrung der **Eigentumsrechte** der Nutzerinnen und Nutzer an digitalen Inhalten, Identitäten und Vermögenswerten spielen eine entscheidende Rolle im Konzept des Web3. Im Gegensatz zur Konzentration auf wenige, große Plattformbetreiber und zu der Intransparenz bei der Verarbeitung von Inhalten im Web2.0 soll im Web3 die Nutzerkontrolle über Inhalte sichergestellt werden (Cao, 2022). Das dezentrale Web-Ökosystem basierend auf Web3-Technologien soll dafür sorgen, dass Nutzerinnen und Nutzer ihre digitalen Inhalte, Identitäten und Vermögenswerte unabhängig von einer zentralen Instanz selbst verwalten können (Krause, 2024).

Die Eigenschaft der Datensouveränität wird im Web3 unter anderem durch eine **manipulationssichere und verteilte Datenspeicherung** ermöglicht. Anders als im Web 2.0, in dem Daten meist auf zentral verwalteten Servern einzelner Unternehmen gespeichert werden – selbst wenn diese geografisch verteilt sind –, erfolgt die Speicherung im Web3 in dezentralen Netzwerken, die auch die Kontrolle über die Datenverarbeitung auf viele unabhängige Akteure verteilen können (Wan et al., 2024). Diese verteilte Datenspeicherung bedeutet bei einem Ausfall von Servern eine erhöhte Verfügbarkeit von Daten, da diese nicht bei einzelnen oder wenigen Akteuren bzw. Plattformen konzentriert sind, sondern redundant bei vielen Teilnehmerinnen und Teilnehmern im Netzwerk vorliegen. Dadurch wird einerseits die Abhängigkeit von einzelnen Plattformen reduziert und andererseits ein höherer Schutz vor Manipulation und Zensur erreicht (Kovacova et al., 2022). Die Eigentumsrechte der Nutzerinnen und Nutzer an digitalen Inhalten, Identitäten und Vermögenswerten werden im Kontext von Web3 durch tokenbasierte Ökonomien und kryptografische Verfahren gesichert (Kovacova et al., 2022). *Tokenisierung* ist im Web3 ein Schlüsselelement für ökonomische Anreize und Geschäftsmodelle sowie für die Teilnahme an dezentralen Netzwerken. Durch Tokenisierung können digitale Vermögenswerte in Form von Tokens repräsentiert, transferiert und handelbar gemacht werden (Sockin & Xiong, 2023). Ein weiteres Merkmal, das oft als Ziel von Web3 bezeichnet wird, ist die erhöhte **Transparenz**

[3] DAOs sind Blockchain-basierte Organisationen, die dezentral gesteuert und verwaltet werden. Die autonome Zusammenarbeit in einem offenen Netzwerk basiert auf Regeln, die mithilfe von Smart Contracts (vgl. Kapitel 0) auf der Blockchain gespeichert und ausgeführt werden. Weitere Informationen zu DAOs finden Sie unter anderem bei Santana & Albareda (2022).

der Datenverarbeitung und der Interaktionen, insbesondere bei Transaktionen (Sheridan et al., 2022). Die erhöhte Transparenz wird durch **digitale Verifizierbarkeit** im Web3 erreicht, die es ermöglicht, digitale Inhalte, Identitäten und Transaktionen unabhängig von einer zentralen Instanz und fälschungssicher zu überprüfen.

Ein wichtiger Aspekt dezentraler Netzwerke ist das Lösen des sogenannten *Oracle-Problems*. Es beschreibt die Herausforderung, externe Daten aus der physischen Welt wie zum Beispiel Marktpreise, Wetterdaten oder Messwerte vertrauenswürdig und überprüfbar in ein Web3-Ökosystem zu integrieren. Die Integrität analoger oder digitaler Daten bei der Übertragung in ein Web3-Ökosystem muss sichergestellt werden, um eine durchgängige digitale Verifizierbarkeit und Transparenz von Daten und Transaktionen in einem Web3-Ökosystem zu ermöglichen. Dienste oder Protokolle, die Integrität, Verifizierbarkeit und Transparenz gewährleisten und damit als vertrauenswürdige Brücke zwischen der physischen Welt und einem Web3-Ökosystem fungieren, werden als *Oracles* bezeichnet.[4] Die Vertrauenswürdigkeit dieser Oracles wird im Web3 durch kryptografische und/oder ökonomische Mechanismen abgesichert. Dies soll verhindern, dass die Oracle-Schnittstellen als Angriffsvektor genutzt werden, um die Integrität des gesamten nachgelagerten Systems zu gefährden (Caldarelli & Ellul, 2021; Hassan et al., 2023). Die Verifizierbarkeit einer dezentralen Infrastruktur setzt ein hohes Maß an Interoperabilität voraus. Denn in Ermangelung einer zentralen Instanz, die Vertrauen garantiert, müssen in dezentralen Systemen Dienste oder Identitätsanbieter gegenseitig Informationen wie digitale Signaturen oder Zertifikate über Systemgrenzen hinweg überprüfen können. **Interoperabilität** zielt darauf ab, verschiedene Netzwerke, (Kommunikations-)Protokolle und Anwendungen insbesondere über Standards miteinander kompatibel zu machen (Beck, 2022; Cao, 2022).

Eine wesentliche Rolle in der Ausgestaltung des Web3 und der Web3-Technologien spielt die Frage nach einer **dezentralen Governance**. Durch eine verteilte, partizipative Gestaltung und Verwaltung von Entscheidungsprozessen soll das Problem der Machtkonzentration von Plattformen im Kontext des Web2.0 überwunden werden (Cao, 2022). Während klassische Plattformen im Web2.0 durch ihre Betreiber kontrolliert werden, zielt das Web3 auf die Entwicklung alternativer Modelle ab, die einen Konsens über Systemänderungen, Entscheidungsprozesse und auch ökonomische Fragestellungen durch Partizipation erreichen. Die Frage nach der Governance im Web3 ist von entscheidender Bedeutung, da dezentrale Systeme klare Mechanismen benötigen, um Strukturen, Prozesse und Regeln zu definieren und ihre Einhaltung sicherzustellen (Allen et al., 2023; Calzada, 2024). Es müssen daher (ökonomische) Anreize geschaffen werden, damit sich Nutzerinnen und Nutzer an Entscheidungsprozessen beteiligen, während gleichzeitig Mechanismen zur Vermeidung von Machtkonzentration in den Händen weniger Akteure implementiert werden müssen.

Das Web3 ist eine Weiterentwicklung des Internets hin zu dezentralen und modularen Ökosystemen, die auf dem Einsatz von technologisch erprobten und funktionsfähigen Web3-Technologien basieren. Im Nachfolgenden werden die wichtigsten Web3-Technologien und technischen Konzepte vorgestellt und ihre Entwicklung wird diskutiert. Die beschriebenen Technologien und Konzepte sind dabei integriert zu betrachten, da sie oft erst im Zusammenspiel bzw. in Wechselwirkung miteinander die zuvor aufgeführten Eigenschaften des Web3 hervorbringen.

[4] Weitere Erläuterungen zur Funktionsweise von Oracles finden Sie unter anderem bei Caldarelli & Ellul (2021) und Li et al. (2024).

2.1 Distributed-Ledger-Technologien

Distributed-Ledger-Technologien (DLTs) sind eine Klasse dezentraler Datenspeicherungs- und Datenverwaltungssysteme, die über ein Netzwerk von Knoten arbeiten. Ein Distributed Ledger kann als ein „digitales, verteiltes Register" verstanden werden, angelehnt an das Konzept von Hauptbüchern aus der betriebswirtschaftlichen Buchführung[5] (Weimert, 2020). Vorgänge, das heißt Transaktionen, werden gespeichert, indem identische Kopien des gesamten Ledger an viele unabhängige teilnehmende Knotenpunkte (*Nodes*)[6] verteilt werden. Wenn neue Einträge dem Distributed Ledger hinzugefügt werden sollen, muss sich eine ausreichende Anzahl von Knoten konsensual auf die Gültigkeit verständigen. Hierbei müssen nicht alle Knoten zustimmen, aber sie müssen die Veränderung zumindest akzeptieren[7], indem sie sie in ihre Kopie des Distributed Ledger übernehmen. Erst mit der Konsensfindung über den aktuellen, gültigen Zustand des Distributed Ledger wird er bei allen Knotenpunkten (d. h. für jede Kopie) aktualisiert (Lashkari & Musilek, 2021). Dieser Mechanismus macht nachträgliche Manipulationen von Einträgen äußerst aufwendig und damit gespeicherte Inhalte in einem Distributed Ledger fälschungssicher.

Mittlerweile existieren unterschiedliche Formen von DLTs. Abbildung 2 stellt eine beispielhafte Kategorisierung dieser Formen dar. Die erste und meistverbreitete Form von DLTs, die Blockchain-Technologie, wird in diesem Kapitel im Detail vorgestellt. Das Folgekapitel 0 geht auf technologische Entwicklungen der Blockchain-Technologie und daraus hervorgegangene DLT-Formen wie beispielsweise Directed Acyclic Graphs (DAGs) ein.

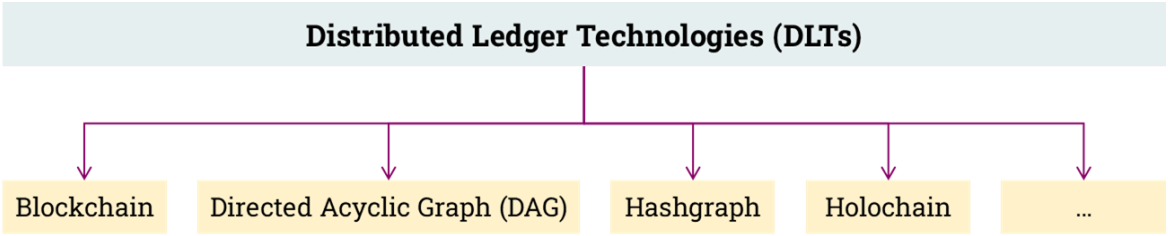

Abbildung 2: Überblick über unterschiedliche Formen von DLTs (Lashkari & Musilek, 2021)

Blockchains waren die erste Form von DLTs und sind zum jetzigen Zeitpunkt auch die am weitesten verbreitete Ausprägung. Die erste Blockchain entstand konzeptionell im Jahr 2008 mit dem Bitcoin Whitepaper. Dabei handelt es sich um eine technisch-mathematische Abhandlung über die Möglichkeit, ein direktes elektronisches Bezahlsystem ohne Intermediäre zu entwickeln (Nakamoto, 2008). Eine Blockchain fungiert technisch als ein zwischen den teilnehmenden Nodes verteiltes, digitales Hauptbuch, in dem Transaktionen[8] in chronologisch geordneten und kryptografisch verknüpften Blöcken gespeichert werden. Die Blöcke sind dabei die Grundeinheit einer Blockchain und enthalten validierte Transaktionen sowie Metadaten. Zu den Metadaten eines Blocks gehören unter anderem ein Zeitstempel, eine eindeutige Identifikationsnummer und

[5] Der Begriff „Hauptbuch" kommt aus der Buchführung und bezeichnet eine Reihe von nummerierten Konten, mit denen Unternehmen ihre Finanztransaktionen nachverfolgen.
[6] Der Begriff „Nodes" (Knotenpunkte) bezieht sich im Kontext von DLTs auf die einzelnen teilnehmenden Computer. Weitere Erläuterungen zu der Rolle und den Arten von Nodes in einem Netzwerk finden Sie unter anderem bei Strüker (2019).
[7] Es müssen nicht alle Knoten zustimmen, weil sich die Sicherheit aus dem Konsensmechanismus und nicht aus vollständiger Zustimmung ergibt. Darüber hinaus bleibt ein DLT-System auf diese Weise auch dann funktionsfähig, wenn einige Knoten offline oder sich uneinig sind.
[8] Der Begriff „Transaktionen" bezieht sich im Kontext von DLTs nicht nur auf finanzielle Transaktionen, sondern auf die Übertragung und Speicherung von Inhalten (z. B. Daten, Eigentumsrechte).

der kryptografische Hash[9] des vorherigen Blocks (Narayanan et al., 2016). Die Unveränderlichkeit bzw. Manipulationssicherheit der gespeicherten Daten wird durch diese Verkettung (nahezu) sichergestellt, da nicht nur der betroffene Block, sondern auch alle nachfolgenden Blöcke verändert werden müssten (siehe Abbildung 3). Um zu validieren, ob ein neuer Block korrekt ist, bevor er dauerhaft zur Blockchain hinzugefügt wird, werden verschiedene Konsensmechanismen angewandt (Lashkari & Musilek, 2021):

- **Proof of Work (PoW):** Erfordert das Lösen komplexer mathematischer Probleme zur Validierung neuer Blöcke. Je länger die Kette an Blöcken ist, desto größer ist der Rechenaufwand für die Validierung und geht daher mit einem steigenden Stromverbrauch einher.
- **Proof of Stake (PoS):** Bestimmt Validierer basierend auf ihrem Einsatz (*Stake*)[10], wodurch der Energieverbrauch gesenkt und die Effizienz gesteigert wird.
- **Proof of Authority (PoA):** Hier erfolgt die Validierung durch vorab ausgewählte, aus Sicht des Netzwerks vertrauenswürdige Knotenpunkte – sogenannte Autoritäten.

Neben den drei aufgeführten Konsensmechanismen gibt es noch weitere Konzepte, die die Konsensbestimmung an alternative knappe Ressourcen wie Speicherkapazität oder die Delegation von Stimmrechten binden.[11]

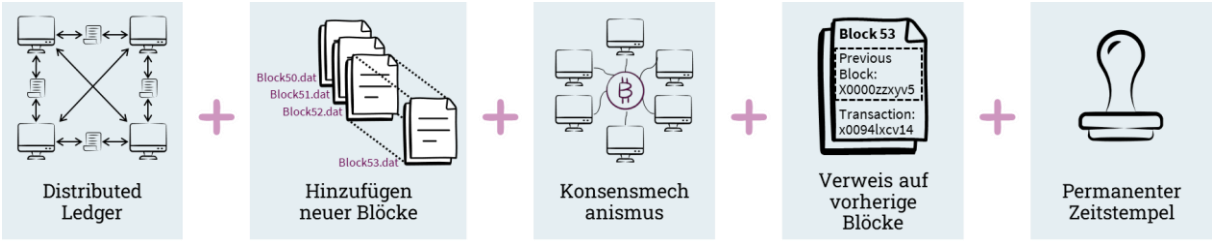

Abbildung 3: Funktionsweise von Blockchains

Blockchains weisen hinsichtlich ihrer Gestaltung von Zugangsrechten sowie der Rollenverteilungen und Rollendefinitionen sehr heterogene Ausgestaltungen auf. Bezüglich der Lesezugriffe und Schreibrechte unterscheidet man zwischen *permissionless* Blockchains, bei denen jeder am Netzwerk teilnehmen kann und Inhalte für alle Teilnehmerinnen und Teilnehmer einsehbar und zugänglich sind (z. B. Bitcoin, Ethereum), und *permissioned* Blockchains, bei denen Inhalte nur für autorisierte Teilnehmer einsehbar sind und die häufig innerorganisatorisch oder in Konsortien genutzt werden (Wüst & Gervais, 2018). Ebenso gibt es die begriffliche Unterscheidung von öffentlichen (*public*) und privaten (*private*) Blockchains. Diese Unterscheidung ist jedoch nicht einheitlich definiert und wird manchmal mit der offenen bzw. eingeschränkten Möglichkeit der Beteiligung bei der Konsensfindung assoziiert (Wüst & Gervais, 2018) oder mit den Begriffen permissionless (= public) und permissioned (= private) gleichgesetzt (Solat et al., 2021).

[9] Die Blöcke in einer Blockchain sind durch die sogenannte Hash-Funktion miteinander verknüpft. Mehr Informationen zu Hash-Funktionen und ihrer unterschiedlichen Ausgestaltung und Performance finden Sie unter anderem in Kuznetsov et al. (2021).
[10] Der Einsatz (Stake) ist in der Regel ein bestimmter Betrag an Tokens bzw. ein monetärer Wert, den ein Teilnehmerinnen und Teilnehmer einsetzen muss, um die Chance zu erhalten, für die Validierung von Transaktionsblöcken ausgewählt zu werden (vgl. Saad & Radzi, 2020).
[11] Weitere Erläuterungen zu Konsensmechanismen finden Sie unter anderem bei Lashkari & Musilek (2021).

Technischer Entwicklungsstand

Die Blockchain-Technologie hat sich seit der konzeptionellen Einführung im Bitcoin Whitepaper im Jahr 2008 und der Implementierung im darauffolgenden Jahr technologisch erheblich weiterentwickelt und zusätzliche Anwendungsfelder erschlossen (Nakamoto, 2008). Ursprünglich entwickelt, um digitale Zahlungstransaktionen ohne zentrale Autorität zu ermöglichen, hat sich die Blockchain-Technologie über den Finanzsektor hinaus verbreitet und eine Vielzahl von DLT-Anwendungen wie beispielsweise für das Lieferkettenmanagement inspiriert (Chen et al., 2024; Khanfar et al., 2021). Mit der Einführung der Ethereum-Blockchain im Jahr 2015 und der damit einhergehenden Unterstützung von selbstausführenden Programmen (d. h. Smart Contracts, vgl. Kapitel 0) wurde das Anwendungsspektrum von Blockchains über den reinen Transfer von Kryptowährungen hinaus erweitert (Li et al., 2019; Sonmez et al., 2023; Tikhomirov, 2017; Wamba & Queiroz, 2020). Da die frühen Anwendungen der Blockchain-Technologie insbesondere im Bereich der Kryptowährungen zu finden waren, wurde sie lange Zeit eng mit diesem Anwendungsbereich assoziiert (Gramlich et al., 2023a). Faktoren wie neue Ertragsmöglichkeiten im Bereich der sogenannten Decentralized Finance (DeFi) und der entstandene Hype rund um Kryptowährungen führten zu einem deutlich gesteigerten Marktinteresse und zu entsprechend hohen Investitionssummen in die Weiterentwicklung der Blockchain-Technologie. Schwerpunkte der Weiterentwicklung waren und sind die Bewältigung der zentralen Herausforderungen wie der hohe Stromverbrauch, die begrenzte Skalierbarkeit von Blockchain-Netzwerken sowie Fragen des Datenschutzes und der Governance (Liu et al., 2023; Zheng et al., 2018).

Der **Stromverbrauch** von Blockchains war insbesondere bei den frühen Blockchain-Netzwerken wie Bitcoin sehr hoch. Dies ist durch den Konsensmechanismus PoW bedingt, der in diesen Netzwerken genutzt wird. Da die Wahrscheinlichkeit, einen Block zu validieren und die damit verbundene Belohnung[12] zu erhalten, proportional zur eingesetzten Rechenleistung steigt, entsteht ein Wettbewerb um immer leistungsstärkere Hardware und damit einhergehend ein stetig wachsender Stromverbrauch (Sedlmeir et al., 2020). Andere Netzwerke setzen daher zunehmend auf andere Konsensmechanismen wie PoS oder PoA und entwickeln neue Konsensmechanismen[13]: Der Wechsel von einem PoW- zu einem PoS-Konsensmechanismus auf der Ethereum-Blockchain hat ihren Stromverbrauch um 99,998 Prozent reduziert, was belegt, dass eine erhebliche Senkung durch den Wechsel auf einen anderen Konsensmechanismus erreicht werden kann. Bei Blockchain-Netzwerken, die nicht auf den PoW-Mechanismus setzen, hängt der Stromverbrauch stark vom Grad der Dezentralisierung – also von der Anzahl sowie der durchschnittlichen Rechenleistung der einzelnen Nodes – ab (Gramlich et al., 2024). Diese Faktoren sollten bei der Auswahl oder Gestaltung einer Blockchain-Lösung aktiv berücksichtigt werden, um so das Problem des Stromverbrauchs zu adressieren.[14]

[12] Die Belohnung ist in der Regel eine festgelegte Menge an nativer Kryptowährung, also der inhärenten Währung einer Blockchain, die in das Protokoll einer Blockchain integriert ist.
[13] Einen Vergleich von Konsensmechanismen und dem damit einhergehenden Stromverbrauch von Blockchain-Transaktionen finden Sie unter anderem bei Sedlmeir et al. (2020) und Xie et al. (2023).
[14] Einen ausführlichen Leitfaden über die Gestaltung von stromverbrauchsoptimierten Blockchains finden Sie unter anderem bei Deutsche Energie-Agentur (2023a).

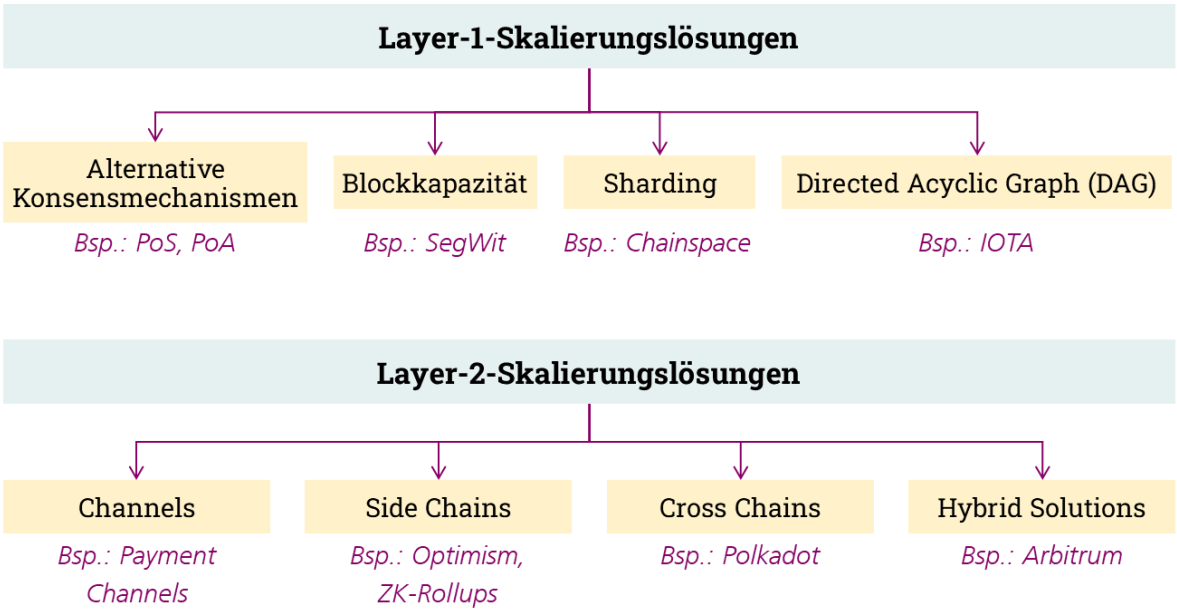

Abbildung 4: Formen an Skalierungslösungen für DLTs in Anlehnung an Gangwal et al. (2023)

Eine weitere technische Herausforderung von Blockchain-Netzwerken ist ihre begrenzte **Skalierbarkeit** (Zheng et al., 2018). Insbesondere der begrenzte Transaktionsdurchsatz bei einigen Blockchain-Netzwerken führt zu Nutzungsengpässen und hohen Transaktionsgebühren (Principato et al., 2023). Diese Limitierung – insbesondere bei zeitkritischen Transaktionen – gab den Anreiz, Blockchain-Architekturen weiterzuentwickeln und neue DLT-Architekturen zu designen, die eine effizientere Verarbeitung von Transaktionen ermöglichen (sogenannte **Layer-1-Lösungen**). Abbildung 4 gibt einen Überblick über unterschiedliche Formen von Layer-1-Skalierungslösungen. Wie bei der Herausforderung des Stromverbrauchs haben die gewählten Konsensmechanismen Einfluss auf die Skalierbarkeit von DLTs.[15] Neben der gezielten Gestaltung der Konsensmechanismen wurden auch Skalierungsmethoden entwickelt, die die Kapazität der Blöcke einer Blockchain steigern oder die Transaktionshistorie im Netzwerk auf sogenannte Shards aufteilen, um die Effizienz im Blockchain-Netzwerk zu erhöhen.[16,17] Auch alternative DLT-Architekturen zu der Blockchain, wie zum Beispiel *Directed Acyclic Graphs (DAGs)*, können die Skalierbarkeit erhöhen. Bei DAGs werden Transaktionen nicht wie bei der Blockchain in Blöcken gebündelt und aneinandergereiht, sondern direkt als einzelne Knoten in einer gerichteten Datenstruktur verbunden, sodass eine eindeutige Reihenfolge abgebildet wird.[18] Ein prominentes Beispiel für eine DAG-basierte Architektur ist IOTA.[19] Allerdings gestaltet sich die praktische Umsetzung von DAGs oft noch als schwierig, weshalb die kommerzielle Reife noch sehr begrenzt ist. So musste beispielsweise IOTA nach langer Entwicklungszeit und technischen Herausforderungen das ursprüngliche DAG-basierte Konzept verwerfen und auf ein Blockchain-basiertes Protokoll und andere Skalierungslösungen zurückgreifen (Omelchenko, 2025).

[15] Einen Vergleich von Konsensmechanismen und der damit einhergehenden Skalierbarkeit von DLT-Architekturen finden Sie unter anderem bei Xie et al. (2023).
[16] Mehr Informationen zur Steigerung der Blockkapazität und beispielhafte Entwicklungen finden Sie unter anderem bei Gangwal et al. (2023) und Weimert (2020).
[17] Mehr Informationen zum Sharding und beispielhafte Entwicklungen finden Sie unter anderem bei Dang et al. (2019) und Gangwal et al. (2023).
[18] Mehr Informationen zu DAG-Architekturen finden Sie unter anderem bei Živić et al. (2020).
[19] Mehr Informationen zu DAGs und IOTA finden Sie unter anderem bei Silvano & Marcelino (2020) und Weimert (2020).

Eine wichtige Entwicklung für die Skalierbarkeit sind **Layer-2-Lösungen**, die auf bestehenden Blockchain-Netzwerken (sogenannte Layer 1) aufbauen, aber unabhängige Ökosysteme (sogenannte Layer 2) mit höheren Transaktionskapazitäten schaffen. Diese Architektur erhöht nicht nur die Skalierbarkeit, da Layer-1-Netzwerke entlastet werden, sondern senkt auch die Kosten, indem sie Transaktionen aus der Haupt-Blockchain auslagert und stattdessen innerhalb des Layer-2-Netzwerks verarbeitet (Deutsche Energie-Agentur, 2023a; Gangwal et al., 2023). Ein Beispiel hierfür ist die Sidechain-Lösung Optimism (vgl. Abbildung 4)[20], die eine skalierbare Architektur schafft, um die Haupt-Blockchain (z. B. Ethereum) zu entlasten. Die Entlastung funktioniert über sogenannte **Rollups**. Mithilfe eines Rollup können Transaktionen außerhalb der Haupt-Blockchain verarbeitet und anschließend gebündelt zur Validierung auf die Haupt-Blockchain übertragen werden (Gangwal et al., 2023). *Optimistic Rollups*[21] sind ein spezifischer Typ von Rollups, die annehmen, dass Transaktionen gültig sind, solange kein Betrugsnachweis erbracht wird. Daher werden deutlich weniger Rechnungen für die Validierung benötigt, was die Skalierbarkeit der Architektur erhöht. Wird ein Fehler nachgewiesen, werden die gebündelten Transaktionen mit der fehlerhaften Transaktion wieder zurückgesetzt (Thibault et al., 2022).

Trotz der Entwicklung einer Vielzahl an Layer-1- und Layer-2-Lösungen und der dazugehörigen Protokolle bleibt die Skalierbarkeit eine der größten Herausforderungen für DLT-Netzwerke. Zudem ergeben sich bei den resultierenden, neu entwickelten DLT-Architekturen einerseits Trade-offs zwischen verbesserter Skalierbarkeit und Effizienz und andererseits zwischen abnehmender Dezentralisierung und Manipulationssicherheit. Zudem steigt bei Layer-2-Lösungen generell die Komplexität und das allgemeine Sicherheitsniveau sinkt bei sonst gleichbleibenden Bedingungen gegenüber Layer-1-Lösungen.

Die wesentlichen Merkmale von DLTs sind ihre inhärente Transparenz und ihre Unveränderbarkeit. Sie sichern die Nachvollziehbarkeit jeder Änderung und Transaktion und bilden damit die Basis für möglichst hohe Manipulationssicherheit. Gleichzeitig sind dadurch alle Transaktionen für alle Teilnehmerinnen und Teilnehmer im Netzwerk dauerhaft sichtbar, was den **Datenschutz** und die **Datensouveränität** der Nutzerinnen und Nutzer beeinträchtigt (Akanfe et al., 2024). Die Transparenz steht hier im Konflikt mit grundlegenden Anforderungen an den Schutz personenbezogener Daten, da finanzielle Transaktionen, Identitätsnachweise oder andere sensible Informationen nicht nur potenziell offengelegt, sondern auch aufgrund der Unveränderlichkeit der Daten dauerhaft gespeichert bleiben (Haque et al., 2021).

Um diese Problematik zu adressieren, wurden Ansätze entwickelt, die Datenschutz in Blockchain-Anwendungen integrieren. Ein wichtiger Lösungsbaustein bildet der Einsatz von *Zero-Knowledge Proofs (ZKPs)*. Mit diesem kryptografischen Verfahren können Aussagen verifiziert werden, ohne sensible Details über die zugrunde liegenden Informationen preiszugeben (vgl. Kapitel 0; Genkin et al., 2018; Li et al., 2020). Solche Datenschutzlösungen können wiederum mit Skalierungslösungen kombiniert werden. Ein Beispiel hierfür sind die sogenannten *Zero-Knowledge Rollups (ZK-Rollups)* (vgl. Abbildung 4). Dabei verarbeiten ZK-Rollups eine große Anzahl an Transaktionen außerhalb der Layer-1-Blockchain und übermitteln lediglich die kryptografischen Beweise (das heißt die ZKPs) an die Blockchain (Thibault et al., 2022). Da nur die Gültigkeit der Transaktionen, nicht aber ihre spezifischen Details auf der Layer-1-Blockchain veröffentlicht werden müssen, steigert sich einerseits der Transaktionsdurchsatz und andererseits wird die Privatsphäre der Nutzerdaten gewahrt (Principato et al., 2023). Um Datenschutz und Skalierbarkeit in einer DLT-Anwendung zu gewährleisten, ist es daher besonders wichtig, zu entscheiden, welche Daten *offchain* (das heißt außerhalb des verteilten Ledger, zum Beispiel in externen Datenbanken oder Speichersystemen) und welche *onchain* (das heißt

[20] Mehr Informationen zu anderen Layer-2-Lösungen finden Sie unter anderem bei Gangwal et al. (2023).
[21] Mehr Informationen zu Rollups und insbesondere zu Optimistic Rollups finden Sie unter anderem bei Gangwal et al. (2023) und Thibault et al. (2022).

direkt auf der DLT-Infrastruktur gespeichert und dort für alle Teilnehmerinnen und Teilnehmer einsehbar und nachverfolgbar) verarbeitet werden sollen.[22]

Obwohl ein DLT-Netzwerk bei einer großen Anzahl verteilter Knoten technisch dezentralisiert ist, können gleichzeitig auf der Governance-Ebene[23] signifikante Zentralisierungspunkte existieren. Dies ist beispielsweise der Fall, wenn grundlegende Regeln des DLT-Netzwerks von wenigen Akteuren geändert werden können. Um die Dezentralisierung von DLTs auch auf der Governance-Ebene zu erreichen, ist es notwendig, zu verstehen, dass die DLTs aus mehreren Komponenten bzw. Layern bestehen, die unterschiedliche Zentralisierungsgrade aufweisen können (Sai et al., 2021). Um ein dezentrales Netzwerk zu erreichen, darf also kein einzelner Layer von nur wenigen Entitäten kontrolliert werden, da eine zentralisierte Ebene die Dezentralität des gesamten Systems gefährdet.

Zur Messung der Dezentralität werden verschiedene Metriken verwendet, wie zum Beispiel der Nakamoto-Koeffizient[24] oder der Gini-Koeffizient[25] für die Verteilung der verwalteten Vermögen eines Netzwerks (Lin et al., 2021). Für Bitcoin wurden mehrere mögliche Angriffsvektoren identifiziert, die aufgrund verschiedener Zentralisierungsfaktoren möglich wurden (Apostolaki et al., 2017). Auch bestehende Governance-Modelle und Entscheidungsprozesse über die Weiterentwicklung der Netzwerke sind komplex und variieren stark in ihrer tatsächlichen Dezentralisierung (Schletz et al., 2023). Einige öffentliche Blockchains werden beispielsweise von zentralen Stiftungen verwaltet. So nutzt Hedera – ein *Hashgraph*-basiertes DLT-Netzwerk[26] – ein relativ zentralisiertes Governance-Modell, in dem das Netzwerk von einem ausgewählten Vorstand verwaltet wird und nur eine begrenzte Anzahl an Teilnehmerinnen und Teilnehmern am Konsensmechanismus mitwirken dürfen. Durch dieses Governance-Modell wird die Skalierbarkeit zwar erhöht, jedoch der Grad der Dezentralität reduziert (Wang et al., 2023). Ein weiteres Beispiel für eine relative Zentralisierung der Governance ist Worldcoin (WLD), ein auf der Blockchain-Technologie basierendes Identitäts- und Kryptowährungsprojekt. Für die Finanzierung der Weiterentwicklung der Lösung ist vorrangig Tools for Humanity (TFH), ein privates Unternehmen, verantwortlich und auch die dazugehörende Kryptowährung ist zu einem beträchtlichen Anteil in der Hand der Projektgründer (Gent, 2023). Im Gegensatz dazu zielt der Ethereum-Improvement-Proposal-Prozess (EIP) auf Dezentralisierung durch Community-Abstimmungsprozesse ab. Der DAO-Hack-Vorfall 2016 hat gezeigt, dass dennoch eine kleine Gruppe einflussreicher Entwickler die technische Umsetzung kritischer Entscheidungen kontrollieren kann (Morrison et al., 2020).[27]

[22] Mehr Informationen zu Offchain- und Onchain-Trade-offs und Gestaltungsmöglichkeiten einer DLT-Anwendung finden Sie unter anderem bei Eren et al. (2025) und Fernández-Iglesias et al. (2024).
[23] Governance bezeichnet hier den Ordnungsrahmen für Entscheidungsrechte und Verantwortlichkeiten innerhalb eines dezentralen Netzwerks. Die Ausgestaltung der Entscheidungsrechte bestimmt dabei den Grad der Zentralisierung, das heißt, ob die Entscheidungsgewalt bei einer einzelnen Person, einer kleinen Gruppe oder einer breiten Masse liegt. Weitere Erläuterungen zum Verständnis von Governance im DLT-Kontext finden Sie unter anderem bei Beck et al. (2018).
[24] Der Nakamoto-Koeffizient ist definiert als die Mindestanzahl von Teilnehmerinnen und Teilnehmern in einem Blockchain-Netzwerk, die sich zusammentun müssen, um mehr als 51 Prozent der gesamten Mining-Leistung zu erreichen und ein Blockchain-System zu kompromittieren (vgl. Lin et al., 2021).
[25] Der Gini-Koeffizient stammt aus der Volkswirtschaftslehre und wird häufig als Maß für wirtschaftliche Ungleichheit verwendet, indem er die Vermögensverteilung innerhalb einer Bevölkerung misst. Im Kontext von Blockchains kann der Gini-Koeffizient genutzt werden, um die Ungleichverteilung der Mining-Leistung unter den Minern zu messen (vgl. Lin et al., 2021).
[26] Ein Hashgraph ist eine DLT-Architektur basierend auf DAGs und virtueller Abstimmung. Mehr Informationen zum Hedera Hashgraph finden Sie unter anderem bei Baird et al. (2019).
[27] Der DAO-Hack-Vorfall hat zu Veränderungen im EIP-Prozess geführt, aber auch die Ethereum-Community in Bezug auf den richtigen Umgang mit dem Vorfall gespalten. Mehr Informationen zu den Folgen des DAO-Hack-Vorfalls finden Sie unter anderem bei Mehar et al. (2019) und Ungureanu et al. (2025).

Zu erwartende Entwicklungen

Erfolgreiche Anwendungsfälle von DLTs haben sich insbesondere in den Bereichen **Decentralized Finance (DeFi)** und **Regenerative Finance (ReFi)** gezeigt. DeFi nutzt vor allem die programmierbare und automatisierte Abwicklung finanzieller Transaktionen über Smart Contracts (vgl. Kapitel 0). Sie ermöglichen eine schnelle und vollständig digitale Abwicklung von Krediten, Zahlungen oder Derivatgeschäften ohne einen klassischen Intermediär (Gramlich et al., 2023a). Durch die stark steigende Zahl an DLT-basierten Finanztransaktionen erstellen zunehmend mehr Staaten regulatorische Rahmenbedingungen für DeFi. Diese reichen von eher lockeren Ansätzen (z. B. in Malta und Singapur), die darauf abzielen, das Potenzial zur Demokratisierung des Finanzsystems zu nutzen, bis hin zu sehr restriktiven Rahmenbedingungen (z. B. in China), die die Risiken für Geldwäsche, Betrug und Marktmanipulation reduzieren möchten (Auer et al., 2024; Uzougbo et al., 2024). Entsprechend sind für DeFi-Anwendungen die Vorteile wie effiziente Abwicklungen gegen die Nachteile für die Finanzmarktstabilität sorgfältig abzuwägen. Im Bereich ReFi liegt der Fokus auf der Förderung nachhaltiger Geschäftsmodelle, z.B, durch tokenisierte CO_2-Zertifikate oder dezentrale Finanzierungsmodelle für Erneuerbare-Energien-Projekte (Schletz et al., 2023). DLTs werden hierbei genutzt, um eine fälschungssichere Nachverfolgbarkeit von Emissionen oder nachhaltigen Investitionen zu ermöglichen. Auch bei der Gestaltung von Anwendungen im ReFi-Bereich müssen potenzielle Risiken, wie die Nachhaltigkeit der gewählten DLT-Technologie selbst, berücksichtigt werden (Mulligan et al., 2024).

Neben diesen Anwendungsfällen haben sich auch die Rahmenbedingungen und die Bedeutung von DLTs für den öffentlichen Bereich weiterentwickelt. Ein exemplarisches Projekt in diesem Kontext ist die „European Blockchain Services Infrastructure (EBSI)“, eine von der Europäischen Union (EU) initiierte, grenzüberschreitende Infrastruktur. Ziel von EBSI ist es, vertrauenswürdige digitale öffentliche Dienstleistungen bereitzustellen und durch die Entwicklung gemeinsamer technischer Standards eine interoperable und rechtssichere Nutzung von Blockchain-Technologien innerhalb der EU zu fördern (Europäische Kommission, 2025a). Die Infrastruktur basiert auf einem PoA-Konsensmechanismus, bei dem autorisierte Knoten in den Mitgliedstaaten die Validierung übernehmen. Dadurch sollen sowohl die Skalierbarkeit als auch die Einhaltung regulatorischer Vorgaben gewährleistet werden (Deutsche Energie-Agentur, 2023a). Innerhalb des EBSI-Ökosystems existieren erste Pilot-Anwendungen[28], die eng mit den folgenden Technologien Identitätsmanagement (vgl. Kapitel 2.2) und Datenräume (vgl. Kapitel 2.4) kombiniert sind.

Im Energiesektor gibt es zahlreiche Forschungsprojekte und erste Piloten, die untersuchen, wie DLTs (insbesondere Blockchain) die Transformation des Sektors unterstützen können (Begleitforschung Smart Service Welt II & Institut für Innovation und Technik (iit), 2020; Roth et al., 2022). Insbesondere das Potenzial von DLTs, historisch überprüfbare Transaktionen in einem Umfeld abzubilden, in dem kein durchgehendes Vertrauen zwischen den Akteuren vorhanden ist, könnte im Energiesektor relevant werden. Beispiele für DLT-Anbieter, die sich auf Anwendungsfälle im Energiesektor spezialisiert haben, sind die Energy Web Foundation, Powerledger und Daylight, die unterschiedliche Anwendungen wie Stromkennzeichnung und Peer-to-Peer-Handel für den Energiemarkt auf Basis von DLTs entwickelt haben (Croutzet & Dabbous, 2021; Daylight Energy LLC, 2025; Kim et al., 2019). Darüber hinaus zeigt das Forschungsprojekt BANULA (Barrierefreie und Nutzerfreundliche Lademöglichkeiten schaffen), wie ein DLT-basiertes Ökosystem zur Optimierung von Energiesystemen, insbesondere an Schnittstellen zu anderen Sektoren, realisiert werden könnte.

[28] Eine Übersicht über Pilotprojekte im EBSI-Ökosystem finden Sie unter https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Make+information+easy+to+verify+and+almost+impossible+to+fake#sec-8 (Europäische Kommission, 2025b).

Weiterhin offen bleiben eine Reihe von Fragestellungen bei Design und Implementierung einer DLT-basierten Infrastruktur, etwa ob sie bei hoher Transaktionslast und Echtzeit-Anforderungen im Energiemarkt ausreichend performant und skalierbar ist. Zudem ist zu klären, wie regulatorische Anforderungen an Datenschutz, IT-Sicherheit und Markttransparenz in einer dezentralen DLT-Infrastruktur effizient und effektiv umgesetzt werden können (Stetter et al., 2024). Für eine flächendeckende Nutzung für Anwendungsfälle im Energiesektor müssen technische und regulatorische Herausforderungen daher noch stärker adressiert werden (Roth et al., 2022). Hierbei spielt auch die zielgerichtete Kombination mit anderen Web3-Technologien und -Konzepten eine Rolle.

2.2 Digitale Identitäten

Neben DLT als bekanntester Web3-Technologie stellen digitale Identitäten eine wichtige Sammlung von Web3-Technologieansätzen dar. Um die Entwicklung des Identitätsmanagements im Internet nachvollziehen zu können, ist zunächst eine präzise Klärung des Begriffs „Identität" erforderlich: Die **Identität** einer Person, einer Organisation oder eines Assets wie einer Anlage besteht aus einer Vielzahl von *Teilidentitäten*, die jeweils spezifische *Attribute* einer Entität repräsentieren. Zu diesen Attributen gehören bei einer natürlichen Person beispielsweise persönliche Daten, die von Behörden, Finanzdienstleistern oder einer Krankenkasse verwaltet werden können. Das Internet (Web1.0) entstand ohne Identitätsmanagement, da für die Weitergabe von Inhalten vor allem die Adresse eines Computers eindeutig identifiziert werden musste. Diese hat jedoch keine Aussagekraft über die Person oder Organisation, der dieses Gerät gehört (Preukschat & Reed, 2021). Mit der Weiterentwicklung in Richtung Web2.0 wurde die Identität einer Person im digitalen Kontext vornehmlich als Zusammensetzung aus Benutzerkonten, Profilinformationen, personenbezogenen Daten und Verhaltensmustern verstanden. Digitale Identitäten[29] und Identitätsmanagement sind im heutigen Internet von essenzieller Bedeutung. Sie bilden die Basis für das Zugangsmanagement zu den meisten Online-Dienstleistungen (z. B. Plattformen wie sozialen Netzwerken), indem sie Vertrauen herstellen und Missbrauch von Personenidentitäten vermeiden sollen (Gramlich et al., 2023b; Strüker et al., 2021a; Torres et al., 2012). Mit der Weiterentwicklung des Internets haben sich verschiedene neue Ansätze des digitalen Identitätsmanagements herausgebildet, die sich insbesondere hinsichtlich ihrer Verwaltungsstruktur und Nutzerkontrolle unterscheiden lassen (vgl. Abbildung 5)[30]:

- **Isoliertes Identitätsmanagement:** Bei diesem Ansatz überprüft jeder Diensteanbieter die Identität einer Nutzerin oder eines Nutzers individuell und unabhängig. Aus der Nutzerperspektive kann dabei unterschieden werden, ob die Identität der Nutzerinnen und Nutzer jeweils von einer zentralen Instanz verwaltet wird (*zentralisiertes Identitätsmanagement*) oder sie den Zugang zu Diensten jeweils selbst verwalten (*nutzerzentriertes Identitätsmanagement*).[31] Die Identitäten sind in beiden Formen in der Regel nicht zwischen verschiedenen Dienstleistern übertragbar, wodurch Nutzerinnen und Nutzer für jeden Dienst ihre Identität neu anlegen und damit separate Registrierungs- und Authentifizierungsprozesse durchlaufen müssen. Dies kann zu redundanten Identitätsprüfungen, erhöhtem administrativen Aufwand und einer eingeschränkten Interoperabilität zwischen Diensten führen (Jøsang & Pope, 2005).

[29] Digitale Identitäten bezeichnen die digitale Repräsentation einer Menge von Identitätsattributen, die die Identifikation einer Person, einer Organisation oder eines Assets im digitalen Raum ermöglichen. Weitere Erläuterungen zum Begriff und Verständnis von digitalen Identitäten finden Sie unter anderem bei Strüker et al. (2021a) und Zwitter et al. (2020).
[30] Das Management von Identitäten entwickelt sich kontinuierlich weiter, weshalb diese ausgewählte Kategorisierung von Identitätsmanagement dynamisch ist und sich mit der Weiterentwicklung von Identitätsmanagement ändern kann.
[31] Weitere Informationen zu zentralisiertem und nutzerzentriertem Identitätsmanagement finden Sie unter anderem bei Strüker et al. (2021a).

- **Föderiertes Identitätsmanagement:** Dieser Ansatz basiert auf zentralisierten Identitätsanbietern (z. B. Google und Apple), die Identitätsinformationen aggregieren und als Verbundidentitätsanbieter fungieren. Nutzerinnen und Nutzer können sich dann mit einem einzigen Identitätskonto über diesen Identitätsanbieter bei verschiedenen Diensten anmelden (Chadwick, 2007). Dieses Modell erhöht den Komfort für die Nutzerinnen und Nutzer durch Funktionen wie SSO (z. B. „Anmelden mit Google“) und entlastet Diensteanbieter von der Benutzerverwaltung. Ein föderiertes Identitätsmanagement geht jedoch auch mit Abhängigkeitsverhältnissen gegenüber den Identitätsanbietern einher (beispielsweise aufgrund der eingeschränkten Möglichkeit, Identitätsinformationen zu einem anderen Identitätsanbieter mitzunehmen bzw. bei diesem wiederzuverwenden). Zudem besteht ein Risiko hinsichtlich des Schutzes der Privatsphäre und der Qualität der Identitätsinformationen, da Nutzerinnen und Nutzer nur begrenzt Einfluss darauf haben, wie der Identitätsanbieter die Identitätsinformationen speichert und weitergibt (Aldosary & Alqahtani, 2021; Maler & Reed, 2008). Grundlegend für die Nutzung solcher Identitätsanbieter ist daher das Vertrauen der Nutzerinnen und Nutzer in diese Anbieter.
- **Selbstsouveränes Identitätsmanagement:** Im Gegensatz zu den vorangegangenen Ansätzen strebt das Konzept der selbstsouveränen Identitäten (*Self-Sovereign Identities*, SSI) nach einer unabhängigen und dezentralen Verwaltung von Identitätsinformationen mit einer vollständigen Portabilität[32] der digitalen Identität über unterschiedliche Dienste hinweg. Die wesentliche Herausforderung eines Identitätsmanagements ohne zentralen Identitätsanbieter – wie im Fall des föderierten Identitätsmanagements – besteht darin, die Vertrauensbeziehung zwischen den Nutzerinnen und Nutzern und dem zentralen Intermediär durch eine technische Bestätigung der Vertrauenswürdigkeit der Beteiligten zu ersetzen. Nutzerinnen und Nutzer sollen dabei stets die Kontrolle über ihre digitalen Identitäten und Identitätsattribute besitzen (Allen, 2016; Tobin & Reed, 2016).[33] Ein SSI-basiertes Identitätsmanagement soll dazu führen, dass selektiv nur jene Informationen weitergegeben werden, die für einen bestimmten Anwendungsfall erforderlich sind, beispielsweise der Nachweis der Volljährigkeit oder der Adresse (sogenannte *selektive Offenlegung*). Zudem sollen Korrelationen zwischen verschiedenen Identitätsattributen durch technische Mechanismen minimiert werden, um ungewünschte Profilerstellungen zu verhindern. Ziel ist eine prüfbare Verwaltung digitaler Identitäten, die nutzerzentriert organisiert ist und nicht auf zentrale Identitätsanbieter angewiesen ist – mit dem Anspruch, Datenschutz und Datensouveränität zu stärken (Schardong & Custódio, 2022; Sedlmeir et al., 2022, Strüker et al., 2021a).[34]

[32] (Daten-)Portabilität bezeichnet die Fähigkeit, Daten flexibel an Dienste bzw. zwischen Diensten übermitteln zu können. Im Kontext von Web3 wird damit zudem das Ziel verbunden, dass die Kontrolle für die Datenübermittlung bei den Nutzerinnen und Nutzern verbleibt.
[33] Das SSI-Paradigma wird meist anhand bestimmter Designprinzipien definiert. Allen (2016) und Tobin & Reed (2016) haben beispielsweise basierend auf ihrer ersten SSI-Definition bereits Designprinzipien formuliert. Insbesondere die von Allen postulierten zehn Prinzipien werden häufig für die Definition von SSI herangezogen. Zu diesen Prinzipien zählen unter anderem Kontrolle, Transparenz, Portabilität, Interoperabilität und Minimierung. Das Konzept von SSI hat sich seitdem weiterentwickelt, weshalb auch die zugeordneten Designprinzipien nicht immer identisch sind (siehe unter anderem Sedlmeir et al., 2022).
[34] Das SSI-Paradigma adressiert insbesondere das Ziel der Datensouveränität im Web3, indem es den Nutzerinnen und Nutzern erlaubt, ihre Identitäten sicher und privat ohne einen zentralen Intermediär über ein dezentrales Register zu verwalten (Bambacht & Pouwelse, 2022). Die SSI-Prinzipien (siehe vorherige Fußnote) lassen sich zumindest eingeschränkt auch im Web2.0 bzw. ohne eine vollkommen dezentrale Infrastruktur realisieren.

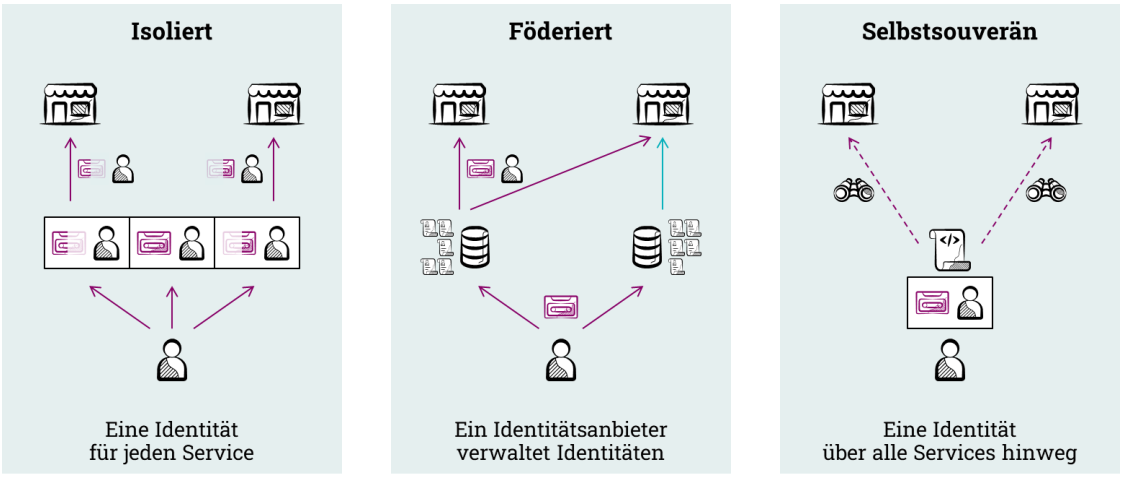

Abbildung 5: Drei Formen des Identitätsmanagements

Ein SSI-basiertes Identitätsmanagement beinhaltet drei wichtige Rollen: **Issuer** (Aussteller), **Holder** (Inhaber) und **Verifier** (Prüfer) (vgl. Abbildung 6; Davie et al., 2019). Der Issuer stellt dabei **Verifiable Credentials (VCs)** aus. VCs sind digital signierte Nachweise, die mehrere überprüfbare Informationen enthalten. Diese überprüfbaren Informationen bzw. Aussagen werden als **Verifiable Claims** („verifizierbare Behauptungen“) bezeichnet (Babel et al., 2025; Strüker et al., 2021a).[35] Bei den Verifiable Claims kann es sich um Aussagen zu einer Person, einer Organisation oder einer Maschine handeln, wie zum Beispiel Stammdaten (z. B. Name, Adresse), Beziehungen (z. B. Mutter, Tochter) oder Berechtigungen (z. B. rechtlicher Status, Zugangsrechte). Diese Aussagen müssen nicht zwangsweise Identitätsattribute darstellen. Die VCs werden von einem Issuer mithilfe einer digitalen Signatur kryptografisch bestätigt und sind in einer sogenannten **Digital Wallet** auf dem Gerät des Holders, also der Nutzerin oder des Nutzers, gespeichert (Preukschat & Reed, 2021; Sedlmeir et al., 2021). Im Fall eines Authentifizierungsprozesses fragt der Verifier verifizierbare Behauptungen an (z. B. spezifische Identitätsattribute). Die notwendigen Informationen werden dann aus einem VC extrahiert und in Form einer **Verifiable Presentation (VP)** mit einer kryptografischen Signatur an den Verifier übermittelt (vgl. Abbildung 6). Durch diese digitale Signatur können sowohl der Issuer des VC als auch die Echtheit und Richtigkeit der Informationen im VC selbst überprüft werden. Da diese Verifizierung unabhängig von einem zentralen Intermediär erfolgt und Nutzerinnen und Nutzer gezielt freigeben, welche Informationen sie teilen, behalten sie die Kontrolle über ihre Daten (Babel et al., 2025). Dabei interagieren die Nutzerinnen und Nutzer (in ihrer Funktion als Holder) jeweils bilateral mit dem Issuer und dem Verifier. Verifier haben nur eine indirekte Vertrauensbeziehung zu den Issuern, was zum sogenannten „Vertrauensdreieck“ führt (vgl. Abbildung 6; Babel et al., 2025).

[35] Die Begriffe Verifiable Claim und Verifiable Credential werden teilweise auch synonym verwendet (vgl. Mühle et al., 2018).

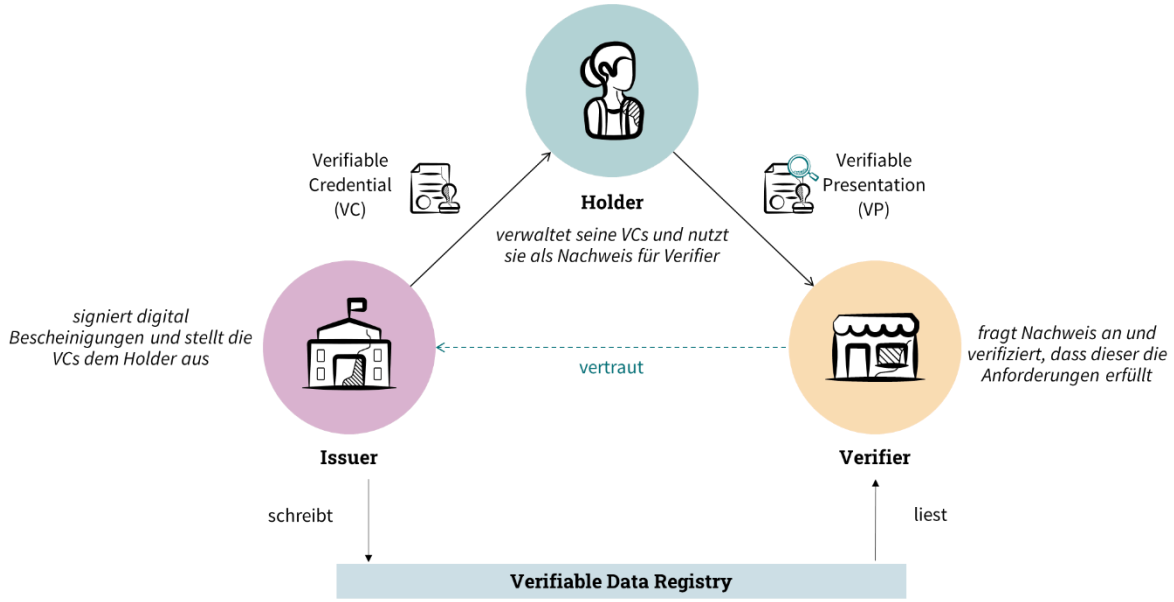

Abbildung 6: Digitaler Authentifizierungsprozess und Vertrauensdreieck mit SSI in Anlehnung an Babel et al. (2025)

Um die einzelnen Akteure mit ihren Rollen in einem SSI-basierten Identitätsmanagement eindeutig zu identifizieren, können sogenannte **Decentralized Identifiers** (dezentrale Identifikatoren, DIDs) verwendet werden (Butincu & Alexandrescu, 2024). DIDs funktionieren ähnlich wie die Telefonnummern in einem Telefonbuch. Über die DID-Methode wird zusätzlich gespeichert, wie eine sichere Kommunikation zu einer bestimmten Entität aufgebaut werden kann. DIDs sind eindeutige, standardisierte[36] und dezentral vergebene Identifikationsnummern für Entitäten wie Personen oder Organisationen und verweisen auf dazugehörige DID-Dokumente, die kryptografische Schlüssel und Daten für die Authentifizierung und Interaktion enthalten (vgl. Abbildung 7; Sporny et al., 2022). Der Holder kann den Besitz einer DID durch seinen privaten Schlüssel[37] nachweisen. Issuer und Verifier können wiederum das öffentlich zugängliche DID-Dokument einsehen, das wie die DID selbst in einer **Verifiable Data Registry** (überprüfbares Datenregister) gespeichert ist (Butincu & Alexandrescu, 2024; Mazzocca et al., 2025).[38]

[36] DIDs folgen einem standardisierten Schema, das vom World Wide Web Consortium (W3C) veröffentlicht wurde (vgl. Sporny et al., 2022).
[37] Schlüssel (*Keys*) und Schlüsselrotation (*Key Rotation*) spielen eine zentrale Rolle für die Sicherheit von DIDs und SSI-basierten Identitätsmanagementsystemen. In solchen Systemen erfolgt die sichere, dezentrale Identifizierung mithilfe einer *Public Key Infrastructure* (PKI) und dazugehöriger Schlüsselpaare: Der private Schlüssel bleibt geheim bei seinem Besitzer (zum Signieren), während der öffentliche Schlüssel für alle sichtbar ist (zur Verifikation). Mehr Informationen dazu finden Sie unter anderem bei Ernstberger et al. (2023), Everspaugh et al. (2017) und Park & Nam (2021).
[38] Weitere Informationen zu den Komponenten und der Funktionsweise einer DID-Architektur finden Sie unter anderem bei Sporny et al. (2022).

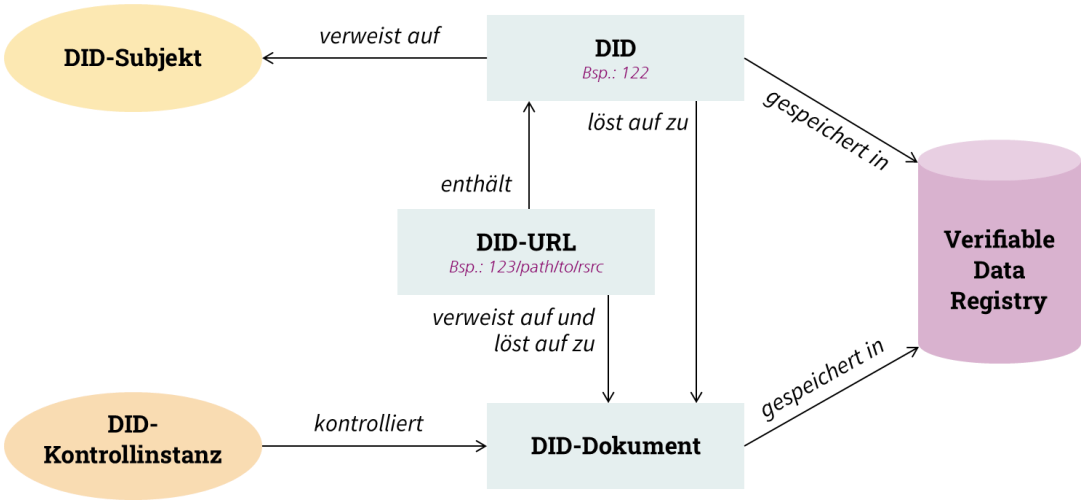

Abbildung 7: Übersicht über die DID-Architektur und die Beziehungen der grundlegenden Komponenten in Anlehnung an Sporny et al. (2022)

Die Verifiable Data Registry ist ein zentrales Element der dezentralen Identitätsinfrastruktur, um DIDs und VCs verwalten zu können. Um ein skalierbares und sicheres System zu gewährleisten, kann die Identitätsinfrastruktur in drei Schichten mit unterschiedlichen Aufgaben aufgeteilt werden: Die Zugriffe auf das Identitätsmanagementsystem erfolgen über den sogenannten *Entry Layer*, der als Frontend für die Nutzerinnen und Nutzer dient und Sicherheitsaspekte kontrolliert. Der *Core Layer* ist für die Ausführung der Prozesse verantwortlich und der *Storage Layer* für die Dokumentation des gesamten Systemzustands.[39] Der Storage Layer kann je nach Architektur ein Distributed Ledger (vgl. Kapitel 2.1) oder ein verteiltes Dateisystem bzw. Peer-to-Peer-Netzwerk (vgl. Kapitel 2.3) sein oder alternativ auch mit einer zentralen Datenbank bei einer vertrauenswürdigen Instanz (z. B. einer Behörde) umgesetzt werden (Butincu & Alexandrescu, 2024). Ein Wallet-basiertes Identitätsmanagement mit Identifiern wie DIDs muss also nicht zwingend auf einer Blockchain basieren, um den SSI-Prinzipien gerecht zu werden. Zur Reduktion der Komplexität und zur Steigerung der Skalierbarkeit können auch alternative Speicherungen von dezentralen Identifiern umgesetzt werden.

Technischer Entwicklungsstand

Die ersten Implementierungen eines SSI-basierten Identitätsmanagements basierten auf DLTs, insbesondere der Blockchain, um Dezentralisierung und Nachvollziehbarkeit zu erreichen. Der Distributed Ledger fungiert dabei als Verifiable Data Registry, in der jene Daten gespeichert werden, die in SSI-basierten Systemen zum Zwecke der Überprüfung öffentlich zugänglich sein müssen (Drăgnoiu, 2021; Ghaffari et al., 2022). Die Nutzung von DLTs für SSI-basierte Systeme geht jedoch auch mit Limitationen einher, zum Beispiel im Zusammenhang mit Datenschutz oder Governance (vgl. Kapitel 0, Rieger at al., 2019). Daher sind bei der Entwicklung von SSI-basierten Systemen für spezifische Anwendungsfälle (z. B. Know-Your-Customer-Prozesse im Finanzwesen, elektronische Rezepte im Gesundheitswesen) unterschiedliche Architekturen entstanden, die sich beispielsweise darin unterscheiden, welche Informationen auf einem Distributed Ledger (*onchain* bei Blockchains) gespeichert werden und wer Zugang zu ihnen hat (*permissionless* vs. *permissioned* bei Blockchains) (Babel et al., 2025; Höß et al., 2022; Deutsche Energie-Agentur, 2025b).

[39] Der Storage Layer enthält damit insbesondere die Daten, die zum Herstellen des Vertrauens im dezentralen Identitätsmanagementsystem und für die Interaktionen von Holder, Issuer und Verifier benötigt werden (z. B. öffentliche Schlüssel).

Im Laufe der Zeit wurden auch alternative SSI-Implementierungsansätze entwickelt, die nicht auf einer DLT basieren (van Bokkem et al., 2019). Diese Entwicklungen zeigen, dass ein SSI-basiertes System nicht an eine spezifische Infrastruktur gebunden ist. So können SSI-Lösungen auch mit bestehenden Identitätsmanagementsystemen kombiniert werden, um den Übergang zu dezentralen Identitäten schrittweise zu erleichtern (Sedlmeir et al., 2021). Ein konkretes Beispiel für die Integration in bestehende Identitätsmanagementsysteme ist Keycloak, eine Open-Source-Software für das Identitäts- und Zugriffsmanagement, die durch Erweiterungen die Authentifizierung mit SSI-basierten Identitäten auf Basis bekannter Protokollstandards wie OAuth 2.0 und OpenID ermöglichen will (Castellano et al., 2024; de Oliveira et al., 2024). Während solche Lösungen die Integration von SSI in bestehende Identitätsmanagementsysteme voranbringen können, müssen für einen schrittweisen Übergang zu SSI-basierten Systemen bestehende Limitationen und offene Fragestellungen zu Standardisierung und Interoperabilität (z. B. mit bestehenden Identitätsmanagementlösungen) beantwortet und bei dem Design von SSI-basierten Architekturen berücksichtigt werden (Babel et al., 2025; Schardong & Custódio, 2022).

Im Bereich der Standardisierung von SSI-basierten Systemen und der dazugehörigen vorgestellten Kernelemente gab es in den letzten Jahren bereits einige Fortschritte. Die Standardisierungsaktivitäten fokussieren sich dabei zuerst auf digitale Identitäten von natürlichen Personen. Das spiegelt sich unter anderem in der novellierten eIDAS-Verordnung (*eIDAS 2.0*, Electronic Identification, Authentication, and Trust Services) wider (Europäische Union, 2024). Die novellierte Verordnung schafft auf EU-Ebene den regulatorischen Rahmen, um eine harmonisierte Infrastruktur für digitales Identitätsmanagement über alle Mitgliedstaaten hinweg technisch aufzubauen. Ein wichtiger Bestandteil der Verordnung ist die Verpflichtung für die EU-Mitgliedstaaten, ihren Bürgerinnen und Bürgern eine digitale Wallet (sogenannte *EUDI-Wallet*) gemäß dem „EUDI Architecture and Reference Framework“ zur Verfügung zu stellen (Ebadi Ansaroudi et al., 2025; Europäische Kommission, 2024). Die EUDI-Wallet soll zukünftig die in eIDAS 2.0 festgelegten Sicherheits- und Interoperabilitätsanforderungen für digitales Identitätsmanagement erfüllen und es den EU-Bürgerinnen und -Bürgern ermöglichen, persönliche Identifikationsdaten (z. B. digitale Personalausweise) und andere Nachweise (z. B. digitale Führerscheine, digitale Bildungszertifikate) in Form von VCs selbst zu verwalten. Dabei kommen zunehmend technische Standards wie OpenID for Verifiable Credential Issuance (OID4VCI) und OpenID for Verifiable Presentations (OID4VP)[40] zum Einsatz, um innerhalb bestehender, dezentraler europäischer Infrastrukturen wie der EBSI SSI-basierte Identifikation und Autorisierung durchzuführen sowie VCs und VPs auszustellen (European Blockchain Services Infrastructure, 2022; European Blockchain Services Infrastructure, 2025). Durch den standardisierenden Rahmen von eIDAS 2.0 für europäische digitale Identitäten sollen Authentifizierungen und die Nutzung von Online-Diensten grenzübergreifend innerhalb der EU möglich sein (Ebadi Ansaroudi et al., 2025; Urbach et al., 2024).

Eine weitere Herausforderung und Governance-Fragestellung besteht in der Entwicklung eines sektorenübergreifenden und akzeptierten Trust Framework für die Einführung und Nutzung von digitalem und dezentralem Identitätsmanagement. Ein *Trust Framework* ist ein System von Regeln, Standards und Vereinbarungen, das definiert, wie Vertrauen zwischen verschiedenen Parteien in einem digitalen Identitätssystem aufgebaut, verwaltet und erhalten wird (de Salve et al., 2023; Jeyakumar & Kubach, 2025, Deutsche Energie-Agentur, 2025b). Für den Vertrauensaufbau zwischen den verschiedenen Akteuren innerhalb eines Sektors sowie sektorenübergreifend müssen daher unterschiedliche Fragestellungen beantwortet werden. Das betrifft z.B.

[40] OID4CI und OID4VP basieren auf den Industriestandards OAuth 2.0 für Autorisierung und OpenID Connect (OIDC), für Authentifizierung. OID4CI definiert (API-)Schnittstellen und auf OAuth 2.0 basierende Autorisierungsmechanismen zur Ausstellung von VCs. OID4VP definiert die Mechanismen auf Basis von OAuth 2.0, mit denen die Präsentation von Verifiable Claims in Form von VCs ermöglicht wird. Weiterführende Informationen zur Funktionsweise mit EBSI finden Sie unter anderem bei European Blockchain Services Infrastructure (2022).

die Frage der Authentifizierung, die je nach Akteur durch andere Identitätsmerkmale erfolgen könnte (Beispiel: „Welcher Akteur hat das Recht, zu bestimmen, dass eine bestimmte Maschine ein E-Fahrzeug ist?“). Es bedarf klarer Definitionen dazu, welche Daten eine digitale Identität enthalten muss, um eine eindeutige Identifikation zu gewährleisten (Beispiel: „Was ist ein E-Fahrzeug?“). Diese Definitionen sind für physische Objekte und für ihre digitale Repräsentation notwendig, um die digitale Identität und die dazugehörigen Identitätsmerkmale über unterschiedliche Anwendungsfälle hinweg zu nutzen (Luecking et al., 2020).

Damit digitale Identitäten sektorenübergreifend genutzt werden können, muss daher ein einheitliches und akzeptiertes Framework geschaffen werden. Die resultierende Interoperabilität digitaler Identitäten über Sektorengrenzen kann dazu beitragen, dass einmal ausgestellte Identitäten für unterschiedliche Anwendungsfälle wiederverwendet werden können, ohne dass redundante Verifizierungsprozesse erforderlich sind (Funke et al., 2024). Für ein solches funktionierendes Ökosystem braucht es jedoch eine kritische Masse an Anwendungsfällen und Akteuren, die sich auf ein bestimmtes Trust Framework einigen. In der Energiewirtschaft könnten insbesondere die bereits bestehenden Vertrauensstrukturen und Definitionen der Marktrollen dazu beitragen, frühzeitig eine kritische Masse zu erreichen und ein entsprechendes Trust Framework für den Energiesektor zu etablieren (EnBW Energie Baden-Württemberg AG, 2025; Gramlich et al., 2023b).

Zu erwartende Entwicklungen

Mit der fortschreitenden Entwicklung von digitalen und dezentralen Identitätsmanagementsystemen entstehen zunehmend neue Anwendungsfelder, die über den Bereich der Identifizierung natürlicher Personen hinausgehen. Dazu zählen insbesondere erste Ansätze für digitale Identitäten von Organisationen wie Behörden oder Unternehmen (d. h. juristischen Personen), die ihre sichere Authentifizierung und Autorisierung ermöglichen. Mit der EUDI-Wallet könnten beispielsweise auch juristische Personen ihre Identität verwalten. Durch die Verknüpfung von digitalen Personen- und Organisationsidentitäten könnte zudem zukünftig die Delegation von Rechten und Vertretungsberechtigungen digital festgehalten und genutzt werden (Deimel et al., 2025). Ebenso nimmt das Interesse zu, dezentrale Maschinen-Identitäten zu entwickeln, die beispielsweise im Kontext des Internet of Things (IoT) intelligente Geräte und Sensoren eindeutig identifizieren und verwalten können und somit die Kommunikation zwischen Maschinen sicherer gestalten könnten (Schukat & Cortijo, 2015). Eine Maschine könnte sich dann mit den in der Maschinen-Wallet gespeicherten Identifiern (z. B. DIDs) und digitalen Zertifikaten (z. B. in Form von VCs) selbst ausweisen (Hühnlein et al., 2025; Su et al., 2020) und so sicher an automatisierten Prozessen teilnehmen.

Die Entwicklung von Maschinen-Identitäten könnte eine Vielzahl an energiewirtschaftlichen Anwendungsfällen vereinfachen, in denen Anlagen und Sensoren identifiziert werden müssen, um sichere und effiziente Interaktionen im Energiesektor zu ermöglichen. Während eIDAS 2.0 bereits einen regulatorischen Rahmen für die Entwicklung von digitalen Identitätslösungen für natürliche und juristische Personen fördert, existieren für Maschinen-Identitäten und dazugehörige Wallets noch keine etablierten Lösungen oder Standards (Babel et al., 2025). Eine zentrale Herausforderung in diesem Zusammenhang ist die Integration dezentraler Identifikationsmechanismen in die übergeordneten Prozesse der Energiewirtschaft. Bislang fehlt im Energiesektor ein konsistentes digitales Zielbild für plattform- und anwendungsübergreifende Interoperabilität eines möglichen dezentralen Identitätsmanagementsystems (Dognini et al., 2024). Dies ist aber notwendig, um standardisierte Mechanismen und Infrastrukturen zu entwickeln und Maschinen wie dezentral verteilte Energieanlagen digital sicher in das Energiesystem einbinden zu können. Daher ist eine sichere und vertrauenswürdige Maschinenkommunikation bisher nur eingeschränkt möglich ist.

Für die Entwicklung dezentral verwalteter digitaler Identitäten ergibt sich der Zielkonflikt zwischen einem offenen Identitätsmanagementansatz und der Sicherheit.[41] Dabei kann dem Ziel der maximalen Sicherheit und einer damit verbundenen strikten Regulierung eines solchen Ansatzes die Offenheit und damit Wiederverwendbarkeit von digitalen Identitäten für mehrere Anwendungsfälle entgegenstehen. So zeigt sich am Beispiel des Smart Meter Gateway (SMGW) bzw. des intelligenten Messwesens in Deutschland, dass sich digitale Identitäten aufgrund der sehr hohen regulatorischen Sicherheitsanforderungen nur mit hohem Aufwand in die SMGW-Infrastruktur integrieren lassen (Bundesamt für Sicherheit in der Informationstechnik, 2025; Deutsche Energie-Agentur, 2025a; Förderer et al., 2019; Kroener et al., 2020). Um den Grad an Offenheit und Wiederverwendbarkeit eines Identitätsmanagementansatzes zu erhöhen, ohne dabei die Sicherheit zu gefährden, können für die eindeutige Identifikation von Anlagen Hardware Security Modules eingesetzt werden. Sie binden die digitale Identität dauerhaft und sicher an eine physische Anlage (Babel et al., 2023).

Eng verbunden mit der Diskussion zum Grad der Sicherheit ist die Notwendigkeit der technischen Interoperabilität. Auch wenn sichere Hardwarekomponenten eindeutige Identifikatoren ermöglichen, könnten unklare Zuständigkeiten oder proprietäre Schnittstellen neue Abhängigkeiten schaffen und damit die Offenheit der Identitätsinfrastruktur stark einschränken. Für die Akteure im Energiesektor bedeutet dies unter anderem, dass eine gemeinsame Governance-Struktur für ein dezentrales Identitätsmanagement erarbeitet werden muss. Diese Governance-Struktur sollte die folgenden Fragestellungen beantworten: Wer darf Identitäten oder Zertifikate ausstellen? Wer verwaltet und überprüft sie? Wie lassen sich potenzielle Lock-in-Effekte durch zentralisierte und/oder proprietäre Identitätsmanagementlösungen vermeiden?

Im Hinblick auf die Skalierbarkeit eines dezentralen Identitätsmanagements ist ein weiterer Diskussionspunkt, ob DIDs oder andere Identifier für alle Anlagen innerhalb eines Energiesystems notwendig wären. So könnte es auch ausreichen, wenn nur bestimmte zentrale Akteure wie Netzbetreiber und nicht jede Kleinstanlage mit einer DID ausgestattet werden.[42] Ebenfalls sollte diskutiert werden, inwiefern es sinnhaft wäre, Ansätze des dezentralen Identitätsmanagements mit Elementen aus zentralisierten Ansätzen zu verknüpfen. So muss beispielsweise die Bereitstellung von gespeicherten Identifiern nicht zwingend mittels einer dezentralen Infrastruktur erfolgen, sondern mithilfe eines zentralen Registers bei einer unabhängigen Partei.

Identitätslösungen – insbesondere solche, die die SSI-Prinzipien realisieren – könnten für den Aufbau und die Nutzung von Datenräumen eine zentrale Rolle spielen, indem sie das Identitäts- und Zugriffsmanagement deutlich vereinfachen: Wenn Nutzerinnen und Nutzer ihre digitalen Identitäten selbst verwalten und selektiv Informationen freigeben können, lassen sich diese Identitäten datenraumübergreifend einsetzen. So entsteht eine interoperable Identitätsinfrastruktur, die eine vertrauenswürdige Verknüpfung unterschiedlicher digitaler Ökosysteme ermöglicht – und damit nicht nur Skaleneffekte nutzt, sondern auch zur Stärkung der europäischen Datenökonomie beiträgt. In Projekten wie EDDIE (European Distributed Data Infrastructure for Energy)[43] und energy data-X[44] werden dezentrale Identitätslösungen bereits im Zusammenhang mit Datenräumen erarbeitet (Hartner et al., 2024; Stöcker, 2025). Im Rahmen des Aufbaus eines Dateninstituts beschreibt die dena im „Use Case Energie“ ein Referenzsystem für den anwendungsorientierten Datenaustausch im Energiesystem (Deutsche Energie-Agentur, 2025c).

[41] Dezentral verwaltete digitale Identitäten basieren auf einem offenen Ansatz, bei dem Quellcode, Schnittstellen und Protokolle öffentlich zugänglich sind (Transparenz). Statt auf Security-by-Obscurity setzt dieses Modell auf Security-by-Design und Security-by-Transparency. Durch den offenen Ansatz können Fehler schneller erkannt und behoben werden. Zwar ist die Angriffsfläche bei einem offenen Ansatz potenziell größer (mehr Informationen sind öffentlich), jedoch ist bei einem geschlossenen, proprietären System der potenzielle Schaden bei erfolgreichen Angriffen oft höher.
[42] Ein Beispiel dafür, wie eine Identitätslösung aussehen kann, die mehrere Identitätsmanagementansätze miteinander vereint, finden Sie unter anderem bei Gödde et al. (2020).
[43] Weitere Informationen zum Projekt EDDIE finden Sie unter https://eddie.energy/ (European Distributed Data Infrastructure for Energy, 2025).
[44] Weitere Informationen zum Projekt energy data-X finden Sie unter https://www.energydata-x.eu/ (energy data-X, 2025).

2.3 Dezentrale Speicherung

Die Datenspeicherung im Web1.0 und Web2.0 basiert auf einer zentral ausgerichteten Infrastruktur, in der einzelne Organisationen zentrale Knotenpunkte betreiben. Mit der Entwicklung von Cloud Computing ermöglichten solche zentralisierten Strukturen der Datenspeicherung eine bis dahin nicht gekannte effiziente und skalierbare Verwaltung von Daten und Services für Nutzerinnen und Nutzer (Armbrust et al., 2009).[45] Diese zentralisierten Strukturen der Datenspeicherung haben jedoch in der Folge dazu geführt, dass marktbeherrschende Unternehmen personenbezogene Daten sammeln und monetarisieren können – ohne die Zustimmung der Nutzerinnen und Nutzer einholen zu müssen oder sie darüber zu informieren (Shi et al., 2025). Mit dem Web3 sind mit der dezentralen Speicherung von Daten technische Ansätze entwickelt worden, um das Vertrauen in mächtige Intermediäre zu ersetzen. Bei diesen Ansätzen werden Daten auf verteilten Netzwerken statt auf zentralisierten Servern gespeichert, wodurch verhindert wird, dass Daten bei einem oder wenigen Akteuren konzentriert gespeichert werden. Diese dezentralen Datenspeicherlösungen werden oftmals als der *Storage Layer* eines dezentralisierten Webs oder als *Peer-to-Peer Data Networks* bezeichnet (Daniel & Tschorsch, 2022; Trautwein et al., 2022). Die dezentrale Datenspeicherung im Web3 zeichnet sich insbesondere dadurch aus, dass die Verwaltung von Daten nicht bei einem einzelnen Akteur liegt (vgl. Abbildung 8).

Es gibt unterschiedliche Ausprägungen und Entwicklungsstufen von dezentralen Speicherlösungen: Einer der ältesten und dadurch am weitesten verbreiteten und untersuchten Ansätze ist das *InterPlanetary File System (IPFS)*, das Dateien über ein Peer-to-Peer-Netzwerk verteilt. Neben IPFS gibt es weitere Ansätze wie Storj, das Cloud-Speicher auf einer dezentralen Plattform bereitstellt, wobei die Nutzerinnen und Nutzer ihre ungenutzte Festplattenkapazität zur Verfügung stellen. Swarm und Arweave sind weitere Beispiele für Peer-to-Peer-Netzwerke, die auf einem Blockchain-ähnlichen Protokoll aufbauen. Im Nachfolgenden werden die Funktionsweise und die Entwicklung von dezentraler Datenspeicherung im Vergleich zu zentralisierten Architekturen am Beispiel von IPFS erläutert.[46]

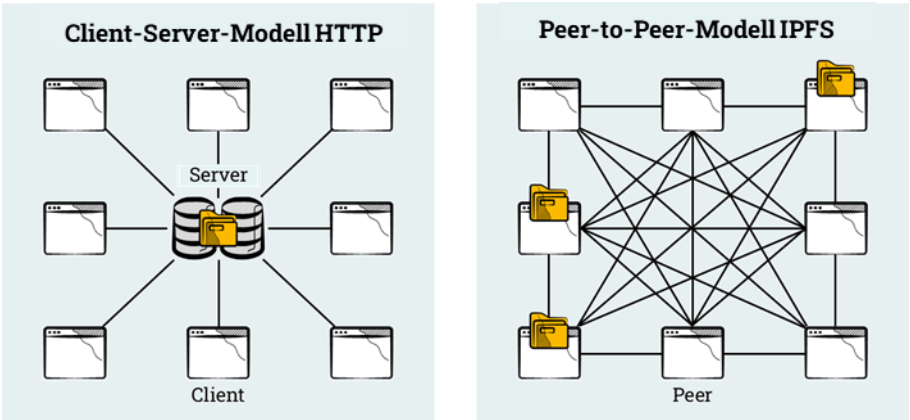

Abbildung 8: Zentralisierte vs. dezentralisierte Datenspeicherung am Beispiel von IPFS

[45] Cloud Computing ermöglicht eine effiziente Datenverwaltung und Bereitstellung von Services durch eine flexible und bedarfsgerechte Nutzung von Rechenressourcen sowie eine zentralisierte Optimierung der dazugehörigen Datencenter. Die Datenverwaltung wird zudem oft durch zentralisierte API-Schnittstellen zur Speicherung, zur Verarbeitung und zum Zugriff über die gesamte Cloud-Infrastruktur hinweg koordiniert. Weitere Erläuterungen finden Sie unter anderem bei Armbrust et al. (2009).

[46] Die Erläuterung weiterer Ansätze für dezentrale Datenspeicherung finden Sie unter anderem bei Daniel & Tschorsch (2022).

Anders als herkömmliche Web-Protokolle, die Inhalte über ortsbasierte URLs (z. B. Domain- oder Serveradressen) adressieren, verwendet IPFS **Content Addressing**: Jedes Objekt (z. B. eine Datei) in einem IPFS wird in einzelne Stücke bzw. Blöcke unterteilt, die durch einen einzigartigen kryptografischen *Hash* identifiziert werden können, den **Content Identifier (CID)** („Inhaltsidentifikator" bzw. „Inhaltsadresse") (Daniel & Tschorsch, 2022). Er leitet sich ausschließlich aus dem Inhalt einer Datei ab und ist unabhängig vom Speicherort (Kumar et al., 2021; Trautwein et al., 2022). Dadurch kann ein bestimmter Datensatz jederzeit verlässlich referenziert werden, unabhängig davon, wo er gespeichert ist. Diese Verteilung verhindert, dass ein einzelner oder wenige Akteure den Zugriff auf die Daten bzw. die Datei oder den Datenfluss kontrollieren können. Ebenso kann die Zerlegung von Dateien in kleine Blöcke die Dezentralisierung und Skalierbarkeit gewährleisten. Diese Hashes werden in einer hierarchischen Struktur, einem *Merkle-DAG*[47], organisiert. Mithilfe dieses Merkle-DAG können selbst große Dateien effizient adressiert und überprüft werden. Der *Root Node* des Merkle-DAG fasst dann alle CIDs der Blöcke zusammen, die zu einer Datei gehören (Protocol Labs, 2021; Trautwein et al., 2022). Das Prinzip der *Versionierung* ermöglicht zudem eine integre und manipulationssichere Datenstruktur, da jede Änderung am Inhalt automatisch zu einer neuen CID führt. Dadurch ist die dezentrale Speicherung *zensurresistent*. Ebenso kann somit kein einzelner Akteur eine Datei offline nehmen oder den Zugriff zur Datei gefährden (Daniel & Tschorsch, 2022; Trautwein et al., 2022).

Wie andere Web3-Technologien greifen Lösungen zur dezentralen Datenspeicherung wie IPFS, Swarm und Arweave auf bekannte Bausteine einer Peer-to-Peer-Kommunikation zurück, die je nach Lösung anders ausgeprägt sein können. In Bezug auf die dezentrale *Netzwerk-Architektur* unterscheiden sich die Lösungen beispielsweise nach strukturierten und unstrukturierten Netzwerken. Bei strukturierten Netzwerken (z. B. Swarm) ist die Auswahl eines Nachbarknotens (Peer) von der Identität[48] eines Knotens abhängig. Bei unstrukturierten Netzwerken (z. B. IPFS) können Knoten ohne spezifische Regeln und ohne Berücksichtigung von Identitätsmerkmalen eine Verbindung aufbauen. Ein strukturiertes Netzwerk ermöglicht eine effizientere Datensuche und einen effizienteren Datenabruf im dezentralen Netzwerk. Zudem ist ein solches Netzwerk durch die systematische Topologie der Knoten skalierbarer und einfacher zu verwalten als ein unstrukturiertes Netzwerk. Im Gegensatz dazu ist das Aufsetzen eines strukturierten Netzwerks deutlich komplexer und weniger resilient gegenüber gezielten Angriffen als ein unstrukturiertes Netzwerk (Daniel & Tschorsch, 2022).

In Bezug auf das *File Handling*[49] werden, ähnlich wie bei der Torrent-Technologie (z. B. BitTorrent) als Vorgänger von dezentralen Speicherlösungen, Dateien fragmentiert, wobei die Lösungen unterschiedliche Ansätze zur Verteilung, Adressierung und Suche von Datenstücken verfolgen. Die *Informationssicherheit* wird durch Verschlüsselung, Content Addressing und Replikation gewährleistet, wobei Vertraulichkeit über Zugriffskontrollen und Integrität über Hashes erreicht wird. Um kooperatives Verhalten und langfristige Datenverfügbarkeit zu fördern, setzen die meisten Netzwerke auf Anreizmechanismen wie Tokens (vgl. Kapitel 0), wobei sowohl Speicherung als auch Datenabruf belohnt werden und unkooperatives Verhalten sanktioniert wird (Daniel & Tschorsch, 2022). Durch die Redundanz der auf mehreren verteilten Systemen gespeicherten Dateien entfällt die Notwendigkeit zentraler Server, was das Risiko eines *Single Point of Failure* reduziert (Daniel & Tschorsch, 2022; Huang et al., 2020). Peers im Netzwerk können Daten gegenseitig bereitstellen, ohne dass ein direktes Vertrauensverhältnis erforderlich ist. Die Redundanz im verteilten System erhöht zwar

[47] Ein Merkle-DAG ist eine Struktur ähnlich einem Merkle-Tree. Weitere Informationen zum Merkle-DAG in IPFS finden Sie unter anderem bei Protocol Labs (2021).
[48] Die Identität eines Knotens ist meist der öffentliche Schlüssel oder sein Hash der für die Identifizierung im dezentralen Netzwerk angelegten Schlüsselpaare. Bei Swarm setzt sich die Knotenidentität beispielsweise aus der Netzwerk-ID und einer Ethereum-Adresse zusammen (vgl. Daniel & Tschorsch, 2022).
[49] File Handling bezeichnet in einer dezentralen Datenspeicherungslösung die Prozesse, die mit dem Speichern, Teilen und Abrufen von Daten bzw. Dateien innerhalb des dezentralen Netzwerks einhergehen.

die Ausfallsicherheit und damit die *Datenverfügbarkeit*, steht jedoch im Zielkonflikt mit einer oft geringeren Geschwindigkeit im Vergleich zu herkömmlichen Web-Protokollen und ist daher insbesondere für die Nutzung von Echtzeit-Daten nicht immer geeignet.

Technischer Entwicklungsstand

IPFS ist heute ein weit verbreitetes dezentrales Netzwerk für die Datenspeicherung und bildete die Grundlage für die Entwicklung weiterer dezentraler Datenspeicherungslösungen.[50] Eine beispielhafte Entwicklung basierend auf IPFS, die die Nutzung solcher Lösungen vorangebracht hat, ist *Filecoin*. Filecoin entstand 2017 und integriert ein ökonomisches Anreizsystem, das es den Nutzerinnen und Nutzern ermöglicht, Speicherkapazitäten zu vermieten und eine dauerhafte Speicherung von Daten sicherzustellen (Protocol Labs, 2017). Damit fungiert Filecoin als wirtschaftliche Schicht in einem verteilten Ökosystem. Swarm und Secure Access For Everyone (SAFE) sind weitere Netzwerke, die unter anderem neue Formen für das File Handling und die Verschlüsselung von Dateien integriert haben und, im Falle von Swarm, mit einer Blockchain (hier: Ethereum) integriert sind (Daniel & Tschorsch, 2022). Neben der Verknüpfung mit Web3-Technologien nimmt auch die Interoperabilität mit Nicht-Web3-Anwendungen und -Systemen zu. So sind IPFSs zunehmend mit bekannten Browsern wie Opera und Brace kompatibel, was den Zugang zu IPFS vereinfacht (Doan et al., 2022). Ebenso besitzen einige dezentrale Netzwerke Schnittstellen zu zentralen Cloud-Diensten[51], um die Migration für die Nutzerinnen und Nutzer einfacher zu gestalten (Daniel & Tschorsch, 2022; Trautwein et al., 2022).

Trotz der genannten Fortschritte bestehen einige Herausforderungen, die die Nutzung von dezentralen Datenspeicherungslösungen einschränken. Ein zentrales Problem ist die **Persistenz der Daten**. IPFS und andere dezentrale Datenspeicherungslösungen können noch nicht garantieren, dass ein einmal hinzugefügter Inhalt dauerhaft im Netzwerk bleibt. Entfernt ein Knoten den Inhalt oder geht offline und es gibt keine weiteren Kopien im Netzwerk, ist die Datei über den zugehörigen Hash nicht mehr abrufbar. Die Verfügbarkeit von Inhalten ist daher primär nur durch Redundanz sichergestellt. Um das Speichern und das Kopieren von Dateien für die Teilnehmerinnen und Teilnehmer im Netzwerk attraktiv zu gestalten, bieten Lösungen wie Filecoin, SAFE (mit dem Safecoin) und BitTorrent (mit dem BitTorrent Token) finanzielle Anreize, die meist auf Kryptowährungen basieren. Dadurch soll die dezentrale Speicherung preiswerter werden als die zentrale Speicherung über Cloud-Dienste (Daniel & Tschorsch, 2022; Doan et al., 2022). Dieser Ansatz adressiert das Problem der Persistenz, weshalb erste Anbieter wie Filebase oder Web3.Storages eine langfristige Verfügbarkeit von Dateien gewährleisten können.[52]

Zum aktuellen Entwicklungsstand von IPFS und ähnlichen verteilten Ökosystemen existieren zum Teil erhebliche Bedenken hinsichtlich des **Datenschutzes**. Jeder, der den Inhaltsidentifikator (d. h. die CID) einer Datei kennt, kann sie abrufen bzw. herunterladen. Das IPFS selbst bietet keine eingebaute Zugriffskontrolle. Das bedeutet, dass Daten vor dem Upload verschlüsselt oder anonymisiert werden müssen. Hier könnten beispielsweise ZKPs oder andere kryptografische Ansätze verwendet werden, um die Privatsphäre der Nutzerinnen und Nutzer zu schützen oder selektiven Zugriff auf bestimmte Informationen zu ermöglichen, während gleichzeitig die Integrität der Daten gewährleistet bleibt (Doan et al., 2022; Shibano et al., 2024; Tiwari & Kumar, 2025). Wie bei anderen Formen dezentraler Technologien entsteht ein erhöhter Aufwand für die Nutzerschaft durch die steigende Eigenverantwortung bei der Datensicherheit. Der Aufwand geht daher

[50] Laut Protocol Labs hostete das IPFS-Netzwerk Anfang 2025 mehr als 450 Millionen Dateien und verfügte weltweit über mehr als 300.000 aktive Knoten. Diese Zahlen basieren auf internen Messungen von Protocol Labs (Protocol Labs, 2025).
[51] Die dezentrale Datenspeicherungslösung Storj hat beispielsweise eine Schnittstelle zu einem Cloud-Dienst von Amazon (Storj Labs Inc., 2024).
[52] Hierfür werden unter anderem *Pinning Services* genutzt. Weitere Informationen zu Pinning finden Sie unter anderem bei Trautwein et al. (2022).

mit einem gewissen Komfortverlust einher, sodass die Akzeptanz für eine solche Technologie maßgeblich von der Bereitschaft zu verändertem Nutzerverhalten abhängt. Datenschutzbedenken bestehen in einer dezentralen Datenspeicherungslösung auch in Bezug auf Informationen zu den Erstellern der Inhalte, den Speicherknoten und den Nutzerinnen und Nutzern, die die Inhalte anfordern. Während es bei IPFS möglich ist, durch die Beobachtung der Datenanfragen die jeweiligen Anfrager zu identifizieren, wird bei Swarm und SAFE ihre Identität zumindest durch Proxys abgesichert (Balduf et al., 2022; Daniel & Tschorsch, 2022).

Ein weiteres bedeutendes Problem sind die **Skalierbarkeit** und die **Performanz** von IPFS. Die Architektur von IPFS ist nicht auf Geschwindigkeit[53] optimiert, was insbesondere für Anwendungen wie Echtzeit-Übertragungen (z. B. Videostreaming via YouTube) Einschränkungen mit sich bringt (Shen et al., 2019, Wennergren et al., 2018). Zentrale Systeme wie beispielsweise Server, Content Delivery Networks oder zentrale Cloud-Architekturen werden voraussichtlich weiterhin schneller und responsiver sein als dezentrale Speichersysteme. Diese Einschränkungen sind besonders relevant für *zeitkritische Anwendungen*. Beispielsweise ist die Nutzung von IPFS für Live-Messdaten aus dem Energiesystem oder für IoT-Sensoren, die in Echtzeit Daten liefern müssen, im Nachteil gegenüber bestehenden zentralen Speicheroptionen, da das dezentrale Speichermodell kritische Verzögerungen verursachen könnte. Zum jetzigen Zeitpunkt sind dezentrale Speichermodelle daher eher für die langfristige, verifizierbare Datenspeicherung geeignet.[54] Trotzdem können (z. B. bei IPFS) neue Protokolle (z. B. IPFS Cluster) oder vergleichbare neue Indexierungsmechanismen dazu führen, dass der Datenzugriff schneller erfolgt, und somit neue Anwendungsfälle ermöglichen (Lamichhane & Herbke, 2024).

Zu erwartende Entwicklungen

Während sowohl DLTs als auch dezentrale Datenspeicherlösungen darauf abzielen, Daten sicher und ohne zentrale Kontrolle zu speichern und bereitzustellen, unterscheiden sie sich grundlegend in ihrem Einsatzzweck und ihrer Funktionsweise. Blockchain ist primär für Transaktionsdaten konzipiert und eignet sich besonders für Anwendungen, bei denen Transparenz und Nachvollziehbarkeit entscheidend sind. Dezentrale Netzwerke zur Datenspeicherung sind hingegen für die Speicherung großer, statischer Daten optimiert. Während auf einer Blockchain aufgrund von Skalierbarkeits- und Kostenproblemen nur in sehr begrenztem Umfang Daten gespeichert werden sollten, ermöglichen dezentrale Speicherungslösungen die dezentrale Ablage umfangreicher Dateien wie Dokumenten, Bildern oder Videos. Daher steigt beispielsweise die Nutzung von dezentraler Datenspeicherung in Bereichen wie verteilten Datenarchiven. Zudem finden sich bereits viele Anwendungsfälle, die insbesondere Blockchains und dezentrale Datenspeicherungslösungen miteinander verbinden. So wird IPFS bereits von vielen Nutzerinnen und Nutzern verwendet, um ihre Non-Fungible Tokens (NFTs)[55] zu speichern (Shi et al., 2024; Trautwein et al., 2022). Perspektivisch könnten Kombinationen beider Technologien auch für andere Anwendungsfälle eine Rolle spielen: Beispielsweise können in einer Blockchain nur die Hashes (CIDs) von Dateien gespeichert werden, während die eigentlichen Inhalte über dezentrale Speicherlösungen verteilt sind. Solch ein Modell könnte insbesondere für Herkunftsnachweise (HKNs) genutzt werden, da ein solcher Ansatz die Integrität der Daten gewährleistet, ohne die Blockchain unnötig vor Effizienzprobleme zu stellen.

[53] Geschwindigkeit bezieht sich in diesem Fall insbesondere auf die Latenzzeit beim Datenzugriff.
[54] Dezentrale Speicherlösungen zeichnen sich – wie in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** ausgeführt – durch eine verteilte S truktur aus, die dadurch eine erhöhte Widerstandsfähigkeit gegenüber wirtschaftlichen, technischen oder politischen Ausfällen zentraler Akteure hat. Dadurch lässt sich eine zuverlässige und langfristige Verfügbarkeit von Daten gewährleisten, die unabhängig von einzelnen Die nstleistern ist.
[55] Weitere Erläuterungen zu NFTs finden Sie in Kapitel 0.

2.4 Datenräume und -ökosysteme

Der Übergang vom Web2.0 zum Web3 geht mit einem stärkeren Fokus auf Datensouveränität und Dezentralisierung einher. Datenplattformen im Kontext des Web2.0 sind zentralisierte Infrastrukturen, die primär der Speicherung, Verarbeitung und Bereitstellung von Daten dienen. Durch den Ansatz der „Alles aus einer Hand"-Lösung haben sich eine hohe Nutzerfreundlichkeit und eine entsprechende Anwendungsfreundlichkeit entwickelt. Dem gegenüber stehen bekannte Risiken wie eine große Abhängigkeit und Datenmissbrauch (vgl. Kapitel 2). Der Gegenentwurf im Web3 sind sogenannte Datenräume (Data Spaces). Im Gegensatz zu Plattformen handelt es sich bei Datenräumen um **föderierte Dateninfrastrukturen**, die den Austausch von Daten über organisations- und plattformübergreifende Grenzen hinweg ermöglichen, ohne dass die Daten zentral gespeichert werden müssen. Abbildung 9 illustriert die Unterschiede zwischen Datenräumen und Datenplattformen (in Anlehnung an Strnadl & Schöning, 2023). Der Datenaustausch zwischen teilnehmenden Akteuren (Datenanbieter sowie Datennutzerin oder Datennutzer) erfolgt bei Datenplattformen über eine zentralisierte Architektur. Eine Datenplattform wird von einem Plattformanbieter betrieben, der die entsprechenden Plattformdienste für die Identifizierung und Authentifizierung von Teilnehmerinnen und Teilnehmern und die Datenverarbeitung bereitstellt. In diesem Modell verlieren die Nutzerinnen und Nutzer jedoch die Kontrolle über ihre eigenen Daten, da diese innerhalb der Plattform gespeichert und verarbeitet werden. In Datenräumen hingegen werden die Daten nicht durch den Datenraumanbieter gespeichert oder verarbeitet. Er ermöglicht den Teilnehmerinnen und Teilnehmern lediglich den Zugriff auf einen gemeinsamen Datenkatalog, der der gesamten Nutzerschaft des Datenraums offensteht. Um die Datensouveränität der teilnehmenden Akteure zu gewährleisten, ermöglicht der Datenraumanbieter die Identifikation und Authentifizierung der Teilnehmerinnen und Teilnehmer sowie die Protokollierung von Metadaten für die Datentransaktionen.[56] Der Datenaustausch findet Peer-to-Peer über Datenraumkonnektoren statt.

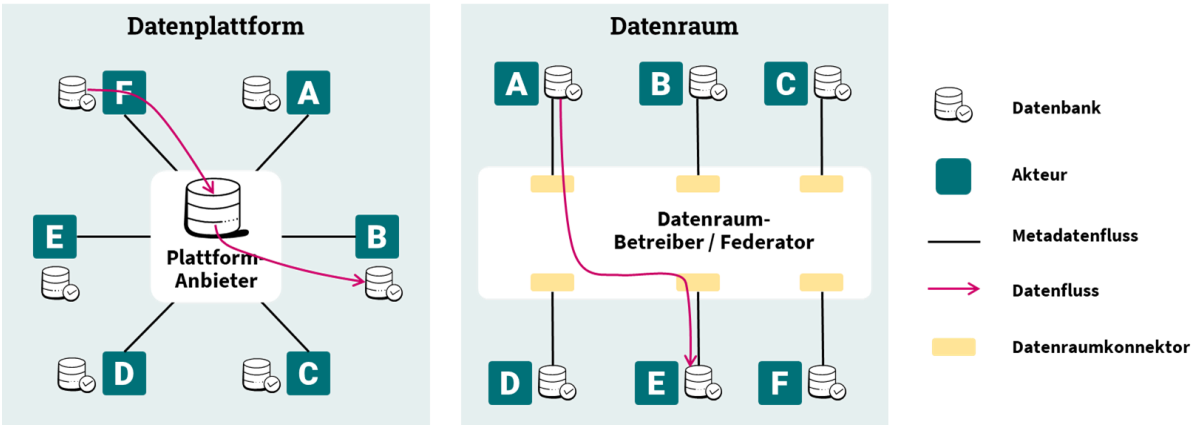

Abbildung 9: Datenplattform- und Datenraumkonzepte im Vergleich (in Anlehnung an Strnadl & Schöning, 2023)

Durch die föderierte Architektur können Datenräume den Austausch von Daten zwischen verschiedenen Unternehmen und Individuen ermöglichen, ohne dabei die Datensouveränität der Beteiligten zu gefährden

[56] Der Datenraumanbieter stellt nicht zwangsläufig eine einzelne Einheit dar. Auch mehrere Dienstleister, die selbst Datenraumteilnehmer sind, können diese Rolle übernehmen. Eine detaillierte Erläuterung der Rollen und Verantwortlichkeiten von Datenraumbetreibern sowie der dafür geltenden Vorschriften finden Sie unter anderem beim Data Spaces Support Centre (DSSC) unter https://dssc.eu/space/BVE2/1071253470/Intermediaries+and+Operators#3.2.-Intermediaries-and-operators (Data Spaces Support Centre, 2025b).

(Farell et al., 2023; Jurmu et al., 2023). Im Kontext des organisations- und plattformübergreifenden Datenaustauschs ist Interoperabilität ein entscheidender Erfolgsfaktor. Sie gewährleistet, dass Daten aus unterschiedlichen Quellen, Plattformen und Bereichen zusammengeführt, interpretiert und weiterverarbeitet werden können. Das European Interoperability Framework[57] unterteilt Interoperabilität in vier Stufen: legale, organisationale, semantische und technische Interoperabilität. Datenräume fördern alle vier Stufen von Interoperabilität, indem sie klare technische, organisatorische und rechtliche Rahmenbedingungen für den Zugriff und die Nutzung von Daten setzen (Steinbuss et al., 2024), und schaffen damit die Grundlage für innovative digitale Geschäftsmodelle (Otto, 2022; Schleimer et al., 2024).

Tabelle 3: Definition Datenraum

Datenraum
„Eine föderierte, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht.“ (Bundesministerium für Wirtschaft und Klimaschutz, 2022).

Damit eine Datenrauminfrastruktur ihre Funktion erfüllen kann, sind spezifische grundlegende Komponenten erforderlich, die einen sicheren, interoperablen und vertrauenswürdigen Datenaustausch gewährleisten. Die genannten Komponenten werden terminologisch als „Bausteine“ bezeichnet. Datenraumbausteine bilden fundamentale funktionale Anforderungen ab, die für den Aufbau und Betrieb einer Datenrauminfrastruktur essenziell sind. Diese Bausteine werden im Blueprint des Data Spaces Support Centre (DSSC)[58] in zwei Kategorien unterteilt: **ökonomische und organisationale** Bausteine sowie **technische** Bausteine (vgl. Abbildung 10). Für jeden Baustein existieren potenziell unterschiedliche Software-Implementierungen, die jedoch die gleichen funktionalen Anforderungen erfüllen müssen.

Unter den ökonomischen und organisationalen Bausteinen legen *Business*-Bausteine die wirtschaftliche Grundlage des Datenraums fest, indem sie Geschäftsmodelle, Anwendungsfälle und die Rollen von Intermediären und Anbietern definieren. *Governance*-Bausteine definieren die Regeln und Mechanismen für den sicheren und souveränen Datenaustausch zwischen den Datenraumteilnehmern. *Legal*-Bausteine stellen sicher, dass alle Aktivitäten im Datenraum rechtskonform erfolgen, zum Beispiel durch regulatorische und vertragliche Vereinbarungen zwischen den Teilnehmern.

Technische Bausteine erfassen die funktionalen Fähigkeiten, die für die Umsetzung von Datenräumen notwendig sind, und dienen als Grundlage für standardisierte, interoperable Spezifikationen (Data Spaces Support Center, 2025a). Die Unterkategorien von technischen Bausteinen adressieren die Anforderungen für den sicheren und souveränen Datenaustausch. Unter den *Data Sovereignty & Trust*-Bausteinen sind beispielsweise *Identity & Attestation Management*-Funktionalitäten zusammengefasst, die die Identitäten der Teilnehmer eines Datenraums sicherstellen. Dadurch wird gewährleistet, dass ausschließlich autorisierte Akteure Zugriff auf die Daten erhalten. Dies ist entscheidend, um Datensouveränität für teilnehmende Individuen, Organisationen und, im erweiterten Rahmen, Staaten zu gewährleisten, indem ein grundlegendes Mitspracherecht etabliert ist, wer, wann und unter welchen Bedingungen auf die Daten im Datenraum zugreifen

[57] Weitere Informationen zum European Interoperability Framework finden Sie unter anderem unter https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf (Europäische Union, 2017) und https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/3-interoperability-layers (Europäische Kommission, 2025c).
[58] Das DSSC wird im Rahmen des Digital Europe Programme der EU finanziert (Grant Agreement Number: 101083412). Das DSSC fungiert als Anlaufstelle für Unternehmen und den öffentlichen Sektor, um die Schaffung gemeinsamer europäischer Datenräume zu unterstützen.

darf. Die *Data Interoperability*-Bausteine beschreiben Funktionalitäten für einen standardisierten und semantisch harmonisierten Datenaustausch, etwa durch die Nutzung einheitlicher Datenmodelle, Formate und Schnittstellen (APIs). Die Bausteine der Kategorie *Data Value Creation Enablers* bilden Funktionalitäten ab, die für die wirtschaftliche Nutzung von Daten notwendig sind, indem sie etwa die Registrierung und Auffindbarkeit von Datenangeboten sowie die Integration in datengetriebene Dienste und Anwendungen ermöglichen.

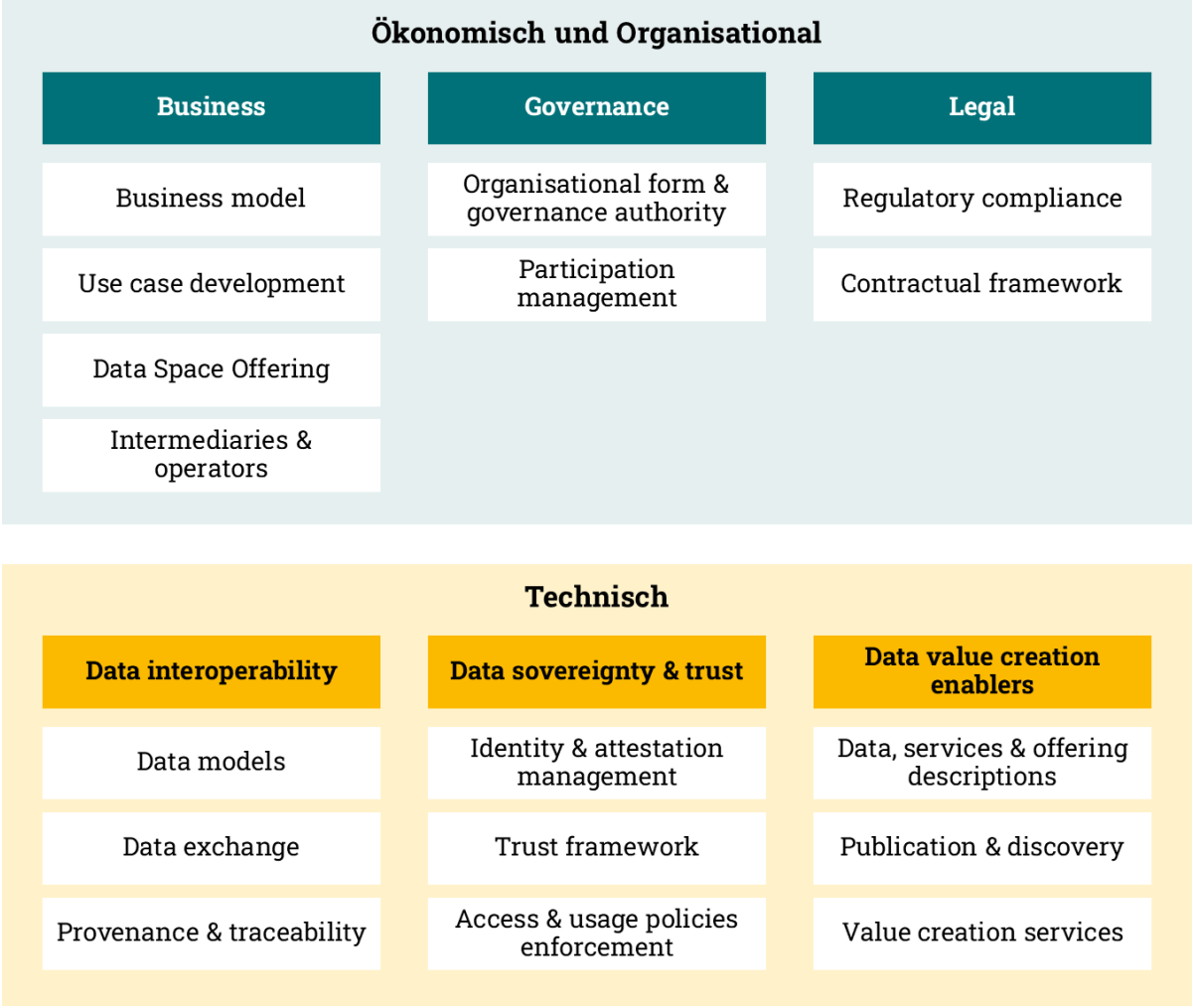

Abbildung 10: Datenraumbausteine gemäß dem DSSC-Blueprint v2.0 (Data Spaces Support Centre, 2025a)

Ein **Datenraumkonnektor** ist in einem Datenraum eine wichtige Komponente. Mithilfe von Konnektoren werden die zuvor vorgestellten technischen Bausteine technisch implementiert und zusammengeführt. Über die Konnektoren werden die Schnittstellen für den Datenaustausch gebildet und damit Interoperabilität, Sicherheit und Datensouveränität gewährleistet.

Einzelne Akteure und ihre Datenplattformen verfügen in der Regel nicht über alle notwendigen Daten, um eigenständig innovative datenbasierte Dienste und Geschäftsmodelle zu entwickeln (Pettenpohl et al., 2022). Das Datenökosystem kann als übergeordnete Einheit zum Datenraum betrachtet werden. Es umfasst neben den Austauschprozessen, die in einem Datenraum stattfinden, auch die vorgelagerten und nachgelagerten

Prozesse zur Gewinnung und Verarbeitung von Daten (Kraemer et al., 2022). In dieser Hinsicht gehen Datenökosysteme über die Funktionalität einzelner Datenräume hinaus, indem sie nicht nur den Datenaustausch, sondern auch die kollaborative Entwicklung und Nutzung datenbasierter Dienste fördern (Strnadl & Schöning, 2023). Durch eine Kombination aus technischen Standards, föderierten Architekturen und verbindlichen Governance-Regeln ermöglichen sie den vertrauenswürdigen und interoperablen Austausch von Daten über Organisationsgrenzen hinweg. Dadurch kann eine umfassende Wertschöpfung aus den geteilten Daten generiert werden (Otto, 2022).

Die sogenannten **FAIR-Prinzipien** (Findability, Accessibility, Interoperability, and Reusability) stellen sicher, dass die ausgetauschten Daten maschinenlesbar auffindbar sind, in standardisierten Formaten beschrieben werden und somit interoperabel und wiederverwendbar sind. Es gibt derzeit verschiedene Initiativen, Datenräume zu etablieren, die jeweils unterschiedliche Eigenschaften hinsichtlich Zugänglichkeit und Wiederverwendbarkeit von Daten unter der Einhaltung der FAIR-Prinzipien versprechen (Bacco et al., 2024).

Technischer Entwicklungsstand

Die Etablierung von Datenräumen wird sowohl auf der europäischen als auch auf der deutschen Ebene strategisch vorangetrieben.[59] Der technische Entwicklungsstand von Datenräumen befindet sich in einer dynamischen Phase, die von kontinuierlichen Weiterentwicklungen in den Bereichen Interoperabilität und Sicherheit sowie der technischen Implementierung von Bausteinen geprägt ist. Implementierungen für Datenraumbausteine und Governance-Modelle werden durch verschiedene europäische Datenrauminitiativen wie Gaia-X, DSSC und Catena-X aktiv vorangetrieben. Dabei orientieren sich viele dieser Projekte an den Spezifikationen der International Data Spaces Association (IDSA), einem gemeinnützigen Verein zur Förderung souveräner und vertrauenswürdiger Dateninfrastrukturen.[60] Obwohl Gaia-X und IDSA lediglich Referenzarchitekturen und Bausteine für Datenräume definieren, unterscheiden sich diese in ihren Systemmodellierungsansätzen. Beispielsweise ist die IDSA-Architektur durch ein zentrales Identitätsmanagement gekennzeichnet, wohingegen die Gaia-X-Architektur ein dezentrales Identitätsmanagement vorsieht (Gabriel et al., 2024).

Für den Energiesektor stellt der Blueprint der Common European Energy Data Spaces (CEEDS, vgl. Abbildung 11; Dognini et al., 2024) eine Referenzarchitektur für die Gestaltung und Implementierung von Energiedatenräumen in Europa bereit und definiert Bausteine, die für die Umsetzung von Datenräumen im Energiesektor erforderlich sind. Dazu gehören unter anderem Governance-Strukturen, Identitäts- und Zugriffsmanagement, Interoperabilitätsstandards und Mechanismen für den sicheren Datenaustausch.[61]

[59] Eine Übersicht über die europäischen Datenrauminitiativen finden Sie unter anderem unter https://digital-strategy.ec.europa.eu/en/policies/data-spaces (Europäische Kommission, 2025d).
[60] Weitere Informationen zum IDSA-Referenzarchitekturmodell finden Sie unter anderem unter https://internationaldataspaces.org/offers/reference-architecture/ (International Data Spaces e. V., 2025).
[61] Eine ausführliche Diskussion zu den verschiedenen Bausteinen finden Sie unter anderem bei Data Spaces Support Centre (2025a) und Dognini et. al (2024).

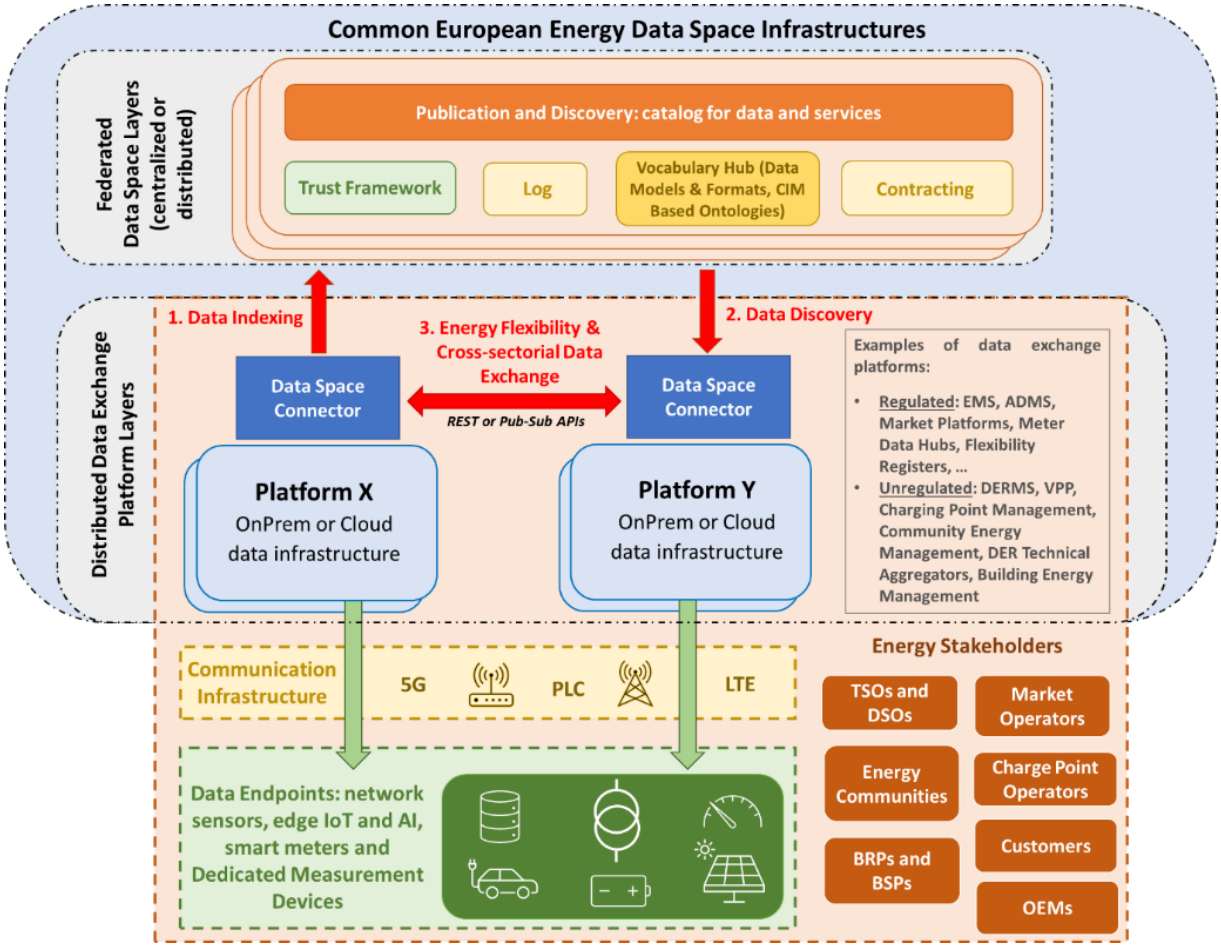

Abbildung 11: CEEDS-Referenzarchitektur (Dognini et al., 2024)

Eine Vielzahl von Implementierungen für Datenraumbausteine, insbesondere der Datenraumkonnektor, basieren auf offenen Spezifikationen von Organisationen wie IDSA, Gaia-X und W3C. Der IDSA-Datenraumkonnektor stellt eine frühe Implementierung eines solchen Konnektors dar und fungierte als Referenzimplementierung für weitere Datenraumkonnektoren (Bacco et al., 2024). Er setzt grundlegende Prinzipien von souveränem Datenaustausch und Interoperabilität um, basierend auf den Spezifikationen der IDSA. Inzwischen existieren über 30 verschiedene Datenraumkonnektoren, die für unterschiedliche Anwendungen entwickelt wurden[62]. Sie variieren in ihrer technischen Reife. Einige bieten maßgeschneiderte Lösungen für domainspezifische Anwendungsfälle: Der OneNet Connector[63] ist ein spezialisierter Datenraumkonnektor, der für den spezifischen Einsatz in Energieanwendungsfällen konzipiert wurde. Dieser Konnektor bietet mehr als 60 standardisierte Datenmodelle und datenbasierte Dienste für Stakeholder aus dem Energiesektor und soll so einen nahtlosen und mit geringen Abstimmungskosten verbundenen Datenaustausch entlang der energiewirtschaftlichen Wertschöpfungskette ermöglichen. Daneben existieren mehrere Konnektoren wie der Eclipse Dataspace Connector und der FIWARE Data Space Connector, die domänenunabhängig konzipiert wurden. Diese Konnektoren können angepasst werden, um den domänenübergreifenden Datenaustausch zu ermöglichen.

[62] Eine Übersicht über bestehende Konnektoren für unterschiedliche Anwendungsbereiche finden Sie unter anderem bei Giussani et al. (2024).
[63] Weiterführende Informationen zum OneNet-Datenraumkonnektor finden Sie unter anderem unter https://www.onenet-project.eu/onenet-connector-included-in-the-idsa-data-connector-report/ (OneNet, 2023).

Eine erste Implementierung des Minimum Viable Product (MVP) eines Energie-Datenraums, bestehend aus Datenraumkonnektoren, Identitäts- und Zugriffsmanagement sowie Datenmodellen für einen Redispatch 3.0 Use Case, wurde im Forschungsprojekt dena-ENDA (Deutsche Energie-Agentur, 2024a) getestet. Der Aufbau prototypischer Energiedatenräume, die zusätzliche Bausteine zum Beispiel für Data Value Creation Enablers in ihre Implementierung einbeziehen, werden in verschiedenen laufenden Datenraumprojekten[64] wie Enershare[65] und energy data-X[66] entwickelt. Im Fall des Enershare-Projekts basiert die Implementierung des Baustein „Data Value Creation Enabler" auf Smart Contracts und ermöglicht eine nachvollziehbare digitale Vertragsverhandlung sowie Peer-to-Peer-Transaktionen. Im Rahmen aktueller Forschungsprojekte wie Enershare und EDDIE werden für den Baustein „Identity Management" verschiedene dezentrale Identitätsmanagementlösungen evaluiert, darunter etwa SSI (vgl. Kapitel 2.2). Schließlich gibt es im Energiesektor (z. B. Projekt energy data-X) sowie im Industriesektor (z. B. Projekt Factory-X) insbesondere in Deutschland Datenraumprojekte, die den Aufbau operativ nutzbarer Datenräume anstreben (Gabriel et al., 2024).

Zu erwartende Entwicklungen

Aus den in Kapitel 0 beschriebenen Initiativen und Pilotprojekten ergeben sich laufend neue Erkenntnisse, weitere Anforderungen und absehbare Weiterentwicklungen. In diesem Zusammenhang ist die technische und semantische Interoperabilität von Datenräumen eine wichtige Anforderung, um den Datenaustausch über sektorale und systemische Grenzen hinweg zu ermöglichen – besonders im Hinblick auf die Entwicklung sogenannter *Common European Data Spaces*, in denen sektorenübergreifende Datenökosysteme realisiert werden sollen. Ein Beispiel für das Erfordernis einer sektorenübergreifenden semantischen Interoperabilität ist die Nutzung eines individuellen niederländischen Stromtarifs eines E-Fahrzeug-Halters, wenn er in Deutschland Strom laden möchte. Bislang kennt das Marktstammdatenregister (MaStR) in Deutschland keine E-Fahrzeuge, sodass sich das Fahrzeug zusammen mit seinem Halter nicht im Stromsystem identifizieren kann. Ebenso können aktuell die Angaben zum geladenen Strom (Transaktionsdaten) nicht zwischen den Bilanzkreisverantwortlichen bzw. Stromlieferanten in einem dem Roaming in der Telekommunikationsbranche vergleichbaren Prozess ausgetauscht werden. Datenräume adressieren exakt diese Lücken zwischen dem Mobilitätssektor und dem Energiesektor sowie zwischen EU-Mitgliedsländern.

Bislang sind die in Datenökosystemen verwendeten Datenraumkonnektoren untereinander nicht interoperabel, was einen Lock-in-Effekt bedeutet und verhindert, dass sich offene Datenökosysteme uneingeschränkt realisieren lassen. Das von der IDSA vorgeschlagene Data Spaces Protocol[67] geht dieses Problem an, indem es eine Trennung zwischen der **Control Plane** und der **Data Plane** schafft. Die Begriffe „Data Plane" und „Control Plane" stammen aus dem Bereich des Software Defined Networking. Während die Data Plane für die eigentliche Verarbeitung und Weiterleitung der Daten zuständig ist, ist die Control Plane für die Steuerung, Verwaltung und Regelsetzung innerhalb des Systems verantwortlich. Es wird erwartet, dass dieses Protokoll in naher Zukunft in mehreren Datenraumkonnektoren implementiert und dadurch die Grundlage für sektorenübergreifende Datenökosysteme gelegt wird.

In Verbindung mit der Weiterentwicklung der Datenraumtechnologien wird die Implementierung von Datenräumen im Energiebereich in Pilotprojekten erprobt. Die Analysen im Rahmen der fünf europäischen

[64] Eine Übersicht über die verschiedenen Pilotprojekte für Datenräume in der Energiewirtschaft finden Sie unter anderem bei Gabriel et al. (2024).
[65] Weitere Informationen zu der Architektur und Implementation des Enershare Marketplace finden Sie unter anderem bei Arnone et al. (2024).
[66] Weitere Informationen zum Projekt energy data-X finden Sie unter https://www.energydata-x.eu/ (energy data-X, 2025).
[67] Weitere Informationen zum Data Spaces Protocol finden Sie unter anderem unter https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol (International Data Spaces e. V., 2024).

Forschungsprojekte (Data Cellar, Enershare, EDDIE, Synergies und int:net) sowie im Projekt dena-ENDA (Deutsche Energie-Agentur, 2024a) haben gezeigt, dass die Heterogenität der Datenformate und -modelle aufgrund der großen Heterogenität von Systemen und Schnittstellen in der Energiewirtschaft eine Herausforderung für die Integration und Interpretation von Daten in Energiedatenräumen darstellt (Jiménez, 2025). Obwohl Datenräume grundlegende Elemente für die semantische Integration vorsehen, ist die Harmonisierung der Datenmodelle mithilfe von domänenspezifischen Standards wie dem Common Information Model[68] erforderlich, um die Dateninterpretierbarkeit und -nutzbarkeit zu verbessern (Monti et al., 2023).

Verschiedene Implementierungen der Bausteine (z. B. Identity Management, Publication and Marketplace Services) basieren auf unterschiedlichen Web3-Technologien. Entsprechend werden Weiterentwicklungen dieser Technologien auch Einfluss auf die Weiterentwicklung von Datenräumen haben.

2.5 Unterstützende Technologien und Konzepte

Smart Contracts

Das Konzept der sogenannten Smart Contracts wurde von Nick Szabo bereits in den 1990er Jahren vorgestellt. Basierend auf der Blockchain-Technologie können Smart Contracts heute Transaktionen umsetzen, speichern und replizieren. Dabei entfällt die Notwendigkeit für eine zentrale dritte Instanz zum Aufsetzen und Durchführen (Khan et al., 2021). Das liegt an der Funktionsweise von Smart Contracts (vgl. Abbildung 12). Smart Contracts sind als digitaler Programmcode zu verstehen, der ausgeführt wird, wenn zuvor festgelegte Bedingungen erfüllt sind (sogenannte selbstausführende Verträge). Zuvor festgelegten Bedingungen entsprechend können Smart Contracts somit definierte Transaktionen automatisiert, schnell und effizient auslösen und ausführen. Sobald ein Smart Contract auf eine Blockchain geschrieben ist (in der Regel auf eine Haupt-Blockchain wie Ethereum), ist er nicht mehr nachträglich veränderbar – selbst nicht von den Personen, die den Programmcode ursprünglich geschrieben haben. Da der Smart Contract daher automatisiert und unveränderbar abläuft und die festgelegten Vertragsbedingungen durch das Netzwerk geprüft werden, braucht es keinen Intermediär zur Überwachung oder Durchsetzung. Diese Eigenschaft macht Smart Contracts einzigartig, da keine andere Software dieselbe Unveränderlichkeit nach der Bereitstellung aufweist.[69] Smart Contracts können zudem die technologische Grundlage für erweiterte Blockchain-Funktionalitäten sein: Im Gegensatz zu Blockchain-Netzwerken, die lediglich native Token-Transfers unterstützen, ermöglichen Netzwerke wie Ethereum darüber hinaus durch Smart Contracts ganze Programmabläufe und damit vielfältige Anwendungsfälle[70] wie auch die Implementierung zusätzlicher Token-Standards[71] (Hewa et al., 2021; Khan et al., 2021).

Derzeit können mittels Smart Contracts in nur wenigen Jurisdisktionen (z. B. Malta und Singapur) rechtsverbindliche Vereinbarungen eingegangen werden (Dwivedi et al., 2021; Ferreira, 2021).[72] In Deutschland und in

[68] Weitere Informationen zum Common Information Model finden Sie unter unter https://www.entsoe.eu/digital/common-information-model/ (ENTSO-E, 2025).
[69] Diese Eigenschaft hat weitreichende Implikationen für die Kontrolle über Software: In klassischen IT-Systemen kann Hardware über Software bestimmen – wer die Hardware kontrolliert, kann Programme deaktivieren oder verändern. In Blockchain-basierten Systemen ist das grundlegend anders: Nach der Veröffentlichung eines Smart Contract kann dessen Ausführung nicht mehr von einzelnen Knoten im Netzwerk (d. h. der Hardware einer Blockchain) kontrolliert oder verändert werden (vgl. unter anderem Erbguth & Morin, 2018).
[70] Die potenziellen Anwendungsfälle von Smart Contracts reichen von der Abbildung von Finanztransaktionen bis hin zur Nachverfolgung von Produkten im Supply Chain Management. Weitere Informationen zu Anwendungsfällen von Smart Contracts finden Sie unter anderem bei Hewa et al. (2021) und Rouhani & Deters (2019).
[71] Weitere Informationen finden Sie in Kapitel 0.
[72] Malta hat mit dem „Malta Digital Innovation Authority Act“ sowie weiteren Rechtsvorschriften eine gesetzliche Grundlage geschaffen, die die Anerkennung von Smart Contracts als Bestandteil digitaler Innovationen sicherstellt. Diese Verträge sind bindend, sofern sie die allgemeinen Voraussetzungen des Vertragsrechts erfüllen. Eine vergleichbare rechtliche Anerkennung besteht in Singapur, wo die Regierung Rahmenbedingungen etabliert hat, die Smart

der Europäischen Union können Smart Contracts als erlaubnispflichtige Finanzdienstleistungen gelten und somit zum Beispiel die Kreditvergabe, den Handel mit digitalen Assets oder versicherungsähnliche Leistungen grundsätzlich automatisiert abbilden. Allerdings ist die automatisierte Durchführung von Finanzoperationen mittels Smart Contracts im Rahmen von DeFi-Anwendungen in der EU rechtlich komplex und stark reguliert (vgl. die Markets in Crypto-Assets Regulation (MiCAR); BaFin, 2025). DeFi-Anwendungen versprechen insbesondere, Prozesse deutlich effizienter und transparenter zu gestalten als traditionelle Finanzangebote. Im Energiesektor wird die Anwendung von Smart Contracts daher vor allem für Transaktionen diskutiert, die aufgrund der zunehmenden Zahl und Dezentralität der Akteure hohe Kosten durch einen zentralen Dritten und Vertragsabwickler verursachen würden.[73] Die Anwendungsfälle von Smart Contracts im Energiesektor fokussieren sich somit auf die Transaktion von Energiemengen mit Endkundinnen und -kunden (Kirli et al., 2022).

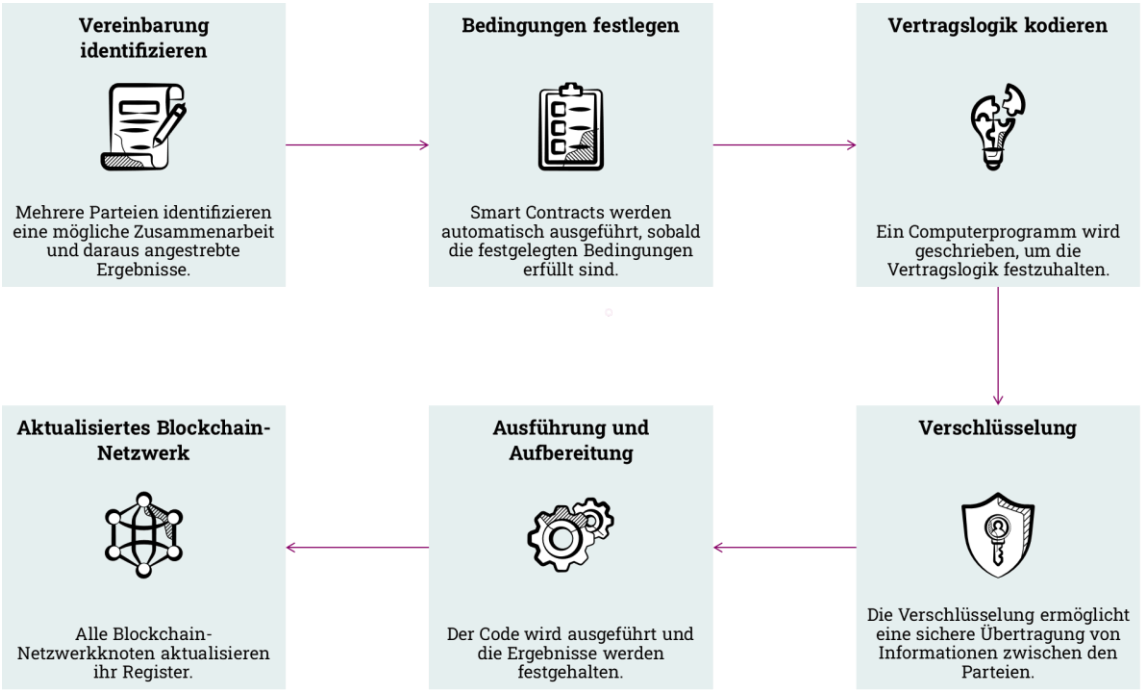

Abbildung 12: Funktionsweise eines Smart Contract

Tokenisierung

Ein Token ist eine digitale Einheit oder digitale Repräsentation, die zumeist auf einem DLT-Netzwerk verwaltet wird und für verschiedene Zwecke verwendet werden kann. Tokens stellen eine digitale Repräsentation von unter anderem Zahlungsmitteln (z. B. Kryptowährungen), Eigentumsnachweisen (z. B. digitale Vermögenswerte) oder Zugangsschlüsseln zu bestimmten Dienstleistungen und Anwendungen dar (Harwood-Jones, 2019). Die Ausgabe und Verwaltung von Tokens erfolgt in der Regel automatisiert über Smart Contracts (vgl. Kapitel 0). Obwohl digitale Tokens als Konzept bereits vor 2009 in verschiedenen Kontexten wie Videospielen oder proprietären Online-Plattformen existierten, wurde mit Bitcoin erstmals

Contracts als durchsetzbare Verträge ansehen, vorausgesetzt, sie erfüllen die grundlegenden Anforderungen des Vertragsrechts wie Angebot, Annahme und Gegenleistung. Weitere Informationen finden Sie unter anderem bei Malta Digital Innovation Authority (2025) und Monetary Authority of Singapore (2024).

[73] Ein Beispiel hierfür ist der Handel von Kleinstflexibilitäten mit/durch Haushalte.

das Konzept eines dezentralen, Blockchain-basierten Tokens eingeführt, der als erste dezentralisierte Kryptowährung die Grundlage für digitale Wertübertragungen ohne einen zentralen Intermediär bildete (Nakamoto, 2008).

Eine bedeutende Weiterentwicklung erfolgte mit dem Ethereum-Netzwerk im Jahr 2015. Dabei unterscheidet man zwischen nativen Tokens wie Ether[74], die direkt in das Protokoll einer Blockchain integriert und für deren grundlegende Funktionalität unerlässlich sind, und non-nativen Tokens, die durch Smart Contracts auf einer bestehenden Blockchain implementiert werden und deren Funktionalität und Regeln durch den Smart Contract definiert sind. Die Ethereum-Blockchain erlaubt mit dem *ERC-20-Standard* (Ethereum Request for Comments) aber zum einen auch die Erstellung von **Fungible Tokens** (d. h. Tokens mit einem einheitlichen Wert, die untereinander austauschbar sind). Zum anderen lassen sich mit dem *ERC-721-Standard* sogenannte **Non-Fungible Tokens (NFTs)** erstellen. Sie sind im Gegensatz zu Fungible Tokens nicht 1:1 austauschbar, sondern eindeutig zuordenbar und ermöglichen somit weitere Anwendungsfälle, beispielsweise für digitale Kunst- und Sammlerstücke oder Eigentumsnachweise. Schließlich wurde der *ERC-1155-Multi-Token-Standard* eingeführt, der Effizienzvorteile bietet und Fungible und Non-Fungible Tokens in einem Smart Contract vereint.[75] Des Weiteren wurden **Security Tokens** entwickelt, die finanzielle Rechte wie Aktien, Immobilien oder Anleihen repräsentieren. Da sie durch die Übertragung von herkömmlichen Finanzinstrumenten auf die Blockchain entstanden sind, unterliegen sie den regulatorischen Vorschriften der entsprechenden Finanzinstrumente und bilden automatisiert deren Compliance ab. Ein Security Token ist daher auch durch einen realen Wert des Finanzinstruments gedeckt (di Angelo & Salzer, 2020; Wang et al., 2021).

Das Thema Skalierbarkeit und Interoperabilität spielt auch für Tokens eine große Rolle. Layer-2-Technologien wie Zero-Knowledge Rollups oder Optimistic Rollups bieten Lösungen, indem sie Transaktionen außerhalb der Haupt-Blockchain (Layer 1) bündeln und dadurch die Geschwindigkeit und Kosteneffizienz steigern (vgl. Kapitel 2.1). Darüber hinaus kommen zunehmend Interoperabilitätsprotokolle zum Einsatz, um einen effizienten und vor allem flexibleren Austausch von digitalen Vermögenswerten wie Tokens über isolierte Blockchain-Netzwerke hinweg zu ermöglichen.

Die Anwendungsfälle, in denen Blockchain-basierte Tokens eine Rolle im Energiesektor spielen, sind oft eng verwandt mit den Anwendungsfällen von Smart Contracts, da Smart Contracts überhaupt erst die Erstellung und Verwaltung komplexer Token-Funktionalitäten ermöglichen (Roth et al., 2022). So können beispielsweise Fungible Tokens als eine Einheit für den digitalen Handel einer definierten Strommenge in einem Peer-to-Peer-Netzwerk mithilfe von Smart Contracts fungieren (vgl. Daylight Energy LLC, 2025). Fungible und Non-Fungible Tokens können zudem für die Zertifizierung der Strom- bzw. Wasserstoff-Herkunft aus erneuerbaren Energiequellen genutzt werden (Babel et al., 2022). Im Falle von Fungiblen Tokens wird eine einheitliche Eigenschaft repräsentiert (z. B. „grüner“ Wasserstoff nach einem bestimmten Standard). NFTs hingegen könnten eine stärkere Differenzierung der Herkunfts- oder der Nachhaltigkeitseigenschaften abbilden, da die Nachweise nicht identisch austauschbar sein müssen. Security Tokens wiederum können bei Investitionen in neue Energieerzeugungsanlagen wie Solar- und Windparks angewandt werden.

[74] Ether ist der native Token der Ethereum-Blockchain.
[75] Weiterführende Informationen zu Token-Standards finden Sie unter anderem bei di Angelo & Salzer (2020) und Wang et al. (2021).

Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKPs) sind kryptografische Protokolle und ein elementarer Baustein, um Datensouveränität und annähernd vollständige Anonymisierung von Akteuren zu ermöglichen. Erste grundlegende Arbeiten an dem Konzept erfolgten durch Goldwasser et al. (1985), die ein **interaktives Argument of Knowledge** formulierten. Das Grundkonzept von Goldwasser et al. (1985) sieht vor, dass ein *Prover* („Beweis-Erbringer“) einen *Verifier* („Beweis-Prüfer“) in arbiträr vielen Iterationen davon überzeugen kann, dass der Prover über eine bestimmte Information verfügt – beispielsweise dass sein Alter über 18 Jahre liegt –, ohne dabei weitere sensible Details preiszugeben – wie etwa das genaue Geburtsdatum. Der Verifier kann dabei festlegen, wie viele „Beweise“ der Prover erbringen muss, bevor er die Aussage durch die hohe statistische Sicherheit akzeptiert. Für die Realisierung dieses interaktiven Modells müssen der Prover und der Verifier jedoch kontinuierlich miteinander kommunizieren, um den iterativen Beweisprozess durchzuführen, was die Anwendungsmöglichkeiten lange Zeit stark einschränkte.

Ein entscheidender Fortschritt gelang Ende der 1980er Jahre mit der Arbeit von Fiat & Shamir (1987), die ein **nicht interaktives Modell** entwickelten. Durch dieses Verfahren konnte der Prover eine einmalige, kryptografisch signierte Beweiskette generieren, die anschließend asynchron von einem Verifier geprüft werden konnte. Dieses Modell reduzierte den Kommunikationsaufwand erheblich und erweiterte dadurch das Anwendungsspektrum von ZKPs. Allerdings war die praktische Implementierung dieser Konzepte durch die enormen Rechenanforderungen lange Zeit stark eingeschränkt. Mit dem exponentiellen Anstieg der Rechenleistung und der zunehmenden Bedeutung kryptografischer Technologien im Zuge des Blockchain-Booms fanden ZKPs erste realweltliche Anwendungen. Ein prägnantes Beispiel sind Privacy-Coins wie ZCash, die durch ZKPs eine verifizierbare und zugleich anonyme Transaktionsabwicklung ermöglichen. Darüber hinaus kommen ZKPs zunehmend in Layer-2-Lösungen für Blockchains zum Einsatz, um die auftretenden Skalierungsprobleme zu lösen und die Transaktionsgeschwindigkeiten zu erhöhen. Hierbei spielen Verfahren wie ZK-Rollups eine zentrale Rolle, die durch Aggregation zahlreicher Transaktionen die Blockchain-Performance erheblich steigern (vgl. Kapitel 0).

In den letzten Jahren haben ZKPs erhebliche Fortschritte gemacht, sowohl in Bezug auf die Effizienz als auch hinsichtlich ihrer Anwendungsvielfalt. Die kontinuierliche Optimierung der zugrunde liegenden Algorithmen hat die Performance der Verfahren gesteigert, während neue Programmierumgebungen ihre Integration in bestehende Systeme erleichtern.[76] Diese Entwicklungen haben dazu beigetragen, das sogenannte Blockchain-Trilemma – den Zielkonflikt zwischen Dezentralisierung, Sicherheit und Skalierbarkeit – zu lösen bzw. zumindest maßgeblich zu entschärfen (Principato et al., 2023). Beispielsweise zeigen sogenannte *Shielded NFTs* durch den Einsatz von ZKPs, dass die Authentifizierung und Verarbeitung von Nachweisen erfolgen können, während die eigentlichen Inhalte und sensible Daten verborgen bleiben. ZKPs fungieren dabei als kryptografischer Mechanismus, der die Überprüfung der Gültigkeit von Token-Informationen erlaubt, ohne dass die konkreten Daten offengelegt werden müssen (Körner et al., 2024a). Die Technologie spielt insbesondere im Bereich digitaler Identitäten eine entscheidende Rolle, da Nutzerinnen und Nutzer in Anwendungsfällen wie *Selective Disclosure* (Selektive Offenlegung) durch ZKPs gezielt einzelne Informationen preisgeben können, ohne alle Daten zu ihrer Identität offenlegen zu müssen (vgl. Abbildung 13). Damit

[76] Weitere Informationen zu ZKP-Modellen und -Lösungen finden Sie unter anderem bei Ernstberger et al. (2024), Grassi et al. (2021) und Sun et al. (2021).

leisten ZKPs einen wesentlichen Beitrag zur Datensouveränität im Web3 und bieten einen vielversprechenden Ansatz für datenschutzkonforme und zugleich nachweisbare digitale Interaktionen.

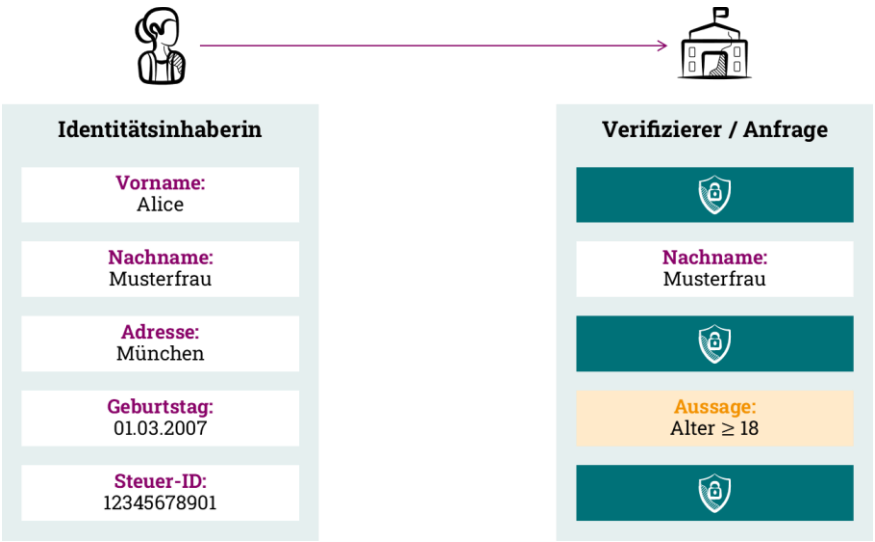

Abbildung 13: Illustration der ZKP-Anwendung „Selective Disclosure“

Ausblick

Der dargestellte Entwicklungsstand der Technologien basiert auf dem Redaktionsschluss im September 2025. Zukünftig könnten Web3-Technologien zunehmend mit Anwendungen aus dem Bereich der Künstlichen Intelligenz (KI) kombiniert werden und damit Einsatz im Energiesektor finden. Insbesondere im Netzbetrieb ist es von großer Bedeutung, dass KI-basierte Entscheidungsempfehlungen oder automatisierte Steuerung nachvollziehbar und überprüfbar sind und nicht zu sogenannten Halluzinationen[77] führen. Hierbei sind die Quantität und die Qualität der Daten für das Training der Lösungen entscheidend, genauso wie der Komplexitätsgrad des Trainings. In diesem Zusammenhang kann die Integration von Web3-Technologien zur Erhöhung der Datenqualität (insbesondere im Sinne einer nachweisbaren Datenherkunft und Datenintegrität) zielführend sein. Diese Integration kann insbesondere mit Federated-Learning-Ansätzen erfolgen, die das Trainieren von KI-Modellen direkt auf den Endgeräten und damit dezentral ohne Datenübertragung an zentrale Server ermöglichen. Auch der Einsatz verteilter Large Language Models (LLMs), deren Trainingsprozesse über mehrere Knoten oder Geräte hinweg aufgeteilt werden, lässt sich mit Web3-Technologien verknüpfen. Die Trainingsprozesse können dadurch dezentral organisiert werden, was die Notwendigkeit reduziert, Daten mit einer zentralen Instanz zu teilen. Durch die erhöhte Datensicherheit in dezentralen Ansätzen und eine effiziente Nachweisbarkeit der Datenherkunft und -entstehung könnten KI-Anwendungen in Kombination mit Web3-Technologien in KRITIS-Anwendungen getestet und später eingesetzt werden.

[77] Eine Halluzination eines KI-Modells (insbesondere eines Large Language Model (LLM)) ist eine Ausgabe scheinbar plausibler, aber faktisch falscher oder erfundener Informationen (z. B. Angabe einer wissenschaftlichen Quelle, die in Wirklichkeit nicht existiert). Weitere Informationen finden Sie unter anderem bei Maleki et al. (2024).

3 Anwendungsfelder von Web3-Technologien im Energiesystem

In diesem Kapitel werden mögliche Anwendungsfelder von Web3-Technologien im Energiesystem dargestellt. Nach einem kurzen Überblick werden zunächst die jeweiligen Anforderungen erläutert und anschließend anhand ausgewählter Beispiele potenzielle Anwendungen spezifischer Web3-Technologien vorgestellt.

3.1 Redispatch 3.0

Der erste vielversprechende Anwendungsfall für Web3-Technologien ist der sogenannte Redispatch 3.0. Redispatch-Maßnahmen zielen darauf ab, die Netzstabilität zu gewährleisten, indem sie Engpässe im Stromnetz durch eine dynamische Umverteilung von Stromerzeugung und -verbrauch ausgleichen. In der Vergangenheit nutzten die Netzbetreiber vor allem die von konventionellen Kraftwerken (installierte Leistung >10 MW) bereitgestellte Energieflexibilität, um ein zuverlässiges Engpassmanagement zu gewährleisten (**Redispatch 1.0**). Im Zuge des aktuellen Regimes, des sogenannten **Redispatch 2.0**[78], müssen auch kleinere Anlagen (installierte Leistung >100 kW) am kostenbasierten[79] Redispatch teilnehmen.

Aufgrund fehlender Netzinfrastruktur und des steigenden Anteils an verteilten Kleinstanlagen mit volatiler Erzeugung muss das bestehende Engpassmanagement jedoch angepasst werden.[80] Infolgedessen wird derzeit unter dem Begriff **Redispatch 3.0** ein hybrider, marktbasierter[81] Redispatch-Mechanismus für Kleinstanlagen (<100 kW) diskutiert. Anstatt die Einspeisung von Erneuerbare-Energien-Anlagen (EE-Anlagen) zu drosseln, wenn die eingespeiste Energie wegen Netzengpässen nicht zu den Verbraucherinnen und Verbrauchern transportiert werden kann, verfolgt Redispatch 3.0 das Ziel, die *Energieflexibilität von Verbrauchern* effizienter zu nutzen. Um Netzengpässe zu vermeiden, könnten daher steuerbare Verbrauchseinrichtungen (z. B. E-Fahrzeuge und Batteriespeicher) eingebunden werden.[82] Der Ausbau von EE-Anlagen in Kombination mit der Integration intelligenter und steuerbarer Verbraucher bietet ein großes Potenzial[83], um die verfügbare Kapazität für Redispatch-Maßnahmen zu erhöhen, Redispatch-Kosten zu senken und auch die ökologischen Auswirkungen von Redispatch-Maßnahmen zu reduzieren (Körner et al., 2024a). Der zentrale Gedanke hinter Redispatch 3.0 ist also die *Dezentralisierung des Netzengpassmanagements* sowie die Schaffung flexiblerer Mechanismen durch die intelligente Integration kleiner, dezentraler Erzeuger und Verbrauchseinheiten. Hierbei spielt der verstärkte Austausch von Daten zwischen Netzbetreibern, Endverbraucherinnen und -verbrauchern sowie weiteren Marktakteuren eine entscheidende Rolle. Dazu werden neben den klassischen Netzleitsystemen (NLS) auch cloudbasierte und BSI-Konforme (Bundesamt für Sicherheit in der Informationstechnik)

[78] Weitere Informationen zum Redispatch 2.0 finden Sie unter anderem bei Bundesnetzagentur (2025).
[79] Kostenbasierter Redispatch bedeutet, dass die Redispatch-Maßnahmen in der Reihenfolge steigend nach ihren tatsächlichen Kosten ausgewählt werden.
[80] Weitere Informationen zu bestehenden Engpassproblemen finden Sie unter anderem bei VDE – Verband der Elektrotechnik Elektronik Informationstechnik e. V. (VDE e. V., 2025).
[81] Marktbasierter Redispatch bedeutet, dass die Redispatch-Maßnahmen in einem Markt angeboten und steigend nach ihren Gebotspreisen ausgewählt werden.
[82] Ein Praxisbeispiel für Redispatch 3.0 finden Sie bei Bundesministerium für Wirtschaft und Energie (2025a).
[83] Es wird prognostiziert, dass durch den Aufbau neuer EE-Anlagen sowie durch die Integration von intelligenten Verbrauchern (z. B. E-Ladestationen und automatisierte Lastmanagementsysteme) die verfügbare flexible Leistung von 130 GW bis 2030 auf mehr als 271 GW steigen wird (VDE e. V., Energietechnische Gesellschaft, 2023).

IoT-Lösungen für die direkte Kommunikation mit dezentralen Erzeugungs- und Verbrauchseinheiten mit einer Nennleistung von unter 100 kW erforderlich sein (VDE e. V., 2025).

Die Realisierung solcher Redispatch-Maßnahmen in einem dezentralen, digitalisierten Energiesystem bedingt eine Koordination zwischen verschiedenen Marktakteuren. Dabei ist die Gewährleistung von Cyber-Sicherheit, Datenschutz und Verifizierbarkeit der ausgetauschten Daten von zentraler Bedeutung. Daraus ergeben sich folgende essenzielle **Anforderungen**:

- Eindeutige und verlässliche *Identifikation* von Erzeugungsanlagen und steuerbaren Verbrauchseinheiten
- *Sicherer und souveräner Datenaustausch* zwischen den Akteuren und Anlagen
- *Echtzeitfähiger Datenaustausch*, um eine reaktionsschnelle Steuerung zu ermöglichen

Für die Umsetzung dieses Anwendungsfalls sind verschiedene **Datenquellen** erforderlich:

- *Marktstammdaten:* Bereitstellung von grundlegenden Daten aus dem MaStR
- *Bewegungsdaten:* Erfassung von Daten zur Einspeisung (z. B. von Photovoltaik-Anlagen) sowie zum Verbrauch (z. B. von E-Ladestationen)
- *Marktrollendaten:* Bereitstellung von Daten zu den verschiedenen Marktakteuren und ihren Rollen im Energiesystem

Für eine effizientere Identifizierung von Erzeugungsanlagen und Verbrauchseinheiten für Redispatch-Maßnahmen haben bereits mehrere Projekte die Anwendung von dezentral verwalteten, digitalen Identitäten im Energiesektor untersucht. Das Projekt „DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem“[84] im Auftrag der Deutschen Energie-Agentur (dena) und das vom (ehemaligen) Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderte Schaufensterprojekt „ID-Ideal“[85] haben dabei gezeigt, dass die eindeutige digitale Identifikation von Erzeugungsanlagen die Nachvollziehbarkeit und Effizienz der Identifikations-, Authentifizierungs- und Autorisierungsprozesse erhöhen kann (Körner et al., 2024b). Bei der Optimierung von Redispatch-Maßnahmen können digitale Identitäten auch dazu beitragen, die vorhandenen Energieflexibilitäten zu identifizieren und anschließend korrekt (d. h. basierend auf den Kosten bzw. Geboten) abzurechnen.

Der Einsatz digitaler Identitäten für die Koordination von Energieflexibilitäten wurde und wird unter anderem in den Projekten „Dezentraler Redispatch: Schnittstellen für die Flexibilitätsbereitstellung (DEER)“[86] und „Barrierefreie und Nutzerfreundliche Lademöglichkeiten schaffen (BANULA)“[87] sowie in wissenschaftlichen Arbeiten (z. B. Kilthau et al., 2023) untersucht. Die Ergebnisse aus dem Projekt DEER heben die Nutzung der Blockchain hervor, um Redispatch-Transaktionen zwischen den verschiedenen Akteuren zu protokollieren und so Transparenz und Verifizierbarkeit sicherzustellen, ohne dabei auf zentrale Akteure angewiesen zu sein (Körner et al., 2024a). Für die Transaktionen bzw. die intelligente Steuerung flexibler Assets könnten insbesondere Smart Contracts (vgl. Kapitel 0) zum Tragen kommen, die die Transaktionsrahmenbedingungen

[84] Weitere Informationen zum Projekt DIVE finden Sie unter https://future-energy-lab.de/projects/dive-de/ (Deutsche Energie-Agentur, 2025b).
[85] Weitere Informationen zum Projekt ID-Ideal finden Sie unter https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AbgeschlosseneProgrammeProjekte/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/IDideal/IDideal.html (Bundesministerium für Wirtschaft und Energie, 2025b).
[86] Weitere Informationen zum Projekt DEER finden Sie unter https://deer-projekt.de/ (Fraunhofer-Institut für Angewandte Informationstechnik FIT, 2025).
[87] Weitere Informationen zum Projekt BANULA finden Sie unter https://banula.de/ (Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, 2025).

festhalten und damit eine automatisierte und effiziente Abrechnung der Energieflexibilitätsbereitstellung ermöglichen. Die im DEER-Projekt entwickelte Architektur setzt auf ein SSI-basiertes Identitätsmanagement (vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**), das eine sichere Identifizierung und Authentifizierung der verschiedenen, verteilten Energieanlagen und die Teilnahme am Redispatch ohne Intermediär ermöglicht. Der Projektbericht betont zudem das Potenzial von ZKPs, mit denen die Einhaltung von Redispatch-Vorgaben überprüft werden kann, ohne sensible Verbrauchsdaten offenzulegen (vgl. Kapitel 0).

Wie bereits dargelegt, erfordert die Implementierung von Redispatch 3.0 den Austausch von Daten sowie die Koordination zwischen einer Vielzahl von Akteuren. In diesem Zusammenhang werden auch Datenraumansätze für die Realisierung von Redispatch 3.0 untersucht und implementiert (z. B. in der Initiative Gaia-X[88] oder im Projekt dena-ENDA). Wie in Abbildung 14 dargestellt, wurde in dena-ENDA ein Minimum Viable Data Space für den Redispatch-Anwendungsfall umgesetzt. Auch wenn es sich hierbei nicht um eine vollständige Implementierung bzw. einen voll funktionsfähigen Prototyp eines Energie-Datenraums handelt, liefert die Implementierung wertvolle Erkenntnisse für die Weiterentwicklung entsprechender Datenraumarchitekturen im Energiesektor (vgl. Kapitel 4.1; Deutsche Energie-Agentur, 2024a).

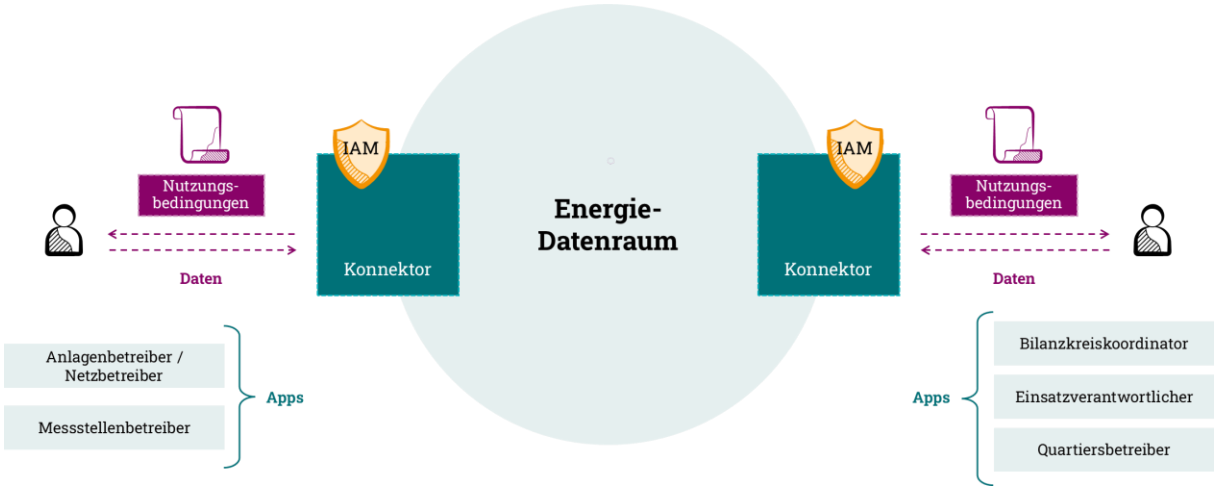

Abbildung 14: Datenraumarchitektur in dena-ENDA (Deutsche Energie-Agentur, 2024a)

3.2 Strom-Herkunftsnachweise

Herkunftsnachweise (HKNs) sind elektronische Dokumente, die gegenüber Endverbraucherinnen und -verbrauchern die Herkunft des Stroms aus erneuerbaren Energien in Europa nachweisen – vergleichbar mit einer Geburtsurkunde. HKNs können heute unabhängig vom physikalischen Stromfluss gehandelt oder verkauft werden. Stromanbieter dürfen demnach nur mit *Grünstrom* bzw. *Ökostrom* werben und diesen verkaufen, wenn sie über eine entsprechende Anzahl dazugehöriger HKNs verfügen. Die HKNs werden durch autorisierte Stellen (Issuing Bodies) ausgestellt, übertragen und entwertet. Nach der Entwertung ist ein Handel mit HKNs nicht mehr möglich. In Deutschland ist das Umweltbundesamt (UBA) die autorisierte Stelle, die für die Verwaltung der HKNs zuständig ist. Für die *Ausstellung*, die *Übertragung* und die *Entwertung von*

[88] Weitere Information zum Gaia-X-basierten Ansatz für die Implementierung von Redispatch 3.0 finden Sie unter anderem bei Bundesministerium für Wirtschaft und Energie (2025a).

HKNs müssen Informationen zwischen verschiedenen Akteuren wie dem Netzbetreiber, den Energieversorgungsunternehmen (EVUs), den Anlagenbetreibern und im Fall von internationalem Import oder Export auch den Händlern ausgetauscht werden.[89] Um Doppelzählungen zu vermeiden, werden die HKNs in Deutschland im **Herkunftsnachweisregister (HKNR)** zentral vom UBA verwaltet. Mit dieser zentralisierten Struktur gehen jedoch auch Herausforderungen wie eingeschränkte Flexibilität, begrenzte Interoperabilität und die Abhängigkeit von einem potenziellen Single Point of Failure einher.

Die aktuellen Prozesse (z. B. Anlagenregistrierung, Entwertung von HKNs) im deutschen HKN-System sind mit einem *hohen manuellen Zeitaufwand* verbunden. In der historisch gewachsenen Software fehlen beispielsweise relevante bidirektionale Schnittstellen (z. B. zum MaStR) und automatisierte Abläufe. Das führt dazu, dass das Management eines Kontos im HKNR und der dazugehörigen HKNs für EVUs mit zahlreichen Arbeitsschritten verbunden ist (Umweltbundesamt, 2025a; Umweltbundesamt 2025b). Die hohe Anzahl manueller Tätigkeiten geht zwangsläufig mit einer erhöhten Fehleranfälligkeit einher. Mit neuen Anforderungen, insbesondere der Erweiterung für die Nachweise von Gasen sowie von Wärme und Kälte, müssen das aktuelle HKN-System und die dahinterliegenden Prozesse sowie die zugrunde liegende Software weiterentwickelt werden, um weiterhin die erforderliche Integrität zu gewährleisten und Missbrauch zu verhindern (Umweltbundesamt, 2025c). Dabei müssen insbesondere die Interoperabilität und damit die Schnittstellenfähigkeit zwischen bestehenden und neu zu entwickelnden HKN-Prozessen geschaffen werden. Dazu zählen beispielsweise möglichst effiziente und eindeutig nachvollziehbare *Konversionsprozesse* (z. B. bei der Herstellung von Wasserstoff aus Strom) und die *Schnittstellen zu anderen Zertifizierungssystemen*, die auf Massenbilanzierung[90] basieren (Chvanova, 2025). Schließlich muss die Interoperabilität des HKN-Systems mit bestehenden Energiemarkt-Infrastrukturen und dem internationalen Handel gewährleistet werden, um eine reibungslose Integration zu ermöglichen.

Weitere Anforderungen an die Weiterentwicklung der bestehenden HKN-Systeme lassen sich aus der notwendigen *Granularität* der HKNs ableiten. Derzeit wird auf europäischer Ebene die Ausstellung von HKNs in unterschiedlichen Zeitintervallen durchgeführt (z. B. monatlich in Deutschland). Die Erneuerbare-Energien-Richtlinie (Renewable Energy Directive III, RED III)[91] zielt darauf ab, die Transparenz des Verbrauchs erneuerbarer Energien zu erhöhen. Dazu sollen die HKN-Systeme der einzelnen EU-Mitgliedstaaten verbessert werden. Gleichzeitig fördert die RED III eine Verlagerung hin zu einer höheren zeitlichen Auflösung bzw. Granularität von HKNs. Der Verband Europäischer Übertragungsnetzbetreiber (European Network of Transmission System Operators for Electricity, ENTSO-E) unterstützt die Entwicklung, dass Stromverbrauch und -erzeugung auf *stündlicher* oder sogar *15-minütlicher* Basis abgeglichen werden, um die Nutzung erneuerbarer Energien in Echtzeit besser widerzuspiegeln (ENTSO-E, 2022). Der Übergang zu **granularen HKNs** stellt jedoch erhebliche Anforderungen an die Speicherung, die Verarbeitung und den Austausch großer Datenmengen in kurzen Zeitintervallen.

In der Wissenschaft wurde die Verwendung von DLT-basierten Lösungen für den Handel mit HKNs bereits diskutiert (Castellanos et al., 2017; Dupont et al., 2024). In den genannten Arbeiten wird beispielsweise Ethereum zur Implementierung einer HKN-Handelsplattform verwendet, während die HKNs selbst als Tokens gehandelt werden (vgl. Kapitel 0). Der dort vorgestellte Peer-to-Peer-HKN-Handel umgeht traditionelle Energielieferanten und -makler und ermöglicht es den Endverbraucherinnen und -verbrauchern, HKNs direkt

[89] Weitere Informationen zu den Begriffsdefinitionen für die Akteure im HKN-System finden Sie bei Umweltbundesamt (2019).
[90] Bei der Massenbilanzierung werden Umweltwirkungen (z. B. in Form von CO_2-Äquivalenten) entlang der Wertschöpfungskette erfasst und die Mengen aufaddiert bzw. bilanziert. Im Gegensatz zu diesem Buchführungssystem ist ein HKN ein entkoppelter Nachweis, der einmalig entwertet und nicht weiter mitgeführt wird.
[91] Weitere Informationen zur RED-III-Richtlinie finden Sie bei Europäisches Parlament & Rat der Europäischen Union (2023).

von den Erzeugern zu erwerben, was mehr Transparenz in den Handelsprozess bringt (Dupont et al., 2024). Eine Blockchain bildet in diesem Kontext fälschungssicher und transparent die Erzeugung, Übertragung und Entwertung von HKNs ab und kann somit dazu beitragen, eine Doppelvermarktung zu verhindern (Beck et al., 2023).[92]

Die oben genannten Arbeiten berücksichtigen jedoch nicht die Frage der überprüfbaren Identifizierung der Handelseinheiten. Körner et al. (2024b) diskutieren diesen Aspekt und stellen ein Konzept auf Basis dezentraler digitaler Identitäten vor, die in die Hardware der Anlagen (z. B. im SMGW) integriert sind. Ziel dieses Konzepts ist es, die Energieerzeugungsdaten (das heißt *Bewegungsdaten*, zum Beispiel in Form von Zählerständen) sicher mit ihrer Quelle (das heißt *Stammdaten* der einzelnen EE-Anlagen, zum Beispiel der Anlagenstandort) zu verknüpfen und damit die Integrität der Daten zu gewährleisten. In der Arbeit von Körner et al. (2024b) werden ZKPs verwendet, um Informationen wie den Anteil der erneuerbaren Quellen im Energiemix verifizieren zu können, ohne detaillierte Transaktionsdaten oder personenbezogene Daten offenlegen zu müssen.

Um die Anforderungen an zeitlich granulare HKNs zu erfüllen, wird in der Initiative „Energy Track & Trace“[93] ein potenzieller Lösungsansatz entwickelt, der auch auf Web3-Technologien zurückgreift. Bei Energy Track & Trace soll der Einsatz eines dezentralen Registers in Kombination mit kryptografischen Bausteinen wie ZKPs und Merkle-Trees die öffentliche Überprüfbarkeit von granularen HKNs ermöglichen (Jokumsen et al., 2023). Die granularen HKNs werden auf Basis digital validierter Erzeugungs- und Verbrauchsmengen sowie ihres zeit- und mengenbasierten Matching ausgestellt und können direkt von Verbraucherinnen und Verbrauchern genutzt werden, um den Energieeinsatz in ihren Produkten nachzuweisen. Die Inanspruchnahme der HKNs wird über einen Dienstleister in einem Blockchain-basierten Register dokumentiert. Eine ähnliche Architektur, basierend auf Web3-Technologien, wurde im vom Bundesministerium für Wirtschaft und Energie (BMWE) geförderten Projekt InDEED[94] entwickelt, um das Labeling von Strom vollständig digital verifizierbar abzubilden (Bogensberger et al., 2023).

3.3 Auflösen von Farbkategorien für die Bewertung von Nachhaltigkeit

Die Umweltwirkungen unterschiedlicher Energiequellen zu ermitteln und ihre Nutzung in den jeweiligen Wertschöpfungsketten transparent weiterzugeben, ist ein essenzielles Steuerungsinstrument für die Dekarbonisierung der Industrie. Gegenwärtig werden die verschiedenen Energiequellen meist in Farbkategorien (z. B. „grüner“ Strom und „grauer“ Strom) eingeteilt, um gezielt klimafreundliche (d. h. „grüne“) Alternativen zu fördern. Diese Kategorisierung ist jedoch auch mit Problemen verbunden: Insbesondere kann eine solche Kategorisierung zu Greenwashing führen, da die tatsächliche Klimawirkung (z. B. in Form von CO_2-Äquivalenten) nicht direkt sichtbar und die Vergleichbarkeit zwischen unterschiedlichen Qualitäten innerhalb einer Kategorie erst einmal nicht möglich ist. Im Kontext von Wasserstoff – einer Energiequelle, die weltweit

[92] Eine ausführliche Erklärung zur Doppelvermarktung als Herausforderung bei HKNs finden Sie unter anderem bei Forschungsstelle für Energiewirtschaft e. V. (2023).
[93] Weiterführende Informationen zu der Initiative „Energy Track & Trace“ finden Sie unter https://energytrackandtrace.com/about/ (Energy Track & Trace, 2025).
[94] Die im InDEED-Projekt erfolgte Implementierung finden Sie unter https://gitlab.com/ffe-munich/indeed-allocation-method (Ferstl, 2023).

gehandelt wird – wird dieses Problem der Kategorisierung besonders sichtbar: Je nach regulatorischer Vorschrift oder Standard (z. B. EU-RFNBO[95] vs. ISO/TS 19870:2023[96]) wird Wasserstoff unterschiedlich bewertet. Die Kategorisierung in Farben (bzw. RFNBO-konformen oder -nichtkonformen Wasserstoff) verhindert dabei beispielsweise, dass Wasserstofferzeuger flexibel ein Portfolio aus Wasserstoffmengen mit unterschiedlichen CO_2-Fußabdrücken zusammenstellen können. Für den Hochlauf der Wasserstoffindustrie könnte jedoch von Vorteil sein, dass neben Strom aus erneuerbaren Quellen (z. B. über Power Purchase Agreements (PPAs)) auch Netzstrom mit der jeweiligen CO_2-Intensität flexibel miteinbezogen werden kann. Anstatt bestimmte *Schwellenwerte für starre Farbkategorien* zu setzen, könnte sich die Bewertung von Energiequellen stärker an ihrer *tatsächlichen CO_2-Intensität* oder anderen Nachhaltigkeitskriterien pro Kilowattstunde orientieren.

Diese Entwicklung gewinnt zunehmend an Bedeutung, da die Erfassung und Bilanzierung von CO_2-Emissionen für Unternehmen aus regulatorischen und markttechnischen Gründen immer wichtiger werden (z. B. im Kontext des EU-Emissionshandelssystems 1 und 2 (EU-EHS)[97], der Corporate Sustainability Reporting Directive (CSRD)[98], der Corporate Sustainability Due Diligence Directive (CSDDD)[99] oder des Carbon Border Adjustment Mechanism (CBAM)[100]). Mit einer zunehmenden Anzahl an politischen Instrumenten zur Dekarbonisierung ist es von zentraler Bedeutung, dass die unterschiedlichen Bewertungsgrößen, Verrechnungen und Verfahren zur Ausstellung bzw. Entwertung von (CO_2-) Zertifikaten über Instrument- und Sektorengrenzen hinweg nachvollziehbar sind. Da Energie in nahezu jedem Schritt einer Wertschöpfungskette zum Einsatz kommt, nimmt der Energiesektor eine Schlüsselrolle in der Nachverfolgung von Umweltwirkungen ein. Eine Weiterentwicklung von Farbkategorien hin zu übertragbaren CO_2-Nachweisen könnte dabei die Transparenz in den Wertschöpfungsketten erhöhen und auch die CO_2-Intensität unterschiedlicher Energieträger über Sektorengrenzen hinweg vergleichbarer gestalten (Leinauer et al., 2022).

Um eine Bewertung der CO_2-Intensität von unterschiedlichen Energiequellen effizient und nachvollziehbar zu ermöglichen, müssen die dahinterliegenden Prozesse der *Datenerfassung, -bewertung und -weitergabe* zunehmend digitalisiert werden. Durch die Erfassung von Erzeugungs- und Verbrauchsmengen in (nahezu) Echtzeit unter Einbeziehung von Sensoren und digitalen Datenquellen (z. B. durch Smart Metering von Photovoltaik- oder Windparks) können sowohl der Aufwand durch manuelle Erfassung als auch die Fehleranfälligkeit reduziert werden. Um die Bewertung der erfassten Daten (z. B. in Form der Allokation von CO_2-Äquivalenten) durchgängig transparent und überprüfbar zu gestalten, ist es notwendig, dass die Datenerfassung *Ende-zu-Ende digital* mit der Bewertung und der potenziell anschließenden Ausstellung von Nachweisen bzw. Zertifikaten verknüpft ist (Leinauer et al., 2022). Für die Verifizierbarkeit und Rückverfolgbarkeit

[95] RFNBO ist die Abkürzung für Renewable Fuels of Non-Biological Origin (Erneuerbare Kraftstoffe nicht biologischen Ursprungs) – also beispielsweise Wasserstoff, der durch Elektrolyse von Wasser mit Strom aus erneuerbaren Quellen hergestellt wurde. Weitere Informationen zu der europäischen Definition und zur Zertifizierung finden Sie unter anderem bei Europäische Kommission, Directorate-General for Energy (2025).
[96] ISO/TS 19870:2023 ist eine technische Spezifikation für Methoden zur Bestimmung der Treibhausgasemissionen bei Produktion, Aufbereitung und Transport von Wasserstoff der International Organization for Standardization (ISO). Weitere Informationen zur technischen Spezifikation finden Sie unter anderem bei ISO (2023).
[97] Das EU-EHS 1 und ab 2027 das EU-EHS 2 bepreist CO_2-Emissionen in bestimmten Sektoren in Form von handelbaren Zertifikaten. Die Menge der handelbaren Zertifikate wird nach dem „Cap and Trade"-Prinzip festgelegt, indem für die betroffenen Sektoren eine jährliche Obergrenze an Emissionen definiert wird. Das EU-EHS 1 adressiert unter anderem die Emissionen von Energieanlagen. Weitere Informationen zum EU-EHS finden Sie unter anderem bei Umweltbundesamt (2025d).
[98] Die CSRD ist eine EU-Richtlinie, die Unternehmen zur standardisierten Offenlegung von Informationen über Umwelt-, Sozial- und Governance-Aspekte (ESG) verpflichtet und damit die bisherigen nichtfinanziellen Berichterstattungspflichten erweitert. Weitere Informationen zur CSRD finden Sie unter anderem bei Europäisches Parlament & Rat der Europäischen Union (2022).
[99] Die CSDDD ist eine EU-Richtlinie, die große Unternehmen dazu verpflichtet, entlang ihrer gesamten Wertschöpfungsketten Sorgfaltspflichten in Bezug auf Menschenrechte und Umweltstandards einzuhalten und darüber zu berichten. Weitere Informationen zur CSDDD finden Sie unter anderem bei Europäisches Parlament & Rat der Europäischen Union (2024a).
[100] Der CBAM ist ein von der EU eingeführtes Instrument zur Verhinderung von Carbon Leakage und zur Vermeidung von Wettbewerbsverzerrungen durch die Bepreisung von CO_2-Emissionen. Mithilfe von CBAM werden Importe bestimmter CO_2-intensiver Produkte in die EU mit einem CO_2-Preis belegt. Weitere Informationen zum CBAM finden Sie unter anderem bei Europäische Kommission (2025e).

ausgestellter Nachweise bzw. Zertifikate ist ebenfalls der Aufbau von durchgängig digitalen Prozessen notwendig. Das ist insbesondere dann der Fall, wenn diese Nachweise beispielsweise in CO_2-Bilanzen angerechnet oder entwertet werden und eine *Doppelvermarktung* von Nachweisen daher ausgeschlossen werden muss (Strüker et al., 2021b).

Im Bereich der Nachverfolgung von CO_2-Emissionen und CO_2-Nachweisen werden Web3-Technologien schon über Jahre hinweg diskutiert und auch eingesetzt (vgl. unter anderem Heeß et al., 2024; Körner et al., 2025). Mit der Verankerung des Konzepts eines **Digitalen Produktpasses (DPP)**[101] durch die EU-Ökodesign-Verordnung für nachhaltige Produkte (Ecodesign for Sustainable Products Regulation, ESPR)[102] hat der Einsatz von Web3-Technologien für digitale Lösungen zur Nachverfolgung von CO_2-Emissionen zugenommen. In den Arbeiten von Körner et al. (2024b) wird beispielsweise der Einsatz von DIDs (vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) für digitale CO_2-Zertifikate für Unternehmen zum verifizierbaren und manipulationssicheren Nachweis von Emissionen im Energiesektor vorgestellt. Dort wird gezeigt, wie die Integrität und Rückverfolgbarkeit von CO_2-Zertifikaten durch den Einsatz von VCs (vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) und NFTs (vgl. Kapitel 0) sichergestellt werden können. Die vorgestellte Architektur ermöglicht es Erzeugungsanlagen, kryptografisch signierte Zertifikate auszustellen, die Stammdaten und Bewegungsdaten von Smart Metern kombinieren, um ein Nachverfolgungssystem für CO_2-Kompensationen zu ermöglichen. Diese Zertifikate werden als VCs bilateral entlang der Lieferkette übertragen, sodass keine zentralen Register mehr erforderlich sind. Um Doppelzählungen zu vermeiden, wird die Verknüpfung jedes CO_2-Zertifikats mit NFTs angeregt. Ein weiteres Beispiel ist das Whitepaper von Tan et al. (2023), das das Potenzial verschiedener Web3-Technologien (insbesondere Dezentralisierung und erhöhte Transparenz) im Kontext des CO_2-Emissionshandels diskutiert. Der Einsatz dezentraler Technologien könnte potenziell zur Stärkung des Stakeholder-Engagements entlang der gesamten Wertschöpfungskette eines Emissionshandels beitragen. Damit können finanzielle Anreize (z. B. durch die Bepreisung von Emissionen oder Emissionsreduktionen) zwischen Investoren, Netzbetreibern sowie Endkundinnen und Endkunden transparent allokiert werden. Dadurch werden Reibungsverluste und Interessenkonflikte zwischen den einzelnen Stakeholdern reduziert. Des Weiteren bietet die Publikation einen systematischen Überblick über bestehende Marktinitiativen, die Web3-basierte Anwendungen in den Bereichen Datenerfassung, Emissionsbilanzierung und Handel integrieren.

3.4 Registersynchronisation und -interoperabilität

Um ein transparentes und effizientes Energiedatenmanagement sowie eine lückenlose Nachweisführung für die Marktakteure zu gewährleisten, werden verschiedene (digitale) Register verwendet. Diese Register dienen als zentrale, vertrauliche Datenquellen für wichtige energiewirtschaftliche Prozesse – beispielsweise im Netzbetrieb oder für die Marktteilnahme. Die Registerbetreiber sind dabei für die Dokumentation und Verwaltung von unterschiedlichen Informationen (z. B. Stammdaten zu Erzeugungsanlagen zur sicheren Identifikation) verantwortlich. Wichtige Register im heutigen und zukünftigen Energiesystem sind unter anderem:

- *Marktstammdatenregister (MaStR):* Das deutsche Marktstammdatenregister fungiert als ein umfassendes behördliches Register des Strom- und Gasmarktes, das von den Behörden und den Marktakteuren des

[101] Digitale Produktpässe (DPPs) sollen für das Ziel einer Kreislaufwirtschaft relevante Informationen zu Produkten (z. B. Rohstoffherkunft, Reparatur- und Recyclingmöglichkeiten, CO_2-Fußabdruck) entlang der Wertschöpfungskette enthalten und damit den Stakeholdern zugänglich machen. Weitere Informationen zu DPPs finden Sie unter anderem bei Publications Office of the European Union (2024) und Walden et al. (2021).
[102] Die ESPR schafft einen Rahmen zur Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte. Die Verordnung hat zum Ziel, die Umweltverträglichkeit von Produkten über ihren gesamten Lebenszyklus zu erhöhen und ressourcenschonende Kreisläufe (bis hin zur Kreislaufwirtschaft) zu fördern. Weitere Informationen zur ESPR finden Sie unter anderem bei Europäisches Parlament & Rat der Europäischen Union (2024b).

Energiebereichs (Strom und Gas) genutzt werden kann. Die im Register gespeicherten Daten umfassen Stammdaten zu Erzeugungsanlagen sowie zu großen Verbrauchseinheiten.

- *Herkunftsnachweisregister (HKNR):* Mithilfe des HKNR wird die Herkunft von Strom aus erneuerbaren Energien in Form von HKNs dokumentiert und verwaltet.
- *Flexibilitätsregister* (Flexibility Register oder Flexibility Resources Register): Die Etablierung eines solchen Registers, das Informationen zu Flexibilitätsoptionen von dezentralen Energieerzeugungsanlagen enthält, wurde in Forschungsprojekten wie Enera[103] und von ENTSO-E[104] diskutiert.

Die *Synchronisierung* dieser Register umfasst die Harmonisierung, Echtzeit-Aktualisierung und Interoperabilität unterschiedlicher zentraler oder dezentraler Datenbanken. Eine Modernisierung und Digitalisierung der bestehenden Register sind insbesondere deshalb notwendig, weil oftmals bestimmte Daten mehrfach in unterschiedlichen Registern gesichert und gepflegt werden. Dazu zählen beispielsweise die Stammdaten von Erzeugungsanlagen, die sowohl im MaStR als auch im HKNR erfasst werden. Eine mehrfache Datenhaltung und fehlende Schnittstellen führen dabei nicht nur zu einem hohen Verwaltungsaufwand und entsprechenden volkswirtschaftlichen Kosten, sondern erhöhen auch das Risiko, dass Aktualisierungen nicht konsistent durchgeführt werden. Um im Zuge der Modernisierung von Registern ein sogenanntes *Once-Only-Prinzip*[105] umzusetzen, spielen die grundlegende Digitalisierung und Interoperabilität der einzelnen Register eine entscheidende Rolle. Während Flexibilitätsregister bislang nicht großflächig implementiert worden sind, treten beispielsweise bei der bestehenden Implementierung des MaStR sowie des HKNR bestimmte Herausforderungen auf: Bei der Implementierung des MaStR besteht insbesondere ein Vertrauensproblem hinsichtlich der Datenqualität und es mangelt an Schnittstellen für die Datennutzung in verschiedenen Anwendungsfällen (Deutsche Energie-Agentur, 2022a). Das HKNR leidet ebenfalls unter dem Fehlen von Schnittstellen, was die Automatisierung der Prozesse im HKN-System behindert (vgl. Kapitel 3.2; Bogensperger et al., 2023).

Web3-Technologien können sowohl bei der Implementierung von Registern als auch bei ihrer Synchronisierung Lösungen anbieten. Beispielsweise schlägt der Abschlussbericht des BMIL-Projekts (Deutsche Energie-Agentur, 2022a) eine Blockchain-basierte Implementierung für das MaStR vor. In dem dort vorgestellten Lösungsansatz werden *Smart Meter Gateways* (SMGWs) mit Krypto-Chips ausgestattet und direkt mit einem Blockchain-basierten Register für Marktstammdaten verbunden. Durch diese *digitale Vertrauenskette* könnte das bestehende Problem bezüglich der Datenqualität gelöst werden. Der Bericht weist zudem auf die Bedeutung von interoperablen Bausteinen hin, um die Synchronisierung von verschiedenen Registern im Energiesektor und damit die Datenintegrität und -konsistenz über unterschiedliche, potenziell Blockchain-basierte Register hinweg sicherzustellen. In diesem Zusammenhang könnten auch Smart Contracts eingesetzt werden, um eine bedingte Integration zwischen verschiedenen Registern zu erzwingen. Beispielsweise könnte ein Smart Contract so programmiert werden, dass vor der Zulassung einer EE-Anlage zur Teilnahme an lokalen Flexibilitätsmärkten oder zur Ausgabe von HKNs für EE-Anlagen geprüft wird, ob die Anlage im nationalen MaStR mit einer gültigen Kennung registriert ist. Dadurch wird sichergestellt, dass Aktualisierungen in einem Register nur dann vorgenommen werden, wenn sie mit den Regeln eines anderen Registers

[103] Eine Diskussion über den Nutzen eines Flexibilitätsregisters finden Sie unter https://projekt-enera.de/wp-content/uploads/enera-roadmap.pdfhttps://www.oeko.de/fileadmin/oekodoc/enera-Roadmap.pdf (Vogel et. al, 2021).
[104] Eine detaillierte Vorstellung des Konzepts eines Flexibilitätsregisters finden Sie bei CEDEC et al. (2019).
[105] Das Once-Only-Prinzip sieht vor, dass Bürgerinnen und Bürger sowie Unternehmen nur einmal Daten und Nachweise einer deutschen Behörde übermitteln müssen und sie dann effektiv zwischen den Behörden ausgetauscht werden. Weitere Informationen zum Once-Only-Prinzip im Kontext der Registermodernisierung finden Sie unter anderem bei Bundesministerium für Digitales und Staatsmodernisierung (2025a).

übereinstimmen. Über die Synchronisation der Register hinaus kann damit auch die Aktualität der enthaltenen Daten erhöht werden, da effizient nachvollzogen werden kann, inwiefern gemeldete Anlagen tatsächlich einspeisen bzw. ob einspeisende Anlagen wirklich korrekt angemeldet sind.

3.5 Effizienterer Netzbetrieb

Wie in Kapitel 1 dargelegt, geht die zunehmende Einspeisung erneuerbarer Energien in unterschiedliche Netzebenen mit neuen Herausforderungen für den Netzbetrieb einher. Insbesondere im Nieder- und Mittelspannungsbereich steigt der Anteil an Ladestationen, Batteriespeichersystemen und Prosumern. Dies erfordert eine zunehmende *Koordination* zwischen verschiedenen Akteuren. Eine solche Koordination ist notwendig, um Netzstabilität und Versorgungssicherheit trotz steigender dezentraler Lasten und zunehmender dezentraler Erzeuger zu gewährleisten. Für einen sicheren und effizienten Datenaustausch im Netzbetrieb ist eine Echtzeit-Übertragung und -Verarbeitung relevanter *Netz- und Steuerungsdaten* mit *niedriger Latenz* erforderlich. Der Einsatz von **Edge Computing** (z. B. intelligente Messsysteme (iMSys), Haushaltsenergiemanagementsysteme (HEMS)[106]) in Kombination mit **Cloud Computing** (z. B. cloudbasierte Netzleitsysteme) könnte dabei ein zentraler Baustein sein, um große Datenmengen bis an die Endpunkte des Netzes verfügbar zu machen (vgl. Abbildung 15; Deutsche Energie-Agentur, 2024b).[107] Neben der niedrigen Latenz ist zudem die Gewährleistung der Datenintegrität und Fälschungssicherheit erforderlich, um Manipulationen zu verhindern und vertrauenswürdige Transaktionen zu ermöglichen. In diesem Kontext spielt auch der Umgang mit Daten von Endnutzerinnen und -nutzern eine entscheidende Rolle. Insbesondere die Erfassung und Verarbeitung verbrauchsbezogener Daten erfordern Mechanismen, um Datenschutzanforderungen zu erfüllen. Dieses Problem könnte durch Web3-Technologien adressiert werden, wenn die Web3-basierten Lösungen nach dem Grundsatz von *Privacy-by-Design* gestaltet werden.

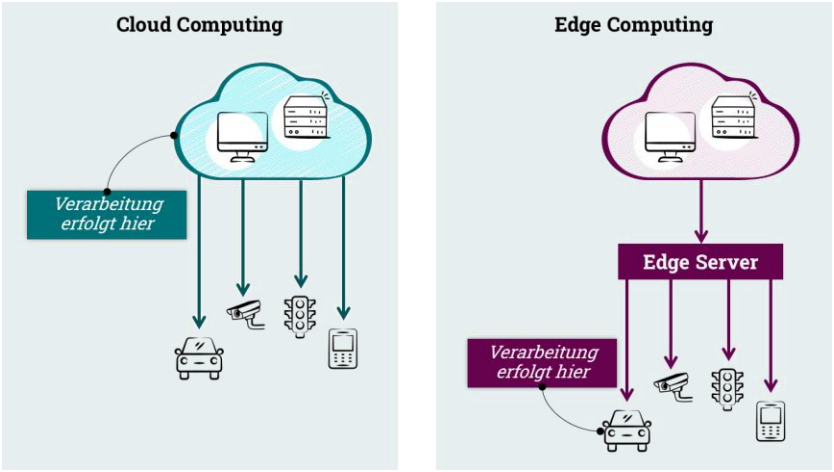

Abbildung 15: Cloud Computing vs. Edge Computing

[106] Heimenergiemanagementsysteme (Home Energy Management Systems, HEMS) sind Systeme zum Monitoring, zur Optimierung und zur Steuerung der Energieflüsse in privaten Haushalten. Mithilfe eines HEMS kann beispielsweise die Nutzung von Assets wie Photovoltaik-Anlagen, Heimspeichern, Wärmepumpen oder E-Fahrzeugen integriert und anhand von Preisinformationen, Wetterprognosen und/oder Nutzerpräferenzen optimiert und gesteuert werden.
[107] Cloud Computing bezeichnet den schnellen, bequemen und bedarfsgerechten Netzwerkzugriff auf eine Vielzahl vorkonfigurierter IT-Ressourcen (z. B. Netzwerke, Server, Speicher und Dienste), die sogenannte Cloud. Unter Edge Computing versteht man die Verarbeitung von Daten in unmittelbarer Nähe zum Gerät (d. h. an der Datenquelle) anstatt ihre Übertragung in eine entfernte Cloud.

Für die Sicherstellung eines effizienten Netzbetriebs könnten insbesondere Datenräume zum Einsatz kommen. Im CEEDS-Blueprint (Dognini et al., 2024) werden unterschiedliche Anwendungsfelder für einen effizienten Netzbetrieb durch die Nutzung von Datenräumen präsentiert. Sie umfassen unter anderem die Optimierung von Betrieb und Wartung (Operation & Maintenance, O&M) von EE-Anlagen und des Lademanagements sowie Roaming-Dienste für E-Fahrzeuge. Letztere ermöglichen es Fahrzeugbesitzerinnen und -besitzern, ihr E-Fahrzeug auch an Ladeinfrastrukturen von Elektromobilitätsdienstleistern (Electric Mobility Service Provider, eMSP) zu laden, mit denen sie keinen direkten Vertrag abgeschlossen haben. In diesem Fall sind die Gewährleistung der Interoperabilität von Roaming-Diensten im Bereich der Elektromobilität und ein reibungsloser Datenaustausch zwischen EVUs, eMSPs, Roaming-Dienstanbietern (Roaming Service Provider, RSP) und Ladepunktbetreibern (Charge Point Operator, CPO) erforderlich. Diese Interoperabilität – sichergestellt durch Datenräume – kann es ermöglichen, E-Fahrzeuge grenzüberschreitend an verschiedenen Ladepunkten zu laden, unabhängig vom jeweiligen Anbieter. In den genannten Anwendungsfällen könnten auch andere Web3-Technologien, wie dezentral verwaltete digitale Identitäten, zur Identifizierung der Teilnehmer im Datenraum genutzt werden. Untersucht wurde und wird der Einsatz der Blockchain-Technologie für den sicheren Datenaustausch zum Beispiel bei der Netzsteuerung (Seshasai et al., 2025), bei der Sektorenkopplung und beim Laden von Elektrofahrzeugen (Okwuibe et al., 2020). Ebenso wurde und wird die Nutzung von Smart Contracts unter anderem für den Peer-to-Peer-Handel (Saeed et al., 2024) und die automatisierte Laststeuerung (Kirli et al., 2022) bereits betrachtet.

3.6 Umsetzung dezentraler Governance-Mechanismen im Energiesystem

Die Dezentralisierung des Energiesystems geht mit neuen Herausforderungen und Chancen für die Governance[108] einher. Die zunehmende Partizipation von Endkundinnen und Endkunden, Prosumern und Aggregatoren führt zur *Entstehung neuer Akteure und Marktrollen*, wodurch neue Governance-Mechanismen und -Strukturen erforderlich werden (Brisbois, 2022). Dies könnte sich beispielsweise in stärker dezentral organisierten Entscheidungsprozessen zur Integration und Bereitstellung von Kleinstflexibilitäten zeigen, während dezentral verteilte Verantwortlichkeiten und Strukturen Innovation und Unabhängigkeit von Lieferanten fördern. Digitale Technologien spielen eine zentrale Rolle für eine effektive Umsetzung dezentraler Governance mit dem Ziel, die Energiewende zu fördern und zu beschleunigen (United Nations Development Programme, 2023). Insbesondere die Anwendung von Web3-Technologien wird oftmals eng mit der Umsetzung dezentraler Governance in Verbindung gebracht. Wie in Kapitel 2 diskutiert, ermöglichen die dezentralen Architekturen von Web3-Technologien eine breite Teilhabe, stellen jedoch nicht automatisch auch die Implementierung einer dezentralen Governance-Struktur sicher. Daher sollte die Entwicklung geeigneter Governance-Strukturen Hand in Hand mit der technologischen Konzeption neuer Lösungen erfolgen. Die zuvor vorgestellten potenziellen Anwendungsfälle von Web3-Technologien (vgl. Kapitel 3.1 bis 3.5) sind daher meist auch mit Änderungen in den bestehenden Governance-Strukturen im Energiesektor verbunden.

Im Energiesektor wird der Einsatz von Web3-Technologien für die Umsetzung von dezentralen Governance-Mechanismen für unterschiedliche Anwendungsfälle diskutiert. In der Arbeit von Diaz Valdivia (2023) wird erörtert, wie durch Web3-Technologien, insbesondere Blockchain, Tokenisierung und Smart Contracts, dezentrale Governance-Mechanismen direkt in Energiehandelsplattformen integriert werden können. Es wird zum Beispiel erörtert, wie stärker partizipative Strukturen (z. B. Vereine, Stiftungen) Entscheidungen

[108] Governance umfasst formelle und informelle Regeln, Normen, Strukturen und Prozesse, die das Verhalten und die Entscheidungsfindung von Akteuren steuern, und ist nicht gleichzusetzen mit Regulatorik. Regulatorik ist eine im Gesetz verankerte Form der Governance. Weitere Diskussion über Governance finden Sie unter anderem bei Engineering X (2025).

über die technologische Entwicklung einer Blockchain, regulatorische Interaktionen oder die Finanzierung außerhalb der Blockchain koordinieren können. Solche sogenannten **Offchain-Governance-Mechanismen** umfassen beispielsweise die Festlegung von *Abstimmungsprozessen* und die Integration von Diskussionen auf Foren. Bestimmte Governance-Mechanismen können auch onchain, also auf der Blockchain selbst, festgehalten und umgesetzt werden (z. B. in Form von Smart Contracts). Solche verankerten Mechanismen ermöglichen es teilnehmenden Akteuren, etwa den Mitgliedern einer Erneuerbare-Energie-Gemeinschaft (EEG) (Energy Sharing Community) oder einer dezentralisierten Energiehandelsplattform, gemeinsame Entscheidungen zu treffen. Diese Mechanismen könnten nicht nur automatisiert umgesetzt werden, sondern fördern auch die Beteiligung der Gemeinschaftsmitglieder am Entscheidungsprozess.

Die Arbeit von Trevisan et al. (2025) präsentiert einen DAO-Ansatz (vgl. Kapitel 2) für eine dezentrale Governance für EEGs. Dieser Ansatz zielt darauf ab, verschiedene Abstimmungsprozesse innerhalb einer EEG effizienter zu gestalten. In ihrer Arbeit präsentieren sie eine Lösung, bei der sich die DAO-Mitglieder mithilfe eines Konsensmechanismus auf eine Reihe von Parametern wie Preisbildungsmechanismen und Netzdienstleistungen einigen, die in einem Distributed Ledger gespeichert werden. Die Mitglieder haben darüber hinaus auch die Möglichkeit, über eine potenzielle Änderung dieser Parameter abzustimmen. Die Implementierung dieser Konsensmechanismen würde zu einer gesteigerten Transparenz, Verständlichkeit und Automatisierung des Prozesses führen und damit den Bedarf an Intermediären reduzieren. Somit kann die Governance der EEG dezentralisiert werden, was auch die Partizipation innerhalb der Gemeinschaft fördert. Die Akzeptanz von EEGs wird durch diese partizipative Struktur erhöht (Trevisan et al., 2025).

Im Kontext des Peer-to-Peer-Energiehandels könnte die Einführung neuer Governance-Mechanismen durch den Einsatz von Smart Contracts (vgl. Kapitel 0) näher untersucht werden. Die Anwendung von Smart Contracts könnte es dabei vor allem kleinen Akteuren ermöglichen, Strom direkt zwischen Produzenten bzw. Prosumern und Konsumenten bzw. Prosumern zu handeln. Mithilfe eines Smart Contract können beispielsweise die Regeln für den automatisierten Handel festgelegt werden und damit dezentral definieren, wie sich Angebot und Nachfrage der beteiligten Akteure im Stromverkauf und -einkauf gestalten. Selbstverwaltete dezentrale Identitäten können hierbei als Basis für die sichere Identifizierung und Verifizierung der Marktteilnehmer in einem dezentralen System eingesetzt werden. In einem Datenraumansatz können vergleichbare Governance-Strukturen durch Usage-Control-Bausteine (vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) implementiert werden, indem Entscheidungen über den Datenaustausch und das Vertragsmanagement direkt an die Konnektoren der Marktteilnehmer verlagert werden.

4 SWOT-Analyse von Web3-Technologien

Dieses Kapitel präsentiert eine **SWOT**-Analyse (Strength, Weaknesses, Opportunities, Threats). Dazu werden die Stärken und Schwächen der in Kapitel 2 präsentierten Web3-Technologien diskutiert. Die daraus resultierenden Chancen und Risiken für die in Kapitel 3 vorgestellten Anwendungsfälle in der Energiewirtschaft werden jeweils im Anschluss vorgestellt. Zur Durchführung einer praxisnahen Analyse wurden semistrukturierte Interviews mit Expertinnen und Experten aus der Energie- und der Technologiebranche geführt, die an der Schnittstelle zu Web3-Technologien tätig sind (vgl. Tabelle 4).

Tabelle 4: Übersicht über die interviewten Expertinnen und Experten

Verweis Expert*in	Unternehmensart	Verweis Expert*in	Unternehmensart
[1]	Technologieanbieter [Web3]	[7]	Forschungseinrichtung [Web3]
[2]	Forschungseinrichtung [Energiesektor]	[8]	Verteilnetzbetreiber / Energieversorgungsunternehmen
[3]	Technologieanbieter [Web3]	[9]	Verteilnetzbetreiber / Energieversorgungsunternehmen
[4]	Technologieanbieter [Energiesektor]	[10]	Verband [Web3]
[5]	Übertragungsnetzbetreiber	[11]	Technologieanbieter [Energiesektor]
[6]	Übertragungsnetzbetreiber		

4.1 Strengths & Opportunities

4.1.1 Stärken der Web3-Technologien im Energiesektor

Für die Anwendung von Web3-Technologien im Energiesektor sehen die interviewten Expertinnen und Experten unterschiedliche Chancen. Potenzielle Anwendungsbereiche reichen von den in Kapitel 3 vorgestellten Fällen bis hin zu spezifischen Lösungen. So bieten Web3-Technologien übergreifend Potenzial im Bereich der Sektorenkopplung und bei der Anbindung von Kleinstflexibilitäten bis hin zum Peer-to-Peer Energiehandel (vgl. Kapitel 2). Mithilfe von Web3-Technologien lassen sich neben neuen *energiewirtschaftlichen Prozessen* bzw. *Geschäftsmodellen* auch *regulatorische Anforderungen* wie beispielsweise der 24-Stunden-Lieferantenwechsel perspektivisch leichter umsetzen [Interview 3]. Pilotprojekte, in denen Marktakteure diese Technologien testen und ihren Mehrwert bereits validieren können, tragen dazu bei, die Einführung von Web3-Technologien zu beschleunigen [Interview 1 & 4]. Die nachfolgenden Analysen fassen die Stärken und Chancen in Bezug auf unterschiedliche Web3-Technologien zusammen.

Stärken von dezentralen Netzwerken

Dezentrale Netzwerke und Register, insbesondere Blockchains, können in einem dezentral organisierten Energiesektor helfen, *finanzielle Prozesse* effizient abzuwickeln und Nutzerinnen und Nutzer stärker einzubeziehen. Derzeit sind Verbraucherinnen und Verbraucher noch weitestgehend von der Finanzierung von Anlagen und der Abrechnung von erzeugter Energie ausgeschlossen. Die *Tokenisierung von Vermögenswerten bzw. Assets* im Energiesektor schafft jedoch die Grundlage für neue Methoden der Teilhabe und Nachweisführung im Energiesektor (vgl. Kapitel 4.1.2 und Kapitel 5.3). In Bezug auf die Teilhabe an Investitionen gab es bereits erfolgreiche Pilotprojekte, in denen Bürgerinnen und Bürger die Möglichkeit hatten, sich in Form von Tokens an der Finanzierung großer Photovoltaik-Anlagen zu beteiligen (Steinschaden, 2021) [Interview 10]. Die Anteilseigentümer der Anlage erhalten beispielsweise für die erzeugten Energiemengen aus ihrem erworbenen Anteil eine bestimme Menge an Tokens, die sie wiederum direkt für ihren Verbrauch (z. B. Laden eines E-Fahrzeugs, Zahlen einer Stromrechnung) einlösen können. Im „Backend" einer solchen Lösung werden die Transaktionen für die Anteilseigentümer dezentral, sicher und transparent abgewickelt, ohne vertrauliche Daten zu ihnen zu teilen. Zudem haben die Entwickler insbesondere darauf geachtet, eine möglichst hohe Nutzerfreundlichkeit durch die dazugehörigen Anwendungen (Apps) zu erreichen, sodass die Nutzerinnen und Nutzer kein Vorwissen zu Web3-Technologien benötigen [Interview 10]. Durch Tokenisierung und damit verbundene Beteiligungsmodelle kann die Akzeptanz von EE-Projekten gefördert und das Potenzial einer Beteiligung für die Nutzerinnen und Nutzer jederzeit beobachtbar und erfahrbar gemacht werden. Tokenisierung kann analog neue *Finanzierungsmodelle* ermöglichen, wie beispielsweise bei der Investition in Großbatteriespeicher oder das Bereitstellen einer neuen Energieflexibilitätsoption durch Mining[109] (Carter et al., 2023; Menati et al., 2023) [Interview 10]. Die politische Entwicklung im Bereich von Kryptowährungen[110] kann die Entwicklung von neuen Finanzierungslösungen zusätzlich beschleunigen (Mičijević, 2025) [Interview 10].

Stärken von digitalen Identitäten / SSI

Mit der zunehmenden Elektrifizierung und Sektorenkopplung im Energiesektor (z. B. durch E-Fahrzeuge, Wärmepumpen, Heim-PV-Anlagen und -Speicher) wächst die Anzahl der Geräte und Akteure, die mit dem Stromnetz interagieren. Um diese Geräte und Akteure für unterschiedliche energiewirtschaftliche Prozesse (z. B. Netzengpassmanagement, Frequenzregelung etc.) in Echtzeit *identifizieren*, *authentifizieren* und miteinander *vernetzen* zu können, ist es erforderlich, derzeitige Identitätsmanagementlösungen weiterzuentwickeln (Europäische Kommission, 2022; Europäische Kommission, 2023) [Interview 6 & 11]. Beispielsweise ist es technisch möglich, dass E-Fahrzeuge an unterschiedlichen Stellen im Energiesystem – zu Hause, bei der Arbeit, an einer Ladesäule – laden und zukünftig mit einer bidirektionalen Ladefähigkeit auch ausspeichern können. Um diese Möglichkeit zu nutzen, das E-Fahrzeug als solches zu erkennen und optimal für unterschiedliche Zwecke wie die Bereitstellung von Energieflexibilität zu authentifizieren und zu autorisieren, ist die sichere und effiziente Weitergabe von Informationen (z. B. Ladekapazität, Ladeleistung, aktueller Ladezustand) notwendig (Deutsche Energie-Agentur, 2022a; Leinauer et al., 2024).

[109] Mining (insbesondere im Zusammenhang mit Bitcoin) bezeichnet die Validierung der Transaktionen auf der Blockchain durch das Lösen von kryptografischen, rechenintensiven Aufgaben (vgl. Kapitel 2.1). Da dieser Vorgang viel Strom benötigt, könnte in Zeiten von Überschusserzeugung von erneuerbaren Energien dieser Überschuss für Mining als flexible Last genutzt werden, anstatt den Strom abzuregeln.

[110] Die politische Regulierung von Kryptowährungen entwickelt sich international zunehmend weiter. Besonders Stablecoins rücken dabei in den Fokus. So sind in den USA beispielsweise Emittenten von US-Dollar-Stablecoins verpflichtet, sichere Reserven im Wert von 1:1 zu hinterlegen. Parallel werden in der EU (z. B. durch MiCAR, vgl. Kapitel 0) und in Großbritannien ähnliche Regelungen zur Förderung von Anlegerschutz, Transparenz und Stabilität von Kryptowährungen umgesetzt (Haun, 2025; Schaaf, 2025).

Für die Integration solcher kleinen, verteilten und teilweise mobilen Anlagen ist eine *zuverlässige* und *sektorenübergreifend* funktionierende Schicht der *Identitätsverwaltung* erforderlich. Die Verwaltung der Identitäten kann auf unterschiedliche Weise erfolgen und ist derzeit in der Regel meist als zentralisiertes System ausgelegt (vgl. Kapitel 2.2). Aufgrund der Sektorenkopplung, in der sich Geräte und Anlagen mit unterschiedlichen Identitätsattributen in verschiedenen Sektoren identifizieren (müssen), bieten dezentrale und Web3-basierte Identitätslösungen einen Mehrwert: Zum einen könnten sie *Datensilos* bei einzelnen Identitätsmanagementanbietern *aufbrechen*. Zum anderen ermöglichen sie insbesondere neuen Akteuren im Energiesystem die *Kontrolle* darüber, welche Identitätsattribute zu ihren Geräten und zu ihrer Person sie zu welchem Zweck mit welchem Dienstleister teilen [Interview 11]. Ein dezentrales und digitales Identitätsmanagement auf Geräteebene kann daher nicht nur eine optimierte und gezielte Steuerung für den Netzbetrieb ermöglichen, sondern auch einen breiteren *Zugang* zu Energiedienstleistungen und Energiemärkten schaffen (beispielsweise einfaches Laden des E-Fahrzeugs im Ausland)[111] (Leinauer et al., 2024; Parameswarath et al., 2022) [Interview 3]. Die regulatorischen Grundlagen in der EU schaffen dabei eine wichtige Basis, unter anderem durch die nach eIDAS 2.0 entwickelten Personen- und Business Wallets, um dezentrale digitale Identitäten im Energiesektor zu nutzen. So können digitale Identitäten beispielsweise auch bei anderen gesetzlichen Anforderungen wie dem Network Code on Demand Response ein grundlegendes Element für eine effiziente, interoperable und sichere Umsetzung sein (Dognini et al., 2024; Kalt et al., 2024) [Interview 6].

Stärken von Datenräumen

Im Kontext von Datenräumen heben die interviewten Expertinnen und Experten hervor, dass sie die *Sicherheit*, *Verfügbarkeit* und *Qualität* der *ausgetauschten Daten* verbessern können. Insbesondere im Energiesektor stellen mangelnde Datenverfügbarkeit und Datenqualität eine Hürde bei der Umsetzung von neuen technischen Anwendungen wie beispielsweise KI-basierten Lösungen dar (Shobanke et al., 2025). Ein potenzieller Anwendungsfall im Energiesystem, der von einer erhöhten Datenverfügbarkeit durch Datenräume profitieren könnte, ist die Situational Awareness[112] (Situationserkennung) in Verteilnetzen [Interview 2]. Zudem können Datenräume *techno-ökonomische Vorteile* für Endnutzerinnen und -nutzer bieten, wie beispielsweise eine verbesserte Benutzerfreundlichkeit und einen erhöhten Datenschutz (Rülicke et al., 2024) oder wettbewerbsfähigere Energiepreise und reduzierte Kosten bei Lieferantenwechsel (Gouriet et al., 2022) [Interview 2]. Darüber hinaus haben Datenräume das Potenzial, den *sektorenübergreifenden Austausch von Daten* zu vereinfachen, zum Beispiel für Bevölkerungswarnsysteme [Interview 3]. Für derartige Systeme ist ein interoperabler Datenaustausch zwischen verschiedenen Organisationen aus unterschiedlichen Sektoren erforderlich. Datenräume ermöglichen für ein Bevölkerungswarnsystem einen nahtlosen Austausch von Daten zwischen Bevölkerungswarnstellen, Netzbetreibern und Betreibern von Ladeinfrastrukturen. Dadurch wären eine temporäre Steuerung von Ladevorgängen im Mobilitätssektor sowie die gezielte Lastverschiebung bei Großverbrauchern aus der Industrie möglich. Parallel dazu könnten Endkundinnen und -kunden informiert werden, dass entsprechende Maßnahmen durchgeführt werden. Zudem könnten beispielsweise Besitzerinnen und Besitzer von E-Fahrzeugen nicht nur über veränderte Ladebedingungen, sondern auch

[111] Das Laden von E-Fahrzeugen im Ausland ist ein Beispiel für das Potenzial von dezentralen Identitätslösungen, da die Identifizierung, Authentifizierung und Autorisierung von Attributen des Mobilitäts- und Energiesektors (z. B. Batteriekapazität, Ladezustand) sowie des Wohnsitzes und Aufenthaltslandes (z. B. Zulassung) abhängt. Die Selbstverwaltung von digitalen Identitäten könnte die Integration von E-Fahrzeugen in den Energiesektor verbessern, indem die jeweils notwendigen Fahrzeug-, Inhaber- und Betreiberinformationen vertrauenswürdig und sicher direkt an den Ladesäulen genutzt werden können.
[112] Für eine umfassende Situationserkennung im Verteilnetz muss der Netzbetreiber den Status aller Schaltanlagen, die Strom- und Spannungswerte, die Leistungsflüsse auf Leitungen und Transformatoren sowie die Netztopologie – einschließlich Knoten und Anlagen, die außer Betrieb sind – überwachen.

über das Umfahren oder Meiden von Gefahrengebieten benachrichtigt werden. Auf diese Weise werden technische Flexibilitäten mit sicherheitsrelevanten Informationen verknüpft, um die Resilienz des Gesamtsystems zu erhöhen.

4.1.2 Chancen und Potenziale für Anwendungsfälle von Web3-Technologien im Energiesektor

Chancen und Potenziale für den Redispatch 3.0

Die interviewten Expertinnen und Experten sehen Chancen und Potenziale durch den Einsatz von Web3-Technologien in den in Kapitel 3 vorgestellten Anwendungsfällen. Am häufigsten wurde dabei das Potenzial von Web3-Technologien für den Redispatch 3.0 angeführt. In diesem Kontext haben die Interviewten nicht nur die Stärken von Web3-Technologien für die Marktkommunikation und Datenverarbeitung, sondern auch bei der Vermarktung, der Abrechnung und dem Nachweis von Energieflexibilität hervorgehoben. Mithilfe von kryptografischen Verfahren und verteilten Infrastrukturen können Web3-Technologien hohe Sicherheits- und Datenschutzstandards realisieren und damit vielversprechende Lösungsansätze für den *sicheren Austausch sensibler Netzdaten* bieten – was wiederum für die operative Steuerung von Maßnahmen im Redispatch 3.0 von Vorteil ist [Interview 5].

In einem Energiesystem, in dem dezentralisierte EE-Anlagen eine große Rolle spielen, bieten dezentrale digitale Identitäten einen wesentlichen Lösungsbaustein. Damit könnte die Identifizierung einer Vielzahl von Anlagen für Maßnahmen im Redispatch 3.0 effizient, automatisierbar und sicher erfolgen. Des Weiteren könnten digitale Identitäten auch einen reibungslosen Wechsel von einem Aggregator[113] zu einem anderen ermöglichen [Interview 11]. Insbesondere eine auf Web3-Technologien basierende und gesicherte *Identitäts- und Rollenzuordnung* bei *Flexibilitätsabrufen* sowie bei der *Nachweisführung der Flexibilitätsbereitstellung* schafft für mehrere interviewte Expertinnen und Experten einen besonders hohen Mehrwert [Interview 3, 5, 8 & 11]. In Pilotprojekten (z. B. Pebbles[114]) wurden mittels Web3-Technologien lokale Energiemärkte und Flexibilitätsnachweise bereits erfolgreich umgesetzt [Interview 8]. Darüber hinaus wird die Integration von E-Fahrzeugen und potenziell weiteren Asset-Typen für Energieflexibilität in mehreren Pilotprojekten implementiert [Interview 5 & 11].

Aufgrund der bereits bestehenden Definition der Marktrollen in der Energiewirtschaft wird der Übergang hin zu einer dezentralen Identitätsverwaltung auf Basis von Web3-Technologien vereinfacht. Es ist lediglich eine Übertragung dieser Marktrollen in eine neue technische Infrastruktur erforderlich [Interview 8]. Die Nutzung der Flexibilität von steuerbaren Lasten kann durch innovative marktbasierte oder quotenbasierte Modelle unter Einsatz dezentraler Identitätslösungen realisiert werden [Interview 8]. Zu solchen Modellen gehört ebenfalls eine *datenschutzkonforme* und *verifizierbare Abwicklung* von *Flexibilitätsabrufen* über Aggregatoren. Bei einem potenziellen Einsatz von dezentralen digitalen Identitäten würde ein Übertragungsnetzbetreiber (ÜNB) dann keinen Zugriff auf einzelne Messdaten benötigen [Interview 5]. Die Anwendung von dezentralem Identitätsmanagement in Kombination mit Datenräumen kann zudem die Aggregation und sichere Verarbeitung von Anlagen- und Flexibilitätsdaten verbessern [Interview 5 & 11]. Datenräume bieten dabei eine strukturierte Umgebung, die die *Harmonisierung von Marktinteraktionen* fördert und die Partizipation der Endkundinnen und -kunden unterstützt [Interview 2].

[113] Ein Aggregator bündelt die Erzeugung und den Verbrauch von Endverbraucherinnen und -verbrauchern und bietet sie am Energiemarkt an. So ermöglicht diese Entität die Anbindung der Energieflexibilitäten der Endverbraucherschaft.
[114] Weitere Informationen zum Projekt Pebbles finden Sie unter https://pebbles-projekt.de/en/project/ (Pebbles, 2025).

Chancen und Potenziale für HKN-Systeme, Auflösen von Farbkategorien und Register

Im Bereich der Nachweisführung sehen die interviewten Expertinnen und Experten zwei große Potenziale, die durch Web3-Technologien realisiert werden können: erstens die *Bereitstellung von digital verifizierbaren Nachweisen zur Stromherkunft und CO_2-Intensität* und zweitens eine *sichere und nachvollziehbare Verwaltung und Weitergabe dieser Nachweise*. Die Bereitstellung von digital verifizierbaren Nachweisen wird durch die einzigartige Verknüpfung von digitalen Identitätslösungen für (Mess-)Geräte und Marktrollen (d. h. Stammdaten, vgl. Kapitel 3.2 bis 3.4) mit den Messwerten (d. h. Bewegungsdaten, vgl. Kapitel 3.2 bis 3.3) ermöglicht. Aus Sicht der Praktiker bietet eine solche digitale Verifizierung sowohl den Mehrwert, dass diese Nachweise für unterschiedliche Zwecke (z. B. HKNs, Digitale Produktpässe) eingesetzt werden können, als auch dass die verifizierbaren Stromerzeugungs- und -verbrauchsdaten deutlich feingranularer nach Zeit, Ort und Objekt (d. h. Anlage) aufgelöst werden können (Babel et al., 2024) [Interview 3, 8, 10 & 11]. Eine *höhere Auflösung* von Stromerzeugungs- und -verbrauchsdaten und daraus abgeleiteten CO_2-Informationen kann dazu beitragen, andere regulatorische Anforderungen (z. B. bei Wasserstoff, CO_2-Reporting) effizienter zu erfüllen und den bürokratischen Aufwand auf allen Seiten zu verringern.

Wenn diese digital verifizierbaren Informationen zur Stromherkunft oder CO_2-Intensität in der Wertschöpfungskette und über Sektoren- und Ländergrenzen hinweg nachvollziehbar und transparent weitergegeben werden sollen, könnte zudem ein dezentrales Register wie eine Blockchain Vertrauen schaffen (Parhamfar et al., 2024; Woo et al., 2021) [Interview 3, 10 & 11]. Der Mehrwert wäre insbesondere dann gegeben, wenn eine zentrale Vertrauensinstanz wie eine Behörde fehlt (z. B. bei einer internationalen Wasserstofflieferkette), denn dann ist die *Gefahr von Double-Spending*[115] besonders hoch. Auch bei bereits etablierten Systemen, wie beispielsweise dem Ausstellen und Anrechnen von HKNs, kann es zu Double-Spending durch die Anrechnung in unterschiedlichen Bilanzierungssystemen kommen. Web3-Lösungen könnten die Anrechnung und Allokation von HKNs und ähnlichen Zertifikaten transparenter gestalten und dabei auf bereits bestehende internationale Standards (z. B. für DIDs, vgl. Kapitel 2.2) für die sektorenübergreifende Implementierung zurückgreifen [Interview 8]. Dafür ist jedoch eine *Ende-zu-Ende digitale Kette der Nachweisführung* nötig. Daher könnte bei bereits bestehenden zentralen Registern der Ausbau von sektorenübergreifenden Datenräumen und zugehöriger Schnittstellen eine große Rolle spielen, um Nachweise mit hoher Flexibilität für verschiedene Marktrollen weiterzugeben (Gaia-X, 2025; Llorca et al., 2024) [Interview 8].

Zusammenfassend bieten Web3-Technologien im Bereich der Nachweisführung, insbesondere bei unterschiedlichen regulatorischen Anforderungen und Methoden zur Bereitstellung von Nachhaltigkeitsinformationen, ein erhebliches Potenzial, um sowohl bestehende (z. B. HKNs, RFNBO-Zertifikate, CSRD) als auch zukünftige (z. B. CSDDD, CBAM) regulatorische Instrumente für Dekarbonisierung effizient umzusetzen. Dadurch kann aus regulatorischen Anforderungen und Berichtspflichten, die derzeit mit einem hohen *Bürokratie-Aufwand* assoziiert werden, ein wirksames und effektives Steuerungsinstrument für Unternehmen und die öffentliche Hand werden – vorausgesetzt es baut auf einer Ende-zu-Ende digitalen Infrastruktur auf (Fisher, 2024) [Interview 10].

[115] Double-Spending bezeichnet die mehrfache Anrechnung ein und derselben Emissionsminderung oder CO_2-Kompensation oder eines HKN durch verschiedene Akteure oder in unterschiedlichen Bilanzierungssystemen.

Chancen und Potenziale für effizienteren Netzbetrieb und Sektorenkopplung

Die zunehmende Anzahl an Akteuren im Netz – insbesondere an der Schnittstelle zu anderen Sektoren – erfordert nicht nur ein effizientes Management von Energieerzeugung, -verbrauch und -flexibilitäten, sondern auch den Umgang mit *Agenten*[116] und *automatisierten Systemen im Netzbetrieb*. Bei dynamischen Preisen und zunehmender Automatisierung (z. B. durch HEMS) besteht die wachsende *Gefahr korrelierter Entscheidungen*, die die Netzstabilität gefährden können (Sánchez Molina, 2025). Ein Beispiel für eine solche Entscheidungsfindung ist, dass alle HEMS in einer Region auf Basis eines bestimmten Preissignals (z. B. sehr günstiger Strompreis) automatisiert E-Fahrzeuge und Heimspeicher laden. Da die HEMS untereinander unkoordiniert sind, könnten solche Szenarien die Netzbetreiber vor erhebliche Herausforderungen (z. B. im Netzengpassmanagement) stellen [Interview 7]. In solchen komplexen Systemen könnten Web3-Technologien helfen, die *Transparenz und Koordination* zu verbessern. Ein wichtiges Anwendungsfeld liegt hierbei in der Entwicklung transparenter Datengrundlagen für die Koordination dezentraler Energiesysteme und Agenten. Transparente Datengrundlagen bezeichnen dabei nachvollziehbare, zugängliche und überprüfbare Daten und Datenmanagementprozesse, die als verlässliche Basis für Entscheidungen, Prozesse oder Bewertungen dienen. Sie ermöglichen es verschiedenen Akteuren, auf dieselben Informationen zuzugreifen, diese einheitlich zu interpretieren und nachzuvollziehen, wie und warum bestimmte Entscheidungen getroffen wurden. DLTs und Smart Contracts könnten dabei als technische Grundlage für entsprechende neue und komplexe Geschäftsprozesse dienen [Interview 7].

An der Schnittstelle zu anderen Sektoren kann – wie in vorherigen Absätzen dargestellt – die Nutzung digitaler Identitäten für einzubeziehende Assets, insbesondere bei einem weitestgehend automatisierten Netzbetrieb, die Effizienz steigern [Interview 10 & 11]. Im Bereich der netzdienlichen Sektorenkopplung und der Einbindung von dezentralen Energieerzeugern und -verbrauchern können innovative Mechanismen wie *Gamification*[117] ein gewinnbringendes Steuerungselement für den Netzbetrieb sein. Technisch ließen sich solche Modelle beispielsweise über *Micro-Payments* basierend auf Blockchains und Kryptowährungen wie Stablecoins realisieren [Interview 10] (vgl. Kapitel 0). Ein Euro-Stablecoin[118] könnte dabei eine Schlüsselrolle spielen, indem er rechtssichere und grenzüberschreitende Transaktionen (z. B. für kurzfristige Flexibilitätsleistungen) vereinfacht. Im Kontext der zunehmenden Automatisierung des Netzbetriebs und damit auch der automatisierten Abwicklung von Transaktionen könnten Stablecoins eine verlässliche Grundlage für die automatisierte Abwicklung von Zahlungen zwischen (KI-basierten) Agenten schaffen.

Chancen und Potenziale für die Umsetzung dezentraler Governance-Mechanismen

Mit dem Wandel hin zu einem stärker dezentralen Energiesystem wächst der Bedarf nach vertrauenswürdigen Governance-Strukturen, die über einzelne Marktakteure hinausgehen und eine gemeinsame Basis für die Interaktion aller Beteiligten schaffen – also insbesondere die *Teilhabe neuer Akteure im Energiesystem*. Der Einsatz von Web3-Technologien könnte dabei ein Instrument sein, um die Partizipation und Selbstbestimmung von Nutzerinnen und Nutzern in energiewirtschaftlichen Prozessen voranzubringen (z. B. im Hinblick auf Datensouveränität und aktiven Konsens) [Interview 11] (vgl. Kapitel 5.3). Eigenschaften wie Datensouveränität sind in dezentralen, auf Web3 basierenden Strukturen transparenter realisierbar.

[116] Ein Agent ist eine autonome Einheit (meist in einem Multi-Agenten-System), die basierend auf vordefinierten Algorithmen eigenständig Entscheidungen trifft und Aufgaben löst. Meist basieren Agenten auf lernenden Algorithmen, die durch die Interaktion mit anderen Agenten oder der Umgebung Daten sammeln und anwenden, um die ihnen zugewiesenen Aufgaben zu erfüllen. Weitere Informationen zu Agenten und Multi-Agenten-Systemen finden Sie unter anderem bei Dorri et al. (2018).
[117] Gamification bezeichnet spielerische Elemente (z. B. ein Punkte- oder Belohnungssystem), mit dem das Verhalten von Nutzerinnen und Nutzern beeinflusst werden kann.
[118] Ein Euro-Stablecoin ist eine Kryptwährung, deren Wert an den des Euro gekoppelt ist.

Bestehende Marktrollen wie Netzbetreiber könnten auch in einem stärker dezentral organisierten Energiesystem die wichtige Funktion einer glaubwürdigen Instanz einnehmen: Sie könnten in Zukunft die Echtheit digitaler Identitäten sowie die tatsächliche Existenz und Leistungsfähigkeit von Erzeugungsanlagen bestätigen – etwa durch das Ausstellen digitaler Zertifikate oder die Eintragung von Attributen in dezentrale Register [Interview 8]. Web3-Technologien können damit erheblich dezentrale Governance-Strukturen unterstützen bzw. realisieren, sind aber nicht auf diese angewiesen. In einer zunehmend dezentralen Energiewirtschaft, die (noch) auf sehr zentralisiert organisierten Prozessen beruht, können Web3-Technologien bereits eingesetzt werden und eine schrittweise Transformation hin zu neuen, dezentralen Governance-Strukturen begleiten. Langfristig eröffnet dezentrale Governance, die durch entsprechende Technologien im Energiesystem verankert ist, neue Möglichkeiten, Kontrolle und Nutzen gleichberechtigt zwischen den Marktrollen bzw. zwischen den Verbrauchern, Prosumern und Infrastrukturbetreibern zu verteilen.

4.2 Weaknesses & Threats

4.2.1 Schwächen von Web3-Technologien im Energiesektor

Obwohl Web3-Technologien das Potenzial haben, verschiedene Anwendungsfälle im Energiesektor zu ermöglichen und somit die Transformation zu einem dezentralisierten Energiesystem zu fördern, weisen sie Vulnerabilitäten und Schwächen auf, die ihre Einführung verhindern bzw. verzögern können. *Regulatorische Hürden* und *langsam fortschreitende Digitalisierung* sind laut mehreren interviewten Expertinnen und Experten die zentralen Herausforderungen im Energiesektor und für eine erfolgreiche Energiewende. Trotz des Potenzials von Web3-Technologien (vgl. Kapitel 4.1) nehmen weder die Technologien selbst noch die strategischen Ziele hinter Web3-Technologien (z. B. Datensouveränität) in der aktuellen Debatte um das Energiesystem eine große Rolle ein [Interview 9]. Als Gründe für die teilweise geringe Auseinandersetzung mit Web3-Technologien sehen mehrere Interviewte die *Komplexität der Technologie* sowie die *mangelnde Skalierbarkeit*. In der nachfolgenden Übersicht werden die technischen Hürden hervorgehoben, die die breite Umsetzung von Web3-Technologien im Energiesektor derzeit behindern.

Schwächen von dezentralen Netzwerken (insbesondere DLTs)

Trotz der fortschreitenden Entwicklung von dezentralen Architekturen, insbesondere Blockchain, zeigen sich in der Praxis weiterhin Schwächen. Ein wesentliches Problem ist die *technologische Komplexität*. Dadurch sind die Implementierung und Einrichtung Blockchain-basierter Lösungen aufwendig und die Wartung ist meist kostenintensiv (Choobineh et al., 2023) [Interview 2]. Trotz Layer-1- und Layer-2-Skalierungslösungen (vgl. Kapitel 0) bestehen zudem grundlegende Limitationen bei der Performanz (z. B. bei der Transaktionsgeschwindigkeit). Diese Limitationen schränken die Anwendbarkeit von Blockchains insbesondere in den Bereichen ein, in denen eine schnelle Datenverarbeitung gefordert ist [Interview 2 & 11]. Daher werden in der Praxis heutzutage in potenziellen Anwendungsbereichen von Blockchains bereits bewährte technische Lösungen (z. B. Event-Processing-Systeme) bevorzugt [Interview 4 & 11]. Auch die hohe Rechenintensität bzw. der relativ hohe Energieverbrauch einiger Blockchains (vgl. Kapitel 0) führt dazu, dass Blockchain-basierte Lösungen bei Verantwortlichen in der Energiewirtschaft Bedenken auslösen [Interview 2 & 4]. Des Weiteren lassen sich nicht in allen Pilotprojekten die von Blockchains versprochenen Vorteile (z. B. im Hinblick auf Dezentralisierung) realisieren. Insbesondere wenn die darüberliegenden Prozesse weiterhin zentralisiert organisiert bleiben, ergibt sich für eine Blockchain-basierte Lösung kein tragfähiges Wertschöpfungsmodell. Die Kosten für eine dezentrale Lösung, die in einem zentralisierten System betrieben wird,

können im Vergleich zu bestehenden Lösungen daher deutlich höher sein und zudem eine faire Kostenverteilung erschweren [Interview 11]. Auch datenschutzrechtlich bringen Blockchains Einschränkungen mit sich (vgl. Kapitel 5.1), weshalb in pilotierten Blockchain-Lösungen mit Offchain-Verweisen gearbeitet wird. Dies kann jedoch neue Angriffsflächen schaffen (z. B. durch mögliche Sicherheitslücken bei den ausgelagerten Daten) [Interview 10].

Schwächen von digitalen Identitäten / SSI

Dezentrale digitale Identitäten bilden die infrastrukturelle Grundlage für weitere Web3-Anwendungen und die digitale Transformation in der Energiewirtschaft im Allgemeinen. Insbesondere SSI-basierte digitale Identitäten können einen Beitrag leisten, indem sie eine vertrauenswürdige Quelle für Identitätsinformationen (d. h. eine sogenannte *Single Source of Truth*) ermöglichen. Die Entwicklung dieser infrastrukturellen Grundlage wird insbesondere im Hinblick auf die *zunehmende Maschine-zu-Maschine-Kommunikation* (z. B. in Form von automatisierten Finanztransaktionen) als zeitkritisch beurteilt. Ohne ein sicheres Identitätsmanagement lassen sich diese Entwicklungen nicht zuverlässig und vertrauenswürdig gestalten [Interview 6 & 10]. Trotzdem fehlt es in der Entwicklung digitaler Identitätslösungen derzeit noch an der wirtschaftlichen Tragfähigkeit der dahinterliegenden Geschäftsmodelle. Das liegt daran, dass digitale Identitäten häufig als *öffentliche Infrastruktur* verstanden werden (z. B. verglichen mit einem physischen (Personal-)Ausweis), weshalb sie dementsprechend meist im öffentlichen Bereich verankert werden. Solange jedoch auf regulatorischer Ebene die Nutzung dezentraler digitaler Identitäten nicht verpflichtend ist, fehlt für Unternehmen ein tragfähiger Markt, um entsprechende Lösungen bereitzustellen [Interview 10]. Der Aufbau eines interoperablen Systems, das alle drei Identitätsebenen (d. h. Identifikation von Personen, Organisationen und Maschinen) abbildet, ist notwendig, aber auch technisch anspruchsvoll und bisher nur unzureichend vorangetrieben worden (Leinauer et al., 2024) [Interview 10].

Mit eIDAS 2.0 und der EUDI-Wallet gibt es zwar auf europäischer Ebene die Rahmenbedingungen, um für Personen und Organisationen erste Lösungen für ein umfassendes dezentrales digitales Identitätsmanagement zu entwickeln. Eine deutsche EUDI-Wallet für Personen wird aber vermutlich erst 2027 zur Verfügung stehen und ist daher insbesondere im energiewirtschaftlichen Alltag noch wenig sichtbar (Bundesministerium für Digitales und Staatsmodernisierung, 2025b). Eine *Beschleunigung des Aufbaus einer europäischen Identitätsinfrastruktur*, insbesondere in Bezug auf die Identifikation von Organisationen und Maschinen, durch staatliche Institutionen ist daher notwendig, um die Grundlage für vertrauenswürdige Dienstleistungen (Trusted Services) auch im Energiesektor zu schaffen [Interview 10]. Wenn die Verantwortlichkeit für die Weiterentwicklung und Bereitstellung der Identitätsinfrastruktur in öffentlicher Hand liegt, besteht neben der Gefahr einer zu langsamen Entwicklung die Möglichkeit, dass sich kein wettbewerblicher Markt entwickelt. Das wäre dann der Fall, wenn nur wenige große Akteure mit der Umsetzung beauftragt werden würden [Interview 10]. Um für Unternehmen in der Energiewirtschaft in Bezug auf die Nutzung von digitalen Identitäten Planungssicherheit zu schaffen, wären daher eine klare Verantwortungsstruktur und ein Umsetzungsplan mit verbindlichen Zeitangaben notwendig [Interview 10].

Schwächen von Datenräumen

In Bezug auf Datenräume betonen mehrere interviewte Expertinnen und Experten, dass der *Reifegrad der Datenraumtechnologien*, der *unklare volkswirtschaftliche Mehrwert* im Vergleich zu bestehenden Lösungen sowie *Missverständnisse über den Begriff* die Einführung verhindern bzw. verlangsamen [Interview 1 & 2]. Eine Einführung von Datenräumen ist oft nur dann gut begründbar, wenn der erwartete Mehrwert präzise quantifiziert werden kann. Allerdings sind Datenräume derzeit noch nicht ausreichend validiert, um in operativen

Umgebungen eingesetzt zu werden. Ihr Mehrwert lässt sich jedoch erst überprüfen, wenn eine kritische Masse an Nutzerinnen und Nutzern erreicht ist, was wiederum eine breite Akzeptanz voraussetzt [Interview 1]. Weiterbildung sowie Awareness-Ansätze für Nutzerinnen und Nutzer sind daher notwendig, um die Akzeptanz von Datenräumen in der Gesellschaft zu fördern [Interview 2].

Ohne eine klare Governance für die *Interoperabilität* von Datenraumlösungen besteht zudem das Risiko, dass die Einführung von Datenräumen zu neuen Datensilos führen kann [Interview 1]. *Proprietäre Protokolle* könnten dabei beispielsweise die Integration von unterschiedlichen Datenraumlösungen behindern [Interview 2]. Auch die fehlende Interoperabilität zwischen verschiedenen Versionen der gleichen Komponenten stellt eine Herausforderung für die Umsetzung von Datenräumen dar. Darüber hinaus ist Interoperabilität zwischen verschiedenen Implementierungen von Datenraumkonnektoren (vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) eine Herausforderung, die die Entwicklung von Datenökosystemen bislang verhindert [Interview 2]. *Regulatorische Unsicherheiten* und *fehlende Standardisierung* stellen ebenfalls ein beträchtliches Hindernis für die Akzeptanz und Einführung von Datenräumen dar [Interview 1 & 5]. Es sind klare Rahmenbedingungen erforderlich, die beispielsweise in Bezug auf die Regulierung von Anreizen für große Akteure zur Weitergabe von Daten, monetäre Anreize für kleine Verbraucher sowie die Governance von Datenräumen definiert werden müssen [Interview 2]. Ungeklärte Fragen zu *Finanzierung* und *Zuständigkeiten* für den Betrieb einer Datenrauminfrastruktur – sowohl im staatlichen als auch im privaten Sektor – können den Aufbau dieser Infrastruktur ebenfalls verzögern [Interview 3]. Auch in der Literatur wird diese Thematik diskutiert und es werden unterschiedliche Vorschläge hinsichtlich möglicher Geschäftsmodelle für den Infrastrukturbetrieb präsentiert (d'Hauwers et al., 2022; van Houwelingen et al., 2024). Diese Modellvorschläge müssen jedoch je nach Industriezweig adaptiert werden. Abschließend sind Energiedatenräume im außereuropäischen Kontext derzeit kein relevantes Thema, weshalb die technische Entwicklung und Innovation im Vergleich zu global entwickelten Technologien langsamer ist [Interview 2].

4.2.2 Risiken und Hürden für Anwendungsfälle von Web3-Technologien im Energiesektor

Risiken und Hürden für den Redispatch 3.0

Für die in Kapitel 3 vorgestellten Anwendungsfälle bestehen Risiken und Hürden für den Einsatz von Web3-Technologien. Mehrere interviewte Expertinnen und Experten betonen beispielsweise, dass für den Redispatch 3.0 die *fehlenden offenen Standards* sowie *regulatorische Rahmenbedingungen* ein Hindernis für die Umsetzung von Web3-Lösungen darstellen [Interview 3, 5 & 6]. Fehlende offene Standards führen meist zu Lock-in-Effekten und verhindern kurzfristige Flexibilitätsbereitstellungen sowie tatsächliche Marktrollenwechsel, da Interoperabilität nicht gewährleistet wird [Interview 3]. Gaming-Risiken[119] auf dezentralen Flexibilitätsmärkten gefährden dazu regulatorische Fortschritte, die die Einführung von Web3-Technologien vorantreiben könnten [Interview 5]. Da der Redispatch 3.0 noch nicht eingeführt ist, herrscht eine hohe Unsicherheit darüber, wie die operative Umsetzung aussehen könnte [Interview 6]. Fehlende regulatorische Rahmenbedingungen für den potenziellen Einsatz von Web3-Technologien für Redispatch 3.0 können deshalb die flächendeckende Nutzung von Energieflexibilitäten aus dezentralen Kleinstanlagen im Markt verhindern. Die *Skalierbarkeit* von bestehenden Piloten ist daher oft (noch) nicht gegeben, weil der regulatorische Rahmen nicht ausreicht, um daraus operative Anwendungen rechtssicher abzuleiten. Es besteht zudem

[119] Eine Analyse der Gaming-Risiken auf Flexibilitätsmärkten im Energiesystem finden Sie unter anderem bei Buchholz et al. (2021).

Unsicherheit, wann regulatorische Vorgaben definiert werden, was wiederum die Planung und Investitionen in Web3-basierte Redispatch-3.0-Lösungen erschwert [Interview 5].

Risiken und Hürden für HKN-Systeme und Auflösen von Farbkategorien

Wie in Kapitel 3 und Kapitel 4.1.2 angeführt, gewinnt die Frage nach effizienten und gleichzeitig vertrauenswürdigen Lösungen für HKNs sowie für die Nachweisführung von CO_2-Emissionen und weiteren Nachhaltigkeitseigenschaften zunehmend an Bedeutung. Blockchain-basierte Lösungen in Kombination mit ZKPs könnten interessant sein, um eine *verteilte Verantwortlichkeit für die Datenverwaltung* zu erreichen und zu vermeiden, dass eine zentrale Drittpartei Betriebsgeheimnisse einsehen könnte [Interview 7].[120] Trotzdem zeigt sich in der Energiewirtschaft bisher, dass Lösungen, die auf enge Kollaboration und API-Schnittstellen setzen, häufig effizienter und einfacher umzusetzen sind als eine *komplexe Blockchain-Anwendung* [Interview 7]. Zudem sind die Skalierbarkeit und Performanz von Blockchains für großflächige Anwendungen, die beispielsweise eine Viertelstundenauflösung für den Gesamtenergiemarkt integrieren, noch nicht ausreichend genug bzw. verlangen ein ausgeklügeltes Design von Onchain- und Offchain-Prozessen [Interview 8]. Zusätzlich verhindern regulatorische Unsicherheiten (auch hier insbesondere in Bezug auf Datenschutzbestimmungen) eine breite Einführung (vgl. Kapitel 5.1). Daher wird Blockchain in der Praxis noch nicht für die Verbesserung der bestehenden HKN-Prozesse bzw. zur Verifizierung von Grünstrom eingesetzt. Die Überprüfbarkeit von HKNs und ähnlichen Nachweisen kann jedoch auch ohne Blockchain digital realisiert werden [Interview 7]. Hierfür spielen insbesondere digitale Identitäten eine Rolle (vgl. Kapitel 4.1.2). Für dezentrale digitale Identitäten und andere Web3-Technologien besteht jedoch eine wesentliche Herausforderung in der Transformation der bestehenden Prozesse: Die Transformation von einem etablierten und langjährig bestehenden System wie dem HKN-Register verlangt eine *langfristige Kompatibilität* zwischen dem alten und dem neuen System und/oder eine für die involvierten Stakeholder risikoarme Weiterentwicklung [Interview 8].

Risiken und Hürden für die Registersynchronisation und -interoperabilität

Die Transformation vom bestehenden System hin zu einem neuen System, das Web3-Technologien gewinnbringend integriert, gestaltet sich insbesondere bei den Registern in der Energiewirtschaft als ein komplexer Prozess. Eine Übergangsphase zwischen Systemen muss sorgfältig ausgestaltet und geplant werden, da auftretende Fehler (z. B. im Übertrag zwischen einem bestehenden und einem neuen, dezentralen Register) die Glaubwürdigkeit des neuen Systems gefährden könnte [Interview 3]. Nicht nur der *Transformationsprozess* selbst kann ein Hindernis für die Einführung neuer, digitaler Register in der Energiewirtschaft darstellen. Da die bestehenden Register im Energiesektor ein zentrales Element der Infrastruktur sind, kann es zu einem sogenannten *Henne-Ei*-Problem zwischen *Infrastrukturentwicklung* und Nutzung der Infrastruktur kommen [Interview 3]. Regulatorische Unsicherheiten im Umgang mit Web3-Technologien können die Transformation hin zu neuen Registeransätzen zusätzlich verzögern. Dazu gehören zentrale Governance-Fragestellungen, zum Beispiel: „Wer fungiert in einer dezentralen Architektur als Systemverantwortlicher?“ [Interview 8]. Zudem müssen die regulatorischen Rahmenbedingungen so angepasst werden, dass ein weiterentwickeltes oder neues Register in bestehende Energiemarktprozesse eingebunden werden kann. Daher bedarf es sowohl auf regulatorischer als auch auf technischer und organisatorischer Ebene umfassender und integrierter Konzepte, die die Interoperabilität und Compliance der unterschiedlichen Prozesse und Register gewährleisten. Dies erhöht wiederum die Komplexität der Implementierung neuer Register [Interview 3 & 8].

[120] Blockchain-basierte Lösungen für HKNs könnten ähnliche Systeme wie bei Z-Cash aufsetzen. Z-Cash ist eine Kryptowährung, mit der durch ZKPs Transaktionen vollständig anonym (d. h. ohne Angabe von Sender, Empfänger und Betrag) abgewickelt werden können.

Risiken und Hürden für effizienteren Netzbetrieb und Sektorenkopplung

Für einen effizienteren Netzbetrieb und die Gewährleistung der Netzstabilität sind Echtzeit-Austausch und -Analyse einer großen Menge an Daten notwendig. Die Erzeugung sicherer und zuverlässiger Messdaten erfordert wiederum eine *flächendeckende Integration von Smart Metern*. Web3-Technologien bieten primär keine Lösung für diesen Mangel an Datenverfügbarkeit [Interview 11]. Auch im Falle der Datenverfügbarkeit bleiben Unsicherheiten bezüglich der Einbeziehung von Verbrauchsdaten im Hinblick auf die Datenschutz-Grundverordnung (DSGVO) [Interview 11]. Aktuelle Herausforderungen für den Netzbetrieb, insbesondere die Kommunikation zwischen verschiedenen Akteuren[121], erfordern daher eher juristische und regulatorische Lösungen, die von Web3-Technologien nicht unmittelbar bereitgestellt werden können (Vionis & Kotsilieris, 2024) [Interview 9]. Zudem existieren für Web3-basierte Prozesse im Netzbetrieb vor allem Pilotprojekte, bei denen die Anwendung von Web3-Technologien nur dann sinnvoll ist, wenn eine Vielzahl von EVUs beteiligt ist. Dies liegt daran, dass sich die Investitionen in die dezentrale Infrastruktur meist nur bei einer Vielzahl von realisierten Anwendungsfällen rechnen [Interview 10].

Risiken und Hürden für die Umsetzung dezentraler Governance-Mechanismen

Trotz des Potenzials von Web3-Technologien und der gezielten Dezentralisierung von Marktprozessen im Energiesektor ist die Einführung einer dezentralen Governance-Struktur mit großen Herausforderungen verbunden. Das liegt zum einen daran, dass die bestehenden Strukturen und Prozesse in der Energiewirtschaft stark zentralisiert sind. Zum anderen ist der Wandel hin zu einer dezentralen Governance sowohl auf regulatorischer und organisationaler als auch auf kultureller Ebene schwierig und langwierig.

Die *historisch gewachsenen, stark zentralisierten Strukturen der Energiewirtschaft*, die auch in die technische Infrastruktur, die regulatorischen Rahmenbedingungen und die organisatorischen Abläufe eingebettet sind, erschweren den Einsatz von dezentralen Technologien erheblich. Ein Beispiel hierfür sind etablierte, zentralisierte Datenaustauschstrukturen [Interview 11]. Ein weiteres Beispiel ist der Peer-to-Peer-Stromhandel. Die Anwendung von Web3-Technologien könnte eine direkte, bilaterale und automatisierte Abwicklung von Transaktionen ermöglichen. Für die Überwachung der Netzrestriktionen ist jedoch weiterhin eine zentrale Instanz, in der Regel der Netzbetreiber, erforderlich. Dies steht im Widerspruch zum Ziel, dass bei einem Peer-to-Peer-Handel einzelne Akteure dezentral und unabhängig von einem zentralen Intermediär Strom ein- und verkaufen können [Interview 7]. Wenn dezentrale Technologien in einem System mit zentralen, eingreifenden Akteuren eingesetzt werden, wird der wirtschaftliche Nutzen dieser dezentralen Ansätze meist erheblich geschmälert [Interview 7 & 11]. Da in der deutschen Energiewirtschaft bereits vertrauenswürdige zentrale Akteure (z. B. Netzbetreiber) etabliert sind, scheinen Web3-basierte Lösungen für einige Anwendungsfälle auf den ersten Blick keinen klaren Mehrwert zu bieten [Interview 9]. Gleichzeitig zeigen Beispiele wie das Marktstammdatenregister, dass zentrale Systeme fehleranfällig sein können und ein Vertrauen in zentrale Akteure zu sogenannten Single Points of Failure führen kann.

Um in einem dezentralisierten Energiesystem die Potenziale dezentraler Technologien realisieren zu können, ist ein aufwendiger Wandel auf regulatorischer und organisationaler Ebene notwendig – das zeigt die Erfahrung aus gescheiterten Projekten [Interview 11]. Folglich müssen Marktstrukturen, regulatorische Rahmenbedingungen und Governance-Mechanismen umfassend angepasst werden, beispielsweise in Bezug auf

[121] Die Marktkommunikation im heutigen Energiesystem ist so gestaltet, dass jeder Akteur bilateral mit den relevanten Marktpartnern Informationen austauscht, was zu einer hohen Komplexität führt. In einem Web3-basierten Marktsystem muss daher zunächst eine Einigung über die Governance-Fragen erzielt werden, um diese Komplexität zu bewältigen.

Netzregulierung, Entgeltstrukturen und Marktsteuerung [Interview 11]. Solche, zum Teil tiefgreifenden Veränderungen der bestehenden Marktstrukturen hin zu einem höheren Grad der Dezentralisierung werden in der Regel nicht allein aus der Energiebranche heraus initiiert. Sie benötigen vielmehr einen größeren regulatorischen Impuls (z. B. auf europäischer Ebene durch die EU-Kommission) und eine *langfristige politische Zielsetzung* [Interview 10 & 11]. Das liegt vor allem daran, dass der Energiesektor als Teil der Kritischen Infrastruktur *sehr stark reguliert* ist.

Die Transformation hin zu einer stärkeren Dezentralisierung auf regulatorischer und organisationaler Ebene wird zudem oft durch eine *unklare Kostenverteilung* erschwert. Wenn die Kosten für die notwendigen Veränderungen und die Entwicklung einer dezentralen Architektur nicht eindeutig zugewiesen werden können, kann dies zu einem Missverhältnis zwischen dem Aufwand für die Transformation und dem Nutzen bei einzelnen Anwendungsfällen führen [Interview 11]. Neben den Kostenfragen bringen dezentrale Governance-Mechanismen auch neue *Sicherheitsfragen* mit sich. So stellt sich die Frage, wer für die Regulierung und Adressierung neuer Risiken zuständig ist und wie damit in unterschiedlichen Jurisdiktionen umgegangen werden kann [Interview 4]. Dabei muss auch berücksichtigt werden, dass durch neue Governance-Mechanismen in dezentralen Systemen ebenso Abhängigkeiten entstehen können. Diese Abhängigkeiten beziehen sich dann nicht auf zentrale Akteure, sondern beispielsweise auf Wissensmonopole oder mächtige Konsortien [Interview 8].

Der Wandel hin zu dezentralen Governance-Mechanismen in der Energiewirtschaft erfordert auch einen tiefgreifenden Mentalitäts- und Kulturwandel. Dies bedeutet vor allem eine grundlegende Änderung der Denkweise, da die bisher vorherrschenden zentral organisierten Strukturen in Frage gestellt werden müssen [Interview 10]. Der *Paradigmenwechsel* von zentraler zu dezentraler Organisation steht dabei häufig im Widerspruch zu den etablierten regulatorischen und organisatorischen Rahmenbedingungen, die eine entsprechende Weiterentwicklung der bestehenden Governance-Struktur erschweren [Interview 11]. Zudem ist der Paradigmenwechsel – bzw. die dahinterliegenden Vorteile – schwer zu erklären und kann insbesondere bei Akteuren im Energiesystem Zweifel hervorrufen, wenn sie mögliche Veränderungen oder Beeinträchtigungen in ihren Prozessen befürchten [Interview 4]. Viele dieser Akteure sehen daher keinen dringenden Handlungsbedarf, da das zentralisierte System bisher (z. B. in Bezug auf die Versorgungssicherheit) funktioniert. Vor diesem Hintergrund stellt sich die Frage, wer den notwendigen umfassenden Wandel vorantreiben soll und kann [Interview 11]. Vielversprechend sind dabei insbesondere Anwendungsfälle, die an der Schnittstelle zu weniger regulierten Sektoren wie dem Mobilitätssektor entstehen [Interview 11]. Dort könnten der erleichterte Zugang und eine damit verbundene Einführung von Web3-Technologien über die Sektorenkopplung durch E-Fahrzeuge perspektivisch auch zu Veränderungen im Energiesektor führen. Weiterhin könnte die Entwicklung dezentraler digitaler Identitäten für elektronische Assets in anderen Sektoren ein Treiber für die Entwicklung einer stärker dezentralen Governance im Energiesektor bilden.

4.3 Weitere Hürden für die Einführung von Web3-Technologien im Energiesektor

Problematik des fehlenden Wertversprechens

Die Integration von Web3-Technologien steht vor mehreren Herausforderungen, die über rein technologische Risiken für die vorgestellten Anwendungsfälle hinausgehen. Neben Standardisierungs- und regulatorischen Fragen ist auch oftmals das *Wertversprechen* hinter einer Web3-Lösung noch fraglich [Interview 7]. Beispielsweise können die *zunehmende Komplexität* und *mangelnde Praktikabilität* von Web3-Lösungen dazu führen,

dass Projekte in der Praxis scheitern oder nicht skalieren. Der unklare Mehrwert von Web3-basierten Lösungen in der Praxis erschwert oft die Rechtfertigung der zusätzlichen Komplexität, die diese Lösungen insbesondere in der Entwicklung mit sich bringen [Interview 7 & 8]. Aktuell existieren daher oft noch keine produktionsreifen, großflächigen Implementierungen von Web3-basierten Lösungen – viele Initiativen befinden sich lediglich auf Prototyp- oder Whitepaper-Ebene. Für die Umsetzung von Web3-basierten Lösungen sind zudem oft *Retrofitting* und ein Software-Rollout bis zum Endgerät erforderlich, beispielsweise bei Wärmepumpen oder Steuerboxen (Critchley, 2024). Dies kann sich in der Praxis als schwierig darstellen, da verschiedene Versionen von potenziellen Lösungen und Umrüstkosten die breite Einführung hemmen und die mit einer Technologieumstellung verbundenen Risiken erhöhen (Jibril & Roper, 2025) [Interview 3 & 8]. Beispielsweise zeigt die Pilotierung einer Web3-basierten Lösung für Crowdbalancing[122], dass trotz schnell voranschreitender technischer Entwicklung die Skalierbarkeit noch unzureichend für die praktische Umsetzung ist [Interview 8].

Problematik der fehlenden Entwicklung der öffentlichen Infrastruktur

Die Implementierung von Web3-basierten Lösungen im Energiesektor ist eng mit der Digitalisierung der zugrunde liegenden Netzinfrastruktur verbunden. In diesem Kontext ist die *Realisierung des Rollouts von Smart Metern* eine grundlegende Voraussetzung, um den Betrieb und die Verwaltung eines Netzes mit einer großen Anzahl verteilter Anlagen zu ermöglichen. Eine Vielzahl von Anwendungsfällen von Web3-basierten Lösungen (z. B. im Lastmanagement, für die Marktintegration von Kleinstflexibilitäten oder die Realisierung dynamischer Tarife) erfordert eine Echtzeit-Datenerfassung im 15-Minuten-Takt, um die Netzstabilität trotz der volatilen Erzeugung im Netz zu gewährleisten. Jedoch schreitet der Smart Meter Rollout in Deutschland nicht schnell genug voran [Interview 9]. Für flexiblere Marktmodelle sind zudem eine *flächendeckende Sensorik und Datenverfügbarkeit* erforderlich, die insbesondere bei kleinen Netzbetreibern oft noch nicht gegeben ist (Mataczyńska et al., 2022) [Interview 8]. Darüber hinaus müssen mit dem Einsatz von Smart Metern und anderen internetfähigen Endgeräten potenzielle Sicherheitslücken in der Kritischen Infrastruktur berücksichtigt werden. Dabei können an unterschiedlichen Stellen in der digitalen Kette erhebliche Angriffsflächen entstehen, die durch Web3-basierte Anwendungen nicht adressiert werden können [Interview 10]. Daher sollten zukünftige Infrastrukturentscheidungen Sicherheitsmaßnahmen nach dem Prinzip „Eine Kette ist nur so stark wie ihr schwächstes Glied“ realisieren. Eine zu strikte Regulierung kann jedoch die Innovation und Einführung von neuen Technologien hemmen (vgl. Kapitel 0) [Interview 8].

Problematik der fehlenden Fachkräfte

Eine bedeutende Hürde für die Einführung von Web3-Technologien im Energiesektor stellt auch der Fachkräftemangel dar. Es gibt nicht genügend qualifiziertes Personal im Bereich IT und Digitalisierung[123], was insbesondere durch parallel aufkommende Trends wie KI, für die ebenfalls Entwicklungspersonal benötigt wird, verstärkt wird [Interview 10]. Zudem fehlt es an Fachkräften mit fundiertem Wissen in den spezifischen Web3-Technologien [Interview 7] sowie an der Schnittstelle zwischen Energiewirtschaft und Web3-Technologien [Interview 6]. Darüber hinaus unterschätzen einige Akteure in der Energiewirtschaft die Komplexität der Technologien [Interview 7].

[122] Crowdbalancing bezeichnet ein Konzept, wodurch Anlagen mit Kleinstflexibilitäten über Aggregatoren gebündelt werden und so direkt am Regelenergiemarkt teilnehmen können.
[123] Eine Bitkom-Umfrage aus dem Jahr 2025 zeigt, dass in Deutschland 109.000 IT-Fachkräfte fehlen (Bitkom e. V., 2025).

Problematik der fehlenden Akzeptanz und Benutzerfreundlichkeit

In Bezug auf Web3-Technologien bestehen erhebliche *Mindset- und Vertrauensprobleme im Markt* und in der Gesellschaft[124]: Begriffe wie „Blockchain“ sind teils im energiewirtschaftlichen Kontext „verpönt“ [Interview 3]. Zudem hat der Begriff „Web3“ keine klare und abgegrenzte Definition (vgl. Kapitel 2) und fungiert daher als Sammelbegriff, der eine Vielzahl an Interpretationen zulässt. Das erschwert die Diskussion über sowie das Verständnis und die Akzeptanz von Web3-Technologien [Interview 9]. Eine Erhebung[125] zeigt beispielsweise, dass häufig noch unklar ist, wo der Unterschied zwischen SSI-basierten und bereits existierenden digitalen Zertifikaten liegt [Interview 9]. Befürworter von Web3 erwarten einen Mentalitätswechsel, der die Dezentralisierung im gesamten Internet und in der Gesellschaft vorantreibt, und fördern deshalb eine frühzeitige Auseinandersetzung mit den entsprechenden Technologien. Nur so lässt sich ihr Mehrwert in konkreten Anwendungsfällen klar aufzeigen [Interview 11].

Ein weiterer kritischer Punkt ist die *mangelnde Benutzerfreundlichkeit* der Web3-Technologien, die jedoch entscheidend für den zukünftigen Einsatz der Technologien ist [Interview 10]. Insbesondere bei der Nutzung von Blockchains ist die Benutzerfreundlichkeit noch nicht hoch, beispielsweise im Management der notwendigen Schlüssel bzw. Zugänge (Khayretdinova et al., 2022). Daher ist es notwendig, Benutzerfreundlichkeit bei der Entwicklung von Web3-basierten Anwendungen sowohl im B2C- als auch im B2B-Kontext zu adressieren. Auch die Benutzerfreundlichkeit bestehender Lösungen sowie die etablierten Gewohnheiten von Nutzerinnen und Nutzern (z. B. bei Identitätslösungen) können die Akzeptanz von Web3-Technologien beeinträchtigen [Interview 9]. Schließlich muss der Transformationsprozess hin zur Nutzung von Web3-basierten Anwendungen im Energiesektor den gesellschaftlichen Wandel widerspiegeln und entsprechend begleitet werden, indem das Bewusstsein für Web3-Technologien und für das Potenzial von dezentralen Lösungen gefördert wird [Interview 8].

[124] Eine Umfrage aus 2024 zeigt, dass es weiterhin Missverständnisse bezüglich der Definitionen von Blockchain und Web3 gibt (Consensys, 2024).
[125] Eine Erläuterung der verschiedenen Missverständnisse, insbesondere im Zusammenhang mit der Blockchain-Technologie und ihrer Anwendung im Energiesystem, finden Sie unter anderem bei Solat (2024).

5 Rechtliche Einordnung

5.1 Datenschutz: Web3-Einsatz im Einklang mit der DSGVO

Der Einsatz von Web3-Technologien wirft datenschutzrechtliche Fragen auf, insbesondere dann, wenn sie auf Basis von DLTs, wie beispielsweise einer Blockchain, betrieben werden. Bei näherer Betrachtung zeigt sich aber, dass bestehende Hürden bei richtiger Implementierung überwunden werden können.

Datenschutzrechtliche Hürden in einer dezentralen Web3-Architektur

In einem dezentralen System ist oft unklar, wer als datenschutzrechtlich Verantwortlicher im Sinne der DSGVO agiert. Gleichzeitig kann die irreversible Speicherung von Daten auf einer Blockchain eine Umsetzung des Rechts auf Löschung praktisch unmöglich machen. Auch andere Betroffenenrechte der DSGVO (Berichtigung, Auskunft, Widerspruch) können mangels Ansprechpartner kaum durchgesetzt werden. Die öffentliche Einsehbarkeit der Daten auf einer Blockchain steht im Spannungsverhältnis zu dem datenschutzrechtlichen Prinzip der Vertraulichkeit. Pseudonyme Adressen bieten nur begrenzten Schutz, da eine Re-Identifizierung nicht immer ausgeschlossen werden kann. Schließlich widerspricht die vollständige, dauerhafte Replikation von Daten auf verschiedenen Knoten dem Gebot der Datenminimierung und Speicherbegrenzung.

Privacy-by-Design als vielversprechender Lösungsansatz

Trotz der benannten Hürden bestehen Ansätze, wie dezentrale Infrastrukturen bzw. DLTs mit datenschutzrechtlichen Vorgaben in Einklang zu bringen sind. Technisch ist dabei vor allem Datensparsamkeit gefragt: Personenbezogene Daten sollten möglichst gar nicht auf einem dezentralen Layer selbst gespeichert, sondern *offchain* verwaltet und nur als Hash oder verschlüsselt *onchain* referenziert werden (vgl. Kapitel 0). Hash-Werte dienen dann als Platzhalter, mit denen sich später die Invarianz der Originaldaten nachweisen lässt, ohne dass die Originaldaten selbst öffentlich sind. In der Studie „DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem – Technische Details und Umsetzung der Basisinfrastruktur“ wird dieser Ansatz bereits aufgegriffen (Deutsche Energie-Agentur, 2025b).

Weiter erlauben es kryptografische Lösungen, Daten durch Verschlüsselung zu schützen und bei Bedarf durch Löschen der Schlüssel faktisch zu entfernen (sogenanntes Crypto-Shredding). Auf diese Weise bleibt die Integrität der DLT-Infrastruktur unangetastet, während die personenbezogenen Daten effektiv entfernt wurden. Dieser Lösungsansatz wird auch vom Europäischen Datenschutzausschuss (EDSA) gesehen und gefordert.

Wenn personenbezogene Daten unbedingt auf der DLT-Infrastruktur selbst gespeichert werden müssen, sollten die Daten so chiffriert werden, dass nur Berechtigte mit dem passenden Schlüssel Zugriff erhalten. Die Verschlüsselung muss dem aktuellen Stand der Technik entsprechen (Art. 32 DSGVO) und sobald möglich müssen die verwendeten Verfahren auch gegen zukünftige Angriffe (z. B. durch Quantencomputer) robust sein.

Auch bei Umsetzung dieser Maßnahmen kann eine Verarbeitung personenbezogener Daten jedoch nicht immer vollständig verhindert werden. So können zum Beispiel über IP-Adressen zumindest kurzzeitig noch Rückschlüsse auf die Anschlussinhaber möglich sein. Die Umsetzung der oben skizzierten Maßnahmen

könnte dann aber die Rechtfertigung der noch notwendigen Verarbeitung stützen. Zumindest dann, wenn Betroffene im vollen Bewusstsein der Folgen freiwillig ihre Daten auf einer DLT-Infrastruktur verarbeiten lassen, könnte in engen Grenzen auch eine Speicherung über die gesamte Lebensdauer einer DLT-Infrastruktur noch gerechtfertigt sein, wenn diese dauerhafte Speicherung gerade Teil des mit der DLT-Infrastruktur verfolgten Zwecks ist. Betroffene könnten dann die verbleibenden minimalen datenschutzrechtlichen Risiken für die Nutzung der Vorteile der neuen Technologie in Kauf nehmen. Als Rechtsgrundlage für diese Datenverarbeitung könnten eine Einwilligung oder die Notwendigkeit der Verarbeitung zur Erfüllung eines Vertrags mit den Betroffenen herangezogen werden.

Governance-Modelle für klare Verantwortlichkeiten

Die oben beschriebenen Maßnahmen müssen in der Praxis umgesetzt werden, wobei ein überzeugendes Governance-Modell für den Betrieb der DLT-Infrastruktur geschaffen werden muss. Private oder konsortiale Lösungen mit Zugriffsbeschränkungen sind gegenüber öffentlichen vorzuziehen. Denkbar ist es, eine gemeinsame Verantwortlichkeit mehrerer Teilnehmer gemäß Art. 26 DSGVO zu vereinbaren. In öffentlichen Web3-Projekten ohne feste Organisation empfiehlt der EDSA, nach Möglichkeit eine juristische Person zu schaffen, die die Infrastruktur betreibt oder koordiniert. Zwar lässt sich damit die dezentrale Philosophie nicht vollständig aufrechterhalten, aber es schafft Rechtssicherheit und Transparenz für die Nutzerinnen und Nutzer sowie für die Aufsichtsbehörden.

Jede Web3-basierte Lösung muss zudem ein robustes Datenschutzmanagement etablieren, das trotz verteilter Struktur die Erfüllung der Pflichten der DSGVO ermöglicht. Nutzerinnen und Nutzer sind transparent zu informieren (z. B. via Datenschutzhinweisen im Whitepaper oder in der App) und gegebenenfalls um Einwilligung zu bitten, bevor ihre Daten in einem unveränderlichen Ledger landen. Intern sollten strenge Policies gelten, die es zum Beispiel untersagen, Klardaten onchain zu schreiben. Durch entsprechende Schulungen sollte sichergestellt werden, dass sich Entwickler dieser Vorgaben bewusst sind. Mit einer Datenschutz-Folgenabschätzung sollten frühzeitig die Risiken analysiert und geeignete Gegenmaßnahmen bestimmet werden.

Ausblick

Für die nahe Zukunft ist nicht zu erwarten, dass der Gesetzgeber datenschutzrechtliche Prinzipien zugunsten von DLTs wesentlich aufweicht. Die Europäische Kommission hat deutlich gemacht, dass sie eine führende Rolle dabei übernehmen will, ein digitales Ökosystem zu schaffen, in dem Datenschutz eine zentrale Rolle spielt. Web3-Technologien, insbesondere DLTs, werden sich daher auch weiterhin an hohen Datenschutzstandards in Europa messen lassen müssen.

Denkbar wäre es aber, über Zertifizierungen, beispielsweise nach Art. 42 DSGVO, Erleichterungen zu schaffen. So könnten Unternehmen ein Gütesiegel für „DSGVO-konforme Web3-Dienste“ erwerben, wenn sie bestimmte Kriterien erfüllen (z. B. nur pseudonyme Daten auf der Chain, implementierte Löschkonzepte etc.). Dies könnte den Markt in Richtung Compliance steuern, ohne direkt Gesetzestexte ändern zu müssen.

Durch Privacy-by-Design, durchdachte Governance und mögliche zukünftige Standardisierung lassen sich faire, rechtskonforme Lösungen finden. Die Konflikte mit der DSGVO beim Einsatz von Web3-Technologien (insbesondere DLTs) sind daher lösbar.

5.2 Energiemarkt-Regulatorik: Flexible Strommärkte treffen auf alte Regeln

Flexible Strommärkte auf Basis von Web3-Technologien haben das Potenzial für eine effizientere und bürgernähere Energieversorgung. Insbesondere Peer-to-Peer-Modelle und dezentraler Flexibilitätshandel könnten Prosumer-getriebene Lösungen ermöglichen. Auch wenn die Regulatorik auf EU-Ebene mit dem „Clean Energy Package“ bereits erste Schritte in diese Richtung gegangen ist, zeigen sich insbesondere in Deutschland noch Hürden, die abgebaut werden müssten, um Web3-basierte Flexibilitätsmärkte vollumfänglich zu fördern.

Klare Regeln zum Energy Sharing for Prosumer

In Deutschland sieht das Energiewirtschaftsgesetz (EnWG) bislang keine Möglichkeit vor, dass Privatpersonen oder Kleinstanlagen über das öffentliche Stromnetz Strom direkt an andere Endkunden liefern. Wer Strom an Dritte liefern möchte, unterliegt derzeit faktisch den vollen Pflichten eines Stromlieferanten, von Anmelde- und Bilanzkreisauflagen bis hin zu Verbraucherschutzbestimmungen.

Mit der im Jahr 2024 beschlossenen Novelle der Elektrizitätsbinnenmarktrichtlinie hat die EU jedoch die rechtliche Grundlage für eine solche Regelung geschaffen. In Deutschland wird ein entsprechender Gesetzesentwurf derzeit im Bundestag diskutiert. Der geplante § 42c EnWG würde es Prosumern erlauben, andere Endkunden zu beliefern, ohne sämtliche Lieferantenpflichten erfüllen zu müssen. Die Umsetzung soll ab dem 1. Juni 2026 zunächst innerhalb des Gebiets eines Verteilnetzbetreibers möglich sein, ab dem 1. Juni 2028 auch in angrenzenden Gebieten.

Diese Gesetzesanpassung ist ein wichtiger Schritt, um Energy Sharing und Peer-to-Peer-Stromhandel rechtssicherer und praktikabler zu gestalten.

Auflockerung starrer Marktrollen

Der bisherige Strommarkt hat starre Marktrollen, die zugunsten eines flexibleren Strommarktes aufgelockert werden könnten. So könnte ermöglicht werden, dass eine Endverbraucherin oder ein Endverbraucher mehrere Stromlieferanten parallel hat (z. B. Grundversorger und Nachbarsolarstrom). Dies erfordert Änderungen in den Bilanzierungsregeln und der IT der Marktkommunikation. Eine zentrale Clearingstelle, wie sie durch eine Internetplattform nach dem Referentenentwurf vom August 2024 in § 20b EnWG-E zwischenzeitlich geplant war, könnte automatisiert Aufteilungsschlüssel umsetzen.

Durch standardisierte Verfahren könnten unabhängige Aggregatoren einfacher agieren. Auf dieser Basis könnten mit Lieferanten die Lastverschiebungen verrechnet werden, ohne jeden Kunden einzeln vertraglich binden zu müssen. Hier sind Feinjustierungen im EnWG und untergelagerten Regelwerken denkbar, um Demand Response und Schwarmsteuerung praxistauglich einzubinden.

Integration digitaler Identitäten und Register

Für einen dezentralen Flexibilitätsmarkt kann es erforderlich sein, die Digitalisierung über den Zähler hinaus zu verlängern. Ein vielsprechender Ansatz ist es, kleine Anlagen und Geräte mit eindeutigen digitalen Identi-

täten auszustatten, die in einem Energie-Identitätsregister erfasst sind. So könnten beispielsweise Netzbetreiber oder Plattformen im Bedarfsfall gezielt ein bestimmtes E-Fahrzeug oder eine bestimmte Wärmepumpe ansteuern und deren Energieflexibilität zertifiziert abrufen (vgl. Kapitel 4.1.2).

Regulatorisch bedarf es dafür einer Öffnung der bestehenden Datensilos. Nutzerinnen und Nutzer der Geräte sollten ihre Gerätedaten kontrolliert freigeben können. Auf EU-Ebene gibt ihnen hierfür der Data Act (Verordnung (EU) 2023/2854) ein rechtliches Mittel an die Hand. Daneben könnte die rechtliche Anerkennung von manipulationssicheren digitalen Nachweisen förderlich sein, um für eingespeiste oder eingesparte Energiemengen innovative Abrechnungssysteme zu ermöglichen. Die eIDAS-Verordnung geht mit der Anerkennung „elektronischer Journale“ bereits in diese Richtung (vgl. Kapitel 0). Förderlich wäre es, wenn die Regulierung zudem – im Einklang mit den Grundsätzen von Datenschutz und IT-Sicherheit – neue Standards für den Energiemarkt schaffen würde, die Vertrauen und Rechtssicherheit für solche Technologien weiter stärken.

Flexibilität durch Experimentierklauseln fördern

Mehr Flexibilität kann auch dadurch geschaffen werden, dass der Raum für Experimente für Netzbetreiber vergrößert wird. Der Gesetzgeber könnte klarstellen, dass Netzbetreiber marktbasierte Lösungen einsetzen dürfen und sollen, bevor sie Anlagen abregeln. Regionale Flex-Plattformen könnten auch regulatorisch unterstützt werden, etwa durch Experimentierklauseln, die es Netzbetreibern erlauben, in definierten Regionen Ausschreibungen für Last- und Einspeiseflexibilität durchzuführen. Der neue § 13k EnWG („Nutzen statt Abregeln“) ist ein erster Ansatz, in diese Richtung zu erproben (z. B. indem überschüssiger Windstrom in Speicher oder Wärmeanlagen vor Ort geleitet wird, statt Windräder abzuschalten). Solche lokalen Nutzungskonzepte ließen sich weiter auszuweiten und nach erfolgreicher Pilotierung in Dauerregelungen überführen.

Ausblick

Der aktuelle Stand der Regulatorik in Deutschland ermöglicht es noch nicht, das Potenzial von Web3-Technologien für die Schaffung von Flexibilitätsmärkten voll auszuschöpfen. Der Gesetzgeber könnte klarere gesetzliche Leitplanken für den Peer-to-Peer-Energiehandel und die Integration von Kleinstanlagen ins Marktdesign sowie neue Anreizmechanismen für netzdienliches Verhalten schaffen. Gelingt diese Gestaltung, könnten die versprochenen Vorteile von Redispatch 3.0 und dezentralem Energy Trading Realität werden. Dies würde im Einklang mit den Zielen des EU-Rechts für ein klimaneutrales und bürgernahes Energiesystems stehen.

5.3 Recht als Innovationstreiber: Web3 als Chance für Compliance

Disruptive Technologien wie Web3-Technologien stellen für die Regulatorik eine besondere Herausforderung dar, da zum Zeitpunkt der Gesetzgebung die neuen technischen Möglichkeiten vom Gesetzgeber oft noch nicht bedacht wurden. Obwohl der europäische Gesetzgeber stets das Ziel einer technologieneutralen Regulierung verfolgt, kann es trotzdem vorkommen, dass Regeln innerhalb weniger Jahre nicht mehr zum Stand der Technik passen. Die daraus entstehenden Hürden fördern die kritische Betrachtung der neuen Technologie.

Im Zuge dessen wird oft auch übersehen, dass Web3-Technologien durchaus Potenzial haben, regulatorische Vorgaben effektiv umzusetzen und neue Marktmodelle rechtssicher zu gestalten. Insbesondere in der neuen

EU-Gesetzgebung zum Datenrecht sind einige Ziele erkennbar, für deren Erreichung der Einsatz von Web3-Lösungen sehr vielversprechend sein kann.

Transparenz und fälschungssichere Dokumentation

Der europäische Gesetzgeber fordert an vielen Stellen Transparenz und Nachvollziehbarkeit. Die DSGVO erhebt dies für personenbezogene Daten sogar zum Grundprinzip. Auch der Data Act (Verordnung (EU) 2023/2854) verankert Transparenzpflichten für Produktdaten von vernetzten Geräten und der Data Governance Act (Verordnung (EU) 2022/868) will für transparenten Datenaustausch Intermediäre schaffen, die neutral und vertrauenswürdig den Datenaustausch im öffentlichen Sektor organisieren sollen. Auch im Energiemarkt selbst ist Transparenz ein zentrales Prinzip. Etwa bei Strom-HKNs oder bei der Abrechnung von dezentral gehandeltem Strom muss Vertrauen in die Richtigkeit der Angaben bestehen.

Web3-Technologien sind für die Herstellung dieser Transparenz ein geeignetes und effizientes Mittel. Sie beinhalten oft ein dauerhaftes, fälschungssicheres Transaktionsprotokoll, das von allen berechtigten Parteien eingesehen und verifiziert werden kann. So lässt sich jederzeit nachvollziehen, wer wann auf welche Daten zugegriffen hat, was neben der Transparenz auch die Erfüllung der damit einhergehenden Rechenschaftspflicht unterstützt.

Die Transparenzvorteile von Web3-Technologien können insbesondere am Energiemarkt ausgespielt werden. Herkunftszertifikate können unveränderlich registriert und Doppelzählungen verhindert werden (vgl. Kapitel 4.1.2). Gerade Energy-Community-Modelle verlangen eine transparente Verteilung von Einnahmen und Kosten. Eine Web3-basierte Plattform könnte automatisiert und für alle Mitglieder nachvollziehbar abrechnen, was manuelle Abrechnungsschritte und potenzielle Fehlerquellen reduzieren könnte. Datenfreigaben oder Handelsgeschäfte können automatisiert protokolliert werden. Nutzerinnen und Nutzer sowie Aufsichtsbehörden können so jederzeit prüfen, wer auf welche Daten zugegriffen hat oder wie viel Energie zwischen zwei Parteien gehandelt wurde.

Datenzugang und Nutzerkontrolle

Eng verwandt mit dem Transparenzgrundsatz ist das Anliegen des europäischen Gesetzgebers, einen umfassenden Anspruch auf Zugang zu Daten für Betroffene bzw. Nutzerinnen und Nutzer zu gewährleisten. Nach der DSGVO haben Betroffene das Recht, jederzeit Auskunft über ihre personenbezogenen Daten zu verlangen. Auch der Data Act schreibt ein Recht für Nutzerinnen und Nutzer auf Zugang zu den Produktdaten und verbundenen Dienstdaten von vernetzten Geräten und verbundenen Diensten vor.

Viele Web3-Lösungen verankern das Prinzip der Datensouveränität und sind damit ein vielversprechender Ansatz zur Erfüllung dieser Anforderungen. In Wallets zur Selbstverwaltung ihrer Identitätsattribute behalten Nutzerinnen und Nutzer die Herrschaft über ihre Daten und Zugriffe (vgl. Kapitel 2.2). Sie könnten ihre Einwilligung zur Datennutzung automatisiert erteilen und widerrufen und Auskünfte könnten automatisiert erteilt werden. Solche Mechanismen könnten die Wahrung der Betroffenenrechte aus der DSGVO technisch einfach umsetzbar machen.

Auch der Gesetzgeber hat das Potenzial einer Vereinfachung durch neue Technologien erkannt. Im seit September 2025 geltenden Data Act wird der automatische Zugang zu Produktdaten sogar als die präferierte

Lösung normiert. Durch Einsatz von Web3-Technologien könnten IoT-Hersteller und Dateninhaber ihre Pflichten (Datenzugang gewähren, Missbrauch verhindern) technisch unterstützen, zum Beispiel indem jeder Datenzugriff onchain geloggt und durch Vertragslogik abgesichert wird.

Cyber-Resilienz und Sicherheit Kritischer Infrastrukturen

Die Stärkung von Datensicherheit ist ein zentrales Anliegen der EU-Gesetzgebung, um europäische Infrastruktur insbesondere gegen extraterritoriale Bedrohungen abzusichern. Die sich derzeit in Umsetzung befindliche NIS2-Richtlinie (Network and Information Security Directive 2) (EU) 2022/2555 verschärft die Anforderungen an die IT-Sicherheit in kritischen Sektoren, wozu auch der Energiesektor zählt. Regulierte Einrichtungen müssen geeignete technische und organisatorische Maßnahmen ergreifen, um Vorfälle, die die Sicherheit ihrer Anlagen betreffen, zu verhindern, zu erkennen und darauf zu reagieren. Auch der ab Dezember 2027 geltende Cyber Resilience Act (EU) 2024/2847 (CRA), ein EU-Regelwerk für die Cyber-Sicherheit von Hard- und Softwareprodukten, zielt auf „Security-by-Design“ und ständige Sicherheits-Updates bei betroffenen Geräten ab. Regelungen zur technischen Sicherheit finden sich im Übrigen auch in der DSGVO, die nach Art. 32 eine Datensicherheit nach „Stand der Technik“ vorschreibt.

Für die Umsetzung dieser Pflichten bietet Web3 potenziell architektonische Vorteile. Dezentrale Netzwerke haben keinen zentralen Schwachpunkt. Sie bleiben auch bei Teilausfällen funktionsfähig und sind weniger anfällig für großflächige Angriffe. Selbst wenn einzelne Systeme ausfallen oder angegriffen werden, bleibt das System als Ganzes funktionsfähig. Das entspricht dem Ziel der NIS2, die Resilienz wichtiger und essenzieller Einrichtungen, insbesondere für die Energieversorgung, zu erhöhen. Eine dezentrale Handels- oder Steuerungsplattform kann zum Beispiel regionale Stromhandelsprozesse weiterführen, selbst wenn Teile des Netzwerks gestört sind, da keine zentrale Kontrollinstanz als Schwachstelle existiert.

Darüber hinaus ermöglicht Web3 integriertes Monitoring: Sicherheitsrelevante Ereignisse können unveränderlich aufgezeichnet werden, was die frühzeitige Erkennung von Angriffen und eine lückenlose Forensik fördert. Dies kann dabei helfen, die in der NIS2 geforderten Meldungen fundiert zu untermauern. Vorteile können sich auch für kleinere Anbieter ergeben: Ist die dezentrale Infrastruktur NIS2-konform, könnten sie sich andocken und mit vergleichsweise geringen Investitionen sichere Dienste anbieten, ohne eigene teure Sicherheitssysteme entwickeln zu müssen.

Auch bei der Umsetzung der CRA-Vorgaben zur Security-by-Design und zur Verwundbarkeitsüberwachung kann Web3 Vorteile bieten. Durch Web3-basierte Geräteidentitäten und Signaturen könnte beispielsweise bei einem Smart Meter oder Ladepunkt sichergestellt werden, dass nur vom Hersteller freigegebene Firmware-Updates akzeptiert werden. Jede aufgespielte Softwareversion ließe sich als Transaktion auf einem Ledger dokumentieren, wodurch Behörden oder Betreiber nachvollziehen können, ob ein Gerät den vorgeschriebenen Sicherheitsstand aufweist. Die Manipulationssicherheit von Web3 garantiert, dass ein Angreifer nicht unbemerkt den Update-Verlauf eines Geräts ändern kann, was für die Integrität des ebenfalls vorgeschriebenen Supply Chain Management zentral ist.

Digitale Identitäten und eIDAS 2.0

Das Vertrauen in digitale Transaktionen benötigt verlässliche Identitätslösungen. Die EU hat mit der eIDAS-Verordnung (EU) Nr. 910/2014 (2014) und ihrem Update eIDAS 2.0 (2024) einen Rahmen geschaffen, der nun auch Web3-Identitäten einbindet, indem „qualifizierte elektronische Journale“ (Ledger) als gleichwertige

Lösungen anerkannt werden. Diese Journale sind als verteilte elektronische Datenaufzeichnung definiert, die gegen unautorisierte Änderungen abgesichert ist. Damit beschreibt der Gesetzgeber quasi Grundprinzipien von DLTs (z. B. Dezentralität, Unveränderbarkeit).

Diensteanbieter, die einen Distributed Ledger betreiben, können sich als „Qualified Trust Service Provider – Electronic Ledger“ zertifizieren lassen, wenn sie strenge Sicherheits- und Zuverlässigkeitsanforderungen erfüllen, damit ihre DLT-Dienste als gleichwertig zu traditionellen Trust Services (wie z. B. klassischen Zeitstempeln oder Siegeln) gelten. Dies kann als regulatorischer Durchbruch für Web3-Technologien betrachtet werden. Die Rechtssicherheit würde erheblich steigen, wenn ein Distributed Ledger beispielsweise im Streitfall gerichtlich wie ein offizielles Register behandelt werden kann.

Eine weitere wichtige Neuerung durch eIDAS 2.0 ist die europäische digitale Identitätsbörse (EUDI-Wallet), die es Bürgerinnen und Bürgern und Unternehmen ermöglicht, amtliche Nachweise digital zu verwalten und zu teilen. In einer solchen Wallet könnten perspektivisch auch Energiegeräte-Zertifikate oder Teilnahmeberechtigungen für Flexibilitätsmärkte als VCs abgelegt werden (vgl. Kapitel 0). Dies vereinfacht grenzüberschreitende Prozesse enorm, da die Echtheit dieser Nachweise über qualifizierte Siegel und Zeitstempel überprüfbar ist. Durch Web3-Technologien realisierte SSIs werden damit potenziell europatauglich. eIDAS 2.0 legt damit einen wichtigen Grundstein dafür, dass mithilfe von Web3-Technologien dezentral verwaltete digitale Identitäten und staatlich anerkannte Identitäten verschmelzen, was der Rechtssicherheit dezentraler Energielösungen enorm zugutekommen kann.

Fazit und Ausblick

Auch wenn ein Web3-Einsatz rechtlich keine zwingende Lösung für eine künftige technische Architektur im Energiesektor ist, hat sie das Potenzial, eine Brücke zwischen Innovation und Regulierung zu bauen. Europäische Gesetze formulieren ambitionierte Ziele (Transparenz, Datenzugang, Sicherheit, Marktöffnung, Verbraucherschutz). Web3-Technologien können hier zukünftig konkrete Angebote liefern, diese Ziele effizient und prüfbar zu erreichen. Wichtig ist dabei eine verantwortungsvolle Gestaltung: Web3-Anwendungen müssen den Privacy-by-Design-Grundsatz beachten und Sicherheitsvorgaben durch robuste Protokolle umsetzen. Gelingt dies, so können Behörden, Unternehmen sowie Verbraucherinnen und Verbraucher gleichermaßen Gewinner sein: Behörden bekommen besser überprüfbare Compliance und Unternehmen können innovative Dienstleistungen anbieten und sich dabei auf dezentrale Lösungen verlassen, die von Anfang an gesetzeskonform sind. Und schließlich profitieren auch die Verbraucherinnen und Verbraucher von neuen Optionen bei zugleich stärkerem Schutz ihrer Rechte.

6 Schlussfolgerungen

6.1 Zusammenfassung der wichtigsten Ergebnisse

Technologien und Anwendungsfälle, wie sie in den vorangegangenen Kapiteln vorgestellt wurden, machen deutlich: Die Entwicklung vom Web2.0 hin zum Web3 schreitet dynamisch voran. Gleichzeitig ist das Web3 ein Themenfeld, das sich noch formt und erst nach und nach an Kontur gewinnen wird. Entsprechend ist aktuell weder in der Wissenschaft noch in der Praxis eine einheitliche Definition von Web3 und den dazugehörigen Web3-Technologien zu finden. Häufig werden Web3-Technologien noch mit ihrer bekanntesten Vertreterin, der Blockchain-Technologie, gleichgesetzt. Die in dieser Studie erfolgte Aufbereitung von Web3 zeigt jedoch, dass Web3-Technologien ein breites Spektrum an Technologien und anknüpfenden Lösungen umfassen. Sie lassen sich anhand spezifischer Charakteristika dem Web3 zuordnen: Definierende Eigenschaften sind insbesondere die *Dezentralisierung* bzw. die dezentralen Strukturen auf der technologischen Ebene, aber auch auf der Governance-Ebene. Weitere Charakteristika von Web3-Technologien sind die Sicherstellung von *Datensouveränität* für Nutzerinnen und Nutzer sowie die erhöhte *Transparenz* und *Nachvollziehbarkeit* bis hin zu der Umsetzung *digitaler Verifizierung*. Im Energiesektor müssen daher für die Anwendung von Web3-Technologien ihre einzelnen Funktionsweisen sowie deren Zusammenspiel betrachtet werden.

Die Anwendung von Web3-Technologien im Energiesektor war zunächst stark geprägt durch das Aufkommen von *Blockchain-basierten Lösungen*. Im Fokus standen dabei der Einsatz von Blockchain-basierten Smart Contracts zur automatisierten Abwicklung von Transaktionen (z. B. für Pilotprojekte im Peer-to-Peer-Handel mit Strom oder Ladevorgänge an E-Ladesäulen).[126] In der Studie „Blockchain in der integrierten Energiewende“ wurde dieser Ansatz bereits aufgegriffen (Deutsche Energie-Agentur, 2019). Trotz fortschreitender technologischer Entwicklung im Blockchain-Bereich und bei anderen DLTs konnten sich Blockchain-basierte Lösungen in der Energiewirtschaft bislang nicht etablieren. Ursachen hierfür liegen unter anderem in weiterhin bestehenden Fragen zur Skalierung und regulatorischen Unsicherheiten (z. B. in Bezug auf den Datenschutz oder die Marktaufsicht). Diese Herausforderungen stellen jedoch keine unlösbaren Probleme dar. Gleichzeitig gewinnen andere Web3-Technologien an Bedeutung: Dazu zählen *digitale Identitäten* und dazugehörige Lösungen, die *SSI-Prinzipien* umsetzen, sowie dezentrale Infrastrukturen wie *Datenräume* für den Datenaustausch. Diese Technologien zeigen sowohl in Kombination mit Blockchain als auch davon unabhängig ein hohes Potenzial für konkrete Anwendungsfälle im Energiesektor – beispielsweise in Bezug auf die Identifizierung von verteilten Assets im Energiesystem und eine rollenbasierte Steuerung dieser Assets (vgl. „Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem (Deutsche Energie-Agentur, 2022c)) Auch die Ausstellung von vertrauenswürdigen Nachweisen (z. B. für die Herkunft aus erneuerbaren Energien) oder der sektorenübergreifende, sichere und kontrollierte Zugang zu Daten zählen zu potenziellen Einsatzbereichen. Die Schaffung von regulatorischen Grundlagen und Referenzarchitekturen (z. B. über eIDAS 2.0, Gaia-X und Referenzsystem für den Datenaustausch im Energiesektor - ReDiE) trägt dazu bei, dass andere Web3-Technologien prototypisch für die Anwendung im Energiesektor umgesetzt werden und eine schrittweise Einführung in den operativen Betrieb finden.

[126] Beispiele finden Sie unter anderem bei Strüker (2019) und Bogensperger et al. (2023).

Ein Großteil der bisherigen Web3-Anwendungen im Energiesektor konzentriert sich auf die Bereitstellung, den Handel und das Management von *Energieflexibilitäten*. Dabei stehen insbesondere Lösungen zur dezentralen Vermarktung, Koordination und automatisierten Abwicklung/Abrechnung von steuerbaren Stromverbräuchen und steuerbarer Stromerzeugung (z. B. bei Batterien) im Vordergrund. In angrenzenden Anwendungsfeldern wie im Bereich des *Netzmanagements* oder der *Marktkommunikation* wird die Implementierung von Web3-Technologien weiter untersucht und verspricht großes Potenzial für die Koordination von Marktakteuren und -assets sowie für die sichere Bereitstellung und Nutzung der dafür notwenige Daten. Durch die zunehmende Elektrifizierung liegt ein wachsendes Anwendungsfeld von Web3-Technologien an der *Schnittstelle des Energiesektors zu anderen Sektoren*. So könnten digitale Identitäten ein zentrales Element für die Identifizierung, Authentifizierung und Autorisierung von E-Fahrzeugen oder Wärmepumpen für die Bereitstellung von Energieflexibilitäten sein. Aufgrund regulatorischer (vgl. eIDAS 2.0, MiCAR und Genuis Act) und technologischer Fortschritte (z. B. ZKPs) können die dahinterliegende Nachweisführung für erbrachte Energieflexibilitäten und dazugehörige Incentivierungsmodelle über Blockchain-basierte Lösungen und Kryptowährungen (vgl. Stablecoins) anders als noch vor ein paar Jahren heute grundsätzlich umgesetzt werden. Auch bei der Ausstellung von HKNs und anderen Treibhausgas-Nachweisen zeigt sich das Potenzial von Web3-Technologien für eine *sektorenübergreifende Nachverfolgung von Emissionen*. Übergreifend könnten Web3-Technologien daher insbesondere bei Anwendungsfällen zum Tragen kommen, bei denen *sektorenübergreifende Datenflüsse* stattfinden müssen und Identitäten von Organisationen und Assets sowie Marktmechanismen transparent, nachvollziehbar und interoperabel gestaltet werden sollen.

6.2 Zukunftsaussichten und Potenzial von Web3-Technologien im Energiesektor

Digitale Identitäten als Grundlage für Web3-Anwendungsfälle

Vor dem Hintergrund einer zunehmenden Dezentralisierung und einer komplexer werdenden Struktur im Energiesektor (insbesondere auf der Erzeugungsseite) bildet eine effiziente und sichere *Identifizierung, Authentifizierung und Autorisierung* sämtlicher energiebezogener Marktakteure und Assets eine zentrale Grundlage für die digitale Transformation des Energiesektors. Die durch die Elektrifizierung zunehmenden Schnittstellen zu anderen Sektoren unterstreichen die Notwendigkeit eines *digitalen Identitätslayers*, der die digitalen Identitäten von Menschen, Organisationen und Maschinen sicher und standardisiert abbildet. Die Lösungen für digitale Identitäten schaffen somit oftmals die Voraussetzung für den Einsatz anderer digitaler Technologien – insbesondere Web3-Technologien – im Energiesektor (z. B. für einen sicheren Datenaustausch über unterschiedliche Akteure hinweg). Die Schaffung eines Identitätslayers auf Basis digitaler Identitäten kann beispielsweise zukünftig dazu beitragen, kleine EE-Anlagen besser in Marktprozesse und das Netzmanagement einzubinden. Zudem können digitale Identitäten die Datensouveränität fördern, was insbesondere beim Einbezug privater Stakeholder sowie beim unternehmensübergreifenden Datenaustausch von großer Bedeutung ist.

Die *Datenökonomie* im Energiesektor wird zu einem entscheidenden Faktor für ein funktionierendes, dezentrales Energiesystem. Ein effektiver Datenaustausch durch eine dezentrale und standardisierte Infrastruktur wie Datenräume ermöglicht neue datenbasierte Anwendungen wie KI-gestützte Vorhersagemodelle und innovative Geschäftsmodelle. Mit der steigenden Bedeutung von *KI-Anwendungen* im Energiesektor wächst

auch der Bedarf an sicherer Datenherkunft und Transparenz beim Datenaustausch. Hier könnte eine Schnittstelle zwischen Web3-Technologien und KI-Anwendungen entstehen, um insbesondere bei zukünftigen Einsatzbereichen im operativen Netzbetrieb eine Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Die durch Web3-Technologien ermöglichte Transparenz bei der Datenherkunft und -verarbeitung in Kombination mit Incentivierungsmodellen und/oder automatisierten Abrechnungen könnte insbesondere für die Bereitstellung von Energieflexibilitäten durch unterschiedliche Assets sowie die Finanzierung von Projekten (z. B. Investitionen in Großbatterien, Wind-/Solarparks) eingesetzt werden. Web3-Technologien bieten hier vielversprechende Ansätze und sind auf konzeptioneller Ebene bereits gut entwickelt. Der Schritt von erfolgreichen Pilotprojekten hin zu einem breiten Einsatz in der Praxis steht allerdings noch aus.

Potenzial von Web3-Technologien abhängig von der Infrastruktur

Das Potenzial von Lösungen basierend auf Web3-Technologien kommt aufgrund der dezentralen Struktur meist erst zum Tragen, wenn eine kritische Menge teilnimmt. Ein weiterer entscheidender Faktor für eine digitale Transformation im Energiesektor, die eine Anwendung von Web3-Technologien erst ermöglicht, ist die *Infrastruktur*. Zu diesen technologischen Grundvoraussetzungen gehört insbesondere der flächendeckende Rollout von intelligenten Messsystemen und die Einbindung der dahinterliegenden Anlagen in moderne und leistungsfähige *Sicherheitsarchitekturen*. Fehlen diese, können Sicherheitslücken entstehen, die besonders im Kontext einer vollständig digitalisierten Energieinfrastruktur gefährdend für die Kritische Infrastruktur sein können. Denn in einer zukünftigen Ende-zu-Ende digital vernetzten Systemarchitektur ist die Gesamtsicherheit maßgeblich durch die am wenigsten abgesicherte Komponente begrenzt. So könnten etwa ungeschützte Kundendaten in Cloud-Umgebungen oder fehlerhafte Geräteauthentifizierung, die anschließend in Web3-basierte Systeme übertragen werden, zu Sicherheitslücken führen. Eine zuverlässige, sichere hardwaregestützte digitale Infrastruktur ist daher eine Voraussetzung, um Vertrauen, Integrität und Resilienz bei der Nutzung von Web3-Technologien im Energiesektor zu gewährleisten und eine flächendeckende Verbreitung zu ermöglichen.

Potenzial von Web3-Technologien abhängig von Governance-Fragestellungen

Die notwendigen Investitionen und die erforderliche Weiterentwicklung der Infrastruktur im Energiesektor sind stark mit dessen Regulierung verbunden. Der Energiesektor zählt zu den am stärksten regulierten Bereichen der europäischen Infrastruktur. Der vorhandene regulatorische Rahmen wirkt sich damit auch direkt auf die Skalierbarkeit und das Potenzial von Web3-Technologien im Energiesektor aus. Viele potenzielle Anwendungen von Web3-Technologien (z. B. im Bereich automatisierter Transaktionen von Energieflexibilität) stoßen auf *regulatorische Hürden*, die eine sehr umfangreiche Anpassung bestehender Markt- und Systemstrukturen erforderlich machen. Daher ist insbesondere die Transformation hin zu für Web3-Technologien angepasste und geeignete regulatorische Rahmenbedingungen mit großen Änderungen verbunden. In dieser starken Reglementierung des Energiesektors kann jedoch auch eine Chance bestehen: Sie kann sofern gewollt von Politik und den Stakeholdern als Hebel für eine schnelle Skalierung genutzt werden. Wenn zentrale Akteure wie Netzbetreiber, Regulierungsbehörden und Marktteilnehmer gemeinsam an der Integration von Web3-Technologien und der Transformation der Regulierung arbeiten, kann so die für neue Technologien notwendige kritische Masse vergleichsweise rasch erreicht werden. Die starke Regulierung im Energiesektor kann daher nicht nur eine Hürde für die Transformation darstellen, sondern auch als *Katalysator* für gezielte Innovation wirken.

Dezentrale Technologien vs. zentralisierte Strukturen und Prozesse im Energiesektor

Neben regulatorischen Aspekten prägen auch *historisch gewachsene zentrale Strukturen und Prozesse* den Energiesektor. Diese Zentralisierung betrifft nicht nur die physische Netzinfrastruktur, sondern auch Marktrollen, Marktmechanismen und Prozesse im Netzmanagement. Dem gegenüber stehen Web3-Technologien, die sich insbesondere über die technologische Dezentralisierung und Interaktionen (z. B. Datenaustausch) ohne zentrale Instanz definieren. Der strukturelle Gegensatz zwischen dezentralen Technologien und der zentral organisierten Ausgestaltung des Energiesektors führt zwangsläufig zu Spannungsfeldern. Der Einsatz dezentraler Web3-Technologien zur Abbildung zentral organisierter Prozesse im Energiesektor ist aus funktionaler Perspektive wenig zielführend und bietet daher oft keinen Mehrwert. Die breite Einführung von Web3-Technologien erfordert daher nicht nur technologische Weiterentwicklungen, sondern vor allem einen grundlegenden Wandel in Denkweisen, etablierten Rollenverständnissen und Prozessstrukturen. Dabei ist zu berücksichtigen, dass die Zentralisierung im Energiesektor auch durch die Einordnung als Teil der Kritischen Infrastruktur und die damit verbundenen Anforderungen an die Systemsicherheit und Resilienz geprägt ist. Vor diesem Hintergrund ist ein differenzierter und abgestimmter Transformationsprozess erforderlich, der Raum für Innovationen und den Einsatz von Web3-Technologien schafft. Dabei müssen insbesondere Fragestellungen in Bezug auf die Gestaltung zentralisierter bzw. dezentraler Strukturen aus einer gesamtheitlichen Perspektive für den Energiesektor beantwortet werden.

6.3 Handlungsempfehlungen zum Umgang mit Web3-Technologien

Aus der Untersuchung von Web3-Technologien und ihrer Anwendbarkeit im Energiesektor ergeben sich folgende Handlungsempfehlungen:

Testen des Potenzials mithilfe von mehr Opportunitäten für Sandboxing

Um den Beitrag von Web3-Technologien für die Digitalisierung von Prozessen im Energiesektor zu evaluieren, sind Sandboxing-Ansätze sehr vielversprechend. Denn durch kontrollierte Testumgebungen können Anwendungen unabhängig von bestehenden regulatorischen Rahmenbedingungen erprobt werden, wodurch das Risiko von Fehlinvestitionen („Sunk Costs“) minimiert wird. Somit kann insbesondere getestet werden, welche bestehenden Prozesse im Energiesystem besonders von einer Transformation profitieren würden und welche spezifischen regulatorischen Anpassungen erforderlich sind, um dies zu ermöglichen. Diese Sandboxing-Ansätze würden darüber hinaus ermöglichen, spezifische Incentive-Mechanismen sowie Governance-Mechanismen für verschiedene Akteure der Energiewirtschaft – beispielsweise Netzbetreiber und Endkundschaft – zu gestalten, ohne dabei den Fokus auf das Gemeinwohl aus den Augen zu verlieren.

Die Einführung solcher Sandboxes wurde bereits in mehreren europäischen Ländern diskutiert und angewandt (vgl. Europäische Kommission, Directorate-General for Energy et al., 2023). Sandboxes sind entsprechend bereits erprobte und geeignete Instrumente, um gezielt Innovationen im Energiesektor anzukurbeln. In Deutschland gibt es Sandboxes für Anwendungen im Mobilitäts- und Energiesektor. Im Norddeutschen Reallabor[127] wird zum Beispiel der Transformationspfad für das Energiesystem durch Wasserstoff und Sektorenkopplung erprobt. Jedoch sollten Sandboxes auch für die Digitalisierung im Energiesektor gefördert werden. In solchen Sandboxes müssen mindestens zentrale Akteure aus dem Energiesektor (z. B. BMWE, BNetzA, ÜNBs, VNBs), Technologie- und Serviceanbieter aus dem Web3-Bereich sowie Akteure aus der Zivilgesellschaft involviert werden. Erkenntnisse aus erfolgreichen Pilotprojekten können dann genutzt werden,

[127] Weitere Informationen zum Norddeutschen Reallabor finden Sie unter https://norddeutsches-reallabor.de/ (Norddeutsches Reallabor, 2025).

um gezielt notwendige regulatorische Anpassungen abzuleiten und die technologische Entwicklung mit rechtlichen Rahmenbedingungen in Einklang zu bringen. Das setzt jedoch voraus, dass diese Erkenntnisse in einem koordinierten Prozess in die Weiterentwicklung von Lösungen und den dahinterliegenden Standards und Rahmenbedingungen einfließen.

Handlungsempfehlung 1

Der Einsatz von Web3-Technologien im Energiesektor sollte innerhalb sogenannter Sandboxes für unterschiedliche Anwendungsfälle getestet werden. Die Ergebnisse aus der Erprobung in den Sandboxes sollten koordiniert und zielgerichtet in Gesetzgebungsprozesse und Standardentwicklung einfließen.

Klare Zielsetzung in Bezug auf Governance und Struktur

Für die Entwicklung und Integration von Web3-Technologien im Energiesektor sollte ein übergeordnetes Zielbild erstellt werden. Es definiert die anzustrebenden Governance-Strukturen und die Systemarchitektur idealerweise präzise, aber gleichzeitig nicht abschließend. Typische Governance-Fragen sind im Web3-Kontext „Welche Systemkomponenten sollen zentralisiert oder dezentral ausgestaltet sein?“ oder „Welche Systemkomponenten sind Teil der öffentlichen und welche der privaten Infrastrukturen und müssen daher auch von den entsprechenden Stakeholdern bereitgestellt werden?“. Bei der Beantwortung dieser Fragestellungen sollten die wichtigsten Zieldimensionen (z. B. Effizienz, Resilienz, Partizipation) identifiziert werden. Ebenso müssen für die Entwicklung eines strategischen Zielbilds die technologischen Entwicklungen und die daraus resultierenden Möglichkeiten (bzw. Freiheitsgrade) berücksichtigt werden. Die technologischen Möglichkeiten beeinflussen maßgeblich, welche Governance-Strukturen realisierbar und tragfähig sind und damit langfristig zum Erreichen von postulierten Zieldimensionen beitragen können. Das Erreichen eines Zielbilds muss anschließend durch einen gerichteten Transformationsprozess (z. B. in Form von Investitionen) unterstützt werden. Bereits vorhandene Vertrauensanker innerhalb des Energiesystems (z. B. in Form regulierter Akteure) können eine schrittweise Transformation hin zu einer stärkeren Dezentralisierung der digitalen Infrastruktur und digitaler Prozesse begleiten. Sie könnten dabei als Bindeglied zwischen bestehenden, etablierten Rollen und neuen, dezentralen Ansätzen fungieren.

Als Beispiel für die Ausarbeitung eines strategischen Zielbilds und des dazugehörigen Umsetzungsplans kann die Entwicklung der notwendigen digitalen Identitätsinfrastruktur gesehen werden: Während eIDAS 2.0[128] die Grundlage für die Entwicklung von digitalen Identitätslösungen für Personen und Organisationen schafft, fehlen für die Identifikation von Maschinen noch die notwendigen regulatorischen Rahmenbedingungen. Im derzeit laufenden Projekt **DIMOS**, das die dena im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWE) durchführt, wird diese Fragestellung unter anderem untersucht. Für die Realisierung und Umsetzung der dazugehörigen digitalen Identitätsinfrastruktur sollen bis 2027 erste EUDI-Wallets zur Verfügung stehen – eine verpflichtende Nutzung ist jedoch noch nicht geplant, was eine zügige und planungssichere Umsetzung vonseiten öffentlicher und privater Institutionen erschwert. Hier ist daher eine Weiterführung des bestehenden Zielbilds und der Implementierungsvorhaben notwendig. Dabei sollten unter anderem folgende Fragestellungen beantwortet werden: „Auf welche Weise erfolgt die Zusam-

[128] eIDAS 2.0 ist eine EU-Verordnung, die die Rahmenbedingungen für elektronische Identifizierung und Vertrauensdienstleistungen (Trusted Services“) für elektronische Transaktionen in der EU beschreibt.

menarbeit zwischen öffentlich bereitgestellten Identitätslösungen und privaten Anbietern von Vertrauensdienstleistungen (Trusted Services)?“, „Wer trägt die Verantwortung für entstandenen Missbrauch von Daten?“, „Wie wird die technische Kompatibilität über Länder- und Branchengrenzen hinweg sichergestellt und umgesetzt?“

Handlungsempfehlung 2

Die relevanten Stakeholder sollten ein übergeordnetes Zielbild für den Grad der Zentralisierung bzw. Dezentralisierung in der Systemarchitektur des Energiesektors definieren. Investitionen in digitale Infrastruktur und regulatorische Anpassungen sollten sich anschließend an diesem Zielbild ausrichten, um die digitale Transformation im Energiesektor gezielt und überprüfbar zu gestalten.

Digitale Souveränität mittels Web3 zur Förderung von Resilienz

Verteilte Rechen- und Speicherarchitekturen können die Resilienz des Energiesystems gegenüber wirtschaftlichen und technischen Ausfällen zentraler Akteure grundsätzlich erhöhen. Der wesentliche Unterschied zwischen verteilten Architekturen wie DLTs und herkömmlichen Verfahren zur Transaktionsverarbeitung liegt in der Entkopplung von Programmen und Daten von den zugrunde liegenden physischen Hardwarekomponenten wie Netzwerken, Prozessoren und Speichergeräten. In klassischen Architekturen hat die Hardware stets die Kontrolle über die darauf ausgeführte Software: Wer die Hardware kontrolliert, kann die Software verändern oder abschalten. In dezentralen Web3-Architekturen, wie sie beispielsweise bei Blockchains umgesetzt werden, gilt dies nicht: Hier haben Hardwarebetreiber (d. h. Betreiber einzelner Knotenpunkte im Netzwerk) keine unmittelbare Kontrolle über die auf der Infrastruktur laufende Software. Diese Trennung von Hardware und Software kann erhebliche Implikationen für die Governance von Programmen und Prozessen haben: Energiewirtschaftliche Abläufe, die mittels Blockchain oder anderer Web3-Technologien dezentral organisiert werden, könnten ceteris paribus ausfallsicherer und potenziell kostengünstiger gestaltet werden als heutige zentral organisierte Ansätze.

Handlungsempfehlung 3

Energiewirtschaftliche Akteure sollten prüfen, in welchen Bereichen der Einsatz verteilter Architekturen mittels Web3-Technologien (Governance-)Risiken reduziert und die Ausfallsicherheit erhöht. Pilotprojekte können dabei helfen, die Resilienz einer dezentralen digitalen Infrastruktur im Vergleich zu bestehenden zentralen Lösungen zu bewerten.

Skills and Training für Fachkräfte

Für die Integration und Entwicklung von Web3-basierten Anwendungen im Energiesystem sind spezifische Fachkenntnisse unerlässlich. Dabei sind sowohl Entwicklerinnen und Entwickler notwendig, die ein tiefgreifendes Verständnis der Technologien haben und sie implementieren können, als auch Fachkräfte an der Schnittstelle zu anderen Disziplinen. Letztere (z. B. Wirtschaftsinformatikerinnen und -informatiker) müssen die Funktionsweise des Energiesystems und ökonomische Fragestellungen verstehen, um Anwendungsfälle von Web3-Technologien und konzipierte Lösungen im energiewirtschaftlichen Kontext entwickeln und bewerten zu können. Da nur eine begrenzte Menge an qualifizierten Fachkräften zur Verfügung steht, sollten Unternehmen in der Energiewirtschaft ein kontinuierliches Angebot für Aus- und Weiterbildung bereitstellen.

Damit kann sichergestellt werden, dass das notwendige Personal über die erforderlichen interdisziplinären Fachkenntnisse (das heißt insbesondere an der Schnittstelle zwischen Informatik und Energiewirtschaft) verfügt.

Handlungsempfehlung 4

Für eine schrittweise Integration von Web3-Technologien in den Energiesektor müssen notwendige Fachkräfte angeworben und/oder geschult werden. Dabei sollen insbesondere auf interdisziplinäre Kenntnisse an der Schnittstelle von Informatik und Energiewirtschaft Wert gelegt werden.

Engere Miteinbeziehung von Nutzerinnen und Nutzern

Endverbraucherinnen und Endverbraucher werden im Rahmen eines zunehmend dezentralisierten Energiesystems eine aktive und entscheidende Rolle übernehmen. Um die erfolgreiche Einführung von Web3-Technologien zu unterstützen, ist es essenziell, diese Zielgruppe frühzeitig einzubeziehen und ein fundiertes Verständnis für die Nutzung der zugrunde liegenden Technologien und ihrer Eigenschaften zu fördern. Missverständnisse oder fehlende Transparenz können die gesellschaftliche Akzeptanz erheblich beeinträchtigen. Durch gezielte Informations- und Beteiligungsformate kann das notwendige Vertrauen geschaffen und die gesellschaftliche Anschlussfähigkeit dezentraler digitaler Lösungen gestärkt werden. Die Akzeptanz dezentraler digitaler Lösungen ist notwendig, um die postulierten Eigenschaften von Web3-Technologien (z. B. in Bezug auf Benutzerkontrolle und Datensouveränität) zu realisieren. Die Nutzung dezentraler digitaler Lösungen wird dabei zu Verhaltensänderungen führen. So müssen Nutzerinnen und Nutzer beispielsweise ihre digitalen Identitäten und die Zugänge zu ihren Wallets selbst verwalten, anstatt sich auf zentrale Anbieter zu verlassen. Gleichzeitig weisen Web3-Technologien einen hohen Grad an Komplexität auf. Ein tiefgreifendes Verständnis der Web3-Technologien kann jedoch nicht bei den Nutzerinnen und Nutzern vorausgesetzt werden. Die Benutzeroberflächen und Interaktionsmechanismen von Web3-basierten Lösungen müssen deshalb so gestaltet werden, dass Web3-basierte Anwendungen und Dienste eine möglichst nutzerfreundliche Bedienung ohne technologisches Vorwissen ermöglichen. Gleichzeitig müssen die Endnutzerinnen und -nutzer jedoch trotzdem für die ihnen neu zur Verfügung stehende Souveränität (und die damit verbundene Verantwortung) sensibilisiert werden.

Handlungsempfehlung 5a

Web3-basierte Lösungen im Energiesystem sollten stets im Hinblick auf die Nutzerinnen und Nutzer der jeweiligen Lösung entwickelt werden: Dabei muss insbesondere für Endkundinnen und -kunden (B2C) ein möglichst nutzerfreundlicher Zugang gestaltet werden, während gleichzeitig das Bewusstsein für den Umgang mit Web3-basierten Lösungen gestärkt wird.

Für Akteure, die in der Energiewirtschaft Web3-Technologien nutzen und ihre Entwicklung aktiv vorantreiben und begleiten, ist ein tiefgreifenderes Verständnis der Technologien nötiger als bei Endkundinnen und -kunden. Aber auch bei Web3-basierten Lösungen, die primär für B2B-Prozesse im Energiesektor bestimmt sind, bleibt die Nutzerfreundlichkeit ein wichtiger Faktor. Allerdings ist es für den Einsatz von Web3-Technologien im B2B-Bereich (vor allem im operativen Netzbetrieb) unerlässlich, dass die Nutzerinnen und Nutzer die

wesentlichen Chancen und insbesondere Risiken einschätzen können. Unternehmen in der Energiewirtschaft sollten daher bei der Entwicklung von Web3-basierten Lösungen sowohl die nutzerfreundliche Gestaltung als auch das zielgerichtete und kontinuierliche Wissensmanagement für Beschäftigte im operativen Betrieb beachten.

Handlungsempfehlung 5b

Web3-basierte Lösungen im Energiesystem sollten stets im Hinblick auf die Nutzerschaft der jeweiligen Lösung entwickelt werden: Dabei muss auch für unternehmensinterne Nutzerinnen und Nutzer (B2B) ein möglichst nutzerfreundlicher Zugang gestaltet werden, während gleichzeitig Potenziale und Risiken der genutzten Web3-Technologien in einen kontinuierlichen Wissensmanagementprozess integriert werden.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Abad, A. V., & Dodds, P. E. (2020). Green hydrogen characterisation initiatives: Definitions, standards, guarantees of origin, and challenges. *Energy Policy*, 138, 111300. https://doi.org/10.1016/j.enpol.2020.111300

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the world wide web: From WEB 1.0 to Web 4.0. *International Journal of Web & Semantic Technology*, 3(1), 1-10. https://doi.org/10.5121/ijwest.2012.3101

Akanfe, O., Lawong, D., & Rao, H. R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, 76, 102753. https://doi.org/10.1016/j.ijinfomgt.2024.102753

Aldosary, M., & Alqahtani, N. (2021). A survey on federated identity management systems limitation and solutions. *International Journal of Network Security & Its Applications (IJNSA)*, 13(3). https://ssrn.com/abstract=3869295

Allen, C. (2016). The Path to Self-Sovereign Identity. *Online verfügbar unter:* http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html [Abgerufen am 22.05.2025]

Allen, D. W., Berg, C., Lane, A. M., MacDonald, T., & Potts, J. (2023). The exchange theory of web3 governance. *Kyklos*, 76(4), 659-675. https://doi.org/10.1111/kykl.12345

di Angelo, M., & Salzer, G. (2020). Tokens, types, and standards: identification and utilization in Ethereum. In: *Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures* (S. 1-10). IEEE. https://doi.org/10.1109/DAPPS49028.2020.00001

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. In: *Proceedings of the 2017 IEEE Symposium on Security and Privacy* (S. 375-392). IEEE. https://doi.org/10.1109/SP.2017.29

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing. University of California at Berkeley, Technical Report No. UCB/EECS-2009-28. *Online verfügbar unter:* https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf [Abgerufen am 01.08.2025]

Arnone, D., Cristofori, L., Mammina, M., Rossi, A., Santoro, S. C., Coelho, F., Andrade, J., Garcia, A., Bessa, R., Kapetanios, A., Kotsalos, K., Stoter, A., Lejarazu, A., & Bilbao, S. (2024). European Common Energy Data Space Framework Enabling Data Sharing – Driven Across – and Beyond – Energy Services. *Online verfügbar unter:* https://enershare.eu/wp-content/deliverables/wp5/Enershare_D5.2_Data%20Value%20Stack%20%28Beta%20version%29-%20v1.0.pdf [Abgerufen am 27.06.2025]

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). *Digital Finance*, 6(1), 55-95. https://doi.org/10.1007/s42521-023-00088-8

Babel, M., Gramlich, V., Guthmann, C., Schober, M., Körner, M. F., & Strüker, J. (2023). Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in

Informationssysteme. *HMD Praxis der Wirtschaftsinformatik*, 60(2), 478-493. https://doi.org/10.1365/s40702-023-00955-3

Babel, M., Gramlich, V., Körner, M. F., Sedlmeir, J., Strüker, J., & Zwede, T. (2022). Enabling end-to-end digital carbon emission tracing with shielded NFTs. *Energy Informatics*, 5(Suppl 1), 27. https://doi.org/10.1186/s42162-022-00199-3

Babel, M., Körner, M. F., Ströher, T., & Strüker, J. (2024). Accelerating decarbonization digitally: Status quo and potentials of greenhouse gas emission tracking and trading. *Journal of Cleaner Production*, 469, 143125. https://doi.org/10.1016/j.jclepro.2024.143125

Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M. F., Sedlmeir, J., Strüker, J. & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets*, 35(1), 1-14. https://doi.org/10.1007/s12525-025-00772-0

Bacco, M., Kocian, A., Chessa, S., Crivello, A., & Barsocchi, P. (2024). What are data spaces? Systematic survey and future outlook. *Data in Brief*, 57, 110969. https://doi.org/10.1016/j.dib.2024.110969

BaFin (2025). Dienstleistungen und Tätigkeiten im Zusammenhang mit Kryptowerten gemäß MiCAR. *Online verfügbar unter:* https://www.bafin.de/DE/Aufsicht/MiCAR/MiCAR_artikel.html [Abgerufen am 02.08.2025]

Baird, L., Harmon, M., & Madsen, P. (2019). Hedera: A public hashgraph network & governing council. *Online verfügbar unter:* https://crebaco.com/planner/admin/uploads/whitepapers/hedera-whitepaper.pdf [Abgerufen am 13.05.2025]

Balduf, L., Henningsen, S., Florian, M., Rust, S., & Scheuermann, B. (2022). Monitoring data requests in decentralized data storage systems: A case study of IPFS. In: *Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems* (S. 658-668). IEEE. https://doi.org/10.1109/ICDCS54860.2022.00069

Bambacht, J., & Pouwelse, J. (2022). Web3: A decentralized societal infrastructure for identity, trust, money, and data. *Online verfügbar unter:* https://arxiv.org/pdf/2203.00398 [Abgerufen am 28.04.2025]

Bari, A., Jiang, J., Saad, W., & Jaekel, A. (2014). Challenges in the smart grid applications: An overview. *International Journal of Distributed Sensor Networks*, 10(2), 974682. https://doi.org/10.1155/2014/974682

Beck, J. (2022). What is Web3? Here are some ways to explain it to a friend. ConsenSys. *Online verfügbar unter:* https://consensys.net/blog/blockchain-explained/what-is-web3-here-are-some-ways-to-explain-it-to-a-friend/ [Abgerufen am 25.04.2025]

Beck, R., European Blockchain Center, Fraunhofer-Institut für Materialfluss und Logistik IML, Gesmann-Nuissl, D., & GS1 Germany (2023). Potentials of Distributed Ledger Technologies for the Economy. WIK-Consult GmbH im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. *Online verfügbar unter:* https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-distributed-ledger-technologies.pdf [Abgerufen am 20.08.2025]

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, 19(10), 1. https://aisel.aisnet.org/jais/vol19/iss10/1

Begleitforschung Smart Service Welt II & Institut für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH (Hrsg.) (2020). Energierevolution getrieben durch Blockchain: Ergebnisse aus

den Projekten BloGPV, ETIBLOGG, pebbles und SMECS. *Online verfügbar unter:* https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SSW_Energierevolution_getrieben_durch_Blockchain.pdf?__blob=publicationFile&v=12 [Abgerufen am 20.06.2025]

Bitkom e.V. (2025). In Deutschland fehlen weiterhin mehr als 100.000 IT-Fachkräfte. *Online verfügbar unter:* https://www.bitkom.org/Presse/Presseinformation/Deutschland-fehlen-IT-Fachkraefte [Abgerufen am 22.08.2025]

Bogensperger, A., Koderer, S., Sylla, S., Ferstl, J., Bruckmeier, A., Hinterstocker, M., & Mertel, S. (2023). Zukunftsfähige Herkunftsnachweise: Konzept für die Ende-zu-Ende-Digitalisierung. Forschungsstelle für Energiewirtschaft e.V. (FfE). *Online verfügbar unter:* https://www.ffe.de/wp-content/uploads/2023/05/Zukunftsfaehige_Herkunftsnachweise_Konzept_fuer_die_Ende_zu_Ende_Digitalisierung.pdf [Abgerufen am 27.07.2025]

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv Preprint.* https://doi.org/10.48550/arXiv.1904.12816

Brisbois, M. C. (2022). Governing Decentralized Electricity: Taking a Participatory Turn. In: *The 4Ds of Energy Transition: Decarbonization, Decentralization, Decreasing Use and Digitalization* (S. 325-346). https://doi.org/10.1002/9783527831425.ch15

Buchholz, S., Tiemann, P. H., Wolgast, T., Scheunert, A., Gerlach, J., Majumdar, N., Breitner, M. H., Hofmann, L., Nieße, A., & Weyer, H. (2021). A sketch of unwanted gaming strategies in flexibility provision for the energy system. In: *Proceedings of the 16th International Conference on Wirtschaftsinformatik, Pre-Conference Community Workshop Energy Informatics and Electro Mobility ICT*. https://www.iwi.uni-hannover.de/fileadmin/iwi/Publikationen/2021_Gerlach_Abstract__WI.pdf

Bundesamt für Sicherheit in der Informationstechnik (2025). Schutzprofil Smart Meter Gateway (BSI-CC-PP-0073). *Online verfügbar unter:* https://www.bsi.bund.de/dok/smgw-schutzprofil [Abgerufen am 13.08.2025]

Bundesministerium für Digitales und Staatsmodernisierung (2025a). Registermodernisierung. *Online verfügbar unter:* https://www.digitale-verwaltung.de/Webs/DV/DE/registermodernisierung/registermodernisierung-node.html [Abgerufen am 14.08.2025]

Bundesministerium für Digitales und Staatsmodernisierung (2025b). Entwicklung der staatlichen EUDI-Wallet und Aufbau des EUDI-Wallet-Ökosystems. *Online verfügbar unter:* https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/start/ [Abgerufen am 22.08.2025]

Bundesministerium für Wirtschaft und Energie (2025a). Redispatch 3.0. In GAIA-X Use Cases. *Online verfügbar unter:* https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/Digitale-Welt/GAIA-X-Use-Cases/redispatch-30.html [Abgerufen am 14.08.2025]

Bundesministerium für Wirtschaft und Energie (2025b). ID-Ideal. *Online verfügbar unter:* https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AbgeschlosseneProgrammeProjekte/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/IDideal/IDideal.html [Abgerufen am 14.08.2025]

Bundesministerium für Wirtschaft und Klimaschutz (2022). Was ist ein Datenraum? Definition des Konzeptes Datenraum. *Online verfügbar unter:*

https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Digitale-Welt/whitepaper-definition-des-konzeptes-datenraum.pdf?__blob=publicationFile&v=1 [Abgerufen am 27.06.2025]

Bundesnetzagentur (2025). Redispatch. *Online verfügbar unter:* https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Netzengpassmanagement/Engpassmanagement/Redispatch/start.html [Abgerufen am 20.08.25]

Butincu, C. N., & Alexandrescu, A. (2024). Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems. *IEEE Access*, 12, 60928-60942. https://doi.org/10.1109/ACCESS.2024.3394537

Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance – A multivocal approach. *Applied Sciences*, 11(16), 7572. https://doi.org/10.3390/app11167572

Calzada, I. (2024). Decentralized web3 reshaping internet governance: Towards the emergence of new forms of nation-statehood?. *Future Internet*, 16(10), 361. https://doi.org/10.3390/fi16100361

Cao, L. (2022). Decentralized AI: Edge intelligence and smart blockchain, metaverse, Web3, and DeSci. *IEEE Intelligent Systems*, 37(3), 6-19. https://doi.org/10.1109/MIS.2022.3181504

Carter, N., Connell, S., Jones, B., Porter, D., & Rudd, M. A. (2023). Leveraging Bitcoin miners as flexible load resources for power system stability and efficiency. *Online verfügbar unter:* https://dx.doi.org/10.2139/ssrn.4634256 [Abgerufen am 12.08.25]

Castellano, D., De Prisco, R., & Faruolo, P. (2024). Login System for OpenID Connect with Verifiable Credentials. In: *Proceedings of the 2024 22nd International Symposium on Network Computing and Applications* (S. 105-112). IEEE. https://doi.org/10.1109/NCA61908.2024.00027

Castellanos, J. A. F., Coll-Mayor, D., & Notholt, J. A. (2017). Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum Blockchain. In: *Proceedings of the 2017 IEEE International Conference on Smart Energy Grid Engineering* (S. 367-372). IEEE. https://doi.org/10.1109/SEGE.2017.8052827

CEDEC, E.DSO, ENTSO-E, Eurelectric, & GEODE (2019). An integrated Approach to Active System Management. *Online verfügbar unter:* https://eepublicdownloads.entsoe.eu/clean-documents/Publications/Position%20papers%20and%20reports/TSO-DSO_ASM_2019_190416.pdf [Abgerufen am 21.08.2025]

Chadwick, D. W. (2007). Federated identity management. In: *International School on Foundations of Security Analysis and Design* (S. 96-120). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03829-7_3

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in industry 4.0: A review. *Information Systems Frontiers*, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Choobineh, M., Arabnya, A., Sohrabi, B., Khodaei, A., & Paaso, A. (2023). Blockchain technology in energy systems: A state-of-the-art review. *IET Blockchain*, 3(1), 35-59. https://doi.org/10.1049/blc2.12020

Chvanova, E. (2025). Rahmenbedingungen des neuen Registers für Gas- und Wasserstoff-HKN. HIC Hamburg Institut Consulting GmbH. *Online verfügbar unter:* https://www.umweltbundesamt.de/sites/default/files/medien/14292/dokumente/tag2_8_chvanova_0.pdf [Abgerufen am 14.08.2025]

Consensys (2024). Consensys releases Global Survey on Crypto and Web3. *Online verfügbar unter:* https://consensys.io/blog/global-survey-on-crypto-and-web3-press-release-2024 [Abgerufen am 22.08.2025]

Critchley, L. (2024). Old becomes new: Retrofitting legacy equipment for smart grid. Tech Insights. *Online verfügbar unter:* https://eepower.com/tech-insights/old-becomes-new-retrofitting-legacy-equipment-for-smart-grid/ [Abgerufen am 26.08.2025]

Croutzet, A., & Dabbous, A. (2021). Do FinTech trigger renewable energy use? Evidence from OECD countries. *Renewable Energy*, 179, 1608-1617. https://doi.org/10.1016/j.renene.2021.07.144

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). *The business of platforms: Strategy in the age of digital competition, innovation, and power* (Vol. 320, S. 1–5). New York, NY: Harper Business.

Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019). Towards scaling blockchain systems via sharding. In: *Proceedings of the 2019 International Conference on Management of Data* (S. 123-140). https://doi.org/10.1145/3299869.3319889

Daniel, E., & Tschorsch, F. (2022). IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks. *IEEE Communications Surveys & Tutorials*, 24(1), 31-52. https://doi.org/10.1109/COMST.2022.3143147

Data Spaces Support Centre (2025a). Data Spaces Blueprint v2.0. *Online verfügbar unter:* https://dssc.eu/space/BVE2/1071251457/Data+Spaces+Blueprint+v2.0+-+Home [Abgerufen am 04.07.2025]

Data Spaces Support Centre (2025b). Intermediaries and operators. *Online verfügbar unter:* https://dssc.eu/space/BVE2/1071253470/Intermediaries+and+Operators#3.2.-Intermediaries-and-operators [Abgerufen am 27.06.2025]

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The trust over IP stack. *IEEE Communications Standards Magazine*, 3(4), 46-51. https://doi.org/10.1109/MCOMSTD.001.1900029

Daylight Energy LLC (2025). Power you control: Join the Daylight Network. *Online verfügbar unter:* https://godaylight.com/ [Abgerufen am 01.08.2025].

Deimel, D., Gericke, C., Hühnlein, D., Kraus, S., Lingl, B., Lume, H., Manecke, A., Philipp, A., Rehder-Lange, J., Schrecker, J., Schwalm, S., Seegebarth, C., Stöcker, C. & Wand, A. (2025). Organisationsidentitäten in der digitalen Welt: Herausforderungen und Lösungsansätze. Bitkom e. V. *Online verfügbar unter:* https://www.bitkom.org/sites/main/files/2025-01/bitkom-whitepaper-organisationsidentitaeten.pdf [Abgerufen am 20.06.2025]

Deutsche Energie-Agentur (2019). Blockchain in der integrierten Energiewende. *Online verfügbar unter:* https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2019/dena-studie_blockchain_integrierte_energiewende_de.pdf [Abgerufen am 05.011.2025]

Deutsche Energie-Agentur (2022a). Digital Machine Identities as a Building Block for an Automated Energy System. *Online verfügbar unter:* https://future-energy-lab.de/app/uploads/2022/10/dena_FEL_Blockchain_Abschlussbericht_engl_web.pdf [Abgerufen am 28.04.2025]

Deutsche Energie-Agentur (2022b). Die Datenökonomie in der Energiewirtschaft: Eine Analyse der Ausgangslage und Wege in die Zukunft der Energiewirtschaft durch die Datenökonomie. *Online verfügbar unter:*

https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2022/ANALYSE_Die_Datenoekonomie_in_der_Energiewirtschaft.pdf [Abgerufen am 28.04.2025]

Deutsche Energie-Agentur (2022c). Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem. *Online verfügbar unter:* https://www.dena.de/infocenter/digitale-maschinen-identitaeten-als-grundbaustein-fuer-ein-automatisiertes-energiesystem [Abgerufen am 05.11.2025]

Deutsche Energie-Agentur (2023a). A guide to electricity-efficient design of decentralized data infrastructure. *Online verfügbar unter:* https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchain_s_Energy_Consumption.pdf [Abgerufen am 19.05.2025]

Deutsche Energie-Agentur (2023b). Das dezentrale Energiesystem im Jahr 2030. *Online verfügbar unter:* https://www.dena.de/infocenter/das-dezentralisierte-energiesystem-im-jahr-2030/ [Abgerufen am 05.11.2025]

Deutsche Energie-Agentur (2024a). Grundlagen und Bedeutung von Datenräumen für die Energiewirtschaft. *Online verfügbar unter:* https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2024/Grundlagen_und_Bedeutung_von_Datenraeumen_fuer_die_Energiewirtschaft.pdf [Abgerufen am 17.05.2025]

Deutsche Energie-Agentur (2024b). EnerComputing – Cloud- und Edge-Technologien für ein dezentrales Energiesystem. *Online verfügbar unter:* https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2024/STUDIE_EnerComputing.pdf [Abgerufen am 17.05.2025]

Deutsche Energie-Agentur (2024c). Was sind dynamische Stromtarife?. *Online verfügbar unter*: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2024/Was_sind_dynamische_Stromtarife.pdf [Abgerufen am 07.11.2025]

Deutsche Energie-Agentur (2025a). Digitale Identitäten im Energiesektor. Ein Beitrag für eine zukunftsgerichtete Dateninfrastruktur. *Online verfügbar unter:* https://future-energy-lab.de/news/dive-abschlussberichtsreihe-digitale-identitaeten-im-energiesektor/ [Abgerufen am 09.09.2025]

Deutsche Energie-Agentur (2025b). DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem. Future Energy Lab. *Online verfügbar unter:* https://future-energy-lab.de/projects/dive-de/ [Abgerufen am 14.08.2025]

Deutsche Energie-Agentur (2025c). Homepage des Use Case Energie. *Online verfügbar unter:* https://future-energy-lab.de/projects/dateninstitut-use-case-energie [Abgerufen am 14.08.2025]

Diaz Valdivia, A. (2023). Between decentralization and reintermediation: blockchain platforms and the governance of 'commons-led' and 'business-led' energy transitions. *Energy Research & Social Science*, 98, 103034. https://doi.org/10.1016/j.erss.2023.103034

Doan, T. V., Psaras, Y., Ott, J., & Bajpai, V. (2022). Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations. *IEEE Internet Computing*, 26(6), 7-15. https://doi.org/10.1109/MIC.2022.3209804

Dognini, A., Monti, A., Kung, A., Medela, A., Joglekar, C. M., Schaffer, C., Stampatori, D., Jimenez, D., Maqueda, E., Coelho, F., & andere. (2024). Blueprint of the Common European Energy Data Space. Interoperability Network for the Energy Transition (int:net). https://doi.org/10.5281/zenodo.12609569

Dorri, A., Kanhere, S. S., & Jurdak, R. (2018). Multi-agent systems: A survey. *IEEE Access*, 6, 28573-28593. https://doi.org/10.1109/ACCESS.2018.2831228

Drăgnoiu, A. E. (2021). Using blockchain technology for software identity maintenance. In: *Proceedings of the 22nd International Middleware Conference: Doctoral Symposium* (S. 25-28). https://doi.org/10.1145/3491087.3493682

Dupont, K. A., Cali, Ü., & Halden, U. (2024). A DLT-based Proof of Concept Marketplace for Trading Guarantees of Origin. In: *Proceedings of the 2024 IEEE Power & Energy Society General Meeting* (S. 1-5). IEEE. https://doi.org/10.1109/PESGM51994.2024.10688931

Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A., & Draheim, D. (2021). Legally enforceable smart-contract languages: A systematic literature review. *ACM Computing Surveys*, 54(5), 1-34. https://doi.org/10.1145/3453475

Ebadi Ansaroudi, Z., Sciarretta, G., De Maria, A., & Ranise, S. (2025). Navigating secure storage requirements for EUDI Wallets: A review paper. *EURASIP Journal on Information Security*, 2025(1), 2. https://doi.org/10.1186/s13635-025-00187-6

EnBW Energie Baden-Württemberg AG (Hrsg.) (2025). Herkunftsnachweis per Blockchain in der Energiewirtschaft. ECO*Journal. *Online verfügbar unter:* https://www.enbw.com/unternehmen/themen/digitalisierung/blockchain.html#sichere-herkunftsnachweise-die-rolle-der-authority-auf-der-blockchain [Abgerufen am 20.06.2025]

energy data-X. (2025). Das Datenökosystem für die Energiewirtschaft. *Online verfügbar unter:* https://www.energydata-x.eu/ [Abgerufen am 01.08.2025]

Energy Track & Trace (2025). About us. Energy Track & Trace. *Online verfügbar unter:* https://energytrackandtrace.com/about/ [Abgerufen am 14.08.2025]

Engineering X (2025). Governance definitions. Engineering X–Safer Complex Systems. *Online verfügbar unter:* https://engineeringx.raeng.org.uk/programmes/safer-complex-systems/safer-governance-of-complex-systems/governance-definitions/ [Abgerufen am 14.08.2025]

ENTSO-E (2022). Views on a Future-Proof Market Design for Guarantees of Origin. ENTSO-E Position Paper. *Online verfügbar unter:* https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Publications/Position%20papers%20and%20reports/2022/entso-e_pp_guarantees_of_origin_220715%20for%20publication.pdf [Abgerufen am 01.08.2025]

ENTSO-E (2025). Common Information Model. *Online verfügbar unter:* https://www.entsoe.eu/digital/common-information-model/ [Abgerufen am 13.08.2025]

Erbguth, J., & Morin, J. H. (2018). Towards governance and dispute resolution for DLT and smart contracts. In: *Proceedings of the 2018 IEEE 9th International Conference on Software Engineering and Service Science* (S. 46-55). IEEE. https://doi.org/10.1109/ICSESS.2018.8663721

Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Applied Sciences*, 15(6), 3225. https://doi.org/10.3390/app15063225

Ernstberger, J., Chaliasos, S., Zhou, L., Jovanovic, P., & Gervais, A. (2024). Do you need a zero knowledge proof?. *Cryptology ePrint Archive*, Paper 2024/050. https://eprint.iacr.org/2024/050

Ernstberger, J., Lauinger, J., Elsheimy, F., Zhou, L., Steinhorst, S., Canetti, R., Miller, A., Gervais, A., & Song, D. (2023). SoK: Data sovereignty. *Cryptology ePrint Archive*, Paper 2023/967. https://eprint.iacr.org/2023/967

Europäische Kommission (2022). Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Digitalisierung des Energiesystems – EU-Aktionsplan. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022DC0552 [Abgerufen am 14.08.2025]

Europäische Kommission (2023). Durchführungsverordnung (EU) 2023/1162 der Kommission vom 6. Juni 2023 über Interoperabilitätsanforderungen und diskriminierungsfreie und transparente Verfahren für den Zugang zu Mess- und Verbrauchsdaten. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1162 [Abgerufen am 14.08.2025]

Europäische Kommission (2024). European Digital Identity – Architecture and Reference Framework. *Online verfügbar unter:* https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.10.0/architecture-and-reference-framework-main/ [Abgerufen am 22.05.2025]

Europäische Kommission (2025a). European Blockchain Services Infrastructure (EBSI). *Online verfügbar unter:* https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home [Abgerufen am 22.05.2025]

Europäische Kommission (2025b). EBSI Projects. *Online verfügbar unter:* https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Make+information+easy+to+verify+and+almost+impossible+to+fake#sec-8 [Abgerufen am 31.07.2025]

Europäische Kommission (2025c). Interoperability layers. *Online verfügbar unter:* https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/3-interoperability-layers [Abgerufen am 27.06.2025]

Europäische Kommission (2025d). Common European data spaces. *Online verfügbar unter:* https://digital-strategy.ec.europa.eu/en/policies/data-spaces [Abgerufen am 27.06.2025]

Europäische Kommission (2025e). Carbon Border Adjustment Mechanism. *Online verfügbar unter:* https://taxation-customs.ec.europa.eu/carbon-border-adjustment-mechanism_en [Abgerufen am 14.08.2025]

Europäische Kommission, Directorate-General for Energy (2025). Renewable hydrogen. *Online verfügbar unter:* https://energy.ec.europa.eu/topics/eus-energy-system/hydrogen/renewable-hydrogen_en [Abgerufen am 20.08.2025]

Europäische Kommission, Directorate-General for Energy, Fraunhofer ISI, Gorenstein Dedecca, J., Ansarin, M., Adsal, K. A., & Blind, K. (2023). Regulatory sandboxes in the energy sector – Final report. Publications Office of the European Union. *Online verfügbar unter:* https://data.europa.eu/doi/10.2833/848065 [Abgerufen am 05.11.2025]

Europäisches Parlament & Rat der Europäischen Union (2022). Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen. Amtsblatt der Europäischen Union L 2464. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2464 [Abgerufen am 14.08.2025]

Europäisches Parlament & Rat der Europäischen Union (2023). Richtlinie (EU) 2023/2413 des Europäischen Parlaments und des Rates vom 18. Oktober 2023 zur Änderung der Richtlinie (EU) 2018/2001, der Verordnung (EU) 2018/1999 und der Richtlinie 98/70/EG im Hinblick auf die Förderung erneuerbarer Energien und zur Aufhebung der Richtlinie (EU) 2015/652. Amtsblatt der Europäischen Union L 2413. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023L2413 [Abgerufen am 14.08.2025]

Europäisches Parlament & Rat der Europäischen Union (2024a). Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit und zur Änderung der Richtlinie (EU) 2019/1937 und der Verordnung (EU) 2023/2859. Amtsblatt der Europäischen Union L 1760. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024L1760 [Abgerufen am 14.08.2025]

Europäisches Parlament & Rat der Europäischen Union (2024b). Verordnung (EU) 2024/1781 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Schaffung eines Rahmens für die Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte, zur Änderung der Richtlinie (EU) 2020/1828 und der Verordnung (EU) 2023/1542 und zur Aufhebung der Richtlinie 2009/125/EG. Amtsblatt der Europäischen Union L 1781. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1781 [Abgerufen am 14.08.2025]

Europäische Union (2017). New European Interoperability Framework. *Online verfügbar unter:* https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf [Abgerufen am 27.06.2025]

Europäische Union (2024). Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität. Amtsblatt der Europäischen Union, L 1183, 30.04.2024. *Online verfügbar unter:* https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401183 [Abgerufen am 22.05.2025]

European Blockchain Services Infrastructure (2022). OpenID Connect – Chapter 6. *Online verfügbar unter:* https://ec.europa.eu/digital-building-blocks/sites/download/attachments/659621351/Chapter%206%20-%20Open%20ID%20Connect.pdf?version=1&modificationDate=1679559942222&api=v2 [Abgerufen am 31.07.2025]

European Blockchain Services Infrastructure (2025). Verifiable Credential Issuance (OIDC4VCI) – EBSI Conformance. *Online verfügbar unter:* https://hub.ebsi.eu/conformance/learn/verifiable-credential-issuance [Abgerufen am 31.07.2025]

European Distributed Data Infrastructure for Energy (2025). About EDDIE. *Online verfügbar unter:* https://eddie.energy/ [Abgerufen am 01.08.2025]

Everspaugh, A., Paterson, K., Ristenpart, T., & Scott, S. (2017). Key rotation for authenticated encryption. In: *Proceedings of the Annual International Cryptology Conference* (S. 98-129). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-63697-9_4

Farrell, E., Minghini, M., Kotsev, A., Soler Garrido, J., Tapsall, B., Micheli, M., Posada Sanchez, M., Signorelli, S., Tartaro, A., Bernal Cereceda, J., Vespe, M., Di Leo, M., Carballa Smichowski, B., Smith, R., Schade, S., Pogorzelska, K., Gabrielli, L., & De Marchi, D. (2023). European Data Spaces – Scientific insights into data sharing and utilisation at scale (EUR 31499 EN). Luxembourg: Publications Office of the European Union. *Online verfügbar unter:* https://doi.org/10.2760/400188 [Abgerufen am 19.07.2025]

Fernández-Iglesias, M. J., Delgado von Eitzen, C., & Anido-Rifón, L. (2024). Efficient Traceability Systems with Smart Contracts: Balancing On-Chain and Off-Chain Data Storage for Enhanced Scalability and Privacy. *Applied Sciences*, 14(23), 11078. https://doi.org/10.3390/app142311078

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution?. *Telecommunications Policy*, 45(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Ferstl, J. (2023). InDEED Allocation Method. FfE München. *Online verfügbar unter:* https://gitlab.com/ffe-munich/indeed-allocation-method [Abgerufen am 14.08.2025]

Fiat, A., & Shamir, A. (1987). How to prove yourself: Practical solutions to identification and signature problems. In: *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques* (S. 186-194). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-47721-7_12

Fisher, M. (2024). Das fehlende Argument im Draghi-Bericht. Tagesspiegel Background: Sustainable Finance. *Online verfügbar unter:* https://background.tagesspiegel.de/finance/briefing/das-fehlende-argument-im-draghi-bericht [Abgerufen am 22.08.2025]

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33, 369-378. https://doi.org/10.1007/s13347-020-00423-6

Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, 58(1), 3-19. https://doi.org/10.1177/0007650317727540

Förderer, K., Lösch, M., Növer, R., Ronczka, M., & Schmeck, H. (2019). Smart meter gateways: Options for a BSI-compliant integration of energy management systems. *Applied Sciences*, 9(8), 1634. https://doi.org/10.3390/app9081634

Forschungsstelle für Energiewirtschaft e. V. (2023). Norwegen und die Doppelvermarktung erneuerbarer Energien. In: Veröffentlichungen. *Online verfügbar unter:* https://www.ffe.de/veroeffentlichungen/norwegen-und-die-doppelvermarktung-erneuerbarer-energien/ [Abgerufen am 14.08.2025]

Fraunhofer-Institut für Angewandte Informationstechnik FIT (2025). DEER – Dezentraler Redispatch. *Online verfügbar unter:* https://deer-projekt.de/ [Abgerufen am 13.08.2025]

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO (2025). BANULA. *Online verfügbar unter:* https://banula.de/ [Abgerufen am 14.08.2025]

Funke, A., Kaltwasser, A., Schmitt, L., Adelhardt, C., Enggaard, C. E., Simon, L., Gaytandjiev, A., von Guttenberg, L., Subiron, S., Matta, J., Nolting, L., & Kranz, T. (2024). Joint Report of the Coalition of the willing on bidirectional charging. *Online verfügbar unter:* https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/P-R/coalition-of-the-willing-on-bidirectional-charging-en.pdf?__blob=publicationFile&v=10 [Abgerufen am 13.08.2025]

Gabriel, P., Künzel, M., Mangelsdorf, A., & Schöllhorn, D. (2024). Standards und Normen für die digitale Sektorenkopplung in Deutschland und Europa – Status quo und Handlungsbedarfe. *Online verfügbar unter:* https://www.iit-berlin.de/wp-content/uploads/2024/09/iit-Studie_digitale-Sektorenkopplung_2024.pdf [Abgerufen am 18.08.2025]

Gaia-X (2025). The Role of Data Spaces in the Digital Economy. *Online verfügbar unter:* https://gaia-x.eu/wp-content/uploads/2025/03/White-Paper_The-Role-of-Data-Spaces-in-the-Digital-Economy-1.pdf [Abgerufen am 07.08.2025]

Gangwal, A., Gangavalli, H. R., & Thirupathi, A. (2023). A survey of Layer-two blockchain protocols. *Journal of Network and Computer Applications*, 209, 103539. https://doi.org/10.1016/j.jnca.2022.103539

Genkin, D., Papadopoulos, D., & Papamanthou, C. (2018). Privacy in decentralized cryptocurrencies. *Communications of the ACM*, 61(6), 78-88. https://doi.org/10.1145/3132696

Gent, E. (2023). Worldcoin launched. Then came the backlash: The globe-spanning cryptocurrency and biometric-identity project has agitated regulators. *Online verfügbar unter:* https://spectrum.ieee.org/worldcoin-2664361259 [Abgerufen am 31.07.2025]

Gerard, H., Puente, E. I. R., & Six, D. (2018). Coordination between transmission and distribution system operators in the electricity sector: A conceptual framework. *Utilities Policy*, 50, 40-48. https://doi.org/10.1016/j.jup.2017.09.011

Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management*, 32(2), e2180. https://doi.org/10.1002/nem.2180

Giussani, G., Steinbuss, S., Prasse, T., & Gras, N. (2024). Data Connector Report (6). International Data Spaces Association. *Online verfügbar unter:* https://doi.org/10.5281/zenodo.13838396 [Abgerufen am 19.07.2025]

Gödde, M., Kaiser, A., Sander, C., Seith, V., Stumpp, M. & Winter, K. (2020). Energy Token Model – Digitales Marktmodell für die Energiewirtschaft. *Online verfügbar unter:* https://it-architecture.enbw.com/theme/files/EnBW-Whitepaper-EnergyTokenModel.pdf [Abgerufen am 01.08.2025]

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. In: *Providing sound foundations for cryptography: On the work of Shafi Goldwasser and Silvio Micali* (S. 203-225). https://doi.org/10.1145/3335741.3335750

Gouriet, M., Barancourt, H., Boust, M., Calvez, P., Laskowski, M., Taillandier, A. S., Tilman, L., Uslar, M., & Warweg, O. (2022). The energy data space: The path to a European approach for energy. In: *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (S. 535-575). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_33

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., & Urbach, N. (2023a). A multivocal literature review of decentralized finance: Current knowledge and future research avenues. *Electronic Markets*, 33(1), 11. https://doi.org/10.1007/s12525-023-00637-4

Gramlich, V., Körner, M.-F., Michaelis, A., Strüker, J. (2023b). SSI in the Energy Sector: A Study. *Online verfügbar unter:* https://eref.uni-bayreuth.de/id/eprint/88642/ [Abgerufen am 20.06.2025]

Gramlich, V., Guggenberger, T., Paetzold, F., Sedlmeir, J., & Strüker, J. (2024). Toward a holistic perspective on blockchain electricity consumption. In: *Proceedings of the International Conference on Information Systems* (Paper-Nr. 2332). https://aisel.aisnet.org/icis2024/blockchain/blockchain/5

Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., & Schofnegger, M. (2021). Poseidon: A new hash function for {Zero-Knowledge} proof systems. In: *Proceedings of the 30th USENIX Security Symposium* (S. 519-535).

Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant block-chains – a systematic literature review. *IEEE Access*, 9, 50593-50606. https://doi.org/10.1109/ACCESS.2021.3069877

Hartner, G., Schmitt, L., Hödl, O., Kashyap, S., & Grünberger, S. (2024). Identification and Authentication in a Common European Data Space (Version 1.0). *Online verfügbar unter:* https://eddie.energy/files/eddie/media/media-library/Identification%20and%20Authentication%20in%20a%20Common%20European%20Data%20Space_v1.0.pdf [Abgerufen am 27.06.2025]

Harwood-Jones, M. (2019). Digital and crypto-assets: Tracking global adoption rates and impacts on securities services. *Journal of Securities Operations & Custody*, 12(1), 49-57. https://doi.org/10.69554/RZIL3872

Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., & Raza, A. (2023). From trust to truth: Advancements in mitigating the Blockchain Oracle problem. *Journal of Network and Computer Applications*, 217, 103672. https://doi.org/10.1016/j.jnca.2023.103672

Haun, K. (2025). Stablecoins can support financial safety. *Online verfügbar unter:* https://www.ft.com/content/3c06170c-0d03-4838-a5b8-f58a07715f20 [Abgerufen am 21.08.2025]

d'Hauwers, R., Walravens, N., & Ballon, P. (2022). Data ecosystem business models: Value and control in data ecosystems. *Journal of Business Models*, 10(2), 1-30. https://doi.org/10.54337/jbm.v10i2.6946%0A

Heeß, P., Rockstuhl, J., Körner, M. F., & Strüker, J. (2024). Enhancing trust in global supply chains: Conceptualizing Digital Product Passports for a low-carbon hydrogen market. *Electronic Markets*, 34(1), 10. https://doi.org/10.1007/s12525-024-00690-7

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 177, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Holzapfel, P. K., Bánk, J., Bach, V., & Finkbeiner, M. (2024). Relevance of guarantees of origin for Europe's renewable energy targets. *Renewable and Sustainable Energy Reviews*, 205, 114850. https://doi.org/10.1016/j.rser.2024.114850

Höß, A., Roth, T., Sedlmeir, J., Fridgen, G., & Rieger, A. (2022). With or without Blockchain? Towards a decentralized, SSI-based eRoaming architecture. In: *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*. http://hdl.handle.net/10125/79899

van Houwelingen, G., van Bommel, J., Gilsing, R., Lamerichs, G., & Berkers, F. (2024). Unlocking the Potential of Data Spaces – Critical Success Factors for Data Space Deployment. Centre of Excellence for Data

Sharing & Cloud (TNO). *Online verfügbar unter:* https://coe-dsc.nl/wp-content/uploads/2024/03/COEDSC-Whitepaper-success-factors-of-data-spaces.pdf [Abgerufen am 21.08.2025]

Huang, H., Lin, J., Zheng, B., Zheng, Z., & Bian, J. (2020). When blockchain meets distributed file systems: An overview, challenges, and open issues. *IEEE Access*, 8, 50574-50586. https://doi.org/10.1109/ACCESS.2020.2979881

Hühnlein, T., Hühnlein, D., Schwalm, S., & Stöcker, C. (2025). Towards the European Business Wallet. In: *Proceedings of the Open Identity Summit 2025 (pp. 127–141).* Bonn: Gesellschaft für Informatik e.V. https://doi.org/10.18420/oid2025_09

Hussain, J., Han, Y., Huang, Q., Wang, C., Hussain, F., & Ahmed, S. A. (2025). A fully decentralized prosumer-centric peer-to-peer energy trading of photovoltaic and battery energy for social welfare maximization considering system voltage constraints. *Renewable Energy*, 123000. https://doi.org/10.1016/j.renene.2025.123000

International Data Spaces e. V. (2024). Dataspace Protocol 2024-1. *Online verfügbar unter:* https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol [Abgerufen am 27.06.2025]

International Data Spaces e. V. (2025). Let's Get Real: The IDS Reference Architecture Model. *Online verfügbar unter:* https://internationaldataspaces.org/offers/reference-architecture/ [Abgerufen am 27.06.2025]

ISO (2023). ISO/TS 19870:2023 Hydrogen technologies – Methodology for determining the greenhouse gas emissions associated with the production, conditioning and transport of hydrogen to consumption gate. *Online verfügbar unter:* https://www.iso.org/standard/65628.html [Abgerufen am 20.08.2025]

Jeyakumar, I. H. J., & Kubach, M. (2025). A trust implementation model for cross-domain decentralized identity ecosystems: architecture, use case, and implementation. *Procedia Computer Science*, 254, 10-19. https://doi.org/10.1016/j.procs.2025.02.059

Jibril, H. & Roper, S. (2025). Factors influencing firms' adoption of advanced technologies: A rapid evidence review. Department for Science, Innovation and Technology (DSIT). *Online verfügbar unter:* https://www.gov.uk/government/publications/barriers-and-enablers-to-advanced-technology-adoption-for-uk-businesses/factors-influencing-firms-adoption-of-advanced-technologies-a-rapid-evidence-review [Abgerufen am 26.08.2025]

Jiménez, S. (2025). Interoperability framework in energy data spaces. International Data Spaces Association. https://doi.org/10.5281/zenodo.15041231

Jokumsen, M., Pedersen, T. P., Daugaard, M. S., Tschudi, D., Madsen, M. W., & Wisbech, T. (2023). Verifiable proofs for the energy supply chain: small proofs brings you a long way. *Energy Informatics*, 6 (Suppl 1), 28. https://doi.org/10.1186/s42162-023-00283-2

Jøsang, A., & Pope, S. (2005). User centric identity management. In: *AusCERT Asia Pacific information Technology Security Conference* (Vol. 22, S. 2005). https://www.academia.edu/download/30355451/10.1.1.60.1563.pdf

Jurmu, M., Niskanen, I., Kinnula, A., Kääriäinen, J., Ylikerälä, M., Räsänen, P., & Tuikka, T. (2023). Exploring the role of federated data spaces in implementing twin transition within manufacturing ecosystems. *Sensors*, 23(9), 4315. https://doi.org/10.3390/s23094315

Kalt, G., Kabinger, A., & Materazzi-Wagner, C. (2024). The Network Code Demand Response: Implications for the Procurement of System Operator Services in Austria. In: *18. Symposium Energieinnovation* (S. 1–15). *Online verfügbar unter:* https://www.tugraz.at/fileadmin/user_upload/tugrazExternal/f560810f-089d-42d8-ae6d-8e82a8454ca9/files/lf/Session_B1/214_LF_Kalt.pdf [Abgerufen am 14.08.2025]

Kelkar, S. (2018). Engineering a platform: The construction of interfaces, users, organizational roles, and the division of labor. *New Media & Society*, 20(7), 2629-2646. https://doi.org/10.1177/1461444817728682

Kenchakkanavar, A. Y. (2015). Facebook and Twitter for academic libraries in the twenty first century. *International Research: Journal of Library and Information Science*, 5(1).

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, 14(5), 2901-2925. https://doi.org/10.1007/s12083-021-01127-0

Khanfar, A. A., Iranmanesh, M., Ghobakhloo, M., Senali, M. G., & Fathi, M. (2021). Applications of blockchain technology in sustainable manufacturing and supply chain management: A systematic review. *Sustainability*, 13(14), 7870. https://doi.org/10.3390/su13147870

Khayretdinova, A., Kubach, M., Sellung, R., & Roßnagel, H. (2022). Conducting a usability evaluation of decentralized identity management solutions. In: *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg* (S. 389-406). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-33306-5_19

Kilthau, M., Asman, M., Karmann, A., Suriyamoorthy, G., Beck, J. P., Regener, V., Derksen, C., Loose, N., Volkmann, M., Tripathi, S., Gehlhoff, F., Korotkiewicz, K., Steinbusch, P., Skwarek, V., Zdrallek, M., & Fay, A. (2023). Integrating peer-to-peer energy trading and flexibility market with self-sovereign identity for decentralized energy dispatch and congestion management. *IEEE Access*, 11, 145395-145420. https://doi.org/10.1109/ACCESS.2023.3344855

Kim, G., Park, J., & Ryou, J. (2018). A study on utilization of blockchain for electricity trading in microgrid. In: *Proceedings of the 2018 IEEE International Conference on Big Data and Smart Computing* (S. 743-746). IEEE. https://doi.org/10.1109/BigComp.2018.00141

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, 158, 112013. https://doi.org/10.1016/j.rser.2021.112013

Körner, M.-F., Nolting, L., Babel, M., Ehaus, M., Heeß, P., Lautenschlager, J., Radtke, M., Schick, L., Strüker, J., Wiedemann, S., & Zwede, T. (2024a). A digital infrastructure for integrating decentralized assets into redispatch. In: *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik* (Nr. 70). https://doi.org/10.15495/EPub_UBT_00008184

Körner, M.-F., Paetzold, F., Ströher, T., & Strüker, J. (2024b). Digital proofs of origin for sustainability: Assessing a digital identity-based approach in the energy sector. In: *Fraunhofer Publica*. https://doi.org/10.24406/publica-3224

Körner, M. F., Leinauer, C., Ströher, T., & Strüker, J. (2025). Digital Measuring, Reporting, and Verification (dMRV) for Decarbonization. *Business & Information Systems Engineering*, 1-13. https://doi.org/10.1007/s12599-025-00953-3

Kovacova, M., Horak, J., & Higgins, M. (2022). Behavioral analytics, immersive technologies, and machine vision algorithms in the Web3-powered Metaverse world. *Linguistic and Philosophical Investigations*, 21, 57-72.

Krämer, J., & Shekhar, S. (2025). Regulating digital platform ecosystems through dat sharing and data siloing: Consequences for innovation and welfare. *MIS Quarterly*, 49(1). https://doi.org/10.25300/MISQ/2024/18428

Kraemer, P., Niebel, C., & Reiberg, A. (2022). Was ist ein Datenraum. Gaia-X Hub Germany. *Online verfügbar unter:* https://gaia-x-hub.de/wp-content/uploads/2022/10/20220914_White_Paper_22.1_Definition_Datenraum_final.pdf [Abgerufen am 12.07.2025]

Krause, D. (2024). Web3 and the Decentralized Future: Exploring Data Ownership, Privacy, and Blockchain Infrastructure. *Online verfügbar unter:* https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5064483 [Abgerufen am 12.05.2025]

Kroener, N., Förderer, K., Lösch, M., & Schmeck, H. (2020). State-of-the-art integration of decentralized energy management systems into the German smart meter gateway infrastructure. *Applied Sciences*, 10(11), 3665. https://doi.org/10.3390/app10113665

Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using Block-chain and IPFS: A comparative analysis with future directions. *Security and Privacy*, 4(5), e162. https://doi.org/10.1002/spy2.162

Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. *International Journal of Computer Network & Information Security*, 13(2), 1-15. https://doi.org/10.5815/ijcnis.2021.02.01

Lamichhane, S., & Herbke, P. (2024). Verifiable Decentralized IPFS Cluster: Unlocking Trustworthy Data Permanency for Off-Chain Storage. In: *Proceedings of the 2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services* (S. 1-4). IEEE. https://doi.org/10.1109/BRAINS63024.2024.10732266

Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, 9, 43620-43652. https://doi.org/10.1109/ACCESS.2021.3065880

Leinauer, C., Körner, M.-F., & Strüker, J. (2022). Toward net 0: Digital CO_2 proofs for the sustainable transformation of the European economy. In: *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik* (Nr. 65). https://doi.org/10.15495/EPub_UBT_00006827

Leinauer, C., Wagon, F., & Strüker, J. (2024). Leveraging Twin Transformation – Digital Infrastructures to Advance Decarbonisation at the Nexus of Energy and Mobility. *Online verfügbar unter:* https://ec.europa.eu/newsroom/dae/redirection/document/107166 [Abgerufen am 21.08.2025]

Li, F., Turvey, N., Dale, L., Scott, J., Padget, J., Flower, I., Fitzpatrick, J. R., Ostler, N., Oldaker, R., & Yeo, S. (2025). Do we need a data sharing infrastructure for the energy sector?. *IET Smart Grid*, 8(1), e12196. https://doi.org/10.1049/stg2.12196

Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in Construction*, 102, 288-307. https://doi.org/10.1016/j.autcon.2019.02.005

Li, J., Tong, W., Yang, L., Gao, X., Dong, Z., & Wang, C. (2024). Blockchain and Oracle-Driven Web3 Architecture for Data Interaction. In: *Proceedings of the 2024 International Conference on Networking and Network Applications* (S. 333-338). IEEE. https://doi.org/10.1109/NaNA63151.2024.00062

Li, W., Guo, H., Nejad, M., & Shen, C. C. (2020). Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. *IEEE Access*, 8, 181733-181743. https://doi.org/10.1109/ACCESS.2020.3028189

Lin, Q., Li, C., Zhao, X., & Chen, X. (2021). Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities. In: *Proceedings of the 2021 IEEE 37th International Conference on Data Engineering Workshops* (S. 80-87). IEEE. https://doi.org/10.1109/ICDEW53142.2021.00022

Liu, C., & Li, Z. (2021). Comparison of centralized and peer-to-peer decentralized market designs for community markets. *IEEE Transactions on Industry Applications*, 58(1), 67-77. https://doi.org/10.1109/TIA.2021.3119559

Liu, Y., Lu, Q., Zhu, L., Paik, H. Y., & Staples, M. (2023). A systematic literature review on blockchain governance. *Journal of Systems and Software*, 197, 111576. https://doi.org/10.1016/j.jss.2022.111576

Llorca, M., Soroush, G., Giovannetti, E., Jamasb, T., & Davi-Arderius, D. (2024). Energy Sector Digitalisation, Green Transition and Regulatory Trade-offs. Copenhagen Business School, CBS. Working Paper / Department of Economics. Copenhagen Business School No. 05-2024, CSEI Working Paper No. 03-2024. *Online verfügbar unter:* https://research.cbs.dk/en/publications/innovation-by-regulation-smart-electricity-grids-in-the-uk-and-it-2 [Abgerufen am 07.08.2025]

Luecking, M., Fries, C., Lamberti, R., & Stork, W. (2020). Decentralized identity and trust management framework for Internet of Things. In: *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency* (S. 1-9). IEEE. https://doi.org/10.1109/ICBC48266.2020.9169411

Lukasik, S. (2010). Why the Arpanet was built. *IEEE Annals of the History of Computing*, 33(3), 4-21. https://doi.org/10.1109/MAHC.2010.11

Lund, P. D., Lindgren, J., Mikkola, J., & Salpakari, J. (2015). Review of energy system flexibility measures to enable high levels of variable renewable electricity. *Renewable and Sustainable Energy Reviews*, 45, 785-807. https://doi.org/10.1016/j.rser.2015.01.057

Maleki, N., Padmanabhan, B., & Dutta, K. (2024). AI hallucinations: a misnomer worth clarifying. In: *Proceedings of the 2024 IEEE Conference on Artificial Intelligence* (S. 133-138). IEEE. https://doi.org/10.1109/CAI59869.2024.00033

Maler, E., & Reed, D. (2008). The venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy*, 6(2), 16-23. https://doi.org/10.1109/MSP.2008.50

Malta Digital Innovation Authority (2025). Fostering Trust in Innovative Technologies. *Online verfügbar unter:* https://mdia.gov.mt/ [Abgerufen am 03.08.2025]

Marty, F. M., & Warin, T. (2020). Digital Platforms' Information Concentration: From Keystone Players to Gatekeepers. *Online verfügbar unter:* https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3753779 [Abgerufen am 28.04.2025]

Mataczyńska, E., Martí Rodríguez, J., van der Heijden, S., Kula, J., & Voumvoulakis, M. (2022). The Road Map on Go4Flex – Grid observability for Flexibility. *Online verfügbar unter:* https://www.edsoforsmartgrids.eu/content/uploads/2024/05/20220513_TF1_ANM_-_Go4Flex_Report.pdf [Abgerufen am 21.08.2025]

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials.* https://doi.org/10.1109/COMST.2025.3543197

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology*, 21(1), 19-32. https://doi.org/10.4018/JCIT.2019010102

Menati, A., Lee, K., & Xie, L. (2023). Modeling and analysis of utilizing cryptocurrency mining for demand flexibility in electric energy systems: A synthetic texas grid case study. *IEEE Transactions on Energy Markets, Policy and Regulation*, 1(1), 1-10. https://doi.org/10.1109/TEMPR.2022.3230953

Mičijević, A. (2025). „Genius Act" sorgt für Krypto-Goldgräberstimmung. Handelsblatt. *Online verfügbar unter:* https://www.handelsblatt.com/audio/today/today-genius-act-sorgt-fuer-krypto-goldgraeberstimmung/100142669.html [Abgerufen am 18.08.2025]

Monetary Authority of Singapore (2024). Global Layer One – Foundation Layer for Financial Networks. *Online verfügbar unter:* https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/guardian/gl1---whitepaper.pdf [Abgerufen am 03.08.2025]

Monti, A., Schmitt, L., Dognini, A., Bessa, R., Boskov-Kovacs, E., Hartner, G., Tsitsanis, T., Diakakis, S., Gallego Amores, S., Damas Silva, C., & Samovich, N. (2023). Energy Data Space Policy Paper. ETIP SNET. *Publications Office of the European Union*. https://doi.org/10.2833/586947

Morrison, R., Mazey, N. C., & Wingreen, S. C. (2020). The DAO controversy: the case for a new species of corporate governance?. *Frontiers in Blockchain*, 3, 25. https://doi.org/10.3389/fbloc.2020.00025

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80-86. https://doi.org/10.1016/j.cosrev.2018.10.002

Mulligan, C., Morsfield, S., & Cheikosman, E. (2024). Blockchain for sustainability: A systematic literature review for policy impact. *Telecommunications Policy*, 48(2), 102676. https://doi.org/10.1016/j.telpol.2023.102676

Murugesan, S. (2007). Understanding Web 2.0. *IT Professional*, 9(4), 34-41. https://doi.org/10.1109/MITP.2007.78

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Online verfügbar unter:* https://assets.pubpub.org/d8wct41f/31611263538139.pdf [Abgerufen am 03.04.2025]

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.

Nath, K., Dhar, S., & Basishtha, S. (2014). Web 1.0 to Web 3.0-Evolution of the Web and its various challenges. In: *Proceedings of the 2014 International Conference on Reliability Optimization and Information Technology* (S. 86-89). IEEE. https://doi.org/10.1109/ICROIT.2014.6798297

Netztransparenz.de (2025). Veröffentlichungspflichten gemäß EU-Transparenzverordnung. *Online verfügbar unter:* https://www.netztransparenz.de/de-de/%C3%9Cber-uns/Informationsplattformen/Ver%C3%B6ffentlichungspflichten-gem%C3%A4%C3%9F-EU-%20Transparenzverordnung [Abgerufen am 28.04.2025]

Norddeutsches Reallabor (2025). Sektorenkopplung – von der Strom- zur Energiewende. *Online verfügbar unter:* https://norddeutsches-reallabor.de/ [Abgerufen am 27.08.2025]

Okwuibe, G. C., Li, Z., Brenner, T., & Langniss, O. (2020). A blockchain based electric vehicle smart charging system with flexibility. *IFAC PapersOnLine*, 53(2), 13557-13561. https://doi.org/10.1016/j.ifacol.2020.12.800

de Oliveira, N. R., dos Santos, Y. D. R., Barbosa, G. N., Reis, L. H. A., Mendes, A. C. R., de Oliveira, M. T., de Medeiros, D. S. V., Mattos, D. M. (2024). Distributed Data Security in Digital Health: Self-Sovereign Identity, Access Control, and Blockchain-based Log Records. In: *Proceedings of the 2024 6th International Conference on Blockchain Computing and Applications* (S. 558-565). IEEE. https://doi.org/10.1109/BCCA62388.2024.10844453

Omelchenko, D. (2025). What to know about IOTA's Rebased upgrade: Deprecated Firefly wallets, changes in validator tokenomics. Crypto.news. *Online verfügbar unter:* https://crypto.news/what-to-know-about-iotas-rebased-upgrade/ [Abgerufen am 22.05.2025]

OneNet (2023). OneNet Connector included in the IDSA Data Connector Report. *Online verfügbar unter:* https://www.onenet-project.eu/onenet-connector-included-in-the-idsa-data-connector-report/ [Abgerufen am 27.06.2025]

Otto, B. (2022). The evolution of data spaces. In: *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (S. 3-15). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_1

Parameswarath, R. P., Gope, P., & Sikdar, B. (2022). User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential. *ACM Transactions on Management Information Systems*, 13(4), 1-21. https://doi.org/10.1145/3532869

Parhamfar, M., Sadeghkhani, I., & Adeli, A. M. (2024). Towards the net zero carbon future: A review of blockchain-enabled peer-to-peer carbon trading. *Energy Science & Engineering*, 12(3), 1242-1264. https://doi.org/10.1002/ese3.1697

Park, C. S., & Nam, H. M. (2021). A new approach to constructing decentralized identifier for secure and flexible key rotation. *IEEE Internet of Things Journal*, 9(13), 10610-10624. https://doi.org/10.1109/JIOT.2021.3121722

Patel, K. (2013). Incremental journey for World Wide Web: introduced with Web 1.0 to recent Web 5.0 – A survey paper. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(10). https://api.semanticscholar.org/CorpusID:267831946

Pebbles (2025). Projekt – Pebbles Projekt. *Online verfügbar unter:* https://pebbles-projekt.de/projekt/ [Abgerufen am 22.08.2025]

Pettenpohl, H., Spiekermann, M., & Both, J.R. (2022). International Data Spaces in a Nutshell. In: *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (S. 29-40). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_3

Preukschat, A., & Reed, D. (2021). Why the internet is missing an identity layer – and why SSI can finally provide one. In: A. *Preukschat & D. Reed (Hrsg.), Self-sovereign identity: Decentralized Digital Identity and Verifiable Credentials* (S. 3–20). Shelter Island, NY: Manning Publications.

Principato, M., Babel, M., Guggenberger, T., Kropp, J., & Mertel, S. (2023). Towards solving the block-chain trilemma: An exploration of zero-knowledge proofs. In: *Proceedings of the International Conference on Information Systems* (Paper-Nr. 2435). https://aisel.aisnet.org/icis2023/blockchain/blockchain/5

Protocol Labs (2017). Filecoin: A Decentralized Storage Network. *Online verfügbar unter:* https://filecoin.io/filecoin.pdf [Abgerufen am 18.05.2025]

Protocol Labs (2021). Merkle Directed Acyclic Graphs (DAGs). *Online verfügbar unter:* https://docs.ipfs.io/concepts/merkle-dag/ [Abgerufen am 18.05.2025]

Protocol Labs (2025). IPFS KPIs. *Online verfügbar unter:* https://probelab.io/ipfs/kpi/ [Abgerufen am 02.08.2025].

Publications Office of the European Union (2024). EU's Digital Product Passport: Advancing transparency and sustainability. *Online verfügbar unter:* https://data.europa.eu/en/news-events/news/eus-digital-product-passport-advancing-transparency-and-sustainability [Abgerufen am 20.08.2025]

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive*, 18(4). https://doi.org/10.17705/2msqe.00020

Roth, T., Utz, M., Baumgarte, F., Rieger, A., Sedlmeir, J., & Strüker, J. (2022). Electricity powered by blockchain: A review with a European perspective. *Applied Energy*, 325, 119799. https://doi.org/10.1016/j.apenergy.2022.119799

Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, 7, 50759-50779. https://doi.org/10.1109/ACCESS.2019.2911031

Rülicke, L., Fehrle, F., Martin, A., Monti, A., Berkhout, V., Warweg, O., & Möller, S. (2024). Exploring decentralized data management: A case study of changing energy suppliers in Germany. *Energy Informatics*, 7(1), 8. https://doi.org/10.1186/s42162-024-00315-5

Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (PoS) and delegated proof of stake (DPoS). *International Journal of Innovative Computing*, 10(2). https://doi.org/10.11113/ijic.v10n2.272

Saeed, N., Wen, F., & Afzal, M. Z. (2024). Decentralized peer-to-peer energy trading in microgrids: Leveraging blockchain technology and smart contracts. *Energy Reports*, 12, 1753–1764. https://doi.org/10.1016/j.egyr.2024.07.053 [Abgerufen am 14.08.2025]

Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*, 58(4), 102584. https://doi.org/10.1016/j.ipm.2021.102584

de Salve, A., Maesa, D. D. F., Mori, P., Ricci, L., & Puccia, A. (2023). A multi-layer trust framework for Self Sovereign Identity on blockchain. *Online Social Networks and Media*, 37, 100265. https://doi.org/10.1016/j.osnem.2023.100265

Sánchez Molina, P. (2025). Spanischer Netzbetreiber REE: Ursache für Stromausfall war Photovoltaik-Anlage in Badajoz. pv magazine. *Online verfügbar unter:* https://www.pv-magazine.de/2025/06/18/spanischer-netzbetreiber-ree-ursache-fuer-stromausfall-war-photovoltaik-anlage-in-badajoz/ [Abgerufen am 14.08.2025]

Santana, C., & Albareda, L. (2022). Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. *Technological Forecasting and Social Change*, 182, 121806.

Schaaf, J. (2025). From hype to hazard: what stablecoins mean for Europe. *Online verfügbar unter:* https://www.ecb.europa.eu/press/blog/date/2025/html/ecb.blog20250728~e6cb3cf8b5.en.html [Abgerufen am 22.08.2025]

Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, 22(15), 5641. https://doi.org/10.3390/s22155641

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets*, 34(1), 15. https://doi.org/10.1007/s12525-024-00693-4

Schleimer, A. M., Lobig, T., Theissen, N., Pospischil, F., Dörr, S., Wang, D., Bendiek, K., & Koretskaia, D. (2024). Gaia-X 4 KI Whitepaper Datenräume: Vertrauenswürdige Daten- und Diensteökosysteme. *Online verfügbar unter:* https://www.isst.fraunhofer.de/content/dam/isst/publikationen/mobility-and-smart-cities/Gaia-x%204%20KI_Whitepaper_final.pdf [Abgerufen am 18.07.2025]

Schletz, M., Constant, A., Hsu, A., Schillebeeckx, S., Beck, R., & Wainstein, M. (2023). Blockchain and regenerative finance: Charting a path toward regeneration. *Frontiers in Blockchain*, 6, 1165133. https://doi.org/10.3389/fbloc.2023.1165133

Schukat, M., & Cortijo, P. (2015). Public key infrastructures and digital certificates for the Internet of things. In: *Proceedings of the 2015 26th Irish Signals and Systems Conference* (S. 1-5). IEEE. https://doi.org/10.1109/ISSC.2015.7163785

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6), 599-608. https://doi.org/10.1007/s12599-020-00656-x

Sedlmeir, J., Huber, J., Barbereau, T. J., Weigl, L., & Roth, T. (2022). Transition pathways towards design principles of self-sovereign identity. In: *Proceedings of the 43rd International Conference on Information Systems* (Paper-Nr. 1442). https://aisel.aisnet.org/icis2022/is_implement/is_implement/4

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, 63(5), 603-613. https://doi.org/10.1007/s12599-021-00722-y

Seshasai, B., Koley, E., & Ghosh, S. (2025). Blockchain for secure and decentralized power system operation in smart grid systems. In: *Proceedings of the Fourth International Conference on Power, Control and Computing Technologies* (S. 1–5). IEEE. https://doi.org/10.1109/ICPC2T63847.2025.10958672

Shen, J., Li, Y., Zhou, Y., & Wang, X. (2019). Understanding I/O performance of IPFS storage: a client's perspective. In: *Proceedings of the International Symposium on Quality of Service* (S. 1-10). https://doi.org/10.1145/3326285.3329052

Sheridan, D., Harris, J., Wear, F., Cowell Jr, J., Wong, E., & Yazdinejad, A. (2022). Web3 challenges and opportunities for the market. *Online verfügbar unter:* https://arxiv.org/pdf/2209.02446 [Abgerufen am 12.05.2025]

Shi, R., Cheng, R., Fu, Y., Han, B., Cheng, Y., & Chen, S. (2025). Centralization in the Decentralized Web: Challenges and Opportunities in IPFS Data Management. In: *Proceedings of the ACM on Web Conference 2025* (S. 4068-4076). https://doi.org/10.1145/3696410.3714627

Shi, R., Cheng, R., Han, B., Cheng, Y., & Chen, S. (2024). A closer look into IPFS: Accessibility, content, and performance. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 8(2), 1-31. https://doi.org/10.1145/3656015

Shibano, K., Ito, K., Han, C., Chu, T. T., Ozaki, W., & Mogi, G. (2024). Secure Processing and Distribution of Data Managed on Private InterPlanetary File System Using Zero-Knowledge Proofs. *Electronics*, 13(15). https://doi.org/10.3390/electronics13153025

Shobanke, M., Bhatt, M., & Shittu, E. (2025). Advancements and future outlook of Artificial Intelligence in energy and climate change modeling. *Advances in Applied Energy*, 100211. https://doi.org/10.1016/j.adapen.2025.100211

Silvano, W. F., & Marcelino, R. (2020). Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Generation Computer Systems*, 112, 307-319. https://doi.org/10.1016/j.future.2020.05.047

Sockin, M., & Xiong, W. (2023). Decentralization through tokenization. *The Journal of Finance*, 78(1), 247-299. https://doi.org/10.1111/jofi.13192

Solat, S. (2024). Fallacies of blockchain. In: *Proceedings of the 6th International Conference on Blockchain Computing and Applications* (S. 654-668). IEEE. https://doi.org/10.1109/BCCA62388.2024.10844427

Solat, S., Calvez, P., & Naït-Abdesselam, F. (2021). Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *Journal of Software*, 16(3), 95-106. https://doi.org/10.17706/jsw.16.3.95-106

Sonmez, R., Sönmez, F. Ö., & Ahmadisheykhsarmast, S. (2023). Blockchain in project management: a systematic review of use cases and a design decision framework. *Journal of Ambient Intelligence and Humanized Computing*, 1-15. https://doi.org/10.1007/s12652-021-03610-1

Sporny, M., Longley, D., Chadwick, D., Allen, C., & Grant, R. (2022). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. World Wide Web Consortium (W3C). *Online verfügbar unter:* https://www.w3.org/TR/did-1.0/ [Abgerufen am 15.05.2025]

Steinbuss, S., van den Berg, W., Berwanger, S. G., Bilbao Arechabala, S., Fernandez, I., Gil Inchaurza, G. P., Klinker, P., Lähteenoja, V., Müller, A., Stornebrink, M., & Turkmayali, A. (2024). Semantic Interoperability in Data Spaces. International Data Spaces Association. *Online verfügbar unter:* https://doi.org/10.5281/zenodo.10964377 [Abgerufen am 18.07.2025]

Steinschaden, J. (2021). Riddle & Code tokenisiert mit Wien Energie die größte Solaranlage Österreichs. *Online verfügbar unter:* https://www.trendingtopics.eu/riddle-code-tokenisiert-mit-wien-energie-die-groesste-solaranlage-oesterreichs/ [Abgerufen am 20.08.2025]

Stetter, D., Höpfer, T., Schmid, M., Sturz, I., Falkenberger, S., & Knoll, N. (2024). BANULA – A Novel DLT-Based Approach for EV Charging with High Level of User Comfort and Role-Specific Data Transparency for All Parties Involved. *World Electric Vehicle Journal*, 15(3), 79. https://doi.org/10.3390/wevj15030079

Stöcker, C. (2025). Identity & Trust. Energy data-X. *Online verfügbar unter:* https://www.energydata-x.eu/wp-content/uploads/2025/03/OnePager_06_Identity_Trust_03-2025.pdf [Abgerufen am 24.06.2025]

Storj Labs Inc. (2024). Storj: A decentralized cloud storage network framework. *Online verfügbar unter:* https://static.storj.io/storjv3.pdf [Abgerufen am 02.08.2025].

Strnadl, C. F., & Schöning, H. (2023). Datenplattformen, Datenräume und (Daten-) Ökosysteme – Einordnung und strategische Aspekte. In: *Data Governance: Nachhaltige Geschäftsmodelle und Technologien im europäischen Rechtsrahmen* (S. 83-103). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-67556-4_2

Strüker, J. (2019). Technisches und Ökonomisches Gutachten im Rahmen der Multi-Stakeholder-Studie „Blockchain in der integrierten Energiewende“ der Deutschen Energie-Agentur. O*nline verfügbar unter:* https://www.dena.de/newsroom/publikationsdetailansicht/pub/blockchain-in-der-integrierten-energiewende/) [Abgerufen am 03.09.2025]

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F. (2021a). Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth. *Online verfügbar unter:* https://eref.uni-bayreuth.de/id/eprint/66090/ [Abgerufen am 24.06.2025]

Strüker, J., Weibelzahl, M., Körner, M.-F., Kießling, A., Franke-Sluijk, A., & Hermann, M. (2021b). Dekarbonisierung durch Digitalisierung: Thesen zur Transformation der Energiewirtschaft. In: *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik* (Nr. 67). https://doi.org/10.15495/EPub_UBT_00005596

Su, C., & Tang, W. (2023). Data sovereignty and platform neutrality – A comparative study on TikTok’s data policy. *Global Media and China*, 8(1), 57-71. https://doi.org/10.1177/20594364231154340

Su, Y., Wu, J., Long, C., & Wei, L. (2020). Secure decentralized machine identifiers for Internet of Things. In: *Proceedings of the 2020 2nd International Conference on Blockchain Technology* (S. 57-62). https://doi.org/10.1145/3390566.3391670

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network*, 35(4), 198-205. https://doi.org/10.1109/MNET.011.2000473

Tan, Z., Guo, A., & Arunachalam, N. (2023). The Emperor's New Clothes or the Next Big Thing? – Web3 Applications in Real Estate Decarbonization. In: *MIT Center for Real Estate Research Papers* (Nr. 23/16). https://dx.doi.org/10.2139/ssrn.4508114

Tariq, A. H., & Amin, U. (2025). Peer-to-peer multi-energy trading in a decentralized network: A review. *Renewable and Sustainable Energy Reviews*, 208, 114969. https://doi.org/10.1016/j.rser.2024.114969

Thibault, L. T., Sarry, T., & Hafid, A. S. (2022). Blockchain scaling using rollups: A comprehensive survey. *IEEE Access*, 10, 93039-93054. https://doi.org/10.1109/ACCESS.2022.3200051

Tikhomirov, S. (2017). Ethereum: state of knowledge and research perspectives. In: *International Symposium on Foundations and Practice of Security* (S. 206-221). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-75650-9_14

Tiwari, K., & Kumar, S. (2025). A healthcare data management system: Blockchain-enabled IPFS providing algorithmic solutions for increased privacy-preserving scalability and interoperability. *The Journal of Supercomputing*, 81(8), 895. https://doi.org/10.1007/s11227-025-07400-w

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. The Sovrin Foundation. *Online verfügbar unter:* https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf [Abgerufen am 18.06.2025]

Torres, J., Nogueira, M., & Pujolle, G. (2012). A survey on identity management for the future network. *IEEE Communications Surveys & Tutorials*, 15(2), 787-802. https://doi.org/10.1109/SURV.2012.072412.00129

Trautwein, D., Raman, A., Tyson, G., Castro, I., Scott, W., Schubotz, M., Gipp, B., & Psaras, Y. (2022). Design and evaluation of IPFS: A storage layer for the decentralized web. In: *Proceedings of the ACM SIGCOMM 2022 Conference* (S. 739-752). https://doi.org/10.1145/3544216.3544232

Trevisan, R., Ghiani, E., Galici, M., Mocci, S., & Pilo, F. (2025). Transactive Energy Systems in Decentralized Autonomous Renewable Energy Communities. In: *Smart Cyber – Physical Power Systems: Fundamental Concepts, Challenges, and Solutions*, 1(23), 597-615. https://doi.org/10.1002/9781394191529.ch23

Tristán, A., Heuberger, F., & Sauer, A. (2020). A methodology to systematically identify and characterize energy flexibility measures in industrial systems. *Energies*, 13(22), 5887. https://doi.org/10.3390/en13225887

Umweltbundesamt (2019). Herkunftsnachweisregister für Strom aus erneuerbaren Energien. Umweltbundesamt. *Online verfügbar unter:* https://www.umweltbundesamt.de/sites/default/files/medien/372/dokumente/herkunftsnachweisregister_20190715.pdf [Abgerufen am 14.08.2025]

Umweltbundesamt (2025a). Berichte aus den Workshops zur 7. HKNR-Fachtagung vom 02.04.2025. *Online verfügbar unter:* https://www.umweltbundesamt.de/sites/default/files/medien/14292/dokumente/tag_1_workshops.pdf [Abgerufen am 14.08.2025]

Umweltbundesamt (2025b). Workshop 1: Potenzial einer integrierten Digitalisierung der Register und HKNR-Prozesse. *Online verfügbar unter:* https://www.umweltbundesamt.de/sites/default/files/medien/14292/dokumente/tag1ws-1_merkel_theuerkorn.pdf [Abgerufen am 14.08.2025]

Umweltbundesamt (2025c). Aktuelle Informationen zum HKNR. *Online verfügbar unter:* https://www.umweltbundesamt.de/sites/default/files/medien/14292/dokumente/tag1_2_theuerkorn_mohrbach.pdf [Abgerufen am 14.08.2025]

Umweltbundesamt (2025d). Der Europäische Emissionshandel. *Online verfügbar unter:* https://www.umweltbundesamt.de/daten/klima/der-europaeische-emissionshandel#teilnehmer-prinzip-und-umsetzung-des-europaischen-emissionshandels [Abgerufen am 14.08.2025]

Ungureanu, P., Bellesia, F., & Cochis, C. (2025). Dealing with blame in digital ecosystems: The DAO failure in the Ethereum blockchain. *Technological Forecasting and Social Change*, 215, 124096. https://doi.org/10.1016/j.techfore.2025.124096

United Nations Development Programme (2023). Strengthening energy governance systems: An energy governance framework for a just energy transition. *Online verfügbar unter:* https://www.undp.org/publications/strengthening-energy-governance-systems-energy-governance-framework-just-energy-transition [Abgerufen am 13.08.2025]

Urbach, N., Guggenberger, T., Pfaff, H., Stoetzer, J.-C., Feulner, S., Babel, M., Principato, M., & Lautenschlager, J. (2024). EU Digital Identity Wallet – Anwendungsfälle, Nutzungspotenziale und Herausforderungen für Unternehmen. Fraunhofer-Institut für Angewandte Informationstechnik FIT, Institutsteil Wirtschaftsinformatik, Bayreuth. *Online verfügbar unter:* https://doi.org/10.24406/publica-3343 [Abgerufen am 24.06.2025]

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Regulatory frameworks for decentralized finance (DeFi): Challenges and opportunities. *GSC Advanced Research and Reviews*, 19(02), 116-129. https://doi.org/10.30574/gscarr.2024.19.2.0170

VDE e. V., Energietechnische Gesellschaft (2023). Flexibilisierung des Energiesystems. *Online verfügbar unter:* https://www.vde.com/resource/blob/2283424/ecae13601387c8f642140f9f29d09c34/vde-studie-flexibilisierung-des-energiesystems-data.pdf [Abgerufen am 14.08.2025]

VDE e. V. (2025). Experten-Interview: Wie sich mit Redispatch 3.0 Flexibilitäten im Stromnetz besser nutzen lassen. VDE. *Online verfügbar unter:* https://www.vde.com/de/presse/pressemitteilungen/interview-redispatch-3-0 [Abgerufen am 14.08.2025]

Vionis, P., & Kotsilieris, T. (2024). The Potential of Blockchain Technology and Smart Contracts in the Energy Sector: A Review. *Applied Sciences*, 14(1), 253. https://doi.org/10.3390/app14010253

Vogel, M., Bauknecht, D., Flachsbarth, F., Koch, M., Wingenbach, M., Winger, C., Palacios, S., Krieger, S., Borkowski, K., Pfeifer, P., Tran, J., Porada, S., Sprey, J., Wahl, M., Mildt, D., Moser, A., Schyska, B., Heitkötter, W., Medjroubi, W., Vogt, T., Buchmann, M., Pechan, A., Radek, J., Höckner, J., Voswinkel, S., & Weber, C. (2021). Die enera Roadmap – enera übertragen und international verankern. *Online verfügbar unter:* https://projekt-enera.de/wp-content/uploads/enera-roadmap.pdf [Abgerufen am 21.08.2025]

Walden, J., Steinbrecher, A., & Marinkovic, M. (2021). Digital product passports as enabler of the circular economy. *Chemie Ingenieur Technik*, 93(11), 1717-1727. https://doi.org/10.1002/cite.202100121

Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. *International Journal of Information Management*, 52, 102064. https://doi.org/10.1016/j.ijinfomgt.2019.102064

Wan, S., Lin, H., Gan, W., Chen, J., & Yu, P. S. (2024). Web3: The next internet revolution. *IEEE Internet of Things Journal*, 11(21), 34811-34825. https://doi.org/10.1109/JIOT.2024.3432116

Wang, G., Wang, Q., & Chen, S. (2023). Exploring blockchains interoperability: A systematic survey. *ACM Computing Surveys*, 55(13s), 1-38. https://doi.org/10.1145/3582882

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv Preprint. https://doi.org/10.48550/arXiv.2105.07447

Weimert, B. (2020). Bericht AP2.1 | Distributed Ledger Technologies. Blockchain Reallabor. *Online verfügbar unter:* https://blockchain-reallabor.de/wp-content/uploads/2022/03/Forschung_Szenarien_DLT-Overview.pdf [Abgerufen am 12.05.2025]

Wennergren, O., Vidhall, M., & Sörensen, J. (2018). Transparency analysis of distributed file systems: With a focus on interplanetary file system. *Online verfügbar unter:* https://www.diva-portal.org/smash/get/diva2:1221334/FULLTEXT03.pdf [Abgerufen am 12.05.2025]

Woo, J., Fatima, R., Kibert, C. J., Newman, R. E., Tian, Y., & Srinivasan, R. S. (2021). Applying blockchain technology for building energy performance measurement, reporting, and verification (MRV) and the carbon credit market: A review of the literature. *Building and Environment*, 205, 108199. https://doi.org/10.1016/j.buildenv.2021.108199

Wüst, K., & Gervais, A. (2018). Do you need a blockchain?. In: *Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology* (S. 45-54). IEEE. https://doi.org/10.1109/CVCBT.2018.00011

Xie, M., Liu, J., Chen, S., & Lin, M. (2023). A survey on blockchain consensus mechanism: research overview, current advances and future directions. *International Journal of Intelligent Computing and Cybernetics*, 16(2), 314-340. https://doi.org/10.1108/IJICC-05-2022-0126

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647

Živić, N., Kadušić, E., & Kadušić, K. (2020). Directed acyclic graph as hashgraph: An alternative DLT to blockchains and tangles. In: *Proceedings of the 2020 19th International Symposium INFOTEH-JAHORINA* (S. 1-4). IEEE. https://doi.org/10.1109/INFOTEH48170.2020.9066312

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: Universal identity management and the concept of the “self-sovereign” individual. *Frontiers in Blockchain*, 3, 26. https://doi.org/10.3389/fbloc.2020.00026

Abkürzungen

API	Application Programming Interface
B2B	Business-to-Business
B2C	Business-to-Consumer
BANULA	Barrierefreie und Nutzerfreundliche Lademöglichkeiten schaffen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BMWE	Bundesministerium für Wirtschaft und Energie
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
CBAM	Carbon Border Adjustment Mechanism
CEEDS	Common European Energy Data Spaces
CID	Content Identifier
CPO	Charge Point Operator
CRA	Cyber Resilience Act
CSRD	Corporate Sustainability Reporting Directive
CSDDD	Corporate Sustainability Due Diligence Directive
DAG	Directed Acyclic Graph
DAO	Decentralized Autonomous Organization
DEER	Dezentraler Redispatch: Schnittstellen für die Flexibilitätsbereitstellung
DeFi	Decentralized Finance
DID	Decentralized Identifier
DLT	Distributed-Ledger-Technologie
DPP	Digitaler Produktpass
DSGVO	Datenschutz-Grundverordnung
DSSC	Data Spaces Support Centre
EBSI	European Blockchain Services Infrastructure
EDDI	European Distributed Data Infrastructure for Energy
EDSA	Europäischer Datenschutzausschuss
EE	Erneuerbare Energien
EEG	Erneuerbare-Energie-Gemeinschaft

eIDAS	Electronic Identification, Authentication, and Trust Services
EIP	Ethereum Improvement Proposal
eMSP	Electric Mobility Service Provider
ENTSO-E	European Network of Transmission System Operators for Electricity
EnWG(-E)	Energiewirtschaftsgesetz (Elektrizität)
ERC	Ethereum Request for Comments
ESPR	Ecodesign for Sustainable Products Regulation
EU	Europäische Union
EUDI	European Digital Identity
EU-EHS	EU-Emissionshandelssystem
EVU	Energieversorgungsunternehmen
FAIR	Findability, Accessibility, Interoperability, and Reusability
GUI	Graphical User Interface
GW	Gigawatt
HEMS	Home Energy Management System
HKN	Herkunftsnachweis
HKNR	Herkunftsnachweisregister
IDSA	International Data Spaces Association
IMSys	Intelligentes Messsystem
IPFS	InterPlanetary File System
IoT	Internet of Things
ISO	International Organization for Standardization
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastruktur
KW	Kilowatt
LLM	Large Language Model
MaStR	Marktstammdatenregister
MiCAR	Markets in Crypto-Assets Regulation
MW	Megawatt
NFT	Non-Fungible Token
NIS2	Network and Information Security Directive 2

NLS	Netzleitsystem
O&M	Operation & Maintenance
OID4VCI	OpenID for Verifiable Credential Issuance
OID4VP	OpenID for Verifiable Presentations
OIDC	OpenID Connect
PKI	Public Key Infrastructure
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
PPA	Power Purchase Agreement
PV	Photovoltaik
RED	Renewable Energy Directive
ReFi	Regenerative Finance
RFNBO	Renewable Fuels of Non-Biological Origin
RSP	Roaming Service Provider
SAFE	Secure Access For Everyone
SMGW	Smart Meter Gateway
SSI	Self-Sovereign Identity
SSO	Single Sign-On
SWOT	Strengths, Weaknesses, Opportunities, Threats
TFH	Tools for Humanity
UBA	Umweltbundesamt
ÜNB	Übertragungsnetzbetreiber
VC	Verifiable Credential
VNB	Verteilnetzbetreiber
VP	Verifiable Presentation
W3C	World Wide Web Consortium
WLD	Worldcoin
ZKP	Zero-Knowledge Proof
ZK-Rollup	Zero-Knowledge Rollup

Glossar

Begriff	Definition
Blockchain	Technologie zur dezentralen Speicherung und Verwaltung von Daten in chronologisch verketteten Blöcken.
Cloud Computing	Das Konzept, die Datenverarbeitung in eine abstrahierte, zentralisierte IT-Umgebung auszulagern.
Datenmodell	Abstraktes Modell, das Datenelemente, ihre Beziehung zueinander und Eigenschaften realer Entitäten organisiert und standardisiert. Ein Beispiel hierfür ist das Common Information Model (CIM). Es beschreibt die Attribute und Beziehungen zwischen verschiedenen Objekten in einem Stromnetz.
Datenökosystem	Gemeinsame Struktur einer multilateralen Gruppe von Partnern, die bilateral interagieren, damit ein zentrales Wertversprechen in Bezug auf den Datenaustausch zustande kommt.
Datenraum	Koordinierte Menge an technischen Standards, Organisationsrichtlinien und Diensten im Rahmen eines spezifizierten Governance-Modells, um den Datenaustausch zwischen seinen Teilnehmern zu ermöglichen.
Datenraumkonnektor	Zentrale Komponente eines Datenraums, die die Teilnehmer miteinander verbindet und als Schnittstelle für den Datenaustausch dient. Er ermöglicht es angebundenen Teilnehmern, Verträge automatisiert zu verhandeln und anschließend die vereinbarten Daten-Assets sicher auszutauschen.
Datensouveränität	Fähigkeit von Personen oder Organisationen, Nutzerkontrolle auszuüben.
Decentralized Finance (DeFi)	Finanzsystem, das ohne zentralen Vermittler wie eine Bank auskommt und Peer-to-Peer-Transaktionen ermöglicht.
Decentralized Identifiers	Standard, der das Erstellen eines sicheren bilateralen Kommunikationskanals ermöglicht und für eine Ende-zu-Ende-verschlüsselte Verbindung zwischen den beteiligten Akteuren in einem SSI-System sorgt.
Dezentrale Governance	Entscheidungsfindung in digitalen Systemen durch Gemeinschaften von Partnern oder Protokollen, ohne zentrale Autorität.
Dezentralisierung (im Energiesektor)	Beschreibt die gesellschaftliche und wirtschaftliche Veränderung der Energieversorgung hin zu einer breiteren Eigentümerstruktur. Statt weniger zentraler Akteure übernehmen zunehmend Privatpersonen, Genossenschaften und Unternehmen den Betrieb von Energieerzeugungsanlagen.
Digitale Identität	Digitale Repräsentation einer Menge von Identitätsattributen, die die Identifikation einer Person, einer Organisation oder eines Assets im digitalen Raum ermöglichen.

Begriff	Definition
Digitale Wallet	Software zur Aufbewahrung von privaten Schlüsseln, Verifiable Credentials und Decentralized-Identifier-Dokumenten.
Distributed Ledger Technologies (DLTs)	Dezentrale Datenspeicherungs- und -verwaltungssysteme.
Edge Computing	Verfahren, bei dem Daten, Services und Anwendungsinformationen unmittelbar an die logische „Randstelle“ (Edge) eines Netzwerks verlagert werden.
Energieflexibilität	Fähigkeit von Energieverbrauchern, -erzeugern oder -speichern, ihre Netzeinspeisung oder ihren Verbrauch zeitlich flexibel an die Bedingungen im Energiesystem anzupassen, um Netzstabilität zu unterstützen.
FAIR-Prinzipien	Die FAIR-Prinzipien sind Leitlinien für die Organisation von Daten, damit diese auffindbar (findable), zugänglich (accessible), interoperabel (interoperable) und wiederverwendbar (reusable) sind.
Föderiertes Identitätsmanagement	Modell, bei dem zentrale Identitätsanbieter Identitätsinformationen verwalten und Nutzerinnen und Nutzern die Anmeldung bei verschiedenen Diensten mit einem einzigen Konto ermöglichen.
Fungible Tokens	Tokens mit einem einheitlichen Wert, die untereinander austauschbar sind.
Holder	Rolle in einem SSI-System; Besitzer eines Verifiable Credential.
Identitätsattribut	Merkmale einer Person, einer Organisation oder eines Geräts zur Identifikation.
InterPlanetary File System (IPFS)	Dezentrale Speicherlösung, die Dateien über ein Peer-to-Peer-Netzwerk verteilt.
Isoliertes Identitätsmanagement	Modell, bei dem jeder Diensteanbieter Identitäten individuell und unabhängig überprüft, wobei die verifizierten Identitäten nicht zwischen Diensten übertragbar sind.
Issuer	Rolle in einem SSI-System; vertrauenswürdige Partei, deren Identität öffentlich einsehbar ist und die das Verifiable Credential digital signiert.
Non-Fungible Tokens (NFT)	Einzigartige Tokens, die nicht untereinander austauschbar sind.
Nutzerkontrolle	Prinzip in einem digitalen Ökosystem, bei dem Nutzerinnen und Nutzer aktiv selbst über die Nutzung, Weitergabe und Speicherung ihrer Daten entscheiden.
Oracle-Problem	Fundamentale Herausforderung, externe Daten vertrauenswürdig und überprüfbar in Rechnernetze und insbesondere in dezentrale Systeme zu integrieren.
Peer-to-Peer-Netzwerk	Architektur, in der alle Teilnehmer Daten direkt (ohne Intermediär) miteinander austauschen können.

Begriff	Definition
Referenzarchitektur	Bietet ein Architekturmodell im Bereich der Softwarearchitektur für eine bestimmte Domäne zusammen mit einem gemeinsamen Vokabular, mit dem Implementierungen diskutiert werden können – mit dem Ziel, Gemeinsamkeiten hervorzuheben.
Regenerative Finance (ReFi)	Nachhaltiges Finanzparadigma, das Ansätze aus Decentralized Finance nutzt, um einen Übergang zu einer regenerativen Wirtschaft zu erreichen
Security Tokens	Tokens, die reale Vermögenswerte wie Anteile, Immobilien oder Anleihen digital repräsentieren.
Selbstsouveräne Identität (SSI)	Modell zur dezentralen Verwaltung digitaler Identitäten, bei dem Nutzerinnen und Nutzer vollständige Kontrolle über ihre Identitätsdaten behalten und sie selektiv teilen können.
Skalierbarkeit	Fähigkeit eines digitalen Systems, bei wachsender Nutzung (z. B. steigende Transaktionen oder Datenmengen) effizient und leistungsfähig zu bleiben.
Token	Digitale Repräsentation von finanziellen Vermögenswerten und Waren bis hin zu anderen Ressourcen.
Tokenisierung	Prozess der Digitalisierung von finanziellen Vermögenswerten und Waren bis hin zu anderen Ressourcen in Form von Tokens.
Verifiable Credential (VC)	Digital signierter Nachweis über bestimmte Eigenschaften oder Berechtigungen, der kryptografisch überprüfbar ist.
Verifiable Presentation (VP)	Zusammenstellung und Präsentation von Informationen bzw. Behauptungen (Claims) für den Verifier.
Verifier	Rolle in einem SSI-System; fragt Identität und Nachweis von Attributen an und prüft, ob die erhaltenen Nachweise bestimmten Anforderungen entsprechen.
Verifizierbarkeit	Eigenschaft eines Datums bzw. einer Information, deren Echtheit und Herkunft digital überprüfbar ist.
Verteilte Datenspeicherung	Speicherung von Daten über mehrere Standorte oder Systeme hinweg.
Web3	Entwicklungsstufe des World Wide Web hin zu einem dezentralen Internet basierend, auf Technologien, die eine dezentrale Governance und Datensouveränität ermöglichen.
Web3.0	Entwicklungsstufe des World Wide Web, bei der durch semantische Ansätze Dezentralisierung und Datensouveränität ermöglicht werden.
Zero-Knowledge Proof (ZKP)	Kryptografisches Verfahren, mit dem die Gültigkeit einer Aussage nachgewiesen werden kann, ohne ihren Inhalt preiszugeben.

Ein Projekt der

dena

www.dena.de

future-energy-lab.de