Babel, Matthias et al.

Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Babel, Matthias et al. (2023) : Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 2, pp. 478-493, https://doi.org/10.1365/s40702-023-00955-3

HMD Praxis der Wirtschaftsinformatik (2023) 60:478–493
https://doi.org/10.1365/s40702-023-00955-3

SCHWERPUNKT

Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme

Matthias Babel · Vincent Gramlich · Claus Guthmann · Marcus Schober · Marc-Fabian Körner · Jens Strüker

Eingegangen: 16. September 2022 / Angenommen: 7. Februar 2023 / Online publiziert: 13. März 2023

Zusammenfassung Die Vernetzung kommunikationsfähiger Geräte schreitet aktuell schnell voran und verspricht durch eine Ende-zu-Ende-Digitalisierung von Prozessen Effizienzgewinne und neue Anwendungsmöglichkeiten. Die Verifizierung von Endgeräten ist insbesondere bei kritischen Infrastrukturen wie der Energieversorgung eine notwendige Bedingung. Unter anderem für die aktive Integration von Kleinstanlagen wie Photovoltaikanlagen oder Wärmepumpen in das Stromnetz stellt sich die Frage, wie Stamm- und Bewegungsdaten von Verbrauchs- und Erzeugungsanlagen vertraulich und unverändert verfügbar gemacht werden können. Mit der Beantwortung dieser Fragestellung hat sich das Projekt „Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem (BMIL)“ im Rahmen des Future Energy Lab der Deutschen Energie-Agentur (dena) beschäftigt. Für die vertrauensvolle Einspeisung und Integration von dezentral erzeugten Daten folgt das Projekt dem Paradigma der selbstbestimmten Identitäten (engl.: SSI). Hierbei werden intelligente Messsysteme bzw. Smart Meter Gateways (SMGWs) mit Maschinenidentitäten ausgestattet. Dies ermöglicht Vertrauensketten zu nutzen, um Bewegungsdaten verbunden mit verifizierbaren Stammdaten in digitale Strommärkte zu integrieren. Im Rahmen dieses Artikels werden die Ergebnisse des BMIL-Projekts innerhalb einer Fallstudie aufgearbeitet und konkrete Handlungsempfehlungen für die Praxis zur Lösung des Oracle-Problems mit Hilfe von SSI abgeleitet.

Schlüsselwörter SSI · Oracle Problem · Blockchain · Distributed Ledger Technology · Energiesystem

✉ Matthias Babel · Vincent Gramlich · Claus Guthmann · Marcus Schober · Marc-Fabian Körner · Jens Strüker
Institutsteil Wirtschaftsinformatik des Fraunhofer FIT, Kernkompetenzzentrum Finanz- & Informationsmanagement, Universität Bayreuth, Wittelsbacherring 10, 95444 Bayreuth, Deutschland
E-Mail: matthias.babel@fit.fraunhofer.de

Trust through Digital Identification: On SSI's Contribution to the Integration of Decentralized Oracles in Information Systems

Abstract The networking of communicating devices is currently advancing rapidly and promises efficiency gains and new applications through an end-to-end digitization of processes. Verification of edge devices is a necessary condition, especially for critical infrastructures such as energy systems. Among others, for the active integration of small assets such as photovoltaic plants or heat pumps into the power grid, the question arises of how master data and transaction data from consumption and generation assets can be made available confidentially and unaltered. The project "Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem (BMIL)" funded by the Future Energy Lab of the German Energy Agency (dena) addressed this question. For the trustworthy feed-in and integration of decentrally generated data, the project follows the paradigm of Self-Sovereign Identities (SSI). Here, intelligent metering systems or smart meter gateways (SMGWs) are equipped with machine identities. This allows the use of chains of trust to integrate transaction data combined with verifiable master data into digital energy systems. In this article, the results of the BMIL project are analyzed in a case study and concrete recommendations for solving the oracle problem in practice with the help of SSI are derived.

Keywords SSI · Oracle Problem · Blockchain · Distributed Ledger Technology · Energy System

1 Motivation

Das Unternehmen Cisco schätzt, dass im Jahr 2023 die Einwohner*innen Westeuropas durchschnittlich je fast 10 internetfähige Geräte besitzen werden (Cisco 2020). Die Vernetzung dieser Geräte und das damit entstehende Internet-of-Things (IoT) eröffnet die Möglichkeit, große Mengen an Daten automatisiert zu erheben, zu teilen und daraus Erkenntnisse abzuleiten (Li et al. 2015). Diese weiträumig verteilte Erhebung von Echtweltdaten unterstützt eine tiefere Durchdringung der Digitalisierung in Gesellschaft und Industrie. Die sich ergebenden Potenziale reichen von Effizienzsteigerungen in der Infrastruktur von Städten, über die Verbesserung von Liefer- und Fertigungsprozessen in der Industrie bis hin zur Erhöhung der Nachhaltigkeit unter anderem im Energiesektor, zum Beispiel durch gesteigerte Effizienz und Nachvollziehbarkeit beim Ausstoß von CO2-Emissionen und der Einbindung von Kleinstflexibilitäten in das Stromnetz (Li et al. 2015; Strüker et al. 2021a; Babel et al. 2022; Sedlmeir et al. 2021; Roth et al. 2022). Digitale Technologien gelten daher auch als zentraler Schlüssel zur Erreichung von nachhaltigen Entwicklungszielen wie der Agenda 2030 der Vereinten Nationen (Mondejar et al. 2021; Heffron et al. 2020).

Allerdings bringen die beschriebenen Potenziale ebenso Risiken und Herausforderungen mit sich (Körner et al. 2022). Neben verschiedenen informationstechnischen Angriffsvektoren steht die dezentrale und oft personennahe Erhebung von

Daten durch IoT-Geräte in der Kritik die Privatsphäre der Nutzenden zu gefährden (Michael et al. 2015). Mit Zugriff auf die entsprechenden Daten können der digitalen Identität einer Person nicht nur deren Aktivitäten im Internet, sondern auch von IoT-Geräten erfasstes Verhalten in der nicht-digitalen Welt zugeordnet werden. Beispiele sind durch Smart-Watches erfasste Bewegungsabläufe oder der durch intelligente Messstellen erhobene häusliche Stromverbrauch. Dementsprechend gilt es – auch um Konformität mit nationalen und internationalen Datenschutzregularien (wie der deutschen Datenschutz-Grundverordnung (DSGVO)) sicherzustellen – die Verteilung und anschließende Verwendung dieser Daten so zu gestalten, dass Dateneigentümer*innen weiterhin die selbstbestimmte Kontrolle über ihre Daten ausüben können.

Für die Integration der initial zu erfassenden Daten in Informationssysteme spielt die Korrektheit und Integrität dieser Daten eine wichtige Rolle. Hier gilt es nicht nur absichtliche Manipulation auszuschließen, sondern auch beispielsweise die Datenerfassung durch ungenaue oder fehlerhaft installierte Sensoren zu vermeiden. Die Herausforderung, externe Daten manipulationssicher und verifizierbar zu integrieren, wird auch als Oracle-Problem bezeichnet (Caldarelli 2020a). Besonders bekannt ist das Oracle-Problem bei Anwendungen, die auf der Blockchain-Technologie basieren: Hier verliert die Manipulationssicherheit, die die Blockchain für auf ihr gespeicherte Daten gewähren soll, ihren Wert, wenn diese Daten initial aus externen Quellen stammen und ihre Korrektheit nicht verifizierbar gewährleistet werden kann.

Neben anderen Lösungsansätzen, adressiert auch das Paradigma der selbstbestimmten digitalen Identitäten (englisch: Self-Sovereign Identity (SSI)) die zuvor beschriebenen Herausforderungen, nämlich die selbstbestimmte Kontrolle durch Nutzende und die Verifizierung von Daten in digitalen Systemen gegenüber Dritten (Preukschat et al. 2021). In der Praxis findet SSI bislang vorranging bei identitätsbezogenen Daten von Personen wie dem Personalausweis Anwendung. SSI ist allerdings nicht auf Personendaten beschränkt, sondern kann insbesondere auch auf Unternehmens- oder Maschinenidentitäten ausgeweitet werden (Lacity und Carmel 2022). Dies verspricht Vorteile für eine Vielzahl von (Geschäfts-)Prozessen, unter anderem für die Verifizierung der Datenherkunft, bei der Daten eines IoT-Gerätes mit dessen Identität gekoppelt werden können. SSI hat somit das Potenzial, die im Rahmen der IoT-Anwendungen vorherrschenden Strukturen durch die Identifikation mit verifizierbaren Daten sicherer zu machen.

Im Projekt „Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem (BMIL)“ des Future Energy Labs der Deutschen Energie-Agentur (dena) wurde die Verwendung des SSI-Paradigmas und der damit verbundenen Technologie im Kontext des deutschen Energiesystems erprobt (Deutsche Energie-Agentur 2022). Hierbei lag der Fokus auf der verifizierbaren Daten-Bereitstellung von dezentralen Energieerzeugungsanlagen. So wurde beispielsweise die Integration einer privaten Photovoltaik-(PV)-Anlage zur Verwendung in energiewirtschaftlichen Prozessen unter gleichzeitigem Schutz von personenbezogenen Daten untersucht. Dieser Schutz ist höchst relevant, da die unbeschränkte Weitergabe von hochaufgelösten Daten, wie zum Beispiel zur Einspeisung privater PV-Anlagen ins Stromnetz, Rückschlüsse auf das Verbrauchsverhalten der Eigentümer*innen zulas-

sen würden. Ziel dieses Artikels ist es, das im BMIL-Projekt entwickelte Konzept vorzustellen und aufzuzeigen, wie sich die darin gewonnenen Erkenntnisse auf das breitere Spektrum von Anwendungen, in denen die Bereitstellung von verifizierbaren externen Daten benötigt wird, ausweiten lässt. Konkret stellt dieser Beitrag die folgende Frage:

Welche Erkenntnisse und Handlungsempfehlungen können aus der Umsetzung des SSI-Paradigmas innerhalb des BMIL-Projekts für die Implementierung von dezentralen vertrauensvollen Oracles abgeleitet werden?

Hierzu werden zunächst einige konzeptionelle Grundlagen erläutert und die Zielsetzung des BMIL-Projekts sowie die spezifische Verwendung von SSI im Projekt dargestellt. Anschließend diskutiert der Beitrag, wie die Erkenntnisse des BMIL-Projekts in Bezug auf einer auf Nutzende zentrierten und verifizierbaren Integration von Echtweltdaten auf Anwendungsgebiete mit ähnlichen Herausforderungen übertragen werden können.

2 Grundlagen und Stand der Forschung

Im Folgenden wird zunächst auf die grundlegenden Eigenschaften in Bezug auf Blockchains eingegangen, das Oracle-Problem näher dargelegt und abschließend die Bestandteile des SSI-Paradigmas erklärt. Dabei skizzieren wir an ausgewählten Stellen, die für das Verständnis dieses Beitrags wichtig sind, den aktuellen Stand der Forschung.

2.1 Einführung Blockchain

Eine Blockchain ist eine aus verketteten Datenblöcken bestehende Datenstruktur und baut auf bekannten kryptographischen Primitiven auf. Die Blöcke enthalten mit Hilfe asymmetrischer Verschlüsselung signierte Transaktionen, sowie eine durch eine Hashfunktion komprimierte Repräsentation (Hash) ihres vorherigen Blockes. Die Signatur der Transaktionen ermöglicht die Verifizierung der Transaktionsherkunft. Durch das Inkludieren des Hashs des vorherigen Blockes sind die Blöcke chronologisch miteinander verkettet, wodurch eine nachträgliche Änderung des Inhalts eines Blockes in allen späteren Blöcken detektiert werden kann. Dies legt den Grundstein für die Unveränderbarkeit von auf der Blockchain geschriebenen Daten, denn nachträgliche Änderungen von Transaktionen können dadurch leicht erkannt werden (Nakamoto 2008; Schlatt et al. 2016). Ein Konsensmechanismus wählt über einen Anreizmechanismus aus, welche Netzwerkteilnehmenden einen neuen Block erstellen, darin Transaktionen inkludieren und dann der Blockchain anfügen dürfen. Alle weiteren Teilnehmenden erhalten die Möglichkeit, diesen Block auf seine semantische und syntaktische Korrektheit zu prüfen und ggfs. abzulehnen. Durch die Kombination aus Irreversibilität durch Verkettung und der Koordination eines dezentralen Netzwerkes mittels Konsensmechanismus stellen Blockchains so die Korrektheit von bestehenden und neu entstehenden Daten sicher (Beck et al. 2017).

Die erste Anwendung der Blockchain-Technologie war Bitcoin, die Kryptowährung mit der im Jahr 2023 immer noch größten Marktkapitalisierung (Nakamoto

2008). Während sich die Funktionsweise der Bitcoin Blockchain auf einfache Zahlungen beschränkt, sind andere Blockchains, wie zum Beispiel Ethereum, auch in der Lage, Programmcode zu speichern und ausführbar zu machen (Buterin 2014). Mit Hilfe dieser Programmcodes, sogenannter Smart Contracts, können alle Funktionen von klassischen Programmiersprachen abgebildet werden, weshalb man diese Blockchains auch als Turing-Complete bezeichnen kann (Wood 2014).

2.2 Das Oracle Problem

Smart Contracts ermöglichen es, komplexe Sachverhalte auf einer Blockchain zu verwalten (Forte et al. 2017). Anwendungen basierend auf Smart Contracts profitieren direkt von den immanenten Eigenschaften der Blockchain-Technologie, wie Unveränderbarkeit, hoher Verfügbarkeit und der Neutralität der Plattform selbst (Kõlvart et al. 2016). Da Blockchains geschlossene System darstellen, können Smart Contracts zunächst nur auf Informationen zugreifen, die sich auf der Blockchain selbst befinden. Viele Anwendungen benötigen dabei jedoch Zugriff auf Daten, die „off-chain“, also außerhalb des Blockchain-Netzwerkes selbst, erhoben werden, wie zum Beispiel Finanzdaten oder Sensordaten von IoT-Geräten. Sogenannte Oracles ermöglichen es, diese Daten in das Blockchain-System zu integrieren und somit für Smart Contracts zugänglich zu machen (Damjan 2018). Dabei lassen sich zwei Vertrauensmodelle unterscheiden: zentral und dezentral. Im zentralen Modell beruhen die Daten auf einer einzigen Quelle. Dieser Ansatz ist effizienter als der dezentrale, repräsentiert aber einen Single-Point-of-Failure, also eine potenzielle Schwachstelle, von der die Verfügbarkeit und Korrektheit der Daten abhängig ist. In einem dezentralem Modell existieren stattdessen mehrere Oracles, also mehrere voneinander unabhängige Quellen, aus deren Daten ein Konsens gebildet und somit die Gefahr des Single-Point-of-Failure eliminiert werden kann (Al-Breiki et al. 2020). Da in beiden Fällen die Daten und die daraus resultierende Ausführung von Vertragslogiken unveränderbar auf der Blockchain abgespeichert werden, muss die Integrität der off-chain Daten beim Import in das Blockchain-System zuverlässig und automatisiert sichergestellt werden. Ungenauigkeiten oder Fehler an der initialen Datenschnittstelle und damit in den darauf basierenden Berechnungen und Smart Contracts, haben oft irreversible Folgen (Berger et al. 2020; Al-Breiki et al. 2020). Gleichzeitig ist auch die Verfügbarkeit der Oracles von großer Bedeutung, um den reibungslosen Betrieb der auf deren Daten aufbauenden Systeme sicherzustellen. Die Frage, wie die Integrität und Verfügbarkeit der Oracles sichergestellt werden kann, wird in der Literatur dabei als Oracle-Problem bezeichnet (Caldarelli 2020a; Curran 2018). Auch im Anwendungsbereich Energie besteht dieses Problem. Wie von Caldarelli (2020b) angemerkt, wird dies sowohl in der Forschung als auch in Real-Welt-Projekten noch nicht bzw. nur zu gering berücksichtigt. Die im BMIL-Projekt diesbezüglich erlangten Erkenntnisse, die wir mit unserem Beitrag generalisieren wollen, können dabei helfen, diese bestehende Lücke aufzuarbeiten.

2.3 SSI – Selbstbestimmte digitale Identitäten

Das Paradigma der selbstbestimmten digitalen Identitäten verspricht eine auf Nutzende zentrierte digitale Identitätsverwaltung, insbesondere im Internet (Allen 2016). Aktuell vorherrschende Verfahren des Identitätsmanagements im Internet, wie zentrale Anmeldedienste (engl. Single-Sign-On (SSO)) bekannter Internetplattformen, mangelt es häufig an der Wahrung der Privatsphäre für Nutzende, da die Aktivitäten der Nutzenden gegenüber dem Anbieter nahezu transparent sind. Weiterhin stellen zentralisierte Systeme wie SSO einen Single-Point-of-Failure dar, da sie bei Netzwerkausfällen aufgrund der zentralisierten Struktur besonders anfällig sind (Strüker et al. 2021b). Ein auf SSI basierendes Identitätssystem strebt danach, eine digitale, auf Nutzende zentrierte Identitätsverwaltung sicherzustellen. Diese legt die Verwaltung und Verwendung von Identitäten nicht in die Abhängigkeit Dritter, sondern befähigt deren Eigentümer*innen dazu, diese selbstbestimmt kontrollieren zu können (Preukschat et al. 2021). Hierzu greift SSI auf bekannte Mechanismen digitaler Zertifikate wie dem X.509-Standard zurück und reichert sie mit Nutzerfreundlichkeit, Privatsphäre-Features und einer skalierbaren und Domänen-agnostischen Infrastruktur an.

Das Grundkonzept besteht darin, dass vertrauensvolle Institutionen oder Unternehmen (Issuer) Identitätsdokumente, wie Ausweise, Hochschulzertifikate oder Urkunden, für die Nutzenden in Form von digitalen Zertifikaten ausstellen. Diese werden im SSI-Kontext auch oft als Verifiable Credentials (VCs) bezeichnet und können durch Nutzende (Holder) mithilfe einer SSI-Wallet sicher verwaltet und verwendet werden. Holder sind dabei in der Lage, VCs ohne Einbeziehung der Issuer gegenüber anderen Parteien (Verifiern) präsentieren zu können (Allen 2016). Vorgezeigt wird dabei meist nicht das VC selbst, sondern eine Verifiable Presentation (VP), die auf Basis des VCs erstellt wird und es unter anderem ermöglicht bei Bedarf nur ausgewählte Informationen bzw. Ausschnitte des digitalen Zertifikats vorzuzeigen. Zur Identifizierung von Issuern, Holdern und Verifiern sowie dem anschließenden Aufbau einer sicheren Verbindung können sog. Decentralized Identifier (DIDs) dienen (Sporny et al. 2022). Sowohl die Erstellung der VPs, als auch der Aufbau sicherer Verbindungen und das sichere Speichern von zu den VCs passenden Schlüsselpaaren liegt im Aufgabenbereich des Wallets, das somit die Schnittstelle zwischen der zugrundeliegenden Technologie und den Nutzenden darstellt. Zusätzlich wird ein zentrales Register benötigt, um die DIDs zu speichern, Revokation zu ermöglichen und gebündelt Schemata und Metainformationen abzulegen. Dies wird häufig von einer Blockchain übernommen, genannt Identity Blockchain. Das Zusammenspiel zwischen Issuer, Holder und Verifier wird auch als Trust Triangle bezeichnet. In Kombination mit kryptographischen Verfahren, Standards und Software ermöglicht das Trust Triangle die Schaffung von selbstbestimmten, digitalen Identitäten, die die Grundlage für ein neues Identitätsmanagement bilden könnten, das sich an den Anforderungen von digitalen Ökosystemen orientiert (Strüker et al. 2021b).

3 Use-Case: Einbindung dezentraler Oracles im „Blockchain Machine Identity Ledger“ (BMIL) Projekt

Im Zusammenhang mit der Eindämmung des globalen Klimawandels konzentrieren sich zahlreiche Aktivitäten in Forschung, Politik und Wirtschaft auf die Reduzierung des Ausstoßes von klimaschädlichen Treibhausgasen. In Deutschland werden diese Aktivitäten im Energiebereich häufig unter dem Begriff der „Energiewende“ zusammengefasst, der unter anderem den Ausbau von erneuerbaren Energieanlagen und die generelle Elektrifizierung von zuvor nicht elektrifizierten Sektoren wie beispielsweise dem Mobilitätssektor umfasst (Fridgen et al. 2020). Die Folgen sind eine dezentralere und somit volatilere Stromerzeugung und ein insgesamt steigender Strombedarf (Heffron et al. 2021). Um der damit steigenden Komplexität notwendiger Maßnahmen zur Gewährleistung von Versorgungssicherheit und marktlicher Effizienz Rechnung zu tragen, ist es notwendig, Stromerzeugung und -verbrauch aktiv und feingranular aufeinander abzustimmen. Hierfür spielt auch die große Anzahl von dezentralen Kleinstanlagen eine immer größere Rolle, die durch den Einsatz von IoT-Geräten intelligent steuerbar sind (Babilon et al. 2022; Strüker et al. 2021a). Zur aktiven Integration dieser Kleinstanlagen sind dezentrale Lösungen für ein auf Nutzende zentriertes Identitätsmanagement von wachsender Bedeutung. Dies geht aus zahlreichen Konzepten und Projekten zur Erprobung und Umsetzung von dezentralen Ansätzen hervor (Deutsche Energie-Agentur 2019).

3.1 Einführung in das BMIL-Projekt

Die Nutzbarkeit von verifizierbaren Datenquellen ist eine wesentliche Voraussetzung für diverse Anwendungen im Bereich von digitalen Strommärkten (zum Beispiel Zugang von Kleinstanlagen zum Regelenergiemarkt). Diese Herausforderung adressiert das BMIL-Projekt, indem die Rolle von Blockchains als zentrale Register in Kombination mit digitalen Identitäten zur Erfüllung dieser Voraussetzung analysiert und eine mögliche Lösung konzeptualisiert und erprobt wurde. Das BMIL-Projekt beschäftigte sich somit mit einer spezifischen Instanz des Oracle-Problems, nämlich der Integration von dezentral verteilten (IoT)-Geräten und deren Daten in digitale Strommärkte. Als Datenquelle, also Oracles für diese spezifische Instanz des Oracle-Problems, wurden dabei Smart Meter Gateways (SMGWs) betrachtet, die die Kommunikationseinheit intelligenter Messsystemen sind und die Verwendung von viertelstündlichen Bewegungsdaten von Kleinstanlagen im Strommarkt ermöglichen (Deutsche Energie-Agentur 2022).

Energieverbrauchs- und Energieerzeugungsdaten, die durch SMGWs erfasst und kommuniziert werden, sind die Grundlage für viele Anwendungsfälle einer digitalisierten Energiewirtschaft. Folglich muss das Vertrauen in diese Daten jederzeit vorhanden sein und bestehen bleiben. Ein wichtiger Baustein für die Schaffung dieses Vertrauens ist die Möglichkeit, die in das System eingespeisten Daten ihrer jeweiligen Quelle, zum Beispiel dem spezifischen SMGW, zuordnen zu können. Dafür notwendig ist die eindeutige Identifizierung von Maschinen und Anlagen, die am Energiesystem beteiligt sind. Benötigte Maschinenidentitäten enthalten die Stammdaten der Anlage (Anlagentyp, Leistung der Anlage, Lokation, etc.) und ermög-

lichen es, diese Stammdaten mit den gemeldeten Bewegungsdaten zu verknüpfen und dadurch die Datenherkunft nachvollziehbar zu machen. Die Verifizierung dieser Identitäten trägt dabei einen entscheidenden Teil zur Sicherung der Datenintegrität bei. Durch einen vertrauensvollen Installateur/Issuer kann initial Vertrauen in das Gesamtsystem eingebracht werden und die oben erwähnte sichere Verwendung der Bewegungsdaten in spezifischen Geschäftsmodellen ermöglicht werden.

Einen ersten Ansatz zur Identifizierung von Messsystemen und den damit verbundenen Anlagen liefert bereits das seit 2019 bestehende Marktstammdatenregister[1], in dem die Stammdaten aller registrierten Erzeugungsanlagen digital verwaltet werden können. Allerdings können aktuell Betreibende einer Anlage deren Stammdaten nicht selbstbestimmt verwalten und gegenüber Dritten vorzeigen, sondern sind vom Marktstammdatenregister, das als zentrale Instanz, alle Informationen verwaltet, abhängig. Das Marktstammdatenregister muss somit in alle Verifizierungsprozesse direkt eingebunden werden und auch die Korrektheit und Vollständigkeit der darin gespeicherten Informationen ist unter Kontrolle des Registers. Es stellt somit eine zentralisierte Architektur dar, die in der aktuellen Ausgestaltung kein selbstbestimmtes Identitätsmanagement ermöglicht und Datensouveränität und Datenschutz einschränkt.

3.2 Verwendung von SSI im BMIL-Projekt

Um die Verifizierbarkeit von Daten und ihrer Herkunft zu ermöglichen und gleichzeitig nicht auf eine zentrale Partei angewiesen zu sein, wurde im Rahmen des BMIL-Projekts eine Lösung basierend auf dem SSI-Paradigma konzipiert. Die zentrale

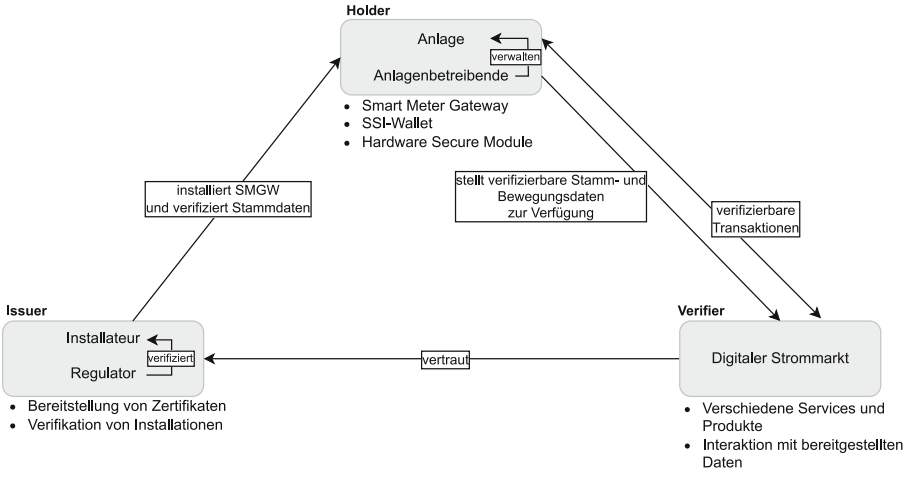

Abb. 1 Zentrale Stakeholder und deren Beziehung im BMIL-Projekt

[1] Marktstammdatenregister. https://www.marktstammdatenregister.de/MaStR. Zugegriffen: 13. September 2022.

Beziehung der verschiedenen Marktakteure wird in der Systemarchitektur (Abb. 1) skizziert und im Folgenden erläutert.

In der Abbildung ist das Trust Triangle (siehe Abschn. 2.3) zwischen Issuer, Verifier und Holder – angelehnt an das SSI-Paradigma für die Konzeptionierung der Gesamtarchitektur – klar erkennbar. Dabei beginnt die Vertrauenskette mit der Verifizierung des Installateurs durch den Regulator, wodurch der Installateur zur Ausstellung von Zertifikaten befähigt wird. Dadurch bekommt er vom Regulator die Rolle des Issuers übertragen, diese Übertragung wird über Zertifikatsketten beweisbar gemacht. Der Regulator muss in diesem Schritt zwingend eine Entität darstellen, der alle Marktteilnehmenden vertrauen. Nur so kann die oben beschriebene Vertrauenskette sichergestellt und das Vertrauen in die Daten, dessen Abwesenheit die Grundlage des Oracle Problems darstellt, geschaffen werden. Die Anlage wird im Rahmen der Installation des SMGWs durch den Installateur mit einer SSI-Wallet ausgestattet (vgl. Abb. 1). Die SSI-Wallet verwaltet alle relevanten Daten der Identität, die durch VCs dargestellt werden, unter anderem auch das Zertifikat, mit dem der Installateur die Stammdaten attestieren kann. Da die SSI-Wallet der Anlage für die Verwaltung einer Vielzahl an verschiedenen VCs von unterschiedlichen Issuern genutzt werden kann, wird so eine Infrastruktur für ein größeres Identitätsökosystem gelegt. Für die Verwendung der Daten in digitalen Strommärkten, deren Akteur*innen die Rolle der Verifier einnehmen, ist eine untrennbare Bindung von digitaler Identität und physischer Anlage von Bedeutung. Dies stellt sicher, dass VCs und die damit verbundenen Identitäten nur von derjenigen Anlage genutzt werden können, auf die diese ausgestellt wurden (=untrennbare Bindung). Um diese Bindung zur gewährleisten, können Hardware Secure Modules (HSMs) verwendet werden. Ein HSM ist ein technisch gesichertes Bauteil, in dem private Schlüssel so gespeichert werden, dass sie zwar vom Gerät verwendet, aber nicht ausgelesen werden können. Dadurch sind die privaten Schlüssel und die darauf ausgestellte Identität und VCs fest an die Anlage gebunden und können nicht auf eine andere Anlage übertragen werden. Die Untrennbarkeit von physischem Gerät und digitaler Identität in Kombination mit der Verifizierbarkeit des Zertifikats und seines Issuers ermöglichen es anderen Akteur*innen der Strommärkte, den übermittelten Daten zu vertrauen. Die Anlage kann sich somit digital und selbstbestimmt ausweisen. Diese Selbstbestimmtheit ermöglicht es den Eigentümer*innen, eigenverantwortlich und in einem digitalen und effizienten Prozess darüber zu entscheiden, an welchen Märkten sie teilnehmen möchten und welche Informationen sie wem gegenüber offenlegen möchten. Insofern bietet die im BMIL-Projekt entwickelte Lösung einen Ansatz für die automatisierte und verifizierte Registrierung von Teilnehmenden in neuen Strommärkten (inkl. Rollenwechsel), indem das Oracle-Problem, durch die Übertragung des bestehenden Vertrauens in den Regulator, mit Hilfe von Vertrauensketten, auf die einzelnen SMGWs und die weitere Hardware, minimiert wird.

Im Folgenden wird der prozessuale Ablauf der Attestierung und Verifizierung der Stammdaten und das Zusammenspiel der verschiedenen Parteien und technischen Komponenten im Kontext von SSI detaillierter erläutert (siehe Abb. 2). Im ersten Schritt der Attestierung schickt die Anlage eine Anfrage an den Installateur der Anlage. Dieser, der zuvor durch den Regulator zur Attestierung befähigt wurde, prüft die Daten, speichert zusätzliche Informationen auf der Identitäts-Blockchain

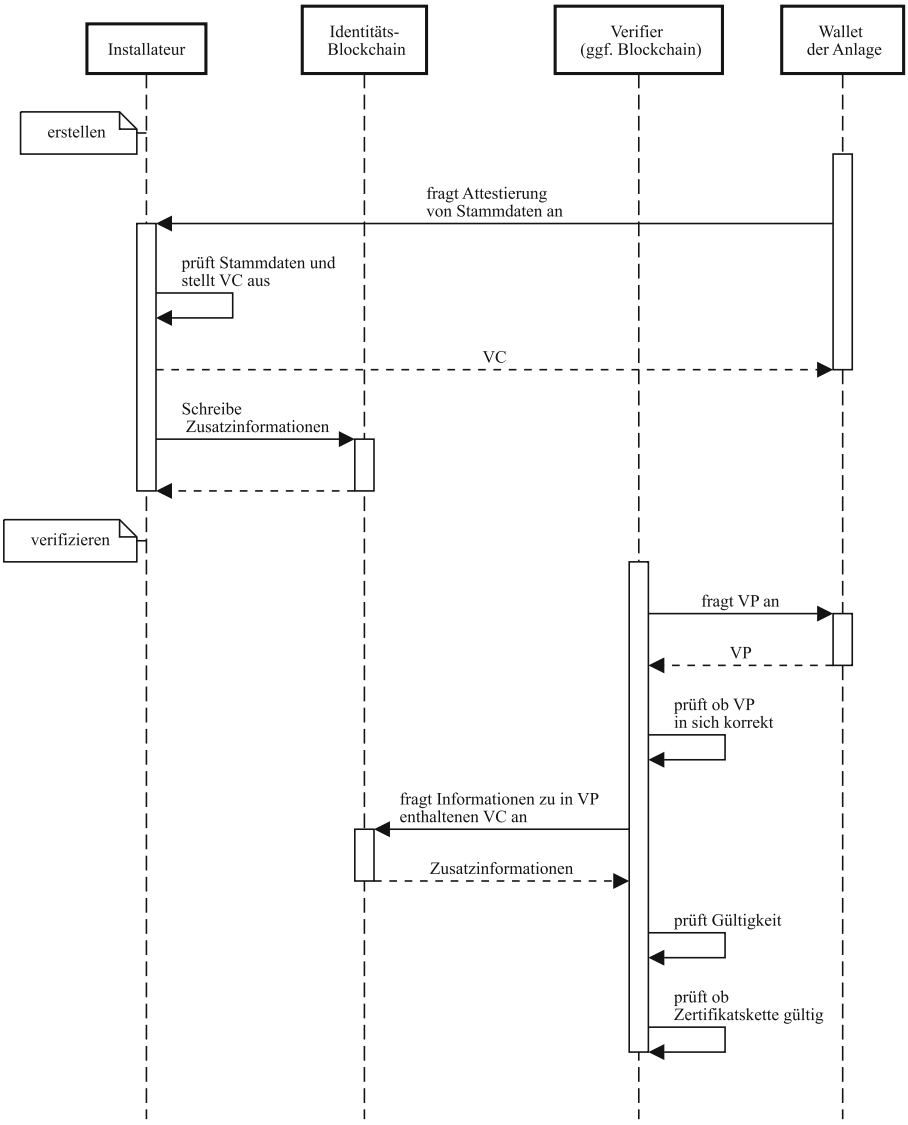

Abb. 2 Stammdaten Attestierung und Verifikation

und erstellt mit Hilfe des eigenen privaten Schlüssels ein VC und sendet dieses an die Anlage.

Möchten Eigentümer*innen einer Anlage, ein oder mehrere Eigenschaften der Stammdaten gegenüber einem Verifier, zum Beispiel anderen Marktteilnehmenden, beweisen, stoßen sie einen Verifizierungsprozess an. Die Verifier fragen zunächst bei der Anlage die zugehörige VP an, welche von der Anlage auf Basis des VC über ihre Stammdaten erstellt und versendet wird. Daraufhin überprüfen die Verifier die Korrektheit der VP und deren Signatur. Anschließend greifen sie auf das auf

der Blockchain gespeicherte Register zu, das die Identitäten von offiziell befähigten Issuern und ein Gültigkeitsregister für alle existierenden VCs verwaltet. Mithilfe dieser Informationen können sie die Gültigkeit des der VP zugrundeliegenden VCs sowie die Legitimität der Issuer des VCs überprüfen, die durch Zertifikatsketten sichergestellt werden. Wenn diese Überprüfungen erfolgreich sind, ist der Verifizierungsprozess abgeschlossen. Ein möglicher Vorteil des SSI-basierten Verifizierungsprozesses ist dabei, dass zu keinem Zeitpunkt eine Kommunikation zwischen Verifier und Issuer benötigt wird. Anders als in zentralistischen Identitätssystemen stellt der Issuer somit keinen Single-Point-of-Failure dar.

Das im BMIL-Projekt erprobte SSI-basierte Konzept stellt eine Lösung zur Bereitstellung und Verifizierung von dezentral erzeugten Stamm- und Transaktionsdaten dar. Die Anlagen und deren Eigentümer*innen sind hierbei in der Lage, eigenständig sichere Kommunikationskanäle zu anderen Marktakteuren herzustellen, darüber selbstverwaltete, verifizierbare Stamm- und Bewegungsdaten weiterzuleiten und somit das Potenzial der SMGWs und der durch sie erfassten Bewegungsdaten zu heben. Dabei wird durch entsprechende Vertrauensketten Vertrauen in das System gebracht und durch die eindeutigen, digitalen Identitäten die Authentizität der Oracles gewährleistet. Dies trägt zur Lösung des Oracle-Problems, nach Definition von (Curran 2018) bei. Während der Einsatz der Hardwarekomponenten sehr anwendungsspezifisch ist, lassen sich das Gesamtkonzept sowie einzelne Softwarekomponenten auch auf andere Instanzen des Oracle-Problems übertragen, insbesondere auf Instanzen, in denen eine Verifizierung von einer Vielzahl von Oracles notwendig ist.

4 Handlungsempfehlungen

Im BMIL-Projekt wurde ein SSI-basiertes Konzept zur sicheren Integration von Anlagendaten in ein digitales Energiesystem erprobt. Im besonderen Fokus stand dabei ein Lösungskonzept für das Oracle Problem, im Speziellen für die digitale und verifizierbare Integration von dezentral verteilten IoT-Geräten durch die Kombination aus einer vertrauensvollen Instanz und digitalen Identitäten. Die Analyse dieses Projektes und die Abstrahierung der gewonnen Erkenntnisse ermöglichen es, die folgenden allgemeinen Handlungsempfehlungen für die Integration dezentraler Oracles in digitale Informationssysteme mithilfe des SSI-Paradigmas abzuleiten:

1. *Verifizierbare Identitäts- bzw. Stammdaten bilden die Grundlage für vertrauenswürdige Oracle-Daten*:
   Damit Oracle-Daten für Informationssysteme von Wert sind, müssen die Oracles als Datenquellen vertrauenswürdig sein. Aufbauend auf dem SSI-Paradigma können diese Oracles von einer vertrauenswürdigen Partei mit einer (digitalen) Identität ausgestattet werden und diese Identität durch kryptographische Verfahren mit denen von ihnen gemeldeten Daten verifizierbar verknüpfen. Dadurch können andere Teilnehmende im System zum einen überprüfen, von welchem Oracle diese Daten gemeldet wurden, und sich zum anderen vergewissern, dass dieses Oracle von einer vertrauenswürdigen Partei installiert oder geprüft wurde. Somit ermöglicht das Vorhandensein von verifizierbaren Identitäts- bzw. Stammdaten, die von

einer vertrauenswürdigen Partei ausgestellt wurden, das Vertrauen in die Oracle Daten.

2. *Für eine zweifelsfreie Verifikation der Daten muss eine starke Gerätebindung gewährleistet sein*:
   Kryptographische Primitive bilden die Grundlage für die in *(1)* erwähnte Verifizierbarkeit von digitalen Identitäten bzw. der Herkunft von Oracle-Daten. So ermöglicht asymmetrische Verschlüsselung die Signatur von Daten, wodurch nachträgliche Manipulation verhindert und gleichzeitig deren Herkunft dem signierenden Schlüssel und der damit verbundenen digitalen Identität zugeordnet werden können. Um dieser digitalen Identität auch das physische Gerät und damit die Datenquelle verlässlich zuordnen zu können, muss eine starke Bindung der verwendeten Schlüssel zum jeweiligen physischen Gerät bestehen. Dies kann durch sichere Hardware, wie z. B. ein Hardware Secure Module, gewährleistet werden, die kryptographischen Schlüssel sicher und unzugänglich speichern können. Nur durch diese Untrennbarkeit kann sichergestellt werden, dass sich hinter der digitalen Identität auch das korrekte physische Oracle befindet, und somit, dass die in *(1)* beschriebene Vertrauenswürdigkeit der Daten gewährleistet werden kann.
3. *Nahtlose Vertrauensketten von vertrauenswürdigen Institutionen zu multiplen Issuern ermöglichen eine skalierbare und gleichzeitig vertrauenswürdige Zertifizierung*:
   Eine Pluralität von Geräten, deren erhobenen Daten und der damit verbundenen Verwertung, erfordert auch eine Pluralität an Issuern. Hierzu benötigt man zum einen vertrauensvolle Institutionen, denen über Domänengrenzen hinweg Dienstleister vertrauen, und zum anderen auch ein Konzept, um Issuer durch vertrauensvolle Institutionen autorisieren und nachvollziehbar identifizieren zu können. SSI kann diese Integration durch Vertrauensketten ausgehend von vertrauensvollen Institutionen ermöglichen. Die Identifikation von Issuern und damit die Herkunft von Zertifikaten sollte dabei für Verifier jederzeit leicht nachvollziehbar sein und stellt für ihn die Grundlage seines Vertrauens dar. Die Vertrauenskette ist nötig, um flexibel zu sein und die Arbeitslast und den Bedarf nach domänenspezifischen Kompetenzen verteilen zu können. Eine vertrauenswürdige Institution ist somit die Wurzel des Vertrauens in die Identität und damit auch in die Oracle-Daten. Die Delegierbarkeit auf multiple Issuer ist dabei notwendig, um dieses Vertrauen auch in einem dezentralen und domänenübergreifenden Oracle System übertragen zu können.
4. *Sichere Kommunikationskanäle und eine zweifelsfreie Identifikation von Verifier und Issuer werden für den Datenaustausch benötigt*:
   Um einem Informationssystem verifizierbare Oracle-Daten bereitzustellen, muss ein sicherer Kommunikationskanal aufgebaut werden können, um die Korrektheit und den Schutz der Daten sicher zu stellen. Zudem ist eine eindeutige Identifikation der jeweiligen Verifier relevant, um zu vermeiden, dass Identitätsdaten mit möglicherweise unberechtigt zugreifenden Parteien geteilt werden. Die im SSI-Konzept enthaltenen DIDs können als Grundlage zum Aufbau eines sicheren Kommunikationskanal, z. B. mithilfe des Kommunikationsprotokolls „DIDComm“, verwendet werden. Indem auch Verifier mit Identitätszertifikaten ausgestattet werden, können sich auch diese gegenüber den Bereitstellenden der

Daten authentifizieren und somit die Weitergabe von Informationen an die dafür bestimmte Partei sicherstellen. Sichere Kommunikationskanäle und die Authentifizierbarkeit von Verifiern werden also benötigt, um die Verifizierbarkeit der Informationen, und damit das daraus entstehende Vertrauen, und die selbstbestimmte Bereitstellung der Daten sicherzustellen. Dies ist insbesondere wichtig, da durch die dezentrale Etablierung von vielen direkten Verbindungen zwischen den Teilnehmenden eine erhöhte Anzahl an Kommunikationskanälen entsteht, was mit mehr potenziellen Angriffszielen einhergeht.

5. *Die Selbstbestimmtheit und Privatsphäre der Nutzenden sind essentiell für dezentrale Oracles*:
   Dezentrale, durch kommunikationsfähige Geräte erzeugte Daten haben in vielen Fällen einen potenziellen Personenbezug. Die Nutzung dieser Daten muss deshalb von deren Besitzenden freigegeben werden und auch widerrufen werden können. Darüber hinaus müssen die Besitzenden auch in der Lage sein, feingranular und spezifisch zu entscheiden welche Informationen sie mit welchen Parteien teilen möchten. Nur so kann die rechtmäßige Verwendung der Daten sichergestellt und Regularien zum Schutz der Privatsphäre, wie die DSGVO, erfüllt werden. Zudem erhöhen Selbstbestimmtheit und Privatsphäre der Nutzenden deren Bereitschaft, entsprechende Daten mit anderen Marktakteilnehmenden zu teilen. Darüber hinaus kann bei einer global umgesetzten Selbstbestimmtheit innerhalb des Systems von Erhöhung des Vertrauens untereinander ausgegangen werden. Notwendig ist daher die Selbstbestimmtheit der Nutzenden, die durch eine SSI-basierte Lösung – wie in den vorangegangenen Kapiteln erläutert – gewährleistet werden kann.

5 Zusammenfassung und Ausblick

Die Pilotierung des BMIL-Projekts zeigt auf, wie intelligente Messstellen mit Maschinenidentitäten ausgestattet werden können, um die Integration von verifizierbaren Bewegungsdaten in digitale Stromsysteme zu ermöglichen. Damit bietet das Ergebnis des BMIL-Projekts auch einen konkreten Ansatz, mit dem dem Oracle-Problem entgegnet werden kann. Eine wesentliche Erkenntnis des Projekts ist dabei, dass nicht nur die fälschungssichere Integration von Gerätedaten, sondern auch die Privatsphäre und Selbstbestimmtheit der Geräteeigentümer*innen mitbetrachtet werden muss. Das SSI-Paradigma, das auf ein dezentrales, selbstbestimmtes und auf Nutzende zentriertes Identitätsmanagement ausgerichtet ist, bietet hierbei die Möglichkeit, diese Anforderungen zu erfüllen. Darüber hinaus zeigt das Projekt auf, warum die Bereitstellung und Verifizierung von dezentral erzeugten Sensordaten nicht durch rein software-basierte Informationssysteme ermöglicht werden kann, sondern auch weitere, anwendungsspezifische Maßnahmen benötigt werden. Im konkreten Anwendungsfall des BMIL-Projekts sind dies sichere Hardware-Komponenten (zur Bindung der digitalen Identität an das physische Gerät) sowie die Etablierung von Vertrauensketten von vertrauensvollen Institutionen zu den Installateuren der intelligenten Messstellen. Insbesondere durch die Charakteristika der Selbstbestimmtheit, der bilateralen Überprüfbarkeit und seiner Flexibilität bietet das

Konzept von SSI eine Lösung für die Bereitstellung und Verifizierung von dezentral erzeugten Sensordaten.

Wenngleich der Ansatz des BMIL-Projekts interessante und wertvolle Anknüpfungspunkte für andere Anwendungsfälle bereithält, bedarf es bei einer Übertragung jedoch immer der Adressierung domänenspezifischer Anforderungen, um eine belastbare Integration von Echtweltdaten in Informationssysteme sicherstellen zu können. Mögliche Anknüpfungspunkte der in diesem Beitrag beschriebenen Erkenntnisse bestehen insbesondere im Zusammenspiel mit Datenräumen. Diese werden aktuell auf nationaler und internationaler Ebene in unterschiedlichen Branchen für die Verwaltung und das Teilen von Daten untersucht (Otto et al. 2022). Ein SSI-basiertes Identitätsmanagement wird aktuell als vielversprechende Lösung angesehen, um, unter anderem, den für den Zugriff auf Datenräume notwendigen Authentifizierungsprozess nutzendenzentriert darzustellen und die Datenqualität in diesen Räumen zu sichern. Zeitgleich überspannen Datenräume bzw. Daten-Ökosysteme verschiedene Informationssysteme innerhalb spezifischer Branchen und Anwendungsgebiete, wie zum Beispiel dem Mobilitäts- oder Logistiksektor, wodurch das Potenzial des SSI-Konzeptes, Identitätsdaten interoperabel verwendbar zu machen, noch stärker genutzt werden kann. Weiterhin schafft dieser Beitrag eine Grundlage für zukünftige Forschung im Bereich der Weiterentwicklung von Registern. In diesem Zusammenhang ergibt sich eine Vielzahl an möglichen Fragestellungen für zukünftige Beiträge, wie zum Beispiel die Interoperabilität der Register oder welche Governance-Strukturen hier zusätzlich geschaffen werden müssen.

Danksagung Wir danken dem Future Energy Lab der Deutschen Energie-Agentur für die Förderung und Zusammenarbeit innerhalb des BMIL-Projekts sowie den beteiligten Partnern. Ein dieser Veröffentlichung zugrunde liegendes Vorhaben wurde zudem mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz im Rahmen des Projektes „ID-Ideal“ unter dem Förderkennzeichen 01MN210011 gefördert.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Al-Breiki H, Rehman MHU, Salah K, Svetinovic D (2020) Trustworthy blockchain oracles: review, comparison, and open research challenges. IEEE Access 8:85675–85685. https://doi.org/10.1109/ACCESS.2020.2992698

Allen C (2016) The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Zugegriffen: 31. Aug. 2022

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 Inform. https://doi.org/10.1186/s42162-022-00199-3

Babilon L, Battaglia M, Robers M, Degel M, Ludwig K (2022) Energy Communities: Beschleuniger der dezentralen Energiewende. Deutsche Energie-Agentur GmbH. https://www.dena.de/newsroom/publikationsdetailansicht/pub/dena-analyse-energy-communities-beschleuniger-der-dezentralen-energiewende/. Zugegriffen: 29. Jan. 2023

Beck R, Avital M, Rossi M, Thatcher JB (2017) Blockchain technology in business and information systems research. Bus Inf Syst Eng 59:381–384. https://doi.org/10.1007/s12599-017-0505-1

Berger B, Huber S, Pfeifhofer S (2020) OraclesLink: An architecture for secure oracle usage. In: 2020 Second International Conference on Blockchain Computing and Applications (BCCA), S 66–72 https://doi.org/10.1109/BCCA50787.2020.9274455

Buterin V (2014) Ethereum: a next-generation smart contract and decentralized application platform. Ethereum. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf. Zugegriffen: 29. Jan. 2023

Caldarelli G (2020a) Real-world blockchain applications under the lens of the oracle problem. A systematic literature review, S 1–6 https://doi.org/10.1109/ICTMOD49425.2020.9380598

Caldarelli G (2020b) Understanding the Blockchain oracle problem: a call for action. Information 11:509. https://doi.org/10.3390/info11110509

Cisco (2020) Cisco annual Internet report (2018–2023). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Zugegriffen: 29. Jan. 2023

Curran B (2018) What are oracles? Smart contracts, chainlink & "The oracle problem". https://blockonomi.com/oracles-guide/. Zugegriffen: 22. Aug. 2022

Damjan M (2018) The interface between blockchain and the real world. Ragion Pratica. https://doi.org/10.1415/91545

Deutsche Energie-Agentur (2019) Blockchain in the integrated energy transition. https://www.dena.de/newsroom/publikationsdetailansicht/pub/blockchain-in-der-integrierten-energiewende/. Zugegriffen: 2. Febr. 2023

Deutsche Energie-Agentur (2022) Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem; Aufbau eines Identitätsregisters auf Basis der Blockchain-Technologie (Pilot: Blockchain Machine Identity Ledger). https://www.dena.de/newsroom/publikationsdetailansicht/pub/bericht-digitale-maschinen-identitaeten-als-grundbaustein-fuer-ein-automatisiertes-energiesystem/. Zugegriffen: 29. Jan. 2023

Forte P, Romano D, Schmid G (2017) Beyond Bitcoin: a critical look at blockchain-based systems. Cryptography 1:15. https://doi.org/10.3390/cryptography1020015

Fridgen G, Keller R, Körner M-F, Schöpf M (2020) A holistic view on sector coupling. Energy Policy 147:111913. https://doi.org/10.1016/j.enpol.2020.111913

Heffron R, Körner M-F, Wagner J, Weibelzahl M, Fridgen G (2020) Industrial demand-side flexibility: A key element of a just energy transition and industrial development. Appl Energy 269:115026. https://doi.org/10.1016/j.apenergy.2020.115026

Heffron RJ, Körner M-F, Schöpf M, Wagner J, Weibelzahl M (2021) The role of flexibility in the light of the COVID-19 pandemic and beyond: Contributing to a sustainable and resilient energy future in Europe. Renew Sustain Energy Rev 140:110743. https://doi.org/10.1016/j.rser.2021.110743

Kõlvart M, Poola M, Rull A (2016) Smart contracts. In: The future of law and eTechnologies, S 133–147 https://doi.org/10.1007/978-3-319-26896-5_7

Körner M-F, Sedlmeir J, Weibelzahl M, Fridgen G, Heine M, Neumann C (2022) Systemic risks in electricity systems: A perspective on the potential of digital technologies. Energy Policy 164:112901. https://doi.org/10.1016/j.enpol.2022.112901

Lacity M, Carmel E (2022) Self-sovereign identity and verifiable credentials in your digital wallet. MIS Quart Exec 21(3):Article 6

Li S, Da Xu L, Zhao S (2015) The internet of things: a survey. Inf Syst Front 17:243–259. https://doi.org/10.1007/s10796-014-9492-7

Michael M, Michael K, Perakslis C (2015) Überveillance the web of things and people: What is the culmination of all this surveillance? IEEE Consumer Electronics Magazine 4(2):107–113. https://doi.org/10.1109/MCE.2015.2393007

Mondejar ME, Avtar R, Diaz HLB, Dubey RK, Esteban J, Gómez-Morales A, Hallam B, Mbungu NT, Okolo CC, Prasad KA, She Q, Garcia-Segura S (2021) Digitalization to achieve sustainable devel-

opment goals: steps towards a smart green planet. Sci Total Environ 794:148539. https://doi.org/10.1016/j.scitotenv.2021.148539
Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. SSRN Journal. https://doi.org/10.2139/ssrn.3977007
Otto B, ten Hompel M, Wrobel S (2022) Designing data spaces https://doi.org/10.1007/978-3-030-93975-5
Preukschat A, Reed D, Searls D (2021) Self-sovereign identity; Decentralized digital identity and verifiable credentials
Roth T, Utz M, Baumgarte F, Rieger A, Sedlmeir J, Strüker J (2022) Electricity powered by blockchain: A review with a European perspective. Appl Energy 325:119799. https://doi.org/10.1016/j.apenergy.2022.119799
Schlatt V, André S, Urbach N, Fridgen G (2016) Blockchain: Grundlagen, Anwendungen und Potentiale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. https://publica.fraunhofer.de/entities/publication/dc9322f0-3063-4792-b69a-b2006982d857/details. Zugegriffen: 29. Jan. 2023
Sedlmeir J, Völter F, Strüker J (2021) The next stage of green electricity labeling: using zero-knowledge proofs for blockchain-based certificates of origin and use. SIGENERGY Energy Inform Rev 1:20–31. https://doi.org/10.1145/3508467.3508470
Sporny M, Longley D, Drummond R (2022) Decentralized Identifiers (DIDs) v1.0; Core architecture, data model, and representations. https://www.w3.org/TR/did-core/. Zugegriffen: 29. Aug. 2022
Strüker J, Weibelzahl M, Körner M-F, Kießling A, Franke-Sluijk A, Hermann M (2021a) Decarbonisation through digitalisation: Proposals for transforming the energy sector https://doi.org/10.15495/EPUB_UBT_00005762
Strüker J, Urbach N, Guggenberger T, Lautenschlager J, Ruhland N, Schlatt V, Sedlmeir J, Stoetzer J-C, Völter F (2021b) Self-Sovereign Identity; Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten (Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT)
Wood D (2014) Ethereum: A secure decentralised generalised transaction ledger. https://files.gitter.im/ethereum/yellowpaper/viyt/paper.pdf. Zugegriffen: 29. Aug. 2022