Bogensperger, Alexander et al.

Working Paper

Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft?

Bayreuther Arbeitspapiere zur Wirtschaftsinformatik, No. 68

Provided in Cooperation with:
University of Bayreuth, Chair of Information Systems Management

Suggested Citation: Bogensperger, Alexander et al. (2021) : Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft?, Bayreuther Arbeitspapiere zur Wirtschaftsinformatik, No. 68, Universität Bayreuth, Lehrstuhl für Wirtschaftsinformatik, Bayreuth, https://doi.org/10.15495/EPub_UBT_00005707

This Version is available at:
https://hdl.handle.net/10419/237670

UNIVERSITÄT BAYREUTH

Bayreuther Arbeitspapiere zur Wirtschaftsinformatik

Alexander Bogensperger, Andreas Zeiselmair, Michael Hinterstocker,
Patrick Dossow, Johannes Hilpert, Maximilian Wimmer, Carsten von Gneisenau,
Nikolas Klausmann, Jens Strüker, Nils Urbach, Benjamin Schellinger,
Johannes Sedlmeir, Fabiane Völter

Diskussionspapier: Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft?

No. 68
Juli 2021

Diskussionspapier

Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft?

FfE

UNIVERSITÄT BAYREUTH

Stiftung Umweltenergierecht

2021

Diskussionspapier

Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft?

Herausgeber:

FfE

Am Blütenanger 71, 80995 München
+49 (0) 89 158121-0
info@ffe.de
www.ffe.de

Diskussionspapier aus dem Projekt

InDEED

Konzeption, Umsetzung und Evaluation einer auf Blockchain basierenden energiewirtschaftlichen Datenplattform für die Anwendungsfelder „Labeling" und „Asset Logging"

Veröffentlicht am:

22.07.2021

FfE-Auftragsnummer:

BMWI-70

Autoren der FfE

Alexander Bogensperger,
Andreas Zeiselmair,
Michael Hinterstocker,
Patrick Dossow

AutorInnen der Universität Bayreuth

Prof. Dr. Jens Strüker,
Prof. Dr. Nils Urbach,
Benjamin Schellinger,
Johannes Sedlmeir,
Fabiane Völter

Autoren der Stiftung Umweltenergierecht

Dr. Johannes Hilpert,
Dr. Maximilian Wimmer,
Carsten von Gneisenau,
Nikolas Klausmann

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Förderkennzeichen:

03E16026 A-D

Inhalt

Vorwort

Bei der Blockchain-Technologie handelt es sich um ein dezentrales elektronisches Register für digitale Transaktionen. Zu den Eigenschaften der Technologie zählen u. a. eine hohe Manipulationsresistenz, welche Vertrauen in digitale Daten erzeugen kann, sowie die Möglichkeit, Prozesse und Transaktionen, ohne Intermediär abzuwickeln. Diese besonderen Eigenschaften ermöglichen die Entstehung eines „Internets der Werte". Während Kryptowährungen den bekanntesten Anwendungsfall darstellen (oft auch „digitale Währungen" oder „Krypto-Token" genannt), sind seit der Einführung der Technologie im Jahr 2008 viele weitere Anwendungsfälle diskutiert worden. Dabei bietet sich die Technologie nicht als Universallösung für jegliche Problemstellungen an. Das nachfolgende Diskussionspapier soll aufzeigen, in welchen Branchen sich die Technologie bereits etabliert hat, welche allgemeinen Missverständnisse die Technologie umgeben und wo ihre energiewirtschaftlichen Einsatzmöglichkeiten liegen. Zudem soll aufgezeigt werden, welche technologieunabhängigen Hürden den Einsatz der Technologie erschweren.

Das nachfolgende Diskussionspapier setzt Grundlagenwissen zur Blockchain-Technologie voraus. Detailinformationen zur Technologie sowie den hier verwendeten Begriffen und technischen Grundlagen ist [1] und [2] zu entnehmen.

1 Blockchain – was bleibt nach dem Hype?

Die Blockchain-Technologie bietet zahlreiche Anwendungsmöglichkeiten, die bereits sukzessiv erste funktionierende Anwendungsfälle und Geschäftsmodelle hervorbringt. In unterschiedlichen Bereichen hat sich die Technologie bereits über einen Proof-Of-Concept-Status hinaus weiterentwickelt. Nachfolgend stellen wir Produktivsysteme vor, bei welchen sich die Technologie bereits im Einsatz befindet.

Compound Finance

Compound Finance ist eine Blockchain-basierte Finanzanwendung und ermöglicht die Aufnahme und Vergabe von Krediten in einem dezentralen Finanzökosystem (DeFi). Nutzer können das Compound-Protokoll nicht nur verwenden, um Krypto-Vermögenswerte zu leihen, sondern auch, um sie an andere NetzwerkteilnehmerInnen zu verleihen. Nutzer dieser Finanzanwendungen profitieren von den Vorteilen einer dezentralen Plattform wie der intermediärsfreien Abwicklung von Krediten sowie der Verwendung von Smart Contracts, die die Verwahrung der Sicherheiten vollständig automatisieren. [3] Über diesen Anwendungsfall hinaus existieren weitere DeFi-Anwendungen wie Stable Coins, dezentrale Börsen oder Finanzderivate. Insgesamt sind bereits über US$ 60 Mrd. in DeFi-Anwendungen an Krypto-Assets hinterlegt. (Stand 18.04.2020).[1]

TradeLens

Die auf Blockchain basierende Plattform TradeLens, welche gemeinsam von der Reederei Maersk und dem Technologiedienstleister IBM entwickelt wird, dient der transparenten, manipulationssicheren Nachverfolgung von Lieferketten in der Container-Schifffahrtsindustrie. Durch den Zusammenschluss von fünf der sechs größten Transportunternehmen in diesem Bereich ist bereits mehr als die Hälfte der weltweiten Containerfracht auf See in diesem System erfasst. Mit der Plattform können Prozesse, welche bisher häufig analog erfasst wurden, digital abgebildet werden. Die Eigenschaften der Technologie als verteiltes System entsprechen der Struktur der Branche.[2]

Building Blocks

Das Welternährungsprogramm der Vereinten Nationen setzt in mehreren Flüchtlingslagern auf den Einsatz von Blockchain-Technologie zur Verteilung von Zuwendungen an Geflüchtete. Dies ist dort sinnvoll, wo Geflüchtete kein Konto eröffnen können oder lokale Finanzsysteme nicht in der Lage sind, eine verlässliche Infrastruktur bereitzustellen. Mittlerweile nutzen 106.000 Geflüchtete das System. Mittels Iris-Scan erfolgt eine Identifizierung der Geflüchteten. Die eigentliche Abrechnung über Fiat-Währung erfolgt nach Verrechnung mit der Blockchain über einen Zahlungsdienstleister.[3]

MediLedger

Die Gesetzgebung vieler Staaten (darunter USA und Europa) im Bereich der Pharmaindustrie schreibt das Tracking von Medizinprodukten und deren Inhaltsstoffen sowie eine eindeutige Identifizierung vor. In großen und weit verzweigten Industrien ist dies jedoch nur schwer über einzelne Insellösungen möglich. Die Blockchain-Technologie ist hier ein neuer

[1] Vgl. www.defipulse.com
[2] Vgl. www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens
[3] Vgl. innovation.wfp.org/project/building-blocks

Industriestandard für alle Akteure entlang der gesamten Wertschöpfungskette. Unter den beteiligten Unternehmen befinden sich u. a. Pfizer, Bayer und Amgen.[4]

Diese Beispiele zeigen, dass die Technologie bereits im produktiven Einsatz ist. Während sich die ersten Anwendungsfälle mit unterschiedlichen Ausgestaltungen von Kryptowährungen befassten, liegt der Fokus der genannten Produktivsysteme für Realgüter auf der Schaffung von Transparenz, Manipulationssicherheit und der Harmonisierung von Strukturen durch Dezentralität. Diese Anwendungsbeispiele zeigen, dass der Einsatz der Technologie in bestimmten Anwendungsfällen bereits heute sinnvoll sein kann. Dennoch kann die Technologie nicht alle (z. T. überhöhten) Erwartungen aus ihren Anfangsjahren erfüllen. Dies liegt unter anderem daran, dass viele Meinungen, Aussagen und Überzeugungen zur Blockchain-Technologie überspitzt und teils auch mittlerweile durch technologischen Fortschritt überholt sind. Die nachfolgende Diskussion verschiedener Thesen soll daher dazu dienen, Missverständnisse aufzuklären und den eigentlichen Wert der Technologie objektiv darzulegen. Neben allgemeinen Thesen liegt der Fokus insbesondere auf der technischen, rechtlichen und energiewirtschaftlichen Perspektive.

[4] Vgl. www.mediledger.com

2 Thesen zur Blockchain-Technologie in der Energiewirtschaft

In diesem Kapitel werden zu Beginn allgemeine Thesen zur Blockchain-Technologie vorgestellt und anschließend spezifische Thesen sowohl aus technischer, juristischer und energiewirtschaftlicher Perspektive näher untersucht. Diese sollen dabei helfen, die Technologie, ihre Eigenschaften, Vor- und Nachteile sowie ihre Bedeutung für die Energiebranche besser zu verstehen. Die folgenden Tabellen fassen die einzelnen Thesen übersichtlich zusammen.

ALLGEMEINE THESEN	
1.	Die Blockchain-Technologie ist vielfältig.
2.	Die Blockchain-Technologie ist für einen intermediärsfreien Wertaustausch zwischen vielen Akteuren eine aussichtsreiche Lösung.
3.	Fast alle Blockchain-Anwendungsfälle könnten auch ohne die Technologie abgebildet werden.
4.	Durch zentrale Instanzen können sich Abhängigkeiten, Single-Points-of-Failure, Ineffizienzen und Monopole ergeben, die für einzelne oder alle beteiligten Akteure ein (wirtschaftliches) Risiko darstellen können.
5.	Kryptowährungen sind der primäre Nutzungszweck von Blockchains.
6.	Auf Basis einer Blockchain-Infrastruktur können (Mikro-)Transaktionen auch auf öffentlichen, zugangsunbeschränkten Blockchain-Lösungen automatisiert und zu geringen Kosten durchgeführt werden.

THESEN ZUR TECHNISCHEN ENTWICKLUNG	
7.	Die Konsensfindung in Blockchain-Systemen ist sehr energieintensiv und somit ressourcenineffizient.
8.	Aufgrund der redundanten Speicherung von Daten ist die Energieeffizienz von Blockchain-Anwendungen systematisch geringer als bei einer energieoptimierten und zentralisierten Lösung.
9.	Die Transparenz und Unveränderbarkeit von Transaktionen auf Blockchains verletzten immer datenschutzrechtliche Vorgaben.
10.	Die Performanz von Blockchain-Lösungen ist immer geringer als die von zentralisierten Lösungen.
11.	Zero-Knowledge-Proofs können die Richtigkeit von Prozessen automatisiert und datenschutzkonform beweisen.
12	Blockchains und Smart Contracts eignen sich für die Verarbeitung großer Datenmengen und die Ausführung komplexer Berechnungen.
13.	Komplexe Berechnungen (z. B. Optimierungen) können off-chain ausgeführt werden.
14.	Smart Contracts sind „smart“.
15.	Smart Contracts eignen sich zur Verarbeitung von verschlüsselten oder gehashten Daten.
16.	Smart Contracts sind sicher.

JURISTISCHE THESEN	
17.	Aufgrund ihrer Unveränderbarkeit dürfen auf einer Blockchain keine personenbezogenen Daten direkt gespeichert werden.
18.	Bei Smart Contracts handelt es sich nicht um Verträge im Rechtssinne, sondern um Programmcode.
19.	Rechtliche Hürden beim Einsatz von Blockchains im P2P-Handel bestehen auch außerhalb des Datenschutzrechts.
20.	Viele Anwendungsfälle der Blockchain-Technologie im Kontext von EEG-Anlagen hängen energierechtlich am Doppelvermarktungsverbot und können dadurch nur in eingeschränktem Maße umgesetzt werden.
21.	Der energierechtliche Ordnungsrahmen spricht nicht gegen die Durchführung von Asset Logging-Anwendungsfällen mittels Blockchain-Technologie.

THESEN ZU ENERGIEWIRTSCHAFTLICHEN EINSATZMÖGLICHKEITEN	
22.	Die Blockchain-Technologie verbessert bestehende und etabliert neue Prozesse in der Energiewirtschaft.
23.	Smart Meter können schon heute direkt mit Blockchains interagieren.
24.	Durch den Einsatz von Zero-Knowledge-Proofs lassen sich viele energiewirtschaftliche Prozesse automatisiert abwickeln.
25.	Die Smart-Meter-Infrastruktur bietet der Blockchain eine optimale Möglichkeit für eine korrekte digitale Datenerfassung.
26.	Der Einsatz der Blockchain im Letztverbrauchersegment ist durch die fehlende Digitalisierung nur schwer skaliert möglich.
27.	Eine eindeutige Identifizierung der beteiligten Akteure oder Anlagen sowie deren Marktrollen, Funktionen oder Eigenschaften ist für viele Anwendungsfälle notwendig.

2.1 Allgemeine Thesen

1) Die Blockchain-Technologie ist vielfältig.

Wenngleich im Nachfolgenden immer „die Blockchain-Technologie" genannt wird, handelt es sich eher um einen Oberbegriff für verschiedenste Ausgestaltungsvarianten. Während die Eigenschaften Redundanz, Resistenz gegen ein Minimum an Ausfällen bzw. Angreifern und Manipulationssicherheit verschiedenste Ausgestaltungsvarianten vereinen, existieren viele verschiedene Lösungsansätze, welche die Schwachstellen der ersten Blockchain (Bitcoin) zu beheben versuchen. Dabei wird teils auf sehr unterschiedliche Ansätze gesetzt. Der Fokus wird daher im Folgenden auf solche Ausgestaltungen der Blockchain-Technologie und weiterführende Konzepte gelegt, die in energiewirtschaftlichen Anwendungsfällen bereits zum Einsatz kommen.

2) Blockchain-Technologie ist für einen intermediärsfreien Wertaustausch zwischen vielen Akteuren eine aussichtsreiche Lösung.

Für einen Wertaustausch mittels Blockchain wird kein vertrauensstiftender Intermediär benötigt[5]. Dabei baut die Blockchain-Technologie auf vielen bereits vorhandenen technischen

[5] Allerdings wird oftmals für die Überprüfung der Integrität von Identitäten auf Intermediäre außerhalb des Netzwerks zurückgriffen.

Lösungen insbesondere aus der Kryptographie auf. Damit wird es möglich, Double-Spending zu verhindern und einen Konsensus über den Netzwerkstatus zu finden. Die wesentliche Innovation der Technologie ist es dabei, Manipulationsresistenz, Vertrauen und Sicherheit in einem dezentralen Netzwerk zu ermöglichen. Grundsätzlich können Daten, beispielsweise mithilfe von digitalen Signaturen, auch ohne Blockchain bilateral übertragen und verifiziert werden. Die Blockchain-Technologie bietet allerdings die Möglichkeit, Geschäftslogiken (mittels Smart Contracts) abzubilden und Werte im digitalen Raum manipulationssicher zu transferieren. Sie ermöglicht es, eine Vielzahl von Akteuren auf einer neutralen, dezentralen Plattform intermediärsfrei zu verbinden. Die Beispiele in Abschnitt 0 zeigen, dass sich die Technologie bereits in einigen Bereichen etablieren konnte.

3) Fast alle Blockchain-Anwendungsfälle könnten auch ohne die Technologie abgebildet werden.

Die wesentlichen Vorteile der Blockchain-Technologie für Anwendungsfälle in der Energiewirtschaft liegen in der manipulationsresistenten und transparenten Datenerfassung und -verarbeitung mit diskreten Zeitstempeln. Für all diese Eigenschaften stehen alternative technische Möglichkeiten und Ansätze der Implementierung zur Verfügung, welche bereits im Praxiseinsatz erprobt sind. Daher ist generell nicht davon auszugehen, dass diskutierte Anwendungsfälle ausschließlich durch den Einsatz einer Blockchain-Lösung umgesetzt und angeboten werden können.

Gleichwohl bietet die Anwendung der Technologie in einigen Fällen die Möglichkeit, Anwendungsfälle mit Beteiligung einer Vielzahl von Parteien kostengünstiger, effizienter, sicherer und mit geringeren Zugangshürden in die praktische Anwendung zu bringen. Dies kann u. a. darauf beruhen, dass sich heterogene Parteien nicht auf einen Intermediär einigen müssen. Es ist also für jede potenzielle Anwendung ausgehend von der notwendigen Funktionalität kritisch und ergebnisoffen zu prüfen, welcher technische Ansatz zweckmäßig und sinnvoll für eine Umsetzung ist.

Zudem erlaubt die Blockchain-Technologie die Gestaltung von bisher noch nicht existierenden Prozessen und neuen Geschäftslogiken. So kann die Blockchain-Technologie in der Energiewirtschaft beispielsweise dazu eingesetzt werden, bilanzielle Energieflüsse und damit die Stromherkunft nachzuweisen, was in solchem Ausmaß bisher noch nicht möglich war. Auch die manipulationsresistente und einheitliche Dokumentation von Betriebs-, Wartungs- und Stammdaten von energiewirtschaftlichen Assets ist so branchenübergreifend möglich [4]. Mittels Decentralized Identifiers (DiDs) kann die Technologie einen Beitrag dazu leisten, auch kleinteilige IoT-Geräte und Prosumer sicher, vertrauenswürdig und datenschutzkonform in die Marktkommunikation zu integrieren. [5] In Kombination mit Zero-Knowledge-Proofs (ZKPs) können viele Kontrollprozesse, die einen Datenaustausch erfordern, vereinfacht und datensparsamer gestaltet werden. Darüber hinaus bietet die Blockchain-Technologie erstmals die technische Möglichkeit, sog. CO_2-Token abzubilden, wodurch CO_2-Emissionen auf transparente Weise über die gesamte Wertschöpfungskette hinweg nachverfolgbar gemacht werden. [6], [7], [8]

4) Durch zentrale Instanzen können sich Abhängigkeiten, Single-Points-of-Failure, Ineffizienzen und Monopole ergeben, die für einzelne oder alle beteiligten Akteure ein (wirtschaftliches) Risiko darstellen können.

Bestehende Plattform-Geschäftsmodelle zeichnen sich durch zentrale Akteure aus, welche sowohl die Bereitstellung der digitalen Plattform an sich als auch die Koordination von

Anbietern und Kunden organisieren. De facto hat der Plattformbetreiber durch die zentrale Rolle eine große Verantwortung, da ohne sein Zutun die (Handels-)Beziehungen auf der Plattform nicht funktionieren. Des Weiteren ergeben sich nicht zuletzt durch die „Economies of Scale" Entwicklungen hin zu einer oder weniger Plattformen, welche, unter anderem auch durch gesteigerte Effizienz, letztlich den Markt dominieren. „Lock-In-Effekte" erschweren einen Wechsel auf andere Plattformanbieter deutlich. Die Konsequenz sind marktdominierende zentrale Instanzen bzw. monopolistische Strukturen. Die starre Bindung an einen Plattformanbieter führt so zu (wirtschaftlichen) Abhängigkeiten, die auch dann bestehen, wenn der Anbieter seine Kostenstruktur oder das zugrunde liegende Geschäftsmodell zum Nachteil der TeilnehmerInnen ändert (Beispiel: Monetarisierung von Youtube). [9] [10] [11] [12] [13] Eine Lösung für dieses Problem stellt häufig die Regulierung der Plattformen dar, welche jedoch sowohl den weiteren Wettbewerb als auch Innovationen erschwert.

Dieses Risiko könnte durch Disintermediation und dezentralen Betrieb der Plattform durch alle beteiligten Akteure deutlich reduziert werden. Eine pauschale Bewertung ist dabei allerdings nicht möglich, da den Potenzialen eines dezentralen Plattformbetriebs auch Herausforderungen gegenüberstehen. So ist möglicherweise die Agilität bei der Weiterentwicklung der Plattform aufgrund von Marktanpassungen durch den notwendigen Konsens eingeschränkt. Auch die gezielte und zeitweise Subventionierung einzelner Marktseiten, welche ggf. große finanzielle Aufwendungen (klassischerweise für den Plattformbetreiber) bedeuten, sind so nicht möglich. Darüber hinaus kann es durch eine redundante Bearbeitung von Prozessen bei dezentralen Lösungen zu Ineffizienzen kommen. Dies sind nur wenige Beispiele für Argumente für oder gegen eine Dezentralisierung, die aus verschiedenen Anwenderperspektiven unterschiedlich bewertet werden können.

5) Kryptowährungen sind der primäre Nutzungszweck von Blockchain.

Ziel des ersten Anwendungsfalls der Blockchain-Technologie war die Schaffung eines digitalen, intermediärsfreien Zahlungssystems. Bitcoin wurde sowohl als Transaktionsgegenstand als auch für die Abwicklung dieser Transaktionen genutzt. Heute wird Bitcoin vor allem als Wertanlage gesehen. Grundsätzlich wird bei öffentlichen, zugangsunbeschränkten Blockchains, wie Bitcoin, angenommen, dass sich einzelne Akteure im Netzwerk korrupt oder böswillig verhalten können. Aufgrund der verborgenen Identitäten in solchen Netzwerken sind gezielte Strafen für regelwidriges Verhalten schwer umsetzbar, weshalb spezifische Anreizsysteme entwickelt wurden. [14]. Da die Erstellung der Blöcke, welche die validierten Transaktionen enthalten, mit hohem Aufwand verbunden sind (z. B. Energieaufwand, Hardwarekosten), wird die Gewährleistung der Netzwerkintegrität durch neu geschaffene Währungseinheiten (BTC) an Miner belohnt. Ähnliche Anreizmodelle werden heute von vielen zugangsunbeschränkten Blockchain-Netzwerken (z. B. Ethereum) genutzt [14]. Hingegen sind bei privaten Blockchain-Implementierungen die Identitäten bekannt und an die jeweiligen Akteure gekoppelt. Ein Anreizmechanismus ist aus diesem Grund nicht erforderlich, da der Verlust der Reputation von TeilnehmerInnen (z. B. ein Unternehmen) in diesem Netzwerk Anreiz genug ist, um ehrlich im Netzwerk zu agieren.

Transaktionen innerhalb eines Blockchain-Netzwerks müssen keinen Transfer von Werten zwischen TeilnehmerInnen darstellen, sie können beispielsweise auch lediglich die Protokollierung eines Datums abbilden (siehe Anwendungsfälle). Zudem ist bei einigen Anwendungsfällen eine monetäre Vergütung von ausführenden Knoten nicht erforderlich. Der Anreiz zur Ausführung einer Transaktion kann sich schon allein vom zugrunde liegenden

Anwendungsfall ableiten: Beispielsweise, wenn alle beteiligten Parteien daran interessiert sind, dass ihre Transaktionen zeitnah verarbeitet werden [15].

6) Auf Basis einer Blockchain-Infrastruktur können (Mikro-)Transaktionen auch auf öffentlichen, zugangsunbeschränkten Blockchain-Lösungen automatisiert und zu geringen Kosten durchgeführt werden.

Für die Abwicklung von Transaktionen fallen bei den meisten zugangsunbeschränkten (permissioned) Blockchains Transaktionsgebühren an, um den hohen rechnerischen und damit kostenintensiven Aufwand für die validierenden Netzwerkknoten zu kompensieren. Zudem können damit ökonomische Hürden aufgebaut werden, wodurch die Überlastung eines Netzwerks durch massenhafte Transaktionsanfragen verhindert wird. Beispielsweise wird die Durchführung einer Transaktion im Ethereum-Netzwerk mit der Einheit „Gas" bepreist, wobei die Höhe der Transaktionsgebühr abhängig von der aktuellen Nachfrage ist [16]. Die hiermit verbundene Unsicherheit und limitierte Skalierbarkeit kann Geschäftsmodelle stark einschränken und macht einige Blockchain-Netzwerke für die wirtschaftliche Abwicklung von Mikrotransaktionen unbrauchbar.

Um die Probleme von Kosteneffizienz und einer begrenzten Skalierbarkeit zu lösen, wurden alternative, sogenannte 2nd-Layer-Konzepte, wie beispielsweise Sidechains oder Payment Channels, entwickelt. [1] Diese Konzepte stellen eine zweite Schicht über dem Basisnetzwerk dar. Zudem bieten Validity Proofs wie Zero-Knowledge-Rollups (ZK-Rollups) (vgl. These 10) die Möglichkeit, die Korrektheit von Transaktionen zu beweisen und effizient von anderen Netzwerkknoten zu verifizieren. Folglich können die Knoten mit demselben Rechenaufwand deutlich mehr oder komplexere Transaktionen abbilden, ohne dabei die Sicherheit und Transparenz signifikant zu reduzieren. Trotz limitierter Blockgrößen können mit derartigen Ansätzen insbesondere Mikrotransaktionen abgebildet werden. Dennoch müssen auch hier Abwägungen getroffen werden, da viele 2nd-Layer-Konzepte auf zentralisierenden Elementen beruhen, welche im Einzelfall möglicherweise weniger vertrauenswürdig erscheinen als Intermediäre.

2.2 Thesen zur technischen Entwicklung

7) Die Konsensfindung in Blockchain-Systemen ist sehr energieintensiv und somit ressourcenineffizient.

Ein Konsensmechanismus stellt sicher, dass sich alle beteiligten Knoten auf den gleichen Stand der Blockchain sowie der neu hinzuzufügenden Blöcke einigen und dieser Stand als einzige valide Version akzeptiert wird. Entsprechend hängt die Sicherheit eines Blockchain-Systems grundlegend von seinem Konsensmodell ab [17] [18]. Die aktuell größten öffentlichen (public) Blockchains (z. B. Bitcoin oder Ethereum) verwenden derzeit Proof-of-Work (PoW) als Konsensmechanismus. Die Kernidee ist dabei, die Verrechnungsrechte und Belohnungen durch einen Wettbewerb von Rechenleistung („Hashing Power") zur Lösung eines kryptographischen Rätsels auf die beteiligten Knoten („Miner") zu verteilen. Die eingesetzte Rechenleistung resultiert in einem entsprechend hohen elektrischen Energieverbrauch [19] [20] [21]. Aufgrund dieser und weiterer Aspekte wurden in der jüngeren Vergangenheit eine Vielzahl alternativer Konsensmechanismen entwickelt [22] [1] [23].

Proof-of-Stake (PoS) ist dabei der für öffentliche und frei zugängliche Blockchains meistdiskutierte Konsensmechanismus, welcher auch schon in kürzlich eingeführten Blockchains wie Algorand, Cosmos, Polkadot oder Tezos Verwendung findet. Bei PoS handelt

es sich um einen spieltheoretisch motivierten Ansatz zur Konsensfindung in öffentlichen, frei zugänglichen Blockchains. Dabei wird durch eine Zufallsauswahl ermittelt, welche NetzteilnehmerInnen die nächsten Blöcke vorschlagen dürfen. Diese „Zufallsauswahl" kann entweder am Anteil der jeweiligen Kryptowährung und/oder nach der Teilnahmedauer der einzelnen NetzteilnehmerInnen im Netzwerk gewichtet sein. Aktuell erhält dieser Konsensmechanismus erhöhte Aufmerksamkeit durch die Umstellung Ethereums von PoW auf PoS. [2] Damit werden u. a. eine bessere Skalierbarkeit sowie eine verbesserte Nachhaltigkeit durch deutlich geringeren Energieverbrauch versprochen – laut [24] entspricht dies einer Reduktion von über 99 %.

Proof-of-Authority (PoA) Konsensmechanismen stellen eine weitere Alternative dar. Diese kommen vorwiegend in zugangsbeschränkten, privaten Blockchains zum Einsatz. Bei PoA wird einzelnen ausgewählten und vertrauenswürdigen Instanzen (sog. „authorities") vorab das Recht zur Validierung von Transaktionen zugesprochen. Da sich der Konsens auf wenige, vorab definierte Knoten beschränkt und somit kein Auswahlprozess notwendig ist, wird auch hier deutlich weniger Energie verbraucht.

Da der energieintensive Teil des PoW-Konsensmechanismus mit den alternativen Ansätzen ersatzlos wegfällt, ist der Energieverbrauch der Validierungsknoten nur unwesentlich höher als der Stand-By-Verbrauch. Berücksichtigt man die Redundanz in einem Blockchain-Netzwerk, skaliert dies allerdings mit der Anzahl an beteiligten Knoten. Abbildung 2-1 gibt eine Abschätzung der Größenordnung des Energieverbrauchs pro Transaktion für verschiedene Architekturen.

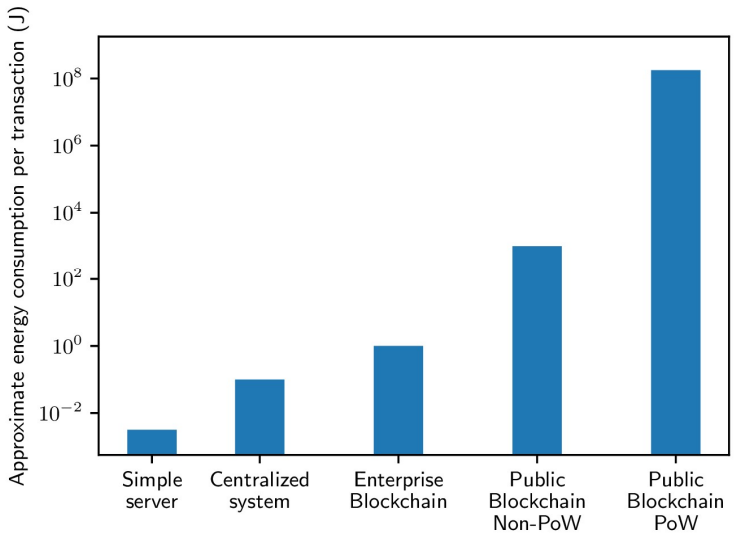

Abbildung 2-1: Geschätzter Energieverbrauch von Transaktionen in verschiedenen Systemen im Vergleich [21]

Demnach ist der Energieverbrauch unter Verwendung von alternativen Konsensmechanismen im Vergleich zur Verwendung von PoW nahezu vernachlässigbar. Im Vergleich zu einer zentralen Serverarchitektur kann sich der Energieverbrauch je nach angestrebter Redundanz und der damit einhergehenden Sicherheit durchaus in einem relevanten Maßstab erhöhen.

8) Aufgrund der redundanten Speicherung von Daten ist die Energieeffizienz von Blockchain-Anwendungen systematisch geringer als bei einer energieoptimierten und zentralisierten Lösung.

Im Vergleich zu zentralisierten Lösungen werden Transaktionen redundant durch alle NetzwerkteilnehmerInnen ausgeführt und gespeichert. Im Gegensatz zu einer zentralisierten Lösung, in welcher die Daten bei Ausfall komplett verloren gingen, kann mit einer redundanten Ausführung die Verfügbarkeit der Daten erhöht werden. Dabei verringert sich zusätzlich die Wahrscheinlichkeit eines Datenverlusts bei Ausfall eines oder mehrerer Netzwerknoten. Um das Netzwerk zu manipulieren, müsste ein Angreifer zudem einen Großteil der ausführenden Knoten auf seine Seite bringen oder einen Großteil der Ressourcen erlangen, die von den ausführenden TeilnehmerInnen aufgebracht werden [2].

Dennoch hat Sicherheit durch Redundanz auch zur Folge, dass Transaktionen i. d. R. durch jeden NetzwerkteilnehmerInnen redundant ausgeführt[6] und Blöcke redundant gespeichert werden. So erfolgt beispielsweise die Prüfung von Signaturen nicht durch eine zentrale Partei, sondern durch alle NetzwerkteilnehmerInnen. Der Energieverbrauch eines Blockchain-Systems steigt dabei proportional mit der Anzahl der NetzwerkteilnehmerInnen.

9) Die Transparenz und Unveränderbarkeit von Transaktionen auf Blockchains verletzten immer datenschutzrechtliche Vorgaben.

Jedem NetzwerkteilnehmerInnen ist in einer öffentlichen Blockchain die komplette Transaktionshistorie zugänglich. Dies macht es möglich, Manipulationen schnell zu identifizieren. Jedoch steht diese Transparenz in starkem Widerspruch zu datenschutzrechtlichen Vorgaben und der Einhaltung der Privatsphäre. Deshalb sollte darauf geachtet werden, dass niemals schützenswerte oder sensible Informationen (beispielsweise durch einen Personenbezug) auf eine Blockchain geschrieben werden. Diese Problematik lässt sich mittels Anonymisierungstechniken, wie beispielsweise Zero-Knowledge-Proofs (ZKPs) (vgl. These 11) oder homomorpher Verschlüsselungen (vgl. These 13), auflösen15).

Da auf der Blockchain geschriebene Daten nicht gelöscht werden können, widerspricht die Technologie den Grundsätzen der Datenschutzgrundverordnung (DS-GVO), wenn es sich dabei um personenbezogene Daten handelt (vgl. These 17).

10) Die Performanz von Blockchain-Lösungen ist immer geringer als die von zentralisierten Lösungen.

Die Performanz von Blockchain-Lösungen wird durch die Redundanz des Netzwerks negativ beeinflusst [15]. Dies gilt vor allem dann, wenn große Datenmengen verarbeitet oder gespeichert werden müssen. So bietet es sich an, Berechnungen auf zentralisierte Systeme auszulagern und nur den Beweis über die Validität dieser Berechnungen auf einer Blockchain abzulegen [26]. Bei diesem Ansatz handelt es sich um ZK-Rollup. Im Rahmen eines solchen ZK-Rollups aggregiert eine externe Entität (Operator) Transaktionen zwischen NetzwerkteilnehmerInnen über einen bestimmten Zeitraum, die nicht auf der Blockchain gespeichert werden. Anschließend sendet der Operator einen Beweis über die Veränderung der Salden an einen Smart Contract, wo dieser verifiziert wird. Im Detail errechnet der Operator den Endsaldenstand auf Basis des Anfangssaldos und den in der Zeitperiode angefallenen Transaktionen und führt diese in zwei Merkle-Bäumen (Anfangs- und Endsaldo) zusammen. Anschließend erstellt der Operator den Beweis in Form eines Zero-Knowledge-Proofs, der sich aus den zwei Merkle-Bäumen und den einzelnen Transaktionen zusammensetzt. Der Beweis wird danach, inklusive der Veränderung der Kontenstände (Delta), an einen Smart Contract zu dessen Verifizierung gesendet. Insbesondere durch die

[6] mit Ausnahmen, siehe Hyperledger Fabric [25]

„Komprimierung" bzw. aggregierte Verifizierung der digitalen Signaturen im Beweis beinhaltet dieser eine weitaus geringere Datenmenge als die anfallenden Transaktionen. Der Einsatz von ZK-Rollups ermöglicht es, Blockchain-Systeme zu skalieren und den Grad der Anonymität zu erhöhen, um letztlich eine signifikante Steigerung der Performanz zu erreichen. Dies zeigt, dass die Blockchain-Technologie keine isoliert zu betrachtende Technologie ist: Um die Performanz zu maximieren, muss innerhalb eines Ökosystems die vorhandene Rechenleistung optimiert werden. Dies kann mithilfe kryptografischer Techniken wie ZK-Rollups geschehen.

Zusätzlich sind auch weitere Technologien bereits in Erprobung, welche z. B. die Transaktionsgeschwindigkeit erhöhen oder verschiedene Blockchains miteinander verknüpfen können, um deren Auslastung zu optimieren (siehe Payment-/State-Channels und Side-Chains in [1]). Ein weiterer, vielversprechender Ansatz sind „serverless" Blockchains für zugangsbeschränkte Netzwerke im Unternehmenskontext. Diese Blockchains können rein Cloud-basiert aufgesetzt werden und damit, im Gegensatz zu ihren serverbasierten Alternativen, elastisch mit den Anforderungen skalieren.

11) Zero-Knowledge-Proofs können die Richtigkeit von Prozessen automatisiert und datenschutzkonform beweisen.

Bei Zero-Knowledge-Proofs handelt es sich im Allgemeinen um einen Beweismechanismus, bei welchem eine Person einer anderen Person belegen kann, dass sie etwas Spezielles weiß oder eine Berechnung korrekt durchgeführt wurde. Dieses Verfahren basiert auf kryptographischen Algorithmen und ermöglicht, bestimmte Eigenschaften von Daten (Attribute) einer zu verifizierenden Partei („Verifier") zu beweisen („Proof"), ohne diese selbst preisgeben zu müssen. Die Erstellung der Beweise geht aus komplexen Berechnungen hervor und ist daher ungeeignet, um auf der Blockchain selbst ausgeführt zu werden (vgl. These 12). Dagegen stellt die Verifizierung eines Beweises durch die Netzwerknoten einen vergleichsweise trivialen Aufwand dar. Blockchain-Technologie kann diese Beweise manipulationssicher dokumentieren und allen NetzwerkteilnehmerInnenn zugänglich machen. Mittels ZKPs werden keine personenbezogenen Daten anonym gespeichert, sondern vielmehr Eigenschaften über Daten gespeichert, ohne dabei einen Personenbezug (oder einen Bezug zu sonstigen schützenswerten Informationen) herstellen zu müssen. Daraus folgt, dass schützenswerte Daten auch tatsächlich geschützt werden und somit im Einklang mit datenschutzrechtlichen Vorgaben stehen [27].

12) Blockchains und Smart Contracts eignen sich für die Verarbeitung großer Datenmengen und die Ausführung komplexer Berechnungen.

Innerhalb eines dezentralen Netzwerks wird jede Transaktion an alle NetzwerkteilnehmerInnen propagiert. Somit müssen alle TeilnehmerInnen alle Transaktionen verarbeiten, also ausführen und speichern[7]. Die benötigte Zeit für die Ausführung ist dabei abhängig von der Datengröße und der Rechenleistung der TeilnehmerInnen. Eine Transaktion kann erst dann als ausgeführt betrachtet werden, wenn sie von einem Großteil der TeilnehmerInnen (abhängig vom Konsensmechanismus) verarbeitet wurde. Somit ist die Zeit (propagation time), in welcher eine Transaktion innerhalb des Netzwerks verbreitet wird, von der schwächsten Latenz, Verfügbarkeit und Rechenleistung der TeilnehmerInnen abhängig [2].

[7] mit Ausnahmen, siehe Hyperledger Fabric [25]

Auch Smart Contracts sind für komplexe Berechnungen ungeeignet. Als Smart Contract bezeichnet man automatisiert ausführbare Programme, die dezentralisiert und somit redundant auf einer Blockchain laufen (vgl. These 12). Der zentrale Mehrwert besteht dabei in der Sicherheit und überprüfbaren Korrektheit der Berechnungen. Die Ausführung von Smart Contract Code erfolgt durch die Validierungsknoten (bei Ethereum im Sinne der Ethereum Virtual Machine). [16] [28]

Die Rechenkapazität ist u. a. aufgrund der verfügbaren Zeit zwischen zwei Blöcken (sog. „block time") und der Übertragungsverzögerung innerhalb des verteilten Netzwerks begrenzt. Aus diesem Grund werden Rechenoperationen in öffentlichen Blockchains anhand eines Kostenmodells (bspw. die Abrechnung in „Gas" im Ethereum-Netzwerk) und einer maximalen Anzahl an Operationen limitiert („Gas limit"). Grund dafür ist, dass die Berechnung komplexer Prozesse die Ressourcen im Netzwerk bindet und dadurch das Netzwerk lahmgelegt werden könnte oder sich die Zeit zwischen der Blockerstellung deutlich erhöhen würde. Entsprechend sind Berechnungen zum einen mit Kosten verbunden, zum anderen nicht in beliebiger Komplexität möglich. Diese Tatsachen führen dazu, dass komplexe Berechnungen auf einer Blockchain mit den aktuellen Ansätzen nicht sinnvoll darstellbar sind.

Weniger komplexe Berechnungen sowie kleinere Datenmengen können die Geschwindigkeit bzw. den Durchsatz von Transaktionen eines Blockchain-Netzwerks erhöhen. Dies sollte für die Ausgestaltung von Prozesslogiken beachtet werden. Ein beispielhafter Anwendungsfall ist die Speicherung von Hashes, also digitalen Fingerabdrücken von Daten. Transaktionen, die lediglich einen Hash-Wert in der Blockchain speichern, können schnell verarbeitet werden und beispielsweise zum Nachweis der Richtigkeit oder Existenz von Daten dienen. Der Ansatz wird ebenfalls bei der dezentralen Datenhaltung, wie bspw. dem InterPlanetary File System (IPFS) [29] oder den in These 10 erläuterten ZK-Rollups angewandt.

13) Komplexe Berechnungen (z. B. Optimierungen) können off-chain ausgeführt werden.

Um umfangreichere Berechnungen in Blockchain-Netzwerke zu integrieren, werden aktuell Möglichkeiten entwickelt, um diese auszulagern und deren Korrektheit nachzuweisen. Eine Möglichkeit wäre ein „Service Node", welcher die Berechnung übernimmt. Mittels Zero-Knowledge-Proofs kann die Richtigkeit von „off-chain" durchgeführten Berechnungsergebnisse nachgewiesen werden [30]. Alternativ kann die Berechnung auf mehrere Parteien aufgeteilt werden. Über sog. „Consensus Oracles" können diese ausgelagert werden. Allerdings müssen die Eingangsdaten offengelegt werden [31]. Um der Offenlegung der Daten entgegenzuwirken, verspricht die (Secure) Multi Party Computation (MPC) Input-Parameter geheim zu halten, beispielsweise auf Basis von homomorpher Verschlüsselung. MPC setzt dabei auf eine verteilte Berechnung, ist aktuell jedoch noch weit von einem praktischen Einsatz entfernt [32]. Allgemein steigern all diese Lösungen die Komplexität des Systems und weisen dementsprechend nur eine begrenzte Performanz auf. Dies ist besonders auf den noch sehr frühen Entwicklungsstadium dieser Ansätze zurückzuführen. Hingegen wurden in den vergangenen Jahren bei ZKPs sowohl theoretisch als auch bei der Implementierung signifikante Verbesserungen erzielt, welche eine praktische Nutzung bereits jetzt zulassen. Die Komplexität der Implementierung ist aber nach wie vor hoch.

14) Smart Contracts sind „smart".

Wie bereits in These 10 definiert, sind Smart Contracts auf der Blockchain gespeicherte Programme, welche durch ein Ereignis automatisch ausgeführt werden, wenn vordefinierte

Bedingungen erfüllt sind [16]. Ein Ereignis bedeutet hierbei konkret, dass Smart Contracts aktiv durch einen anderen Smart Contract oder eine Transaktion ausgelöst („getriggert") werden müssen. Smart Contracts sind in diesem Sinne jedoch keine rechtlich bindenden Verträge, sondern bilden primär Geschäfts- oder Vertragslogiken ab, können Transaktionen prüfen oder andere Smart Contracts ansteuern.

Im Grunde entsprechen Smart Contracts Programmcode (auch als Chain Code bezeichnet), der auf einer Blockchain redundant gespeichert und von allen Netzwerknoten ausgeführt wird (Ausnahmen siehe Hyperledger Fabric) [2]. Da es sich bei dem hinterlegten Code zumeist um simple Logiken (bspw. Wenn-Dann-Funktionen) handelt und die Ausführung stets von einem auslösenden Ereignis abhängt, gelten Smart Contracts als nicht besonders „smart".

15) Smart Contracts eignen sich zur Verarbeitung von verschlüsselten oder gehashten Daten.

Um eine Geschäftslogik (z. B. ein Orderbuch eines Peer-to-Peer-Marktes (P2P)) im Rahmen eines Smart Contracts realisieren zu können, müssen die für die Logik notwendigen Daten (z. B. Energiemengen und Gebote) für den Smart Contract lesbar sein. Dementsprechend kommen hierbei gehashte oder verschlüsselte Daten nicht in Frage. Ein Smart Contract kann dabei nicht genutzt werden, um Daten zu entschlüsseln, da ansonsten die Schlüssel und Daten aller Validierungsknoten offengelegt werden müssten, um die Verarbeitung durchzuführen und zu prüfen. Sind die Daten für diese Zwecke nicht anonymisierbar, kommen Smart Contracts für deren Verarbeitung aus Gründen des Datenschutzes nicht in Frage.

In der Kryptographie existieren jedoch nach heutigem Stand der Forschung Techniken, die es ermöglichen, Berechnungen auf verschlüsselten Daten mittels homomorpher Verschlüsselung oder Multi Party Computation durchzuführen. Dabei beschreibt die Homomorphie in der Mathematik die Transformation eines Datensatzes in einen anderen unter Beibehaltung der Beziehungen zwischen den Elementen in beiden Sätzen. Beim Verschlüsseln bzw. Entschlüsseln in einem homomorphen Verschlüsselungsschema behalten die Daten also eine gewisse Struktur, die genutzt werden kann, um sinnvolle Berechnungen auf verschlüsselten Daten auszuführen, bspw. „Verschlüsselung(A) + Verschlüsselung(B) = Verschlüsselung(A+B)". Bei der Multi Party Computation (MPC) werden Berechnungen verteilt durchgeführt, ohne dabei die Rohdaten oder Zwischenergebnisse zu veröffentlichen. Aufgrund der Eigenschaft der oben aufgeführten Verschlüsselungstechniken, die Beziehung der Daten beizubehalten, kann nur der Eigentümer des privaten Schlüssels die verschlüsselten Daten entschlüsseln und verstehen. In der Theorie lassen sich diese verschlüsselten Daten dadurch problemlos auf der Blockchain speichern und stehen anderen NetzwerkteilnehmerInnen für Analysen und Berechnungen zur Verfügung. Hierbei ist zu erwähnen, dass sowohl die homomorphe Verschlüsselung als auch MPC aktuell nur in Spezialfällen anwendbar und noch nicht ausgereift sind. Beide Technologien weisen aktuell enorme Nachteile hinsichtlich ihrer Performanz aus und stellen somit in naher Zukunft noch keine praktikable Lösung dar.

16) Smart Contracts sind sicher.

Der Programmcode von Smart Contracts ist bei offenen, nicht zugangsbeschränkten Blockchains jederzeit öffentlich einsehbar. Bei geschlossenen Netzwerken ist dieser nur für Leseberechtigte zugänglich. Durch den Open-Source-Charakter werden Fehler, wie beispielsweise Sicherheitslücken, schneller erkannt. Dies hat zwei gegenläufige Implikationen:

Einerseits können solche Lücken schneller ausgenutzt[8] werden, andererseits können Fehler auch schneller behoben werden. In manchem Fall kann es sich lohnen, Smart Contracts von externen Parteien (beispielsweise IT-Auditfirmen) vor der Implementierung zu zertifizieren, um unerkannte Fehler zu vermeiden.

2.3 Juristische Thesen

17) Aufgrund ihrer Unveränderbarkeit dürfen auf einer Blockchain keine personenbezogenen Daten direkt gespeichert werden.

Bei der Verarbeitung von Daten, die einen unmittelbaren oder mittelbaren Personenbezug aufweisen (personenbezogene Daten), sind stets die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) zu berücksichtigen (vgl. These 11). Das Pflichtenprogramm der DS-GVO sieht in Art. 17 das „Recht auf Löschung" vor. Der Verantwortliche muss personenbezogene Daten eines Betroffenen auf dessen Verlangen hin unverzüglich löschen, wenn der ursprüngliche Zweck der Verarbeitung wegfällt oder die Einwilligung widerrufen wird.

Wurden personenbezogene Daten öffentlich gemacht, so müssen auch alle weiteren Parteien, die die personenbezogenen Daten verarbeiten, darüber informiert werden, dass die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien bzw. Replikationen dieser Daten verlangt wurde. Diese umfassende Form der Löschung ist bei der Speicherung von Daten auf einer Blockchain typischerweise nachträglich nicht mehr möglich (vgl. aber These 11 zum Einsatz von Zero-Knowledge-Proofs).

Nach Art. 83 Abs. 5 DS-GVO handelt es sich bei einer Verletzung des Rechts auf Löschung um einen besonders gravierenden Verstoß, für den der Bußgeldrahmen bis zu 20 Millionen Euro beträgt oder im Fall eines Unternehmens bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Wert der höhere ist. Eine Herausforderung in öffentlichen Blockchains ist hier u. a. auch die Frage nach der datenschutzverantwortlichen Partei, die Art. 4 Nr. 7 DS-GVO vorsieht.

18) Bei Smart Contracts handelt es sich nicht um Verträge im Rechtssinne, sondern um Programmcode.

Smart Contracts im Rahmen einer Blockchain bezeichnen Programmcode, den alle TeilnehmerInnen eines Blockchain-Netzwerks umsetzen (vgl. These 15). Letztlich regeln und koordinieren Smart Contracts beliebige digitale Abläufe. Bei der Programmierung von Smart Contracts garantiert die Blockchain-Umgebung die korrekte Ausführung des Codes. Abhängig vom jeweiligen Einzelfall kann der Programmcode vertragsrechtlich relevante Handlungen durchführen.

Smart Contracts finden aktuell häufig zur automatisierten Vertragsabwicklung Verwendung: Zum Beispiel kann Programmcode im Falle des Eintretens bestimmter, auf der Blockchain abgebildeter Ereignisse (Leistung) eine Zahlung vornehmen lassen (Gegenleistung). Für den der Leistungsabwicklung vorgelagerten schuldrechtlichen Vertragsschluss spielen Smart Contracts dagegen eine untergeordnete Rolle. Code selbst ist wohl vor allem – zum Beispiel als Zahlungsmodalität – Gegenstand einer schuldrechtlichen Einigung. Willenserklärungen

[8] Smart Contracts sind zwar anfällig, aber nur ein marginaler Teil wurde bisher ausgenutzt

selbst basieren regelmäßig aber auf der Verwendung einer Nutzeroberfläche und nicht eines dahinterliegenden Smart Contracts.

Führt Programmcode rechtlich relevante Handlungen aus, kann der Rechtsrahmen eine Hürde darstellen. Beispielsweise, wenn die Handlungen differenzierte Pflichten im Falle eines Vertragsschlusses mit Verbrauchern oder unter Nutzung von Allgemeinen Geschäftsbedingungen (AGBs) vorsehen. Insbesondere wäre die Nutzung einer Programmsprache als Ausdruck des Inhalts einer Willenserklärung gegenüber Verbrauchern unter Nutzung von AGBs unzulässig. Auch unbestimmte Rechtsbegriffe lassen sich nicht in Code abbilden, denn dieser kann wohl keine Wertungsentscheidungen treffen; beispielsweise wird die automatisierte Bestimmung einer „angemessenen Frist" daher wohl nicht programmierbar sein.

Letztlich gilt zudem: Wenn der Code nicht im Einklang mit dem Rechtsrahmen handelt, haftet eine Person in der realen Welt für etwaige Schäden. Dies kann, abhängig vom Einzelfall, der Schuldner eines Vertragsverhältnisses sein oder der Ersteller des Codes. Je nach Art der Blockchain (insb. öffentliche Blockchains) sind die dahinterstehenden natürlichen oder juristischen Personen jedoch zumeist pseudonym und/oder unbekannt und können entsprechend nicht haftbar gemacht werden.

19) Rechtliche Hürden beim Einsatz von Blockchains im P2P-Handel bestehen auch außerhalb des Datenschutzrechts.

Bei der Umsetzung eines lokalen P2P-Energiemarktes unter Einsatz der Blockchain-Technologie zeigen sich auch außerhalb der Datenschutz-Problematik zahlreiche rechtliche Hürden. Zwar existieren insoweit keine expliziten rechtlichen Verbote, es zeigt sich jedoch andererseits, dass der gegenwärtige Rechtsrahmen für solche neuartigen Konstruktionen weder gemacht noch gedacht wurde. [33] Zu beachten ist allerdings, dass diese Hürden größtenteils unabhängig von der Nutzung von Blockchains bestehen, sie würden also auch beim Rückgriff auf andere technische Umsetzungsformen eine Rolle spielen.

So gelten etwa für die Erzeuger von Strom, die diesen im Rahmen eines P2P-Handels verkaufen möchten, dieselben umfangreichen Lieferantenpflichten wie für „klassische" Energieversorger. Ausnahmen für Klein- oder Kleinstmengen bestehen nicht. Netznutzungs- und Bilanzkreisfragen sind weiterhin gesondert zu regeln, so dass ein „echter" P2P-Handel ohne zwischengeschaltete Dienstleister derzeit praktisch nicht möglich erscheint. Auf Ebene der Strompreisbestandteile (EEG-Umlage, Netzentgelt, Stromsteuer usw.) bestehen zudem für lokale P2P-Stromlieferungen kaum Privilegierungsmöglichkeiten, so dass regelmäßig der Strompreis in voller Höhe zu zahlen ist. In der Folge mangelt es vielfach an echten Anreizen zur Teilnahme.

20) Viele Anwendungsfälle der Blockchain-Technologie im Kontext von EEG-Anlagen hängen energierechtlich am Doppelvermarktungsverbot und können dadurch nur in eingeschränktem Maße umgesetzt werden.

Speziell zum Doppelvermarktungsverbot sind insbesondere drei Aussagen hervorzuheben:

Erstens schränkt das Doppelvermarktungsverbot in § 80 Abs. 2 EEG 2017 auf Erzeugungsebene die Vermarktung von Strommengen oder Herkunftsnachweisen erheblich ein, weil EE-Anlagenbetreiber z. B. Herkunftsnachweise nicht weitergeben dürfen, wenn sie für ihren EE-Strom eine EEG-Förderung erhalten. Daher kann ein Elektrizitätsversorgungsunternehmen nur nicht-geförderten bzw. ausgeförderten EE-Strom mit einem Herkunftsnachweis versehen und

damit nur einen Bruchteil des gesamten Stroms für LetztverbraucherInnen entsprechend kennzeichnen. Dies betrifft auch P2P-Handel mit detaillierter Information zur Stromherkunft.

Zweitens bezieht das Doppelvermarktungsverbot in § 80 Abs. 1 EEG 2017 auch die nachfolgenden Handels- und Vertriebsebenen ein und führt dazu, dass Elektrizitätsversorgungsunternehmen nur ungeförderten bzw. ausgeförderten EE-Strom mit Herkunftsnachweisen vermarkten dürfen. Eine Blockchain kann dadurch die Herkunft des verbrauchten Stroms nur in einem Bruchteil der Fälle kontrollieren.

Drittens sind entsprechende Verstöße gegen das Doppelvermarktungsverbot in § 80 EEG 2017 unter anderem bußgeldbewehrt.

21) Der energierechtliche Ordnungsrahmen spricht nicht gegen die Durchführung von Asset Logging-Anwendungsfällen mittels Blockchain-Technologie.

Unter Asset Logging wird im Rahmen des Projekts InDEED die Erfassung von Betriebs-, Wartungs- und Instandhaltungsdaten mittels intelligenter Messsysteme (iMSys), Prüforganen oder weiterer angemessener Quellen sowie deren manipulationssichere und zeitdiskrete Speicherung und Verarbeitung verstanden.

Der energierechtliche Ordnungsrahmen sieht für Marktteilnehmer zum Teil Verpflichtungen zur Weitergabe bestimmter anlagenbezogener Informationen vor.[9] Solche können einmalig bei der Inbetriebnahme von Anlagen oder auch in regelmäßigen Abständen anfallen. Die Weitergabeverpflichtung kann gegenüber anderen Marktteilnehmern oder Behörden zu leisten sein. Kommt ein Akteur einer solchen Verpflichtung nicht rechtskonform nach, kann dies Sanktionen zur Folge haben.

In welcher Weise entsprechende Daten erhoben, gespeichert und weitergegeben werden, regelt der Gesetzgeber nicht. Sogenanntes „Asset Logging", also die Erhebung, Speicherung und Verwendung bestimmter Anlagendaten, kann bei der Nutzung vertrauenswürdiger Datenquellen zum Abwickeln einer Verpflichtung dann zum Einsatz kommen, wenn die tatsächlich erhobenen Anlagendaten auch die durch den Rechtsrahmen geforderten Daten sind. Der Mehrwert des Konzeptes liegt dann darin, dass die weitergeleiteten Daten garantiert integer sind und aus vertrauenswürdigen Quellen stammen. Für die beteiligten Akteure sinkt damit entsprechend die Gefahr sich Sanktionen auszusetzen.

Auch im Rahmen der Abwicklung anlagenbezogener zivilrechtlicher Verträge (beispielsweise Pacht-, Wartungs- oder Kaufverträge) stellt Asset Logging einen Mehrwert dar. Anlagendaten, die im Rahmen von Asset Logging erhoben und gespeichert werden, stellen regelmäßig wesentliche Inhalte entsprechender Verträge dar. Asset Logging stellt daher eine Grundlage aus garantiert integren und verlässlichen Quellen stammenden Daten bereit und erfüllt deshalb im Falle von Leistungsstörungen oder Rechtsschutzersuchen eine besondere Beweisfunktion. Allerdings ist zu beachten, dass das Zivilprozessrecht Daten, die mittels Blockchain gespeichert sind, nicht den besonderen Status einer Urkunde oder eines elektronischen Dokuments zusichert[10]. Deren spezifischer Beweismehrwert muss also aktuell etwa mittels eines Sachverständigengutachtens in den Prozess eingeführt werden.

[9] Siehe beispielsweise: § 12 Abs. 2 und § 15 Abs. 2 S. 2 EnWG, oder §§ 4, 4a und 5 EnWG, genauso wie § 3 MaStRV.
[10] Im Finanzwesen gibt es bereits ein Gesetzgebungsverfahren zur Einführung von elektronischen Wertpapieren. (Stand 16.12.2020, siehe [34])

2.4 Thesen zu energiewirtschaftlichen Einsatzmöglichkeiten

22) Die Blockchain-Technologie verbessert bestehende und etabliert neue Prozesse in der Energiewirtschaft.

Die Energiewirtschaft baut auf kritischer Infrastruktur auf und muss daher gemäß § 11 EnWG die „Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse (...)" gewährleisten. Viele Prozesse (z. B. Bilanzkreismanagement, Regelleistung, Redispatch und die Erbringung von Flexibilität) dienen zudem dem Zweck, Nachweise gegenüber Behörden oder anderen Marktteilnehmern (z. B. Übertragungsnetzbetreiber) zu erbringen. Nachvollziehbarkeit und Manipulationsresistenz sind hier elementar wichtige Eigenschaften. Zudem sind Ausfallsicherheit und Redundanz Schlüsselelemente der Energieversorgung. Durch die Redundanz einer Blockchain bleibt diese auch bei großflächigen Stromausfällen verfügbar und kann eine Funktionsfähigkeit auch bei einem Ausfall vieler Knoten gewährleisten (vgl. These 8). Die Transparenz und Unveränderbarkeit der geschriebenen Daten stellen insbesondere im Bereich des Datenschutzes noch eine generelle Herausforderung dar (vgl. These 9) und 17).

23) Smart Meter können schon heute direkt mit Blockchains interagieren.

Eine Interaktion von Smart Meter Gateways mit Blockchain-Lösungen ist heute sowohl technisch als auch rechtlich nicht direkt möglich. So erschweren z. B. die technischen Richtlinien des BSI das Übertragen von Daten aus der Public-Key-Infrastruktur (PKI) in weitere Systeme wie beispielsweise eine Blockchain. Nur in § 49 MsbG explizit erwähnte energiewirtschaftliche Rollen (MSB, Netzbetreiber, BiKo, BKV etc.), autorisierte externe Marktteilnehmer (EMT) sowie AnschlussnutzerInnen dürfen Daten aus Smart Meter Gateways (direkt) auslesen. Zusätzlich dürfen auch vom SMGW signierte Datenpakete, welche über einen EMT an Dritte weitergeleitet, verarbeitet oder auf eine Blockchain geschrieben werden, die PKI nicht signiert verlassen. Hintergrund hierfür sind Sicherheitsbedenken, die ein Kompromittieren der PKI verhindern sollen. Dies erschwert jedoch eine Prüfung der Richtigkeit und Authentizität durch Akteure außerhalb der PKI. Dadurch endet die durch digitale Signaturen gewährleistete Vertrauenskette beim EMT. Überdies sind Daten nur dann für Abrechnungszwecke nutzbar, wenn Sie den heute vorgeschriebenen Weg in der PKI zurückgelegt haben.

Eine Lösung zur Integration von Blockchains in die PKI sind CLS-Mehrwertmodule. Dabei wird zusätzliche Hardware vor Ort installiert, die über die notwendige Rechenleistung und den Speicherplatz verfügt, um beispielsweise einen Blockchain-Knoten zu betreiben oder Proxy-Signaturen zu verwenden. Über den CLS-Kanal sowie das „Wide Area Network" (WAN, mehr dazu in [35]) kann in diesem Zuge mit dem Zähler, lokalen Geräten und der Blockchain kommuniziert werden. Dies gewährleistet eine Vertrauenskette bis in die Blockchain. Nach heutigem Stand sind die Daten jedoch nicht für Abrechnungszwecke zugelassen. [36]

24) Durch den Einsatz von Zero-Knowledge-Proofs lassen sich viele energiewirtschaftliche Prozesse automatisiert abwickeln.

Zero-Knowledge-Proofs ermöglichen die Prüfung von Datenintegrität (z. B. durch Prüfung digitaler Signaturen) oder Prozessen, ohne die zugrunde liegenden Daten aufzudecken. [37], [1] In der Energiewirtschaft existieren viele Prozesse, in denen die Erbringung einer Leistung o. ä. geprüft wird (z. B. Nachweis der Bilanzneutralität, Herkunftsnachweise, Erbringung von Regelleistung). Dabei werden z. B. Lastgänge an Kontrollinstanzen gemeldet, welche diese

Daten wiederum prüfen (z. B. durch Bilden einer Summe beim Nachweis der Bilanzneutralität) [6]. ZKPs können diese Prozesse automatisiert abbilden, ohne einen Datenaustausch erforderlich zu machen und personenbezogene Daten oder Betriebsgeheimnisse preiszugeben. Das Verfahren ermöglicht Datensparsamkeit, ist jedoch noch nicht voll ausgereift.

ZKPs können auch ohne Blockchain zum Einsatz kommen. Die Blockchain-Technologie kann jedoch genutzt werden, um vielen Parteien die Prüfung der ZKPs zu ermöglichen.

25) Die Smart-Meter-Infrastruktur bietet der Blockchain eine optimale Möglichkeit für eine korrekte digitale Datenerfassung.

Die modernen Messeinrichtungen (FNN-Basiszähler) unterliegen dem Mess- und Eichgesetz (MessEG) sowie der Mess- und Eichverordnung (MessEV) und benötigen für das Inverkehrbringen eine Konformitätskennzeichnung. Es dürfen entsprechend nur Messwerte für abrechnungsrelevante Einsätze genutzt werden, die mittels geeichten Messgeräts erfasst wurden. [38] Dadurch wird eine einheitliche, genaue und vertrauenswürdige Messung in der gesamten Energiebranche gewährleistet. Diese Voraussetzung lässt sich in nur wenigen Branchen finden.

Smart-Meter-Gateways wurden auf Basis der technischen Richtlinien des BSI [39] entwickelt und erfüllen insbesondere ein hohes Maß an Sicherheit und Datenschutz. Sie enthalten u. a. ein Sicherheitsmodul und werden im Rahmen einer vom BSI geschaffenen PKI betrieben. Eine Zertifizierung der Geräte ist an entsprechend hohe Anforderungen geknüpft. Auch die Datenverarbeitung seitens (externer) Marktteilnehmer ist an eine ISO 27001-Zertifizierung (aktiver EMT) geknüpft bzw. nur mit Sicherheitskonzept (passiver EMT) möglich [40]. Abgesehen von Datenschutzaspekten ergänzt die Blockchain-Technologie die hohen Anforderungen an Sicherheit, Integrität, Authentizität und erfüllt auf diese Weise viele Anforderungen der technischen Richtlinien (vgl. u. a. die Nutzung von kryptographischen Verfahren, empfohlene Schlüssellängen [41] und Elliptic Curve Cryptography [42]). Für verlässliche Sensordaten als Input für eine Blockchain ist die PKI, die bspw. durch das SMGW bereitgestellt wird, unbedingt erforderlich und sollte noch weiter angereichert werden (z. B. mit Zertifikatsketten). Grundsätzlich besteht bei der Datenerfassung über externe Sensoren oder manuelle Dateneingabe die Gefahr der Datenmanipulation (Oracle-Problematik). Die Vertrauenswürdigkeit der Blockchain ist insoweit von diesen Daten abhängig. Allerdings kann die Energiewirtschaft durch ihren hohen Grad der Standardisierung und der Zertifizierungsvorgänge das Oracle-Problem weitgehend minimieren und somit die Grundlage für eine Vielzahl von energiewirtschaftlichen Anwendungsfällen auf der Blockchain ermöglichen.

Eine große Herausforderung der SMGW-Infrastruktur ist allerdings ihre Verfügbarkeit. Durch den verzögerten Rollout, dessen Zeitplan, die betroffenen Nutzergruppen und den bisher eingeschränkten Funktionsumfang (vgl. [35]) ist die Infrastruktur auf absehbare Zeit nicht großflächig nutzbar. Die Nutzung insbesondere im Umfeld von privaten LetztverbraucherInnen ist entsprechend nicht ohne weiteres möglich.

26) Der Einsatz der Blockchain im Letztverbrauchersegment ist durch die fehlende Digitalisierung nur schwer skaliert möglich.

Unabhängig von der konkreten technischen Umsetzung, ob auf Blockchain-Basis oder mit alternativen technischen Ansätzen, sind digitale Geschäftsmodelle im Letztverbrauchermarkt in Deutschland aktuell schwierig zu implementieren. Dies gilt auch, aber nicht nur, für alle

Varianten der Peer-to-Peer-Konzepte in Bezug auf Energiehandel oder Labeling. Grund dafür ist die derzeit unzureichende digitale Anbindung der Mess- und Zählerinfrastruktur in diesem Marktsegment aufgrund des verzögerten Rollouts intelligenter Messsysteme. [35]

Für eine Umsetzung von Anwendungsfällen bestehen also zwei Möglichkeiten: Entweder eine technische Anbindung über die bereits vorhandene iMSys-Infrastruktur und damit eine drastische Reduktion des potenziellen Kundenkreises aufgrund der nicht erfüllten technischen Voraussetzungen oder die Installation alternativer proprietärer Hardware zur Erfassung und Übertragung der erforderlichen Daten. Letzteres ist allerdings mit finanziellem und organisatorischem Aufwand verbunden und stellt deshalb eine zusätzliche Hürde dar, da die erhobenen Messwerte nicht für eine Abrechnung verwendet werden können. Beide Ansätze erweisen sich also als tendenziell ungeeignet, entsprechende Geschäftsmodelle im aktuellen Marktumfeld in eine breite Anwendung zu bringen. So erscheint derzeit nur eine Erprobung dieser Konzepte im Rahmen von Pilotprojekten als zweckmäßig. Die Skalierbarkeit für eine spätere Erweiterung des Kreises für TeilnehmerInnen-/KundInnenkreises ist dabei jedoch jederzeit zu berücksichtigen.

27) Eine eindeutige Identifizierung der beteiligten Akteure oder Anlagen sowie deren Marktrollen, Funktionen oder Eigenschaften ist für viele Anwendungsfälle notwendig.

Energiewirtschaftliche Prozesse sind auf eine konsistente Datenbasis angewiesen. Aufgrund des „Rollenmodells für die Marktkommunikation im deutschen Energiemarkt" ist genau geregelt, welcher energiewirtschaftliche Akteur welche Aufgaben übernimmt und welche Informationen diesem zur Verfügung stehen [43]. Gerade bei Stammdaten bestehen bereits einige Datenbanken und Identifikationskennzahlen – allen voran das Marktstammdatenregister der Bundesnetzagentur, in welchem sowohl die Akteure des Strom- und Gasmarkts als auch deren Erzeugungsanlagen hinterlegt sind [44]. Hinzu kommt eine Vielzahl an proprietären Datenbanken z. B. von Energieversorgern, Netzbetreibern oder Dienstleistern zur Abwicklung ihrer Geschäftsbereiche.

Die große Herausforderung liegt darin, dass es nach wie vor an Konsistenz, Aktualisierung und Verknüpfung bzw. Synchronisierung der vorhandenen Daten mangelt. Mit der Einführung der Marktlokations- (MaLo) und Messlokationsnummern (MeLo bzw. Zählpunktbezeichnung, ZPB) wurde bereits ein erster Schritt getan, um hier eine Vereinheitlichung zu schaffen [45]. Durch die zunehmende Kleinteiligkeit und digitale Anbindung verschiedenster Komponenten des Energiesystems (bis hin zu IoT-Geräten oder Sensoren) stößt dieses System allerdings an seine Grenzen. Unter anderem beschränken sich erfassbare Anlagen meist auf vorab (offiziell) registrierte, geprüfte und spezifische Anlagentypen. Um diesen Herausforderungen entgegenzuwirken, werden bereits innovative Lösungen diskutiert, die auf Basis einer Identitätsschicht und des Einsatzes von Decentralized Identifiers (DIDs) eine einheitliche Infrastruktur für die Identitäten von Anlagen, Sensoren oder IoT-Geräten digital abbilden können.

3 Fazit

ALLGEMEINE THESEN		ERGEBNIS
1.	Die Blockchain-Technologie ist vielfältig.	Bekräftigt
2.	Die Blockchain-Technologie ist für einen intermediärsfreien Wertaustausch zwischen vielen Akteuren eine aussichtsreiche Lösung.	Bekräftigt
3.	Fast alle Blockchain-Anwendungsfälle könnten auch ohne die Technologie abgebildet werden.	Bekräftigt
4.	Durch zentrale Instanzen können sich Abhängigkeiten, Single-Points-of-Failure, Ineffizienzen und Monopole ergeben, die für einzelne oder alle beteiligten Akteure ein (wirtschaftliches) Risiko darstellen können.	Bekräftigt
5.	Kryptowährungen sind der primäre Nutzungszweck von Blockchains.	Entkräftet
6.	Auf Basis einer Blockchain-Infrastruktur können (Mikro-)Transaktionen auch auf öffentlichen, zugangsunbeschränkten Blockchain-Lösungen automatisiert und zu geringen Kosten durchgeführt werden.	Entkräftet

THESEN ZUR TECHNISCHEN ENTWICKLUNG		ERGEBNIS
7.	Die Konsensfindung in Blockchain-Systemen ist sehr energieintensiv und somit ressourcenineffizient.	Entkräftet
8.	Aufgrund der redundanten Speicherung von Daten ist die Energieeffizienz von Blockchain-Anwendungen systematisch geringer als bei einer energieoptimierten und zentralisierten Lösung.	Bekräftigt
9.	Die Transparenz und Unveränderbarkeit von Transaktionen auf Blockchains verletzen immer datenschutzrechtliche Vorgaben.	Entkräftet
10.	Die Performanz von Blockchain-Lösungen ist immer geringer als die von zentralisierten Lösungen.	Bekräftigt
11.	Zero-Knowledge-Proofs können die Richtigkeit von Prozessen automatisiert und datenschutzkonform beweisen.	Bekräftigt
12	Blockchains und Smart Contracts eignen sich für die Verarbeitung großer Datenmengen und der Ausführung komplexer Berechnungen.	Entkräftet
13.	Komplexe Berechnungen (z. B. Optimierungen) können off-chain ausgeführt werden.	Bekräftigt
14.	Smart Contracts sind „smart“.	Entkräftet
15.	Smart Contracts eignen sich zur Verarbeitung von verschlüsselten oder gehashten Daten.	Entkräftet
16.	Smart Contracts sind sicher.	Entkräftet

JURISTISCHE THESEN		ERGEBNIS
17.	Aufgrund ihrer Unveränderbarkeit dürfen auf einer Blockchain keine personenbezogenen Daten direkt gespeichert werden.	Bekräftigt
18.	Bei Smart Contracts handelt es sich nicht um Verträge im Rechtssinne, sondern um Programmcode.	Bekräftigt
19.	Rechtliche Hürden beim Einsatz von Blockchains im P2P-Handel bestehen auch außerhalb des Datenschutzrechts.	Bekräftigt

20.	Viele Anwendungsfälle der Blockchain-Technologie im Kontext von EEG-Anlagen hängen energierechtlich am Doppelvermarktungsverbot und können dadurch nur in eingeschränktem Maße umgesetzt werden.	Bekräftigt
21.	Der energierechtliche Ordnungsrahmen spricht nicht gegen die Durchführung von Asset Logging-Anwendungsfällen mittels Blockchain-Technologie.	Bekräftigt

THESEN ZU ENERGIEWIRTSCHAFTLICHEN EINSATZMÖGLICHKEITEN		ERGEBNIS
22.	Die Blockchain-Technologie verbessert bestehende und etabliert neue Prozesse in der Energiewirtschaft.	Bekräftigt
23.	Smart Meter können schon heute direkt mit Blockchains interagieren.	Entkräftet
24.	Durch den Einsatz von Zero-Knowledge-Proofs lassen sich viele energiewirtschaftliche Prozesse automatisiert abwickeln. Der Austausch personenbezogener Daten wird vermieden.	Bekräftigt
25.	Die Smart-Meter-Infrastruktur bietet der Blockchain eine optimale Möglichkeit für eine korrekte digitale Datenerfassung.	Bekräftigt
26.	Der Einsatz der Blockchain im Letztverbrauchersegment ist durch die fehlende Digitalisierung nur schwer skaliert möglich.	Bekräftigt
27.	Eine eindeutige Identifizierung der beteiligten Akteure oder Anlagen sowie deren Marktrollen, Funktionen oder Eigenschaften ist für viele Anwendungsfälle notwendig.	Bekräftigt

Die **allgemein** vorgestellten Thesen zeigen, dass die Blockchain-Technologie eine komplexe neue Form der Interaktion und dezentralen Datenhaltung darstellt. Sie kombiniert verschiedene bereits zuvor eingeführte Komponenten und Konzepte in einer innovativen Form. Die aufgestellten Thesen deuten jedoch auch darauf hin, dass die Technologie aufgrund ihrer Komplexität und vielen, teils parallellaufenden Weiterentwicklungen heute noch nicht umfassend zu erfassen und zu bewerten sind. In Kombination mit den allzu hohen Erwartungen und Versprechungen aus Zeiten des Blockchain-Hypes stellt dies bislang eine Herausforderung für einige Produktiveinsätze dar.

Aus den Thesen ist zudem abzuleiten, dass fast alle Anwendungsfälle der Blockchain-Technologie auch durch Intermediäre abbildbar sind. Dennoch bietet die Technologie eine Alternative, bestehende Prozesse nachvollziehbarer, manipulationsresistenter oder sicherer zu gestalten. Auch zeigt sich, dass der Einsatz von Kryptowährungen nur notwendig ist, wenn der Anwendungsfall dies erfordert. Eine meist vorteilhafte und häufig vernachlässigte Eigenschaft der Technologie ist die Schaffung von Neutralität. Blockchain kann bspw. zwischen Konkurrenten in einer Branche als gemeinsame Schnittstelle dienen, ohne einzelne Akteure zu bevorzugen. Dies kann ein Katalysator für die Adaption der Plattformökonomie darstellen und so volkswirtschaftliche Vorteile bedingen, ohne dabei die Monopole einzelner Unternehmen zu fördern.

Die **technische Beurteilung** zeigt, dass sich die Technologie in den letzten Jahren sehr stark weiterentwickelt hat. Viele neue Lösungen für bekannte technologische Schwächen befinden sich in der Entwicklung oder sind Gegenstand von Forschungstätigkeiten. So besteht der ursprünglich kritische Energieverbrauch bei vorhandenen Blockchain-Lösungen wie Bitcoin weiterhin. Für neu aufgebaute Lösungen, insbesondere in privaten oder konsortialen

Bereichen, wird er allerdings durch die Nutzung alternativer Konsensmechanismen vernachlässigbar. Neue 2nd-Layer-Konzepte wie Zero-Knowledge-Proofs ermöglichen den Nachweis über die Korrektheit von Prozessen und Daten. Payment- oder State-Channels, Side-Chains und Sharding ermöglichen eine höhere Skalierbarkeit und Datenschutzkonformität.

Die Redundanz der Technologie führt zu ihren hohen Standards im Bereich der Verfügbarkeit und Sicherheit „by design". Systemimmanent führt Redundanz jedoch immer zu geringerer Effizienz und Performanz. Auch wenn hier technologisch viele Effizienzsteigerungen möglich sind, kann die Technologie in diesen Bereichen nicht mit optimierten, zentralen Lösungen konkurrieren. Dies beinhaltet insbesondere die Ausführung sehr komplexer Berechnungen. Die Technologie ist nicht darauf ausgelegt, im Rahmen von Smart Contracts sehr komplexe Berechnungen zu tätigen. Lösungen, um solche Berechnungen dennoch mit der Technologie verknüpfen zu können, sind teilweise bereits einsetzbar oder befinden sich in der Entwicklung.

Eine Lösung, die insbesondere Nachvollziehbarkeit und Sicherheit mit Skalierbarkeit verbinden kann, sind Zero-Knowledge-Proofs. Wenngleich noch in einem frühen Entwicklungsstadium, kann das Konzept in Kombination mit der Blockchain viele Herausforderungen u. a. im Bereich Datenschutz lösen. Für eine Umsetzung des Konzepts wird eine weitere sichere und bilaterale Kommunikationsschicht benötigt, damit die NetzwerkteilnehmerInnen nicht mehr auf offengelegte Daten auf der Blockchain zugreifen können. Hierfür bieten sich digitale Identitäten (z. B.: Self-Sovereign Identity, vgl. u. a. [5]) an, welche bereits in Erprobung sind.

Die **juristische Analyse** legt offen, dass das „Recht auf Löschung" in Art. 17 DS-GVO den Einsatz der Technologie mit personenbezogenen Daten untersagt. Ist eine vollständige Anonymisierung dieser Daten nicht möglich, dürfen sie aus datenschutzrechtlichen Gründen nicht auf eine Blockchain geschrieben werden. Zero-Knowledge-Proofs bieten hier eine datenschutzkonforme Lösung. Dabei werden keine personenbezogenen Daten auf der Blockchain preisgegeben.

Zudem wird deutlich, dass Smart Contracts keine Verträge im rechtlichen Sinne darstellen, deren Logik jedoch unterstützen bzw. abbilden können. Unbestimmte Rechtsbegriffe, die eine juristische Wertung erfordern – wie das Erfordernis einer „angemessenen Frist" – sind schwerlich über Smart Contracts programmierbar. Eine Analyse des Energierechts anhand ausgewählter Anwendungsfälle zeigt weiterhin, dass insbesondere für den P2P-Handel die Marktrolle des „Prosumers" fehlt. So gelten etwa für die Erzeuger von Strom, die diesen im Rahmen eines P2P-Handels verkaufen möchten, dieselben umfangreichen Lieferantenpflichten wie für „klassische" Energieversorger.

Außerdem ist zu berücksichtigen, dass vielen Anwendungsfällen zum Labeln von Strommengen, die auf nach dem EEG 2021 geförderte erneuerbare Energien ausgelegt sind, das Doppelvermarktungsverbot nach § 80 EEG 2021 entgegensteht. Im Rahmen der Nutzung von Asset Logging-Modellen für Anlagen-Daten ist zu berücksichtigen, dass der spezifische Beweismehrwert von Blockchains aktuell mittels eines Sachverständigengutachtens in den Zivilprozess eingeführt werden muss, also nicht ohne weiteres vorausgesetzt werden kann.

Der Abschnitt zum Einsatz in der **Energiewirtschaft** legt dar, dass die Eigenschaften der Blockchain-Technologie mit den Zielen der kritischen Infrastruktur sehr gut harmonieren. Insbesondere Kontrollprozesse, wie sie in der Branche an vielen Stellen zu finden sind (z. B. Leistungserbringung, Bilanzausgleich etc.), können in Zukunft potenziell mit Hilfe der

Technologie stark vereinfacht werden. Eine ausgemachte Stärke der Branche ist die geeichte, standardisierte und auf Sicherheit ausgelegte Smart-Meter-Infrastruktur. Diese bietet eine geeignete Grundlage zur Datenerfassung, die im Rahmen einer Blockchain-Lösung genutzt werden kann. Nachteilig ist jedoch der aktuelle Grad der Digitalisierung durch Smart Meter, die fehlende Interoperabilität sowie der begrenzte Funktionsumfang.

Welche Zukunft hat die Blockchain in der Energiewirtschaft?

Es lässt sich festhalten, dass durch den Hype in den Jahren 2016/2017 große Erwartungen in die Technologie gesteckt wurden. Darüber hinaus wird deutlich, dass sich die Technologie noch in einem frühen Entwicklungsstadium befindet (vgl. Abschnitt 2.1 & 2.2) und (noch) nicht alle Erwartungen erfüllen kann. Durch Weiterentwicklungen bestehen inzwischen einige Lösungen mit unterschiedlich fortgeschrittener technologischer Reife. Hierzu gehören beispielsweise Zero-Knowledge-Proofs zur verlässlichen Auslagerung komplexer Rechenprozesse (vgl. Abschnitt 2.2). Dennoch stellt der aktuelle Grad der Digitalisierung in der Energiewirtschaft eine nicht zu vernachlässigende Herausforderung für den produktiven Einsatz von Blockchain-Lösungen dar. So muss auf verlässliche Sensordaten zugegriffen werden können und eine Infrastruktur für den organisationsübergreifenden Datenaustausch, beispielsweise mittels eines dezentralen Identitätsmanagements, bestehen (vgl. These 22). Auf dieser Grundlage kann Blockchain in Kombination mit Lösungsansätzen wie ZKPs in der Energiewirtschaft einen Mehrwert leisten (vgl. These 24).

Bei der Digitalisierung ist nicht nur im Energiebereich (vgl. Smart-Meter-Rollout) deutlicher Nachholbedarf zu erkennen. Durch die geringe Verfügbarkeit von SMGW werden die Potenziale von digitalen Mehrwertdiensten (auf Basis der Blockchain) insbesondere im Bereich der post-EEG-Anlagen und bei privaten LetztverbraucherInnen stark eingeschränkt. Insbesondere vor dem Hintergrund des verzögerten Smart-Meter-Rollouts (vgl. These 22) ist daher bei der aktuellen Entwicklungsdynamik der Blockchain-Technologie zu erwarten, dass technische Einschränkungen der Technologie schneller behoben sind, als eine großflächige Digitalisierung der Energiewende erwartet werden kann.

Wie die Abschnitte 2.3 und 0 zeigen, ist die Erfüllung dieser Erwartungen jedoch nicht ausschließlich von Entwicklungen im Bereich der Blockchain-Technologie oder der Digitalisierung abhängig. Viele Anwendungsfälle stehen noch vor regulatorischen Hürden. Insbesondere die fehlende Definition von „Prosumern" stellt (ungeachtet von der Nutzung der Blockchain-Technologie) eine hohe Herausforderung für deren Integration ins Energiesystem dar und geht mit erhöhtem bürokratischem Aufwand und Kosten einher.

Die dargestellten technischen, juristischen und energiewirtschaftlichen Thesen zeigen deutlich, dass eine Nutzung der Technologie in der Energiewirtschaft an vielen Stellen sinnvoll sein kann. Es ist dabei zu erwarten, dass die Technologie in Zukunft ein weiterer digitaler Standardbaustein wird, wenn sie im Rahmen ihrer Praxisanwendung in der Energiewirtschaft ihren Wert beweist und ausreichend Mehrwert für alle Beteiligten im Rahmen sinnvoller Anwendungsfälle bietet. Dies ist insbesondere bei Prozessen mit vielen Akteuren zu erwarten, wobei organisationsübergreifende, manipulationsresistente Nachweise von Transaktionen, Daten oder Werten erforderlich sind. Die derzeitigen Forschungsprojekte (darunter InDEED) zeigen diese Mehrwerte auf. Erste Zwischenergebnisse sind vielversprechend (vgl. u. a. [46], [8]).

4 Literatur

[1] Bogensperger, Alexander; Zeiselmair, Andreas, Hinterstocker, Michael: Die Blockchain-Technologie - Chance zur Transformation der Energieversorgung? - Berichtsteil Technologiebeschreibung. München: Forschungsstelle für Energiewirtschaft e.V. (FfE), 2018.

[2] Schlatt, Vincent et al.: Blockchain: Grundlagen, Anwendungen und Potenziale. Bayreuth: Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, 2016.

[3] Grigo, Julian et al.: Decentralized Finance (DeFi) – A new Fintech Revolution? - The Blockchain Trend explained. Berlin: Bitkom, 2020.

[4] Zeiselmair, Andreas et al.: Asset Logging – transparent documentation of asset data using a decentralized platform. In: Energy Informatics 31/2019. Berlin: Springer Nature, 2019.

[5] Strüker, Jens et al.: Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Bayreuth: Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, 2021.

[6] Bogensperger, Alexander; Zeiselmair, Andreas; Hinterstocker, Michael; Dufter, Christa: Die Blockchain-Technologie - Chance zur Transformation der Energiewirtschaft? - Berichtsteil: Anwendungsfälle. München: Forschungsstelle für Energiewirtschaft e.V., 2018.

[7] Hinterstocker, Michael et al.: Potential Impact of Blockchain Solutions on Energy Markets. In: 15th International Conference on the European Energy Market; Łódź: Forschungsgesellschaft für Energiewirtschaft mbH, 2018.

[8] Hinterstocker, Michael et al.: Blockchain technology as an enabler for decentralization in the energy system. In: 10th Solar & Storage Integration Workshop; Darmstadt: FfE GmbH, 2020.

[9] Behrends, Felix: Plattform-Ökonomie in der Energiewirtschaft - Entwicklung und Anwendung einer Methodik zur Bewertung der Plattformtauglichkeit der deutschen Energiewirtschaft. Masterarbeit. Herausgegeben durch Technische Universität München: München, 2020.

[10] de Reuver, Mark et al.: The digital platform: a research agenda. In: Journal of Information Technology 33, 2018. London, England: The London School of Economics and Political Science, 2018.

[11] Baldwin, Carliss et al.: The architecture of platforms: a unified view. In: Platforms, Markets and Innovation 2009. Cheltenham, England: Edward Elgar Publishing, 2009.

[12] Kenton, Will: Economies of Scale. In: https://www.investopedia.com/terms/e/economiesofscale.asp. (Abruf am 2020-10-15); New York City, NY, USA: Investopedia, 2020.

[13] Tiwana, Amrit: Platform Ecosystems - Aligning Architecture, Governance, and Strategy. Georgia: University of Georgia, 2014.

[14] Voshmgir, Shermin: Token Economy - How Blockchains and Smart Contracts Revolutionize the Economy. Berlin: BlockchainHub, 2019.

[15] Sedlmeir, Johannes et al.: The DLPS: A New Framework for Benchmarking Blockchains. In: Proceedings of the 54th Hawaii International Conference on System Sciences; Honolulu, Hawaii: University of Hawaii, 2021.

[16] Buterin, Vitalik: A Next Generation Smart Contract and Decentralized Application Platform - Ethereum White Paper. Switzerland: Ethereum Foundation, 2014.

[17] Baliga, Arati: Understanding Blockchain Consensus Models. In: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf. (Abruf am 2018-01-23); Santa Clara: Persistent Systems Ltd., 2017.

[18] Castor, Amy: A (Short) Guide to Blockchain Consensus Protocols . In: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/. (Abruf am 2018-01-23); (Archived by WebCite® at http://www.webcitation.org/6wgfJxwXJ); New York: Coindesk, 2017.

[19] Zade, Michel et al.: Is Bitcoin the Only Problem? A Scenario Model for the Power Demand of Blockchains. München: Technische Universität München, 2019.

[20] Gallersdörfer, Ulrich et al.: Energy Consumption of Cryptocurrencies Beyond Bitcoin. München: Technische Universität München, 2020.

[21] Sedlmeir, Johannes et al.: The Energy Consumption of Blockchain Technology: Beyond Myth. Bayreuth: Project Group Business and Information Systems Engineering of the Fraunhofer FIT, 2020.

[22] Bamakan, Seyed Mojtaba Hosseini et al.: A survey of blockchain consensus algorithms performance evaluation criteria. Yazd, Iran, Shenzhen, China: Data Science Research Center, Yazd University, 2020.

[23] Zhang, Changqiang et al.: Overview of Blockchain Consensus Mechanism. Shanghai, China: National University of Defense Technology, China, 2020.

[24] Fairley, Peter: Ethereum will cut back its absurd energy use - The crypto-currency is reducing its energy footprint by 99 percent. New York, USA: IEEE, 2018.
[25] Hyperledger Fabric Model. In: https://hyperledger-fabric.readthedocs.io/. (Abruf am 2021-02-15); San Francisco, USA: Hyperledger, 2019.
[26] Eberhardt, Jacob et al.: Off-chaining Models and Approaches to Off-chain Computations. New York: Association for Computing Machinery, 2018.
[27] Hasan, Jahid: Overview and Applications of Zero Knowledge Proof (ZKP). Nanjing: Nanjing University of Posts and Telecommunications, 2019.
[28] Wood, Gavin: Ethereum: a secure decentralised generalised transaction ledger (EIP-150 REVISION). Zug, Switzerland: ETHCORE, 2014.
[29] Benet, Juan: IPFS - Content Addressed, Versioned, P2P File System. Delaware: Protocol Labs Inc., 2014.
[30] Walfish, Michael et al.: Verifying Computations without Reexecuting Them - From theoretical possibility to near practicality. New York, USA: Communications of the ACM, 2015.
[31] Al-Breiki, Hamda et al.: Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. Abu Dhabi, United Arab Emirates: Khalifa University of Science and Technology, 2020.
[32] Zhong, Hanrui et al.: Secure Multi-Party Computation on Blockchain - An Overview. Singapur: Communications in Computer and Information Science, 2020.
[33] Fietze, Daniela et al.: Der Rechtsrahmen für regionale Peer to Peer-Energieplattformen unter Einbindung von Blockchains. Würzburg: Stiftung Umweltenergierecht, 2020.
[34] BMJV: Gesetz zur Einführung von elektronischen Wertpapieren. In: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Einfuehrung_elektr_Wertpapiere.html. (Abruf am 2021-05-18); Berlin: Bundesministerium der Justiz und für Verbraucherschutz, 2020.
[35] Bogensperger, Alexander; Estermann, Thomas; Samweber, Florian; Köppl, Simon; Müller, Mathias; Zeiselmair, Andreas, Wohlschlager, Daniela: Smart Meter - Umfeld, Technik, Mehrwert. München: Forschungsstelle für Energiewirtschaft e.V., 2018.
[36] Rollout mit Mehrwerten: Theben erhält BSI-Zertifizierung für das Smart Meter Gateway CONEXA 3.0 Performance. In: https://www.smart-metering-theben.de/mehrwerte/. (Abruf am 2021-05-25); Haigerloch: Theben AG, 2020.
[37] Ben-Sasson, Eli et al.: Scalable, transparent, and post-quantum secure computational integrity. Haifa, Israel: Zerocash, 2018.
[38] FNN-Hinweis - FNN-Basiszähler Moderne Messeinrichtung. Berlin: Forum Netztechnik / Netzbetrieb im VDE (FNN), 2017.
[39] Technische Richtlinie BSI TR-03109. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015.
[40] BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008.
[41] Technische Richtlinie TR-02102-1 (TR-02102-1). Ausgefertigt am 2020-03-24; Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020.
[42] Technische Richtlinie-03111 Elliptische-Kurven-Kryptographie (ECC) (TR-03111). Ausgefertigt am 2018-06-01; Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2018.
[43] Rollenmodell für die Marktkommunikation im deutschen Energiemarkt - Strom und Gas. Berlin: BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., 2019.
[44] Marktstammdatenregister - Öffentliche Marktakteursübersicht: https://www.marktstammdatenregister.de/MaStR/Akteur/Marktakteur/IndexOeffentlich; Bonn: Bundesnetzagentur, 2020.
[45] Die neue Marktlokations- Identifikationsnummer - Anwendungshilfe. Berlin: Bundesverband der Energie- und Wasserwirtschaft e.V. (bdew), 2017.
[46] Bogensperger, Alexander et al.: Updating renewable energy certificate markets via integration of smart meter data, improved time resolution and spatial optimization in 17th International Conference on the European Energy Market (EEM2020). Stockholm, Sweden: Forschungsstelle für Energiewirtschaft e.V., 2020.