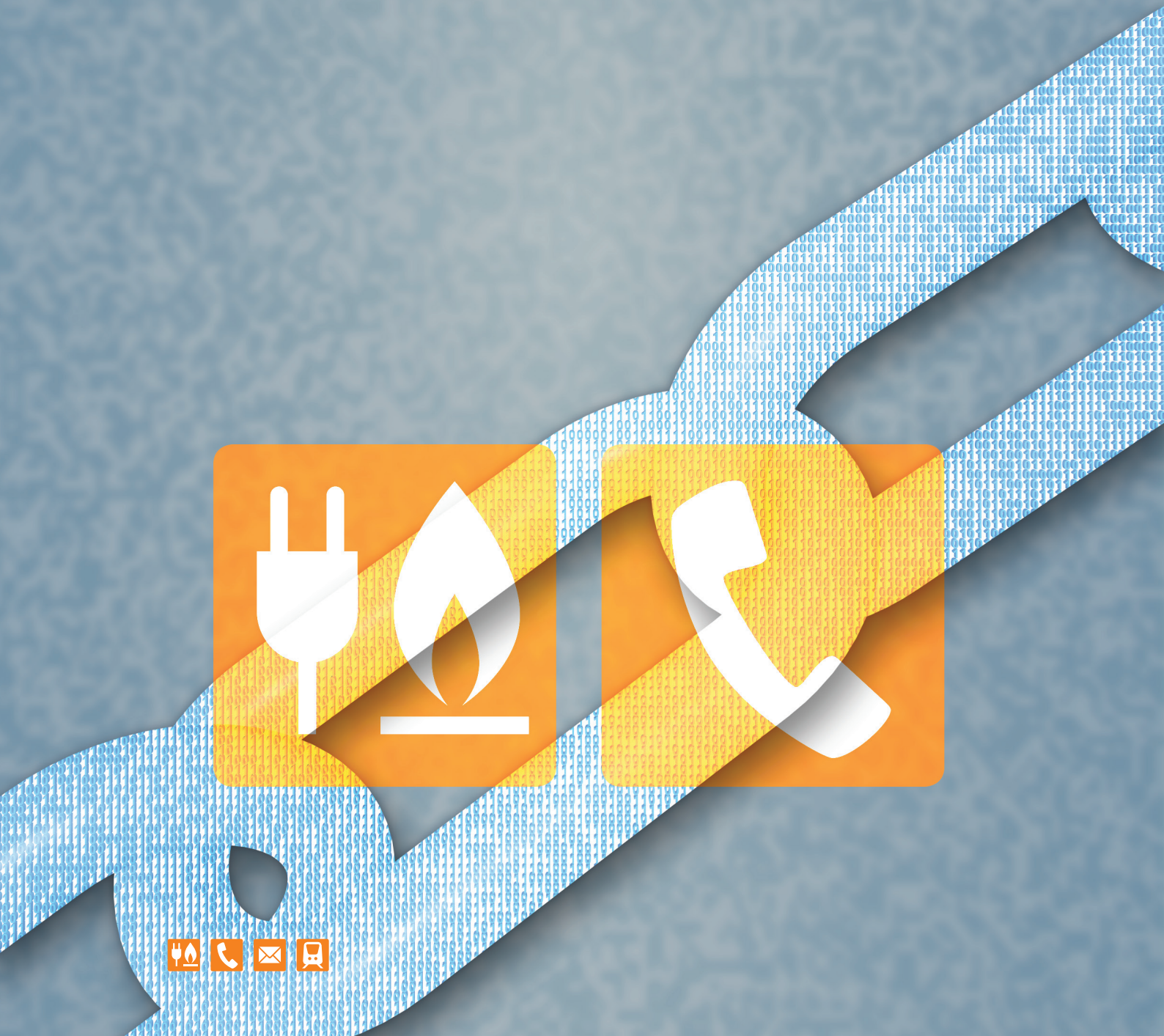
Bundesnetzagentur

Die Blockchain-Technologie

Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation



Die Blockchain-Technologie

Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation

Stand: November 2019

**Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen**

Referat 119 - Digitalisierung und Vernetzung; Internetplattformen

Tulpenfeld 4
53113 Bonn
Tel.: +49 228 14-0
E-Mail: 119-postfach@bnetza.de

Inhaltsverzeichnis

1 Einführung

Spätestens seit die Kryptowährung Bitcoin im Fokus der Öffentlichkeit steht, erhält die ihr zugrundeliegende Blockchain-Technologie immer größere Aufmerksamkeit. Wirtschaft, Wissenschaft, Politik, und Verwaltung diskutieren seitdem über die Bedeutung dieser Technologie und treiben ihre Entwicklung und Verbreitung voran. So wurden in den vergangenen Jahren in ganz unterschiedlichen Wirtschaftsbereichen konzeptionelle Überlegungen zum Einsatz der Technologie angestellt und zahlreiche Blockchain-Anwendungen entwickelt. Auch die Bundesregierung hat im September 2019 eine eigene Blockchain-Strategie veröffentlicht, mit der sie ihre Ziele und Prinzipien hinsichtlich möglicher zukünftiger Blockchain-Anwendungsfelder vorlegt hat. Auf europäischer Ebene werden derzeit Konzepte und Maßnahmen zur Realisierung einer europaweiten, technischen Blockchain-Infrastruktur entwickelt, auf der zukünftig eine Vielzahl grenzüberschreitender digitaler Verwaltungsdienste aufbauen soll.

Die Blockchain-Technologie ist weit mehr als das „Minen“ von Kryptowährungen. Grundsätzlich kann jeder Prozess, der digital darstellbar ist, mithilfe einer Blockchain abgebildet werden. Die Blockchain-Technologie bietet dabei den Vorteil, dass Informationen nicht nur digital gespeichert und ausgetauscht, sondern auch Transaktionen zwischen verschiedenen Akteuren direkt, transparent und manipulationssicher durchgeführt werden können. Auch einzelne Geschäftsprozesse können blockchainbasiert in Form von sogenannten Smart Contracts automatisiert abgewickelt werden. Da die Blockchain-Technologie eine unmittelbare Interaktion zwischen den beteiligten Akteuren ermöglicht, besitzt sie das Potenzial, klassische Aufgaben von Intermediären ganz oder teilweise zu ersetzen.

Auch in den von der Bundesnetzagentur regulierten Netzsektoren ergeben sich potenzielle Anwendungsfälle für die Blockchain-Technologie. Analog zur Entwicklung in vielen anderen Sektoren finden auch in den Netzsektoren derzeit bedeutende digitale Transformationsprozesse statt. Diese sind gekennzeichnet durch das Auftreten neuer Marktakteure, die Entwicklung innovativer Geschäftsmodelle, eine zunehmende Vernetzung von Akteuren, Maschinen und Ressourcen sowie die steigende Bedeutung von Daten. Um die mit diesen Entwicklungen verbundene Komplexität beherrschen und digitale Wertschöpfungspotenziale realisieren zu können, steigen in den Netzsektoren die Anforderungen an die Zuverlässigkeit und Transparenz von (Echtzeit-) Informationen und Transaktionen. Die Blockchain-Technologie bietet hinsichtlich dieser Herausforderungen Lösungsansätze. Die Erwartungen an die Technologie sind deshalb entsprechend hoch.

Vor diesem Hintergrund wird im vorliegenden Papier eine objektive Bestandsaufnahme zum aktuellen Reifegrad der Blockchain-Technologie vorgenommen und es werden ihre Potenziale und Herausforderungen in den regulierten Netzsektoren Energie und Telekommunikation analysiert. Die Bundesnetzagentur hat im Zuge der Erarbeitung des Papiers mit verschiedenen Akteuren aus den beiden Sektoren gesprochen und auch sie um ihre Einschätzung zur Blockchain-Technologie befragt. Die Erkenntnisse dieser Gespräche sind in das Papier eingeflossen.

2 Technologische Grundlagen

Zur Erläuterung der wesentlichen technologischen Grundlagen der Blockchain-Technologie werden nachfolgend zunächst wichtige Begriffe definiert, die Funktionsweise der bei Blockchains üblicherweise eingesetzten Verschlüsselungstechnologien dargestellt und die Rollen und Funktionen der verschiedenen Akteure eines Blockchain-Netzwerks erläutert. Daran schließt sich eine kurze Darstellung der wichtigsten Konsensmechanismen an, mit denen in Blockchain-Netzwerken eine Übereinkunft zwischen den beteiligten Akteuren über die Aufnahme neuer Informationen geschaffen wird. Das Kapitel zeigt außerdem die Unterschiede zwischen öffentlichen, privaten und konsortialen Blockchain-Architekturen auf und geht kurz auf Smart Contracts ein, die als die bisher wichtigste konzeptionelle Weiterentwicklung der Technologie seit der Implementierung der Bitcoin-Blockchain angesehen werden.

2.1 Distributed-Ledger-Technologien

Bei einer Blockchain handelt es sich um eine konkrete Ausprägung sog. Distributed-Ledger-Technologien. Unter Distributed-Ledger-Technologien werden Datenbanksysteme verstanden, die eine synchronisierte Verifizierung und Speicherung von Daten in Peer-to-Peer Netzwerken ermöglichen. Distributed-Ledger-Technologien besitzen weder einen übergeordneten Verwalter noch einen zentralen Datenspeicher. Stattdessen kommunizieren die vernetzten Rechner des Peer-to-Peer Netzwerks miteinander, indem sie neu eingehende Transaktionen im Netzwerk auf Basis verschiedener Konsensmechanismen überprüfen, bestätigen, unveränderbar kryptographisch miteinander verketten und anschließend verteilt abspeichern.[1]

2.2 Blockchain-Technologie

Die bekannteste Ausprägung dieser Distributed-Ledger-Technologien sind Blockchains.[2] Eine Blockchain kann definiert werden als ein verteiltes Register, in dem digitale Datensätze, Ereignisse oder Transaktionen in chronologischer Reihenfolge für alle Teilnehmer nachvollziehbar in Datenblöcken gespeichert („Block“) und unveränderbar miteinander verkettet („Chain“) werden.[3] Da nicht alle Distributed-Ledger-Technologien auf die Verkettung von Blöcken als wesentlichem Ordnungsprinzip zurückgreifen, ist zwar jede Blockchain eine Distributed-Ledger-Technologie, aber nicht jede Distributed-Ledger-Technologie eine Blockchain.[4]

Durch eine Kombination verschiedener technologischer Elemente gewährleisten Blockchains eine hohe Datenintegrität und Systemsicherheit, ohne dabei auf einzelne vertrauenswürdige Instanzen angewiesen zu sein. Die Vertrauensbildung zwischen verschiedenen Akteuren kann bei Blockchains durch Verschlüsselungstechnologien in Verbindung mit verschiedenen Konsensmechanismen zur Validierung neuer Transaktionen geschaffen werden. Ein Intermediär, der klassischerweise für die Durchführung, Protokollierung und Absicherung von Transaktionen verantwortlich ist, wird nicht mehr benötigt.

Die obige Definition macht deutlich, dass der potenzielle Anwendungsbereich von Blockchains sehr groß ist. Alles, was digital darstellbar ist, kann grundsätzlich in einer Blockchain abgebildet werden. Blockchains gibt es in sehr vielen unterschiedlichen Ausprägungen. Sie unterscheiden sich insbesondere im Hinblick auf den

---

[1] Vgl. BMVI (2019).

[2] Vgl. dena (2019).

[3] Vgl. BDEW (2017), ÖFIT (2017).

[4] Vgl. dena (2019).

Kreis der Zugangsberechtigten, den verwendeten Konsensmechanismus zur Validierung neuer Daten bzw. Transaktionen sowie die Zusammensetzung und die Aufgaben der am Blockchain-Netzwerk beteiligten Akteure. Der tatsächliche Nutzen und Effizienzgewinn einer Blockchain-Anwendung ist deshalb stets im Einzelfall zu prüfen.

Zur Veranschaulichung der grundsätzlichen Funktionsweise einer Blockchain wird in diesem Kapitel an einigen Stellen exemplarisch die Bitcoin-Blockchain als ursprüngliche und heute mit Abstand bekannteste Blockchain-Anwendung herangezogen. Zwar setzen moderne Blockchain-Architekturen mittlerweile häufig etwas andere bzw. weiterentwickelte Technologien ein als die Bitcoin-Blockchain; zur Veranschaulichung der idealtypischen Funktionsweise einer Blockchain ist sie aber dennoch gut geeignet, weil sie viele der typischen technologischen Elemente, auf denen Blockchains basieren, verwendet.

Die Bitcoin-Blockchain ist ein für jedermann zugängliches blockchainbasiertes Zahlungssystem. Sie ermöglicht es den Teilnehmern, finanzielle Transaktionen ohne eine vermittelnde Instanz durchzuführen. Die Bitcoin-Blockchain nutzt dazu eine eigene Kryptowährung, die ebenfalls Bitcoin genannt wird. Um das notwendige Vertrauen zwischen den einzelnen Akteuren zu gewährleisten, werden sämtliche Transaktionen, die im Bitcoin-Netzwerk getätigt werden, zu Blöcken zusammengefasst und transparent, chronologisch und unveränderbar auf einer Vielzahl von Rechnern abgespeichert. Das Konzept der Bitcoin-Blockchain wurde im Jahr 2008 im Rahmen eines White-Papers veröffentlicht[5] und im Jahr 2009 realisiert.

In Abbildung 1 wird der Zusammenhang zwischen Distributed-Ledger-Technologien, Blockchains und der Bitcoin als konkreter Blockchain-Anwendung veranschaulicht.

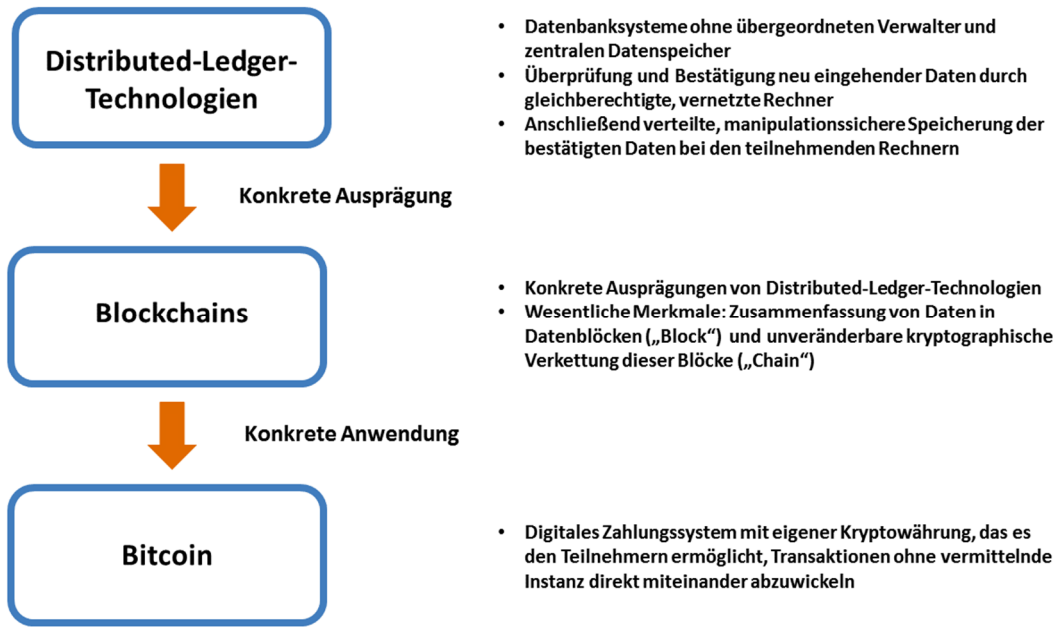


Abbildung 1: Zusammenhang Distributed-Ledger-Technologien, Blockchains, Bitcoin
Quelle: Eigene Darstellung

[5] Nakamoto (2008).

2.2.1 Peer-to-Peer Prinzipien und verteilte Datenspeicherungen

Blockchains basieren in der Regel auf Peer-to-Peer-Prinzipien. Diese besagen zum einen, dass Netzwerkteilnehmer Hardware-Ressourcen zur Verfügung stellen, um Inhalte bzw. Leistungen des Netzwerks bereitzustellen[6] und zum anderen, dass ein direkter Austausch zwischen den Netzknoten stattfindet. Diese Prinzipien tragen dazu bei, dass auf eine zentrale Instanz zur Koordination der Kommunikation zwischen den einzelnen Netzknoten verzichtet werden kann.[7]

Darüber hinaus sind Blockchain-Architekturen verteilte Systeme. Sie bestehen aus gleichberechtigten Rechnern (Netzknoten, „Nodes"), die miteinander kommunizieren und sich automatisch synchronisieren. Da die Daten der Blockchain grundsätzlich an jedem Netzknoten redundant gespeichert werden[8] und die einzelnen Netzknoten alle die gleichen Funktionen ausüben können, hat ein Ausfall einzelner Netzknoten nicht den vollständigen oder teilweisen Ausfall des Netzwerks zur Folge.

2.2.2 Kryptographische Funktionen

Um Teilnehmer in einem Blockchain-Netzwerk zu identifizieren, Transaktionen auszulösen, neue Blöcke zu bilden und diese Blöcke unveränderbar miteinander zu verketten, nutzen Blockchains kryptographische Funktionen. Die beiden wichtigsten Funktionen, die dazu eingesetzt werden, sind Public-Key-Kryptographien und kryptographische Hash-Funktionen.

a) Public-Key-Kryptographie

Bei der Public-Key-Kryptographie wird durch einen Algorithmus ein mathematisch verbundenes Schlüsselpaar generiert, das aus einem privaten und einem öffentlichen Schlüssel besteht. Der private Schlüssel muss vom jeweiligen Nutzer geheim gehalten werden. Der öffentliche Schlüssel ist dagegen allen Mitgliedern im Blockchain-Netzwerk bekannt und wird dazu verwendet, den einzelnen Nutzer im Netzwerk zu identifizieren.[9] Mit Hilfe des privaten Schlüssels kann ein Nutzer einen beliebigen Datensatz signieren und diesen Datensatz an einen Empfänger im Blockchain-Netzwerk senden. Der Empfänger kann den an ihn gerichteten Datensatz dann mit Hilfe des öffentlichen Schlüssels des Versenders überprüfen und die Authentizität des Datensatzes verifizieren (sofern die beiden Schlüssel korrespondieren).[10]

Durch eine digitale Signatur eines Datensatzes können drei Ziele erreicht werden:

- Erstens kann der Datenursprung nachgewiesen werden, da nur der Absender den privaten Schlüssel kennt.
- Zweitens kann der Absender der Daten nicht leugnen, die Daten signiert zu haben.[11]

---

[6] Vgl. Schlatt et al. (2016).

[7] Vgl. Schoder / Fischbach (2002).

[8] Im Gegensatz dazu speichert bei nicht-redundanten dezentralen Systemen ein Netzknoten nicht den gesamten Datensatz ab, sondern lediglich einen Teil des Gesamtdatensatzes.

[9] Vgl. ÖFIT (2017).

[10] Vgl. Badev / Chen (2014).

[11] Die ersten beiden Punkte setzen voraus, dass tatsächlich kein anderer Akteur Zugang zum privaten Schlüssel hat.

- Drittens gewährleistet das bei Public-Key-Kryptographien verwendete Schlüsselpaar aus privatem und öffentlichem Schlüssel die Integrität der Daten, weil die Daten nicht unbemerkt verändert werden können.[12]

b) Kryptographische Hash-Funktionen

Blockchains nutzen außerdem kryptographische Hash-Funktionen. Es handelt sich dabei um Algorithmen, die eine Zeichenfolge von beliebiger Länge in eine Zeichenfolge fixer Länge umwandeln. Diese (in der Regel verkürzte) Zeichenfolge wird Hash-Wert genannt. Hash-Funktionen sind deterministisch. Das bedeutet, dass dieselben Eingangsdaten immer denselben Hash-Wert ergeben. Außerdem führt jede Veränderung der Eingangsdaten zu einem veränderten Hashwert.[13] Das folgende Beispiel soll die Nutzung von Hash-Werten in Blockchains veranschaulichen:

Ein Konsortium aus mehreren Unternehmen verständigt sich auf einen Vertragstext und möchte eine Blockchain dazu verwenden, um den Inhalt des Vertrags manipulationssicher abzuspeichern. Die Unternehmen bilden dazu aus dem Vertragstext einen Hash-Wert, der zum Beispiel „0x4E3F785D“ lautet. Jede auch nur geringfügige Veränderung am ursprünglichen Vertragstext würde einen anderen Hash-Wert ergeben. Die Unternehmen speichern den Hash-Wert dann in der Blockchain ab, der Vertrag im Klartext selbst wird nicht in der Blockchain abgelegt.

Würde nun zu einem späteren Zeitpunkt ein weiteres Unternehmen Interesse an einer Aufnahme in das Konsortium haben, zuvor aber sicher sein wollen, dass für dieses Unternehmen die gleichen vertraglichen Bedingungen gelten, könnte das neue Unternehmen zur Überprüfung aus dem ihr zur Verfügung gestellten Vertragstext selbst noch einmal den Hash-Wert bilden. Sofern der oben genannte Hash-Wert bereits in der Blockchain abgelegt wäre, könnte das Unternehmen sicher sein, dass exakt dieser Vertragstext zwischen den übrigen Mitgliedern des Konsortiums vereinbart wurde.

Kryptographische Hash-Funktionen besitzen darüber hinaus zwei weitere wesentliche Eigenschaften: Aus einem bekannten Hash-Wert kann der ursprüngliche Dateninput mit vertretbarem Aufwand nicht mehr generiert werden. Im obigen Beispiel könnte ein Dritter aus dem Hash-Wert, der in der Blockchain abgelegt ist, den eigentlichen Vertragstext also nicht rekonstruieren (siehe zur Veranschaulichung dazu Abbildung 2). Darüber hinaus ist es mit vertretbarem Aufwand nicht möglich, zwei verschiedene Dateninputs zu finden, die denselben Hash-Wert ergeben.[14]

[12] Für eine detailliertere Darstellung der Public-Key-Kryptographie siehe zum Beispiel Stallings (2003) oder BSI (2019).

[13] Vgl. Schlatt et al. (2016).

[14] Vgl. BMVI (2019).

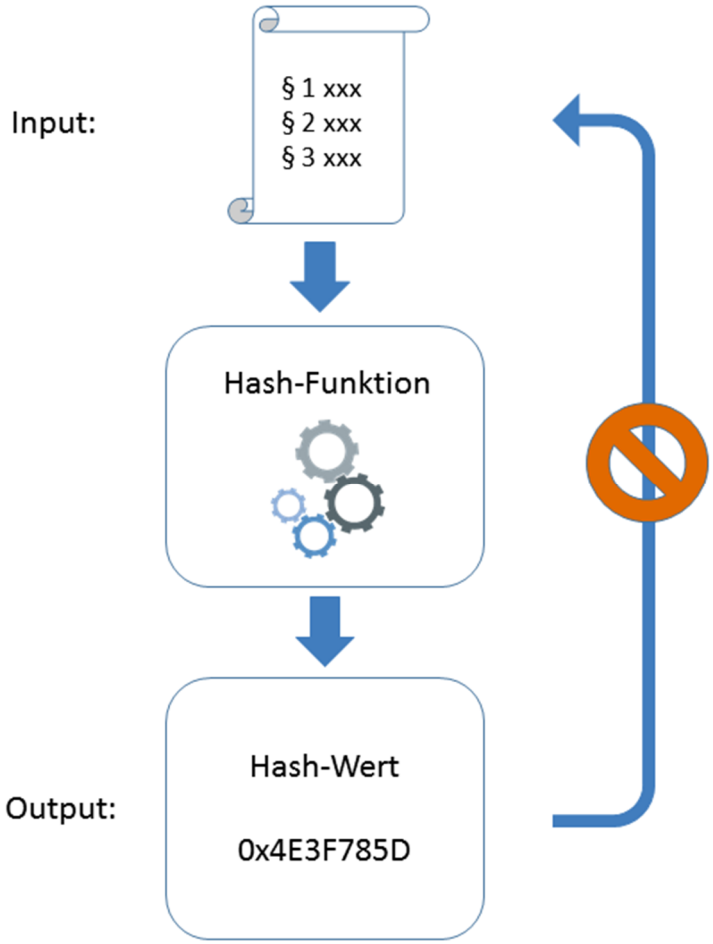


Abbildung 2: Schematischer Ablauf eines Hash-Vorgangs
Quelle: Eigene Darstellung, in Anlehnung an FfE (2018a).

2.2.3 Mitglieder in Blockchain-Netzwerken

Grundsätzlich können drei unterschiedliche Gruppen von Akteuren in Blockchain-Netzwerken unterschieden werden: Teilnehmer, Nodes und Miner. Sie übernehmen jeweils unterschiedliche Aufgaben und Funktionen im Netzwerk.

a) Teilnehmer

Teilnehmer sind die transaktionsberechtigen Nutzer eines Blockchain-Netzwerks. Um das Netzwerk nutzen zu können, muss sich ein Teilnehmer eine entsprechende Software, die als elektronische Brieftasche dient und deshalb auch als wallet bezeichnet wird, auf sein Endgerät herunterladen. In der Wallet wird das Schlüsselpaar aus öffentlichem und privatem Schlüssel verwaltet. Die Software ermöglicht dem Teilnehmer den Zugang zur Blockchain und bietet ihm die Möglichkeit, Transaktionen im Netzwerk auszulösen. Teilnehmer erbringen in der Regel keine Rechenleistung und müssen auch keine Transaktionshistorien speichern. In der Bitcoin-Blockchain sind mittlerweile ca. 40 Millionen Teilnehmer angemeldet.[15] Im Vergleich zu den Nodes

[15] https://www.blockchain.com/de/charts/my-wallet-n-users?timespan=all.

(ca. 9.000)[16] und den Minern (ca. 100.000)[17] bilden die Teilnehmer damit die mit Abstand größte Akteursgruppe im Bitcoin-Netzwerk.

b) Nodes

Nodes (Knoten) sind Computer in Blockchain-Netzwerken, die bestimmte Prüfaufgaben übernehmen. In der Bitcoin-Blockchain überprüfen sie beispielsweise, ob die Teilnehmer, die eine Transaktion ausführen möchten, über ein ausreichendes Guthaben verfügen, ob die für die Transaktionen verwendeten digitalen Signaturen authentisch sind und ob die Miner die korrekten Hash-Werte ermittelt haben. Damit Nodes diese Aufgaben erfüllen können, speichern sie die Historie aller bisher im Netzwerk getätigten Transaktionen.[18] Die Aufgaben eines Nodes sind nicht besonders rechenintensiv und können von jedem handelsüblichen Computer ausgeführt werden. Nodes werden für ihre Prüftätigkeit in der Regel nicht entlohnt. Anreize, dem Blockchain-Netzwerk Nodes zur Verfügung zu stellen, können vor allem darin bestehen, die gesamte Transaktionshistorie einsehen zu können und sich aktiv an der Aufrechterhaltung der Integrität der Blockchain zu beteiligen.[19]

c) Miner

Miner sind Rechner, deren primäre Aufgabe es ist, neue Blöcke in einer Blockchain zu bilden.[20] In der Bitcoin-Blockchain sind Miner Hochleistungsrechner, die versuchen, durch die Ermittlung von Hash-Werten neue Blöcke zu erstellen. Miner können grundsätzlich zwar auch Transaktionen in einer Blockchain auslösen; ihr eigentlicher Anreiz zur Teilnahme an einer Blockchain besteht aber in der Regel darin, für die Blockbildung monetär entlohnt zu werden.[21] In der Bitcoin-Blockchain erhalten Miner für die Erstellung eines neuen Blocks derzeit 12,5 Bitcoins und - sofern diese vorher vereinbart wurde - eine Transaktionsgebühr.[22]

In der Bitcoin-Blockchain sammeln Miner für die Erstellung neuer Blöcke zunächst eine Reihe beliebiger noch nicht validierter Transaktionen, die im Netzwerk aufgegeben wurden und dort quasi frei „herumschwirren". Anschließend versuchen sie im Wettbewerb mit anderen Minern als erstes den korrekten Hash-Wert eines neuen Blocks zu finden. Dieser Hash-Wert ist - wie in Abschnitt 2.2.2 beschrieben - einzigartig und vergleichbar mit einer Prüfsumme oder einem digitalen Fingerabdruck des zu erstellenden Blocks. Sobald ein Miner einen neuen Hash-Wert ermittelt hat, sendet er ihn in das Netzwerk, damit dessen Korrektheit von den Nodes überprüft werden kann. Ein wesentliches Merkmal dieser Hash-Werte besteht dabei darin, dass ihre Ermittlung durch die Miner äußerst komplex, die Überprüfung ihrer Korrektheit durch die Nodes aber sehr einfach ist.[23] Besteht im Netzwerk Konsens über die Korrektheit des vom Miner

---

[16] https://bitnodes.earn.com.

[17] Vgl. BDEW (2017).

[18] Diese Transaktionshistorie umfasst im Bitcoin-Netzwerk derzeit ca. 200 GB und wächst ca. alle zehn Minuten um 1 MB, vgl. Rübe (2018), Blocher (2018).

[19] Vgl. BDEW (2017).

[20] Darüber hinaus können Miner auch die Prüfaufgaben der Nodes wahrnehmen.

[21] Ein guter Überblick zu den Bitcoin-Teilnehmern und ihren Aufgaben findet sich z. B. bei BDEW (2017).

[22] Vgl. ÖFIT (2017).

[23] Vgl. Fraunhofer FIT (2017).

vorgeschlagenen Hash-Werts, so kann der Miner mit dem bestätigten Hash-Wert einen neuen Block bilden und ihn an die bisherige Blockchain anfügen.

2.2.4 Konsensmechanismen

Es existieren verschiedene Mechanismen, mit denen in Blockchains ein Konsens darüber hergestellt wird, wie neue Blöcke entstehen und an die bisherigen Blöcke angefügt werden können.[24]

a) Proof-of-Work

Der Proof-of-Work Mechanismus ist der älteste und bekannteste Konsensmechanismus, der bei Blockchains eingesetzt wird. Auch die Bitcoin-Blockchain basiert auf dem Proof-of-Work. Der Proof-of-Work steht im engen Zusammenhang mit dem im vorherigen Abschnitt beschriebenen Mining-Prozess. Beim Proof-of-Work konkurrieren die Miner im Blockchain-Netzwerk um die Lösung eines kryptographischen Rätsels. Die Lösung dieses Rätsels ist ein Hash-Wert, mit dem die Miner einen neuen Block bilden können. Dieser Hash-Wert ergibt sich – etwas vereinfacht dargestellt – aus den folgenden Eingangsparametern:

- dem bekannten Hash-Wert des vorherigen Blocks,
- den vom Netzwerk noch unbestätigten Transaktionen, aus denen ein Miner einen neuen Block bilden möchte,
- einem Zeitstempel des neu zu bildenden Blocks sowie
- einer unbekannten Variablen, der sogenannte nonce (Abkürzung für "number used only once").

Diese nonce setzt sich aus einer Zahlen- oder Buchstabenkombination zusammen, die einmalig zur Ermittlung des Hash-Wertes benötigt wird. Der Hash-Wert kann nur durch ein sehr rechenintensives Ausprobieren vieler möglicher nonces herausgefunden werden.[25] Ein einzelner Rechner würde in der Bitcoin-Blockchain dafür mittlerweile mehrere Jahre brauchen.[26] Da aber sehr viele Miner im Bitcoin-Netzwerk tätig sind, ist genügend Rechenkapazität vorhanden, um neue Blöcke innerhalb weniger Minuten bilden zu können.[27]

Die Zusammensetzung der einzelnen Blöcke und ihre Verkettung durch Hashwerte werden in Abbildung 3 verdeutlicht:

---

[24] Mittlerweile existieren über 30 Konsensmechanismen, vgl. dazu BMVI (2019).

[25] Für eine detaillierte Darstellung dazu siehe zum Beispiel: Schlatt et al. (2016), Fraunhofer FIT (2017) oder BMVI (2019).

[26] Vgl. BDEW (2017).

[27] Im Algorithmus der Bitcoin-Blockchain ist vorgegeben, dass in Abständen von ca. zehn Minuten neue Blöcke erstellt werden sollen. Um dies zu gewährleisten, verändert der Algorithmus regelmäßig in Abhängigkeit der aktuell zur Verfügung gestellten Rechenkapazität im Netzwerk die Schwierigkeit zur Ermittlung der nonce, vgl. BMVI (2019) oder Fraunhofer FIT (2017).

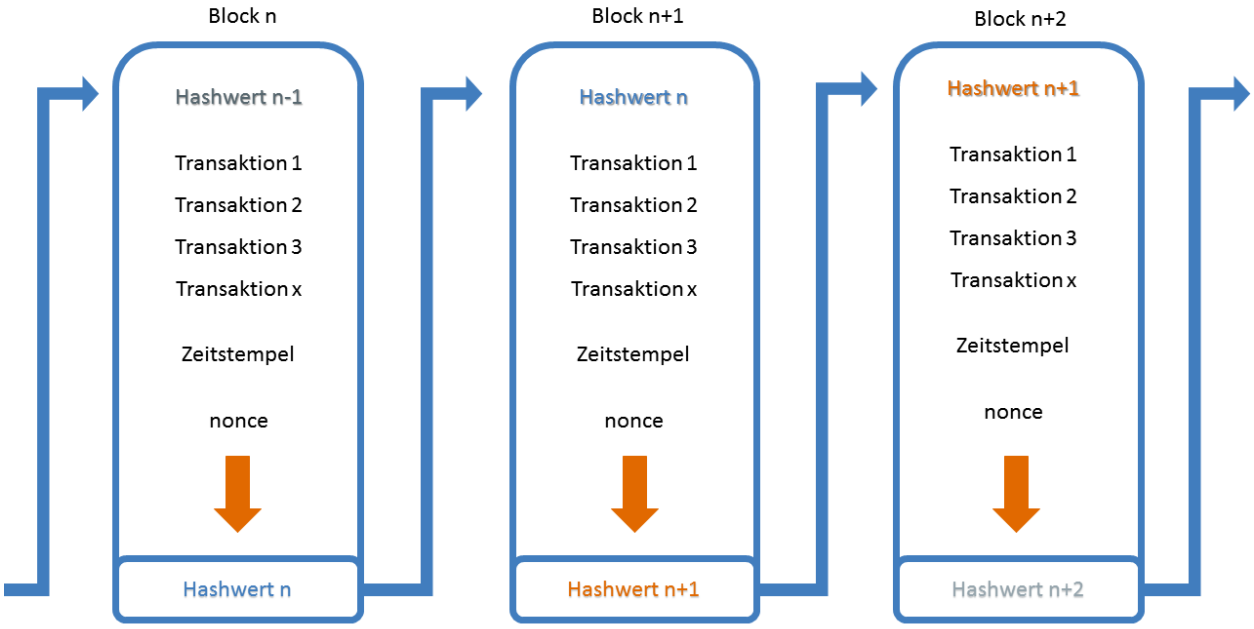


Abbildung 3: Struktur einer Blockchain - Verkettung über Hash-Werte
Quelle: Eigene Darstellung, in Anlehnung an BMVI (2019).

Der Proof-of-Work gilt als der sicherste Konsensmechanismus. Die hohe Datenintegrität ergibt sich vor allem aus der Tatsache, dass jeder neue Hash-Wert auf alle bereits bestätigten Hash-Werte aus den schon gebildeten Blöcken der Blockchain referenziert. Um nachträglich eine Manipulation an bereits vom Netzwerk bestätigten Blöcken vorzunehmen, müsste ein Akteur im Netzwerk deshalb nicht nur den Hash-Wert seines manipulierten Blocks, sondern auch die Hash-Werte für alle danach folgenden Blöcke ermitteln und deren Korrektheit anschließend vom Netzwerk bestätigen lassen.[28] Da die Blockchain als verteilte Datenbank auf einer Vielzahl von Knoten abgespeichert ist, müssten die manipulierten Blöcke zusätzlich gleichzeitig auf allen Knoten ausgetauscht werden.[29] Dies erscheint mit vertretbarem Aufwand derzeit nicht möglich.[30]

Der enorme Stromverbrauch, der aus der hohen benötigten Rechenleistung resultiert, wird als ein wesentlicher Nachteil des Proof-of-Work angesehen.[31] Aufgrund der Komplexität des zu lösenden Rätsels ist außerdem die Transaktionsgeschwindigkeit in der Regel stark limitiert. Viele moderne Blockchain-Systeme (insbesondere konsortiale und private Blockchains) verwenden deshalb andere Konsensmechanismen.

b) Proof-of-Stake

Eine Alternative zum zeit- und rechenintensiven Proof-of-Work ist der Proof-of-Stake-Mechanismus.[32] Dabei wählt der Blockchain-Algorithmus gezielt solche Mitglieder des Blockchain-Netzwerks zur Bildung neuer

[28] Vgl. BMVI (2019).

[29] Vgl. Schlatt et al. (2016).

[30] Vgl. Narayanan et al. (2016).

[31] Siehe dazu Abschnitt 3.2.4.

[32] Vgl. BDEW (2017), Schlatt et al. (2016).

Blöcke aus, die im Vergleich zu den anderen Mitgliedern bereits größere Vermögen bzw. Werte in die Blockchain investiert haben (zum Beispiel, weil sie höhere Anteile an der jeweiligen Kryptowährung besitzen). Dem Proof-of-Stake Mechanismus liegt die Annahme zugrunde, dass diese wohlhabenden Teilnehmer aufgrund ihres eingesetzten Vermögens ein hohes Interesse am Fortbestand und der Integrität der Blockchain haben. Je größer das bereits investierte Vermögen eines Blockchain-Mitglieds in die Blockchain ist, desto höher ist die Wahrscheinlichkeit, vom Algorithmus für die nächste Blockbildung ausgewählt zu werden. Die vom Algorithmus ausgesuchten Mitglieder überprüfen die Transaktionen des Netzwerks und sind für die korrekte Bildung neuer Blöcke verantwortlich. Zugleich haften sie mit ihrem eingesetzten Vermögen für die Korrektheit der Blockbildung. Da die Vertrauenswürdigkeit in die Miner beim Proof-of-Stake im Gegensatz zum zuvor beschriebenen Proof-of-Work a priori vorausgesetzt wird, hat der Proof-of-Stake den Vorteil, dass das Lösen des kryptographischen Rätsels deutlich einfacher ausgestaltet werden kann.[33] Die Bildung neuer Blöcke ist deshalb wesentlich schneller und ressourcenschonender als beim Proof-of-Work. Im Gegenzug setzt der Proof-of-Stake Vertrauen in die vom Algorithmus ausgewählten Akteure voraus, sodass auf einen Teil der hohen Sicherheit, den der Proof-of-Work bietet, verzichtet wird.

c) Proof-of-Authority

Ein weiterer Konsensmechanismus, der insbesondere in privaten Blockchains (siehe Abschnitt 2.2.5) verwendet wird, ist der Proof-of-Authority. Hierbei werden einzelne Teilnehmer, denen die Verwaltung des Blockchain-Netzwerks obliegt, für die Blockbildung bestimmt. Dieser Konsensmechanismus ist noch deutlich schneller und ressourcenschonender als der Proof-of-Stake, setzt allerdings ein sehr hohes Vertrauen in die blockbildenden Teilnehmer voraus.

2.2.5 Blockchain-Varianten

Ein entscheidender Aspekt zur Kategorisierung unterschiedlicher Blockchain-Varianten ist die Ausgestaltung der Zugangsberechtigungen. Vergleichbar zur Unterscheidung zwischen Internet und Intranet können auch Blockchains grundsätzlich unterteilt werden in öffentlich zugängliche (public blockchains bzw. permissionless blockchains) und geschlossene Blockchains (private bzw. permissioned blockchains). Eine Mischform hieraus stellen konsortiale Blockchains dar.

a) Öffentliche Blockchains

An öffentlich zugänglichen Blockchains kann sich jedermann sowohl als Teilnehmer, Node oder Miner beteiligen. Die bekanntesten Blockchains wie Bitcoin oder Ethereum[34] sind öffentlich zugänglich. Öffentliche Blockchains basieren in der Regel auf dem Proof-of-Work Mechanismus. Sie bieten deshalb eine sehr hohe Sicherheit, weisen aber einen hohen Energieverbrauch und eine niedrige Transaktionsgeschwindigkeit auf. Sie können pseudonym genutzt werden und verwenden in der Regel als Anreizmechanismus zur Bildung neuer Blöcke eine digitale Währung wie Bitcoin oder Ether (bei Ethereum).[35] Änderungen an der Blockchain-Architektur (z. B. in Bezug auf den verwendeten Konsensmechanismus, Zugangsberechtigungen oder die Durchführung von Software-Updates) sind bei öffentlichen Blockchains nur mit hohem Aufwand

---

[33] Vgl. BMVI (2019).

[34] Siehe dazu Abschnitt 2.2.6.

[35] Vgl. dazu die Erläuterungen zu Minern in Abschnitt 2.2.3.

umzusetzen, da es weder geschäftsführende Verantwortliche noch eine zentrale Verwaltungsinstanz gibt.[36] Um Änderungen bzw. Aktualisierungen an öffentlichen Blockchains vornehmen zu können, ist eine Mehrheit aller beteiligten Akteure erforderlich.[37]

b) Private Blockchains

In privaten Blockchains ist die Anzahl der Teilnehmer durch festgelegte Kriterien beschränkt. Die zugelassenen Teilnehmer werden von einer zentralen Instanz (zum Beispiel einem Unternehmen oder einer Unternehmenseinheit) aufgenommen und sind deshalb bekannt. Da die Vertrauenswürdigkeit der einzelnen Teilnehmer grundsätzlich vorausgesetzt wird, nutzen private Blockchains in der Regel Konsensmechanismen, die deutlich weniger komplex und damit wesentlich schneller und energieschonender sind als bei öffentlichen Blockchains (z. B. den Proof-of-Stake oder den Proof-of-Authority). Private Blockchains sind wesentlich flexibler als öffentliche, weil Änderungen der „Spielregeln" durch die zentrale Instanz einfach umgesetzt werden können. So ist es beispielsweise möglich, festzulegen, dass nur bestimmte Teilnehmer Einblick oder Zugriff auf bestimmte Daten haben oder dass die Blockchain in bestimmten Zeitabständen abgeschnitten wird. Private Blockchains eignen sich aufgrund ihrer Eigenschaften vor allem für die Organisation unternehmensinterner Prozesse.

c) Konsortiale Blockchains

Als Hybridlösung kommen konsortiale Blockchains in Betracht. Sie werden in der Regel nicht von einer zentralen Instanz verwaltet, sondern von einem Konsortium. Zugang haben wie bei privaten Blockchains nur zugelassene Teilnehmer. In Abhängigkeit des jeweiligen Anwendungszwecks kommen alle in den vorherigen Abschnitten beschriebenen Konsensmechanismen in Betracht. Die Flexibilität ist deutlich höher als bei öffentlich zugänglichen Blockchains, aber im Vergleich zu privaten Blockchains eingeschränkt. Die Daten- und Systemsicherheit, die Geschwindigkeit des Netzwerks und der Energieverbrauch hängen jeweils von der konkreten Blockchain-Architektur ab.

In der folgenden Tabelle sind die wesentlichen Unterschiede zwischen öffentlichen, privaten und konsortialen Blockchains zusammengefasst:

[36] Die meisten öffentlichen Blockchains wie Bitcoin und Ethereum basieren auf einem Open-Source Ansatz, bei dem sich jedermann an der Weiterentwicklung der Blockchain-Architektur beteiligen kann.

[37] Vgl. FfE (2018a).

Vergleich öffentliche, private, konsortiale Blockchains

	Öffentlich	Privat	Konsortial
Zugang	Offen zugänglich	Nur für zugelassene Teilnehmer	Nur für zugelassene Teilnehmer
Personenbezug	Pseudonyme Nutzung	Herstellbar	Herstellbar
Bildung neuer Blöcke	Dezentral durch Ressourceneinsatz der Miner	Zentral durch einzelne Instanz	Je nach Ausgestaltung
Konsensmechanismus	i. d. R. Proof-of-Work, z. T. auch Proof-of-Stake	i. d. R. Proof-of-Stake oder Proof-of-Authority	Je nach Ausgestaltung
(IT)-Sicherheit	Sehr hoch, kein Single-Point-of-Failure, Manipulationen kaum möglich	Eingriffe durch zentralen Akteur möglich, Single-Point-of-Failure	Je nach Ausgestaltung
Energieverbrauch	Hoch (beim Proof-of-Work)	Tendenziell niedrig	Je nach Ausgestaltung
Transparenz	Hoch durch offene Transaktionshistorie	Nur für ausgewählten Teilnehmerkreis	Nur für ausgewählten Teilnehmerkreis
Systemänderungen	Niedrige Flexibilität	Hohe Flexibilität	i. d. R. Konsens im Konsortium notwendig
Änderungen an bereits durchgeführten Transaktionen	Nicht möglich	Möglich durch zentrale Instanz	Möglich (z. B. durch Mehrheitsbeschluss)
Geschwindigkeit der Transaktionen	Gering (beim Proof-of-Work)	Tendenziell schnell	Tendenziell schneller als bei öffentlichen Blockchains
Kryptowährung	i. d. R. als Anreizmechanismus zur Bildung neuer Blöcke notwendig	Optional	Optional

Quelle: Bundesnetzagentur, in Anlehnung an BDEW (2017), FfE (2018a)

Tabelle 1: Vergleich öffentliche, private, konsortiale Blockchains

2.2.6 Smart Contracts

Seit der Veröffentlichung des Bitcoin-Whitepapers „Bitcoin: A Peer-to-Peer Electronic Cash System“[38] im Jahr 2008 hat sich die Blockchain-Technologie rasant weiterentwickelt. Mit Hochdruck werden insbesondere neue Anwendungen erarbeitet und die in den vorherigen Abschnitten beschriebenen technologischen Elemente weiterentwickelt. Als die wichtigste konzeptionelle Weiterentwicklung der Blockchain werden sog. Smart Contracts angesehen.[39] Sie ermöglichen insbesondere eine blockchainbasierte automatisierte Ausführung von

[38] Nakamoto (2008).

[39] Vgl. dena (2019), BEE (2019).

Wenn-dann-Beziehungen.[40] Eine solche könnte zum Beispiel lauten: „Wenn Nachbar A Strom für < 28 Cent / kWh verkauft, dann 15 kWh kaufen“.

Um dies zu realisieren, wird – vereinfacht dargestellt – in das Blockchain-Protokoll ein Platzhalter eingebaut, in den die beteiligten Parteien über die jeweilige Benutzeroberfläche der Blockchain (z. B. einer App) die Bedingungen ihrer Transaktionen eingeben können.[41] Durch das Konzept der Smart Contracts eröffnet sich ein signifikantes Automatisierungspotenzial in allen Blockchain-Anwendungsbereichen. Auch die meisten der angedachten oder derzeit getesteten Anwendungsfälle im Energie- und Telekommunikationssektor basieren auf Smart Contracts.

Als die wichtigste Blockchain, die Smart Contracts ermöglicht, gilt die öffentlich zugängliche Ethereum Blockchain. Sie verwendet ein eigenes Proof-of-Work-Verfahren und eine eigene Kryptowährung, die Ether genannt wird. Ether weist mit ca. 19,9 Mrd. Dollar (Stand 14. Oktober 2019) nach Bitcoin die zweitgrößte Marktkapitalisierung aller Kryptowährungen auf.[42] Ethereum ist darüber hinaus nicht nur eine einzelne Blockchain, sondern auch eine Blockchain-Plattform, die eine besondere Form von blockchain-basierten App-Angeboten ermöglicht. Auf Open-Source-Basis ist eine Vielzahl von öffentlichen zugänglichen Anwendungen (zum Beispiel Musikstreaming-Dienste, Finanzdienstleistungen, Computerspiele) für jedermann als „distributed Apps“ nutzbar.[43]

Neben der Ethereum-Plattform existiert eine Vielzahl weiterer Smart Contract Plattformen, die sich hinsichtlich der verwendeten Konsensmechanismen und vieler weiterer Kriterien zum Teil deutlich voneinander unterscheiden[44].

2.2.7 Orakel

Sofern die Ausführung eines Smart Contracts von einem Ereignis oder einem Zustand außerhalb der Blockchain abhängig ist, müssen die für die Ausführung des Smart Contracts notwendigen Informationen von einer externen Informationsquelle in die Blockchain eingespeist werden. Diese externen Informationsquellen werden als Orakel bezeichnet. Ein Orakel kann z. B. ein Thermometer sein, das eingesetzt wird, um die Einhaltung der Kühlkette während einer Warenlieferung zu überprüfen. Im entsprechenden Smart Contract würde dann z. B. festgelegt, dass die Bezahlung der Ware automatisch erfolgen soll, sobald sie beim Empfänger angekommen ist (dies bestätigt der Empfänger durch einen Eintrag in die Blockchain) und sofern eine bestimmte Temperatur, die in regelmäßigen Zeitabschnitten durch das Thermometer erfasst und in die Blockchain eingespeist wird, während des Transports nicht überschritten wurde. Orakel ermöglichen es so, Transaktionen in der Blockchain an den Eintritt von Zuständen und Ereignissen aus der realen Welt zu knüpfen.

---

[40] Vgl. BMVI (2019).

[41] Für eine detailliertere technische Beschreibung dazu siehe z. B. Schlatt et al. (2016).

[42] https://coinmarketcap.com/

[43] Für weitere Informationen siehe https://www.ethereum.org/.

[44] Ein guter Überblick findet sich zum Beispiel bei dena (2019).

3 Potenziale und Herausforderungen der Blockchain-Technologie

Im folgenden Kapitel werden die Potenziale, die sich bei Blockchains aus der Kombination verschiedener technologischer Elemente ergeben können, kurz beschrieben. Je nach eingesetzter Blockchain-Architektur können die tatsächlichen Mehrwerte variieren und mehr oder weniger stark ausgeprägt sein. Im Anschluss an die Beschreibung der Potenziale werden dann kurz die wesentlichen technologischen und rechtlich-regulatorischen Herausforderungen, die mit der Nutzung der Blockchain-Technologie einhergehen, skizziert.

3.1 Technische und ökonomische Potenziale

Durch die Kombination von Peer-to-Peer-Prinzipien mit redundanten verteilten Datenspeicherungen an jedem Netzknoten versprechen vor allem öffentliche Blockchains eine hohe Ausfallsicherheit.[45] Da alle Netzknoten stets den gesamten Datensatz der Blockchain vorhalten und sie unabhängig voneinander agieren können, weisen sie keinen Single Point of Failure auf.[46] Die Netzwerkfunktionalität und damit auch die permanente Datenverfügbarkeit bleiben deshalb jederzeit gewährleistet.

Durch die kryptographische Verkettung der einzelnen Blöcke gewährleisten Blockchains außerdem eine hohe Datenintegrität. Insbesondere bei öffentlichen Blockchains sind Manipulationen an den vom Netzwerk bestätigten Blöcken aufgrund der Tatsache, dass alle neuen Blöcke auf die vorher bereits bestätigten Blöcke referenzieren, praktisch nicht möglich. Wie in Abschnitt 2.2.4 dargestellt, gilt dabei, dass der Aufwand einen Block nachträglich zu manipulieren umso höher ist, je länger dieser Block bereits Bestandteil der Blockchain ist.

Blockchains sind außerdem sehr transparent, da die gesamte Transaktionshistorie grundsätzlich jederzeit von jedem Mitglied des Netzwerks eingesehen werden kann.[47] Die hohe Datenintegrität und Transparenz schafft zugleich Vertrauen zwischen den Akteuren des Blockchain-Netzwerks. Ein Intermediär, der klassischerweise eine Vermittlungsfunktion zwischen unterschiedlichen Akteuren übernimmt und die Vertrauensbildung zwischen ihnen gewährleistet, ist in vielen Fällen nicht mehr nötig.

Ein weiterer Vorteil ist, dass Blockchains durch die Verwendung eines öffentlichen Schlüssels pseudonym genutzt werden können. Dies ist insbesondere deshalb von Bedeutung, weil die Transaktionshistorie bei Blockchains grundsätzlich für alle Mitglieder jederzeit vollständig einsehbar ist. Es müssen deshalb Mechanismen eingesetzt werden, die – sofern von den Teilnehmern gewünscht – verhindern, dass Rückschlüsse auf sie gezogen werden können.[48] Die Möglichkeit zur pseudonymen Nutzung ist aus datenschutzrechtlicher Perspektive ein wesentlicher Mehrwehrt. Aber auch in unternehmerischer Hinsicht kann die Tatsache, dass keine Zuordnung zu realen Akteuren möglich ist, einen wichtigen Mehrwert darstellen. So ist es zum Beispiel denkbar, Ausschreibungen über eine Blockchain zu organisieren, bei denen

[45] Vgl. Xethalis et al. (2016).

[46] Vgl. T-Systems (2018).

[47] Sofern die Mitglieder die Transaktionshistorie vollständig abspeichern.

[48] Vgl. Schlatt et al. (2016).

die teilnehmenden Unternehmen ihre eigene Identität bei der Abgabe ihrer Angebote gegenüber den anderen Bietern nicht preisgeben müssen.

Darüber hinaus versprechen die technologischen Weiterentwicklungen der Blockchain-Technologie hohe Mehrwerte. Insbesondere Smart Contracts bieten ein signifikantes Automatisierungspotenzial. Dadurch können Transaktionskosten gesenkt und eine hohe Prozessintegrität gewährleistet werden, weil nachträgliche Abweichungen von einmal getroffenen Vereinbarungen nicht mehr möglich oder zumindest deutlich erschwert werden.[49]

3.2 Technische Herausforderungen

Den im vorherigen Abschnitt beschriebenen Potenzialen stehen jedoch noch eine Reihe von technologischen und rechtlich-regulatorischen Herausforderungen gegenüber, die im Folgenden kurz beschrieben werden.

3.2.1 Transaktionsgeschwindigkeit

Bei öffentlich zugänglichen Blockchains, bei denen Vertrauen zwischen den Akteuren durch den komplexen Proof-of-Work-Mechanismus geschaffen wird, ist die begrenzte Transaktionsgeschwindigkeit für einen breiten Einsatz derzeit noch ein wesentlicher limitierender Faktor. In der Bitcoin-Blockchain werden zurzeit lediglich drei Transaktionen pro Sekunde und bei Ethereum 20 Transaktionen pro Sekunde abgewickelt. Das VISA-Zahlungsnetzwerk wickelt im Vergleich dazu durchschnittlich 2.000 Transaktionen pro Sekunde ab (bei einer maximalen Kapazität von sogar 56.000 Transaktionen pro Sekunde). PayPal ermöglicht im Vergleich dazu ca. 150 Transaktionen pro Sekunde.[50] Insbesondere für mögliche zukünftige Anwendungen, die Massentransaktionen bzw. auch eine Vielzahl von Kleinsttransaktionen in kurzen Zeiträumen erfordern – etwa für Anwendungen im Bereich des Internets der Dinge – sind die derzeit möglichen Transaktionsgeschwindigkeiten öffentlicher Blockchains viel zu gering.[51]

Mit Hochdruck wird deshalb an alternativen Möglichkeiten zur Erhöhung der Skalierbarkeit gearbeitet. Vielversprechende Weiterentwicklungen sind zum Beispiel sog. Parachains, bei denen der Rechenaufwand an andere Netzwerke ausgelagert wird, um so durch ein paralleles Verarbeiten von Transaktionen erhebliche Geschwindigkeitszunahmen zu erzielen. Auch sog. State-Channels versprechen eine deutlich höhere Transaktionsgeschwindigkeit. Bei diesem Ansatz werden Transaktionen bilateral zwischen den Akteuren außerhalb der Blockchain abgewickelt und nur noch die jeweiligen Ergebnisse der Transaktionen in der Blockchain festgehalten. Der Rechenaufwand soll dadurch deutlich reduziert und die Transaktionsgeschwindigkeit so erhöht werden.[52] Ein weiterer Versuch, die Transaktionsgeschwindigkeit zu erhöhen, ist das IOTA-Konzept, bei dem auf die Blockbildung völlig verzichtet wird und die einzelnen Transaktionen stattdessen direkt miteinander verknüpft werden.[53]

---

[49] Vgl. BDEW (2017).

[50] Vgl. dena (2019), BDEW (2017).

[51] Schätzungen zufolge werden ca. 130 Geräte pro Sekunde mit dem Internet verbunden, siehe McKinsey (2017). Bis 2030 wird erwartet, dass ca. drei Billionen Geräte mit dem Internet verbunden sein werden, siehe General Electric (2017).

[52] Für Einzelheiten zu diesen Ansätzen siehe beispielsweise dena (2019), BDEW (2017).

[53] Bei diesem Konzept handelt es sich um eine Distributed-Ledger-Technologie, nicht aber um eine Blockchain. Für eine detailliertere Beschreibung siehe zum Beispiel FfE (2018a), BDEW (2017), BMVI (2019).

Bei privaten und konsortialen Blockchains besteht das Skalierungsproblem in aller Regel nicht, weil hier Vertrauen zwischen den einzelnen Akteuren vorausgesetzt wird und deshalb auf den zeit- und energieintensiven Proof-of-Work zur Validierung von Transaktionen verzichtet werden kann.

3.2.2 Dauerhafte IT-Sicherheit und Integrität

Nach dem heutigen Stand der Technik gelten öffentliche Blockchains mit dem Proof-of-Work Verfahren als äußerst manipulationssicher. Mit vertretbarem Aufwand erscheint es derzeit nicht möglich, unbemerkt Transaktionen im Netzwerk zu manipulieren. Bei privaten und konsortialen Blockchains wird das hohe technische Sicherheitsniveau des Proof-of-Work zugunsten einer verbesserten Handhabung (geringerer Energieverbrauch, geringere Komplexität, höhere Skalierbarkeit) eingeschränkt, weil bei diesen Blockchains davon ausgegangen wird, dass die einzelnen Teilnehmer vertrauenswürdig sind.[54]

Eine enorm wichtige Herausforderung für die Blockchain-Technologie besteht aber darin, das derzeitige Sicherheitsniveau auch dauerhaft gewährleisten zu können. Zwar verwenden die meisten Blockchain-Architekturen wie beschrieben bewährte technologische Verfahren; in Zukunft werden aber vermutlich neue, verbesserte Angriffsmöglichkeiten (zum Beispiel auf die verwendeten kryptographischen Funktionen) entwickelt werden. In Kombination mit den kontinuierlich steigenden Rechenleistungen werden dadurch ganz neue Angriffsszenarien möglich.[55] Da sich potenzielle Blockchain-Anwendungen über enorm lange Zeiträume erstrecken können (etwa im Bereich notarieller Beurkundungen) ist es von essenzieller Bedeutung, dass die zugrunde liegenden Blockchains auch zukünftigen Manipulationsversuchen standhalten können. Dies kann insbesondere dadurch gewährleistet werden, dass Blockchain-Architekturen flexibel genug ausgestaltet werden, um adäquat auf neue Bedrohungslagen reagieren zu können.[56] Viele der heutigen Blockchains erfüllen diese Anforderung aber noch nicht.[57]

Eine weitere wichtige Herausforderung besteht darin, auch die Schnittstellen zu anderen Informationssystemen sicher auszugestalten. Dies gilt vor allem für die in Abschnitt 2.2.7 beschriebenen Orakel-Dienste, mit deren Hilfe externe Informationen in die Blockchain eingespeist werden. Das hohe Sicherheitsniveau, das die Blockchain-Technologie bietet, muss auch bei diesen externen Informationsquellen gewährleistet werden. Die meisten der bisher entwickelten Orakeldienste haben ein solch hohes Sicherheitsniveau noch nicht erreicht.[58]

3.2.3 Interoperabilität

Als ein weiterer zentraler Erfolgsfaktor für die Blockchain-Technologie wird die Schaffung von Interoperabilität zwischen unterschiedlichen Blockchain-Architekturen angesehen.[59] Als interoperabel gelten Informationssysteme, wenn Informationen zwischen ihnen geteilt und Operationen systemübergreifend

---

[54] Vgl. Blocher (2018).

[55] Eine Übersicht dazu findet sich zum Beispiel bei: Fraunhofer FIT (2017).

[56] Vgl. Fridgen (2018), BSI (2019).

[57] Für Einzelheiten dazu siehe Fraunhofer FIT (2017).

[58] Vgl. dena (2019), ÖFIT (2017).

[59] Vgl. BDEW (2017).

durchgeführt werden können.[60] In Bezug auf Blockchains würde dies zum Beispiel bedeuten, dass nicht nur Informationen zwischen unterschiedlichen Blockchains ausgetauscht, sondern auch Vermögenswerte in andere Blockchains transferiert oder Smart Contracts auf Basis von unterschiedlichen Blockchains durchgeführt werden können. In den Netzsektoren dürfte ein solche Interoperabilität insbesondere bei sektorübergreifenden Anwendungen – im Energiebereich zum Bespiel im Rahmen von Sektorkopplungen – von hoher Bedeutung sein.

Auch wenn intensiv an der Entwicklung von standardisierten Schnittstellen zum Austausch von Daten zwischen Blockchains gearbeitet wird, besteht heute noch keine Interoperabilität zwischen verschiedenen Blockchain-Architekturen. Erste Ansätze dazu liefern zum Beispiel die Konzepte Polkadot[61], Plasma[62] und MultiChain[63]. Auch die Internationale Organisation für Normung (ISO) hat ein Technisches Komitee für „Blockchain and distributed ledger technologies“ gegründet (ISO/TC 307), das sich mit Fragen von Standardisierung und Interoperabilität von Distributed-Ledger-Technologien beschäftigt.

3.2.4 Stromverbrauch

Der mit dem Proof-of-Work verbundene Miningprozess zur Bildung neuer Blöcke weist einen enorm hohen Stromverbrauch auf. Dieser verursacht hohe Kosten und ggfs. auch erhebliche Umweltbelastungen.[64] Zwar ist der Stromverbrauch nicht exakt ermittelbar, weil zum Mining weltweit unterschiedliche Rechner eingesetzt werden, deren Stromverbrauch nicht zentral erfasst wird. Verschiedene Schätzungen[65] gehen aber davon aus, dass allein der Stromverbrauch der Bitcoin-Blockchain im Jahr 2018 mit ca. 20 TWh etwa 0,1 % des gesamten weltweiten Stromverbrauchs ausmachte. Hinzu kommt, dass auch viele andere Blockchains wie Ethereum aber auch weniger bekannte wie Dash, ZCash oder Monero einen energieintensiven Proof-of-Work Mechanismus verwenden.[66]

Andere Konsensmechanismen wie der Proof-of-Stake oder der Proof-of-Authority weisen deutlich geringere Stromverbräuche auf als der Proof-of-Work und ermöglichen darüber hinaus wesentlich höhere Transaktionsgeschwindigkeiten. Allerdings haben diese alternativen Konsensmechanismen bisher noch nicht den Nachweis erbracht, dass sie ein vergleichbares Sicherheitsniveau wie der Proof-of-Work gewährleisten können. Außerdem bieten sie nicht die gleichen Partizipationsmöglichkeiten wie der Proof-of-Work, vor allem, weil sich nicht jeder Akteur an der Blockbildung beteiligen kann.

Eine weitere wesentliche Herausforderung wird deshalb darin bestehen, diesen Zielkonflikt aufzulösen und Lösungen zu finden, die ein angemessenes Sicherheitsniveau gewährleisten, eine hohe Skalierbarkeit ermöglichen, ausreichende Partizipationsmöglichkeiten (in Bezug auf die Blockbildung, die Transparenz der

---

[60] Vgl. dena (2019).

[61] https://polkadot.network.

[62] https://plasma.io.

[63] https://multichain.com.

[64] Siehe dazu zum Beispiel Schlatt et al. (2016) oder BDEW (2017).

[65] Vgl. https://digiconomist.net/bitcoin-energy-consumption, Vries (2018).

[66] Weitergehende Informationen dazu sowie eine kritische Auseinandersetzung mit dem Stromverbrauch beim Proof-of-Work findet sich z. B. bei Reetz (2019).

Blockchain etc.) einräumen und zugleich einen deutlich geringeren Stromverbrauch aufweisen als der derzeitige Proof-of-Work.[67]

3.3 Rechtliche Herausforderungen

Blockchains werfen eine Vielzahl von komplexen Rechtsfragen auf, die sich insbesondere einteilen lassen in die Themenfelder allgemeines Vertragsrecht und Datenschutzrecht sowie den je nach Anwendungsfall einschlägigen sektorspezifischen Rechtsgebieten wie dem Energie- oder dem Telekommunikationsrecht. Im Folgenden wird ein kurzer Überblick über relevante grundsätzliche Rechtsfragen gegeben, die sich ganz allgemein bei der Implementierung von Blockchain-Anwendungen stellen.

3.3.1 Zivilrechtliche Herausforderungen

Wie in den vorherigen Kapiteln beschrieben wurde, besteht ein wesentlicher Vorteil von Blockchains darin, dass einmal vom Netzwerk bestätigte Daten bzw. Transaktionen aufgrund ihrer kryptographischen Verkettung nicht mehr verändert werden können. Dies schließt allerdings auch falsche, versehentliche oder illegale Daten ein. Da das allgemeine Zivilrecht keine unveränderlichen Transaktionshistorien kennt, kann diese Unveränderbarkeit der Daten aus rechtlicher Sicht problematisch sein, denn sie erschwert die Befolgung ganz fundamentaler Rechtsgrundsätze wie die Nichtigkeit, die Anfechtbarkeit, die Rückabwicklung oder die schwebende Unwirksamkeit von Verträgen.

Da geschädigten Blockchain-Nutzern natürlich dennoch die allgemeinen Rechtsmittel zur Verfügung stehen müssen – etwa wenn trotz Fehlens eines rechtlichen Grundes eine Zahlung geleistet wurde – müssen hierfür angemessene Lösungen gefunden werden. Ein Lösungsansatz besteht darin, eine entsprechende Gegentransaktion (Rückübereignung oder Rücküberweisung) durchzuführen, die – sofern erforderlich – auch mit den Mitteln der Zwangsvollstreckung erzwungen werden kann.[68] In Bezug auf die Rechtsdurchsetzung kann daran allerdings bei öffentlichen Blockchains problematisch sein, dass aufgrund einer pseudonymen Nutzung möglicherweise weder die Identität noch der Aufenthaltsort der Gegenpartei bekannt ist.

Eine weitere rechtliche Herausforderung ergibt sich bei öffentlichen Blockchains aus der Tatsache, dass sie keine zentrale Instanz bzw. keinen übergeordneten Verwalter besitzen. Hier stellt sich insbesondere die Frage, wer bei einer mangelhaften Leistung oder bei einer Nichtleistung des Netzwerks haftet, wenn diese Leistungen auf einen (technischen) Systemfehler zurückzuführen sind.

Grundsätzlich gilt, dass die dargestellte Problematik bei privaten bzw. konsortialen Blockchains deutlich weniger stark ausgeprägt ist. Erstens sind die Teilnehmer hier in aller Regel bekannt und werden als vertrauenswürdig eingestuft und zweitens kann hier die Blockchain-Architektur individuell auch so ausgestaltet werden, dass Rückabwicklungen von Transaktionen oder nachträgliche Eingriffe in die Blöcke möglich sind.[69]

---

[67] Detaillierte Informationen dazu und auch weitere Literaturhinweise zu diesem Zielkonflikt finden sich bei dena (2019).

[68] Vgl. Blocher (2018).

[69] Vgl. Blocher (2018).

3.3.2 Datenschutzrechtliche Herausforderungen

Sofern im Rahmen einer Blockchain personenbezogene Daten verarbeitet (z. B. gespeichert) werden, müssen die einschlägigen datenschutzrechtlichen Bestimmungen, insbesondere die Datenschutzgrundverordnung[70], beachtet werden. Wesentliche Rechte, die sich aus der Datenschutzgrundverordnung für Verbraucher ergeben, sind das Recht auf Löschung der eigenen personenbezogenen Daten[71], das Recht auf „Vergessenwerden“[72] sowie das Recht auf Datenportabilität.[73] Insbesondere das Recht auf Löschung und das Recht auf „Vergessenwerden“ stehen in einem fundamentalen Widerspruch zu den Grundprinzipien der Unveränderbarkeit und jederzeitigen vollständigen Transparenz der Daten in einer Blockchain.[74] Problematisch ist darüber hinaus auch das Erfordernis der Datenschutzgrundverordnung, die Datenverarbeitung einem greifbaren Verantwortlichen zurechnen zu müssen.[75]

Ein möglicher Lösungsansatz bzgl. des Rechts auf Löschung bzw. des Rechts auf „Vergessenwerden“ besteht darin, in der Blockchain lediglich Hash-Werte personenbezogener Daten abzulegen. Die personenbezogenen Daten selbst werden außerhalb der Blockchain abgespeichert und der Bezug zur Blockchain dann über einen Verweis (Link) hergestellt. Dieses Vorgehen ermöglicht es, die außerhalb der Blockchain gespeicherten personenbezogenen Daten jederzeit zu löschen. Der Verweis zur Blockchain würde dann ins Leere laufen.[76]

Um das Innovationspotenzial der Blockchain-Technologie durch die bestehenden datenschutzrechtlichen Grundsätze nicht grundsätzlich zu gefährden, wird zum Teil auch gefordert, das Recht auf Löschung der personenbezogenen Daten bei komplexen, verteilten IT-Architekturen wie der Blockchain zugunsten eines Rechts auf hinreichende Schutzmaßnahmen, insbesondere eine hinreichende Pseudonymisierung, zu reduzieren.[77] In diesem Zusammenhang wird zum Beispiel argumentiert, dass es unionsrechtlich zulässig sei, keine physische Löschung der Daten vornehmen zu müssen, sondern dass es ausreiche, personenbezogene Daten in der Blockchain unkenntlich zu machen.[78] Ein dafür geeignetes Vorgehen wird insbesondere im sog. „Pruning“-Verfahren gesehen, mit dem Informationen aus älteren Blöcken gelöscht werden können, ohne die Funktionsfähigkeit der Blockchain zu beeinträchtigen.[79]

Auch bei den beschriebenen datenschutzrechtlichen Herausforderungen gilt, dass diese vor allem beim Einsatz öffentlicher, genehmigungsfreier Blockchains bestehen. Im Rahmen von zugangsbeschränkten

---

[70] Verordnung 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - Datenschutz-Grundverordnung (EU-DSGVO 2016).

[71] Art. 17 Abs. 1 (EU-DSGVO 2016).

[72] Art. 17 Abs. 2 (EU-DSGVO 2016).

[73] Art. 29 (EU-DSGVO 2016).

[74] Vgl. dena (2019).

[75] Vgl. Blocher (2018).

[76] Eine detaillierte datenschutzrechtliche Bewertung bei der Implementierung von Distributed-Ledger-Technologien findet sich bei BMVI (2019).

[77] Vgl. dena (2019), Blocher (2018).

[78] Vgl. dena (2019).

[79] Vgl. Martini / Weinzierl (2017).

privaten oder konsortialen Blockchains ist die Einhaltung datenschutzrechtlicher Vorgaben aufgrund der höheren Flexibilität der Blockchain-Architekturen wesentlich einfacher.

3.3.3 Smart Contracts

Eine wichtige Fragestellung im Zusammenhang mit Smart Contracts ist ihre korrekte rechtliche Einordnung. Smart Contracts sind entgegen ihrer Bezeichnung per se weder „smart“ noch sind sie ohne weiteres als Verträge im rechtlichen Sinne einzustufen.[80] Zivilrechtlich dürfte ein Smart Contract in der Regel Bestandteil einer außerhalb der Blockchain getroffenen Vereinbarung (im Sinne des sog. „Verpflichtungsgeschäfts“) sein. Der Smart Contract selbst hingegen umfasst in der Regel lediglich das Verfügungsgeschäft bzw. einige Teilaspekte dieses Verfügungsgeschäfts.[81] Aufgrund der Vielzahl möglicher Anwendungsfälle kann eine belastbare juristische Einordnung von Smart Contracts vermutlich nur im Einzelfall erfolgen.[82]

Darüber hinaus gelten für Smart Contracts die gleichen zivilrechtlichen Herausforderungen wie sie in Abschnitt 3.3.1 beschrieben wurden. Zu beachten ist außerdem, dass Smart Contracts nur vergleichsweise triviale Regelungen (Wenn-dann-Beziehungen) abbilden können.[83] Komplexere Vertragsbeziehungen, die ein gewisses Maß an Flexibilität ermöglichen sollen und bei denen im Zeitablauf auch die Notwendigkeit zur Abwägung unterschiedlicher Positionen besteht, sind vermutlich auf Basis von Smart Contracts nicht zu realisieren.[84]

[80] Vgl. dazu auch Blocher (2018), BMVI (2019).

[81] Vgl. Blocher (2018), BMVI (2019).

[82] Vgl. dazu auch: Kaulartz / Heckmann (2016).

[83] Vgl. ÖFIT (2017).

[84] Vgl. BDEW (2017), Schlatt et al. (2016).

4 Die Blockchain-Technologie im Energiesektor

Die Energiewende ist seit mehreren Jahren die prägende Entwicklung für die Energiewirtschaft. Sie wird zu fundamentalen Transformationsprozessen im gesamten Energiesektor führen. Der Begriff Energiewende umfasst schlagwortartig eine Vielzahl von Entwicklungen wie

- den Ausstieg aus der Kernenergie bis zum Jahr 2022,
- das grundsätzliche Ziel, CO2-emittierende Energienutzungen in allen Wirtschafts- und Lebensbereichen zurückzudrängen,
- Stromerzeugung auf Basis erneuerbarer Energien zu betreiben und aus der Kohleverstromung spätestens bis zum Jahr 2038 auszusteigen,
- eine Verlagerung der Stromerzeugung hin zu einer Vielzahl von kleineren Einheiten (insbesondere Wind- und PV-Erzeugungsanlagen), die vor allem an niedrigere Spannungsebenen angeschlossen und zum Teil weit entfernt von den Verbrauchszentren errichtet werden,
- den dadurch notwendigen umfassenden Aus- und Umbau der Stromnetze, um die Erneuerbaren Energien in das Stromversorgungssystem integrieren zu können,
- das Bemühen um eine erheblich gesteigerte Effizienz der Energienutzung,
- den zunehmenden Umstieg des Wärme- und des Mobilitätssektors auf Erneuerbare Energien inklusive der dafür notwendigen Kopplungen der beiden Sektoren mit dem Stromsektor,
- den Umbau der Erdgaswirtschaft hin zu einem klimaneutralen Wirtschaftsbereich, der die direkte Nutzung von Strom als Energieträger in den Bereichen ergänzt, in denen ein electricity only Ansatz nicht zielführend ist sowie
- den Eintritt neuer, zum Teil auch branchenfremder Marktakteure in die Energiewirtschaft und die Entwicklung innovativer digitaler Geschäftsmodelle.

Die genannten Punkte machen deutlich, dass im gesamten Energiesektor eine enorme Komplexität entsteht. Je vielfältiger und je größer die Anzahl der Marktteilnehmer und je höher der Anteil der Erneuerbaren Energien im Energieversorgungssystem ist, desto stärker bzw. intelligenter müssen Erzeugung, Handel, Übertragung, Verteilung, Vertrieb und Verbrauch miteinander verknüpft werden.

Die Digitalisierung und die Vernetzung einer Vielzahl von Akteuren und Anlagen sind dabei entscheidende Instrumente zum Gelingen der Energiewende. Die enorme Komplexität im Energiesektor kann nur mit Hilfe von intelligenten Betriebsmitteln und modernen Datenverarbeitungsmethoden bewältigt werden.[85] Ein effizienter und sicherer Informationsaustausch zwischen den beteiligten Akteuren ist für die Funktionsfähigkeit des gesamten Energiesystems und insbesondere auch für den Erhalt der Versorgungssicherheit von entscheidender Bedeutung. Dabei ist eine klare Zuweisung von Verantwortlichkeiten an bestimmte Instanzen (zum Beispiel Netzbetreiber) bzw. an bestimmte Marktrollen (zum Beispiel Bilanzkreisverantwortliche) essenziell.

[85] Zur Digitalisierung der Energiewirtschaft und zur besonderen Bedeutung von Daten im Zuge der digitalen Transformation siehe auch BNetzA (2017) und BNetzA (2018).

An dieser Stelle setzt die Blockchain-Technologie an: Aufgrund ihrer zuvor beschriebenen Eigenschaften besitzt sie möglicherweise das Potenzial, energiewirtschaftliche Prozesse in allen Wertschöpfungsstufen zu optimieren und einen Beitrag zur Bewältigung der steigenden Komplexität im Energiesystem zu leisten. Die Technologie verspricht vor allem, eine direkte, sichere Interaktion zwischen den Akteuren zu ermöglichen und gleichzeitig die Datenverwendung und die Informationsflüsse kontrollierbar und transparent zu machen.

4.1 Exemplarische Anwendungsfälle

Mögliche Anwendungsfälle der Blockchain-Technologie werden bereits seit einigen Jahren in der Energiewirtschaft diskutiert.[86] Im Vordergrund steht dabei meist die Optimierung bestehender energiewirtschaftlicher Prozesse wie die Verwaltung von Stammdaten, Abrechnungen oder Prozesse zum Wechsel des Stromlieferanten.[87]

Im Folgenden werden beispielhaft einige potenzielle Blockchain-Anwendungsfälle dargestellt und in aller Kürze und ohne Anspruch auf Vollständigkeit regulatorisch eingeordnet. Die Beschreibung der Anwendungsfälle ist ausdrücklich nicht abschließend. Eine Vielzahl weiterer, zum Teil auch recht visionärer Anwendungen, finden sich u. a. in der FfE-Studie „Die Blockchain-Technologie – Chance zur Transformation der Energieversorgung“, der dena-Studie „Blockchain in der integrierten Energiewende“ oder der BDEW-Studie „Blockchain in der Energiewirtschaft“.

4.1.1 Abrechnung von Ladevorgängen im Bereich der E-Mobilität

Eine wesentliche Voraussetzung für die Entwicklung der E-Mobilität ist ein ausreichend ausgebautes Ladesäulennetz. Ein Ansatz, der zum Ziel hatte, einen Beitrag zu dieser Herausforderung zu liefern, war das im Zeitraum von 2017 bis 2018 durchgeführte Share&Charge-Projekt der MotionWerk GmbH in Zusammenarbeit mit den beiden Technologie Start-ups Slock.it und Xtech.[88]

Idee des Projekts war es, Eigentümer von privaten Ladesäulen, die bereit waren, ihre Ladesäulen Dritten gegen Gebühr zum Aufladen zur Verfügung zu stellen und E-Autofahrer, die die Ladesäulen nutzen wollten, mit Hilfe einer App zusammenzubringen, um auf Basis einer Blockchain-Lösung das Aufladen der E-Autos zu ermöglichen und anschließend abzurechnen. Dazu mussten sich die Fahrer der E-Autos und die Ladesäulenbesitzer zunächst in der für das Projekt entwickelten App registrieren. Die Ladesäulenbesitzer mussten außerdem u. a. den exakten Ort der Ladesäule sowie die Bedingungen, zu denen sie bereit waren, Strom an Dritte zu veräußern, hinterlegen. Die Ladesäulen wurden mit einem Schaltschutz, einem Stromzähler sowie einem Hardware-Modul ausgestattet, das die Ladesäule über die private Internetverbindung des Ladesäulenbesitzers mit der im Hintergrund verwendeten Blockchain-Lösung verband.

Die Besitzer der E-Autos hinterlegten in der App ein Ladeguthaben und konnten über eine Suchfunktion die teilnehmenden Ladesäulen sowie deren Ladekonditionen finden. Wenn der Besitzer des E-Autos mit den

---

[86] Siehe dazu zum Beispiel FfE (2018b), dena (2019), BDEW (2017), dena / ESMT (2016), PwC (2016), PwC / BDEW (2018).

[87] Vgl. BDEW (2017).

[88] Weitere Blockchain-Projekte im Zusammenhang mit Ladevorgängen im Bereich der E-Mobilität sind zum Beispiel die Zusammenarbeit zwischen Bosch und EnBW zur Entwicklung einer „intelligenten Ladesäule“ sowie das Projekt „Matrix Charging“ in Österreich.

Ladekonditionen einverstanden war, konnte er in der App den gewünschten Ladevorgang anmelden, sodass die Ladestation für ihn freigeschaltet wurde und das Auto dort geladen werden konnte. Finanziert wurde das Modell über eine Transaktionsgebühr, die die Ladesäulenbesitzer an die MotionWerk GmbH entrichten mussten.

Sowohl das Matching von Angebot und Nachfrage als auch der Abrechnungsvorgang zwischen den Besitzern der E-Autos, den Ladesäulenbetreibern und der MotionWerk GmbH wurde automatisiert auf Basis einer Blockchain-Lösung abgewickelt. Technisch wurde das Projekt im Hintergrund (für die Anwender nicht sichtbar) über die öffentlich zugängliche Ethereum-Blockchain[89] realisiert, bei der die Akteure, die Transaktionen initiieren (hier die MotionWerk GmbH) pro durchgeführter Transaktion eine Gebühr bezahlen müssen. Da die Ethereum-Blockchain dazu eine eigene Kryptowährung verwendet („Ether"), musste im Rahmen des Projekts außerdem eine Lösung gefunden werden, um die von den Kunden eingezahlten Euro-Beträge in die Kryptowährung umzuwandeln. Das von den Nutzern eingezahlte Guthaben wurde dazu zunächst auf ein Treuhandkonto bei einem deutschen Kreditinstitut eingezahlt. Anschließend wurde das eingezahlte Guthaben der Kunden 1:1 in die Kryptowährung Ether umgewandelt. Die Erstellung dieser „Mobility Tokens" und die anschließende Abwicklung der Zahlungen der Ladevorgänge auf Basis der Kryptowährung in der Ethereum-Blockchain wurde mit Hilfe einer Lösung des Technologie-Start-ups XTech umgesetzt.

Ein wesentlicher Mehrwert, den die Blockchain-Technologie in diesem Anwendungsfall bieten kann, bestand laut der MotionWerk GmbH darin, dass sie eine eindeutige Identifizierung aller teilnehmenden Akteure und Ladesäulen ermöglicht. In Verbindung mit den verwendeten Smart Contracts biete die Blockchain-Technologie laut der MotionWerk damit grundsätzlich das Potenzial, Ladeprozesse sehr schnell und sicher abzuwickeln und darüber hinaus zwischen allen Beteiligten unmittelbar abzurechnen. Die Einträge in der Blockchain seien darüber hinaus manipulationssicher und für die jeweiligen Berechtigten über die App jederzeit einsehbar.

Laut der MotionWerk GmbH waren mit der Realisierung des Projekts zugleich aber auch komplexe Herausforderungen verbunden. Diese bestanden insbesondere darin, dass die Abwicklung der Transaktionen über die verwendete Ethereum-Blockchain sehr teuer war, das Konzept der Mobility Tokens inklusive des Treuhandkontos kompliziert und die genutzte Blockchain-Architektur darüber hinaus noch keine ausreichende Skalierbarkeit gewährleistet habe.[90] Neben Fragen des Eichrechts seien außerdem mit der Überlassung der Ladesäulen durch Privatpersonen an Dritte komplexe gewerbe- und steuerrechtliche Fragestellungen verbunden.

Die erste Erprobungsphase des Projekts wurde 2018 abgeschlossen. Das Projekt wird mittlerweile im Rahmen der Share&Charge Foundation, einer im Jahr 2018 neugegründeten Stiftung, der sich eine Vielzahl von Akteuren wie die Universität Mannheim, die TÜV Rheinland AG, die Volkswagen Financial Services AG und

---

[89] Die Ethereum-Blockchain wurde 2015 entwickelt und bot als erste Blockchain die Möglichkeit, Prozesse automatisiert über Smart Contracts abzubilden. Ethereum nutzt eine eigene Kryptowährung, die Ether genannt wird. Ether können in die Untereinheit „Gas" umgewandelt werden. Mit Gas werden in der Ethereum-Blockchain Transaktionengebühren bzw. Gebühren für die Ausführung von Smart Contracts bezahlt, vgl. BMVI (2019).

[90] Eine ausführlichere Darstellung dazu findet sich unter: https://medium.com/share-charge/the-next-share-charge-bc5f6807ddd6.

die envia Mitteldeutsche Energie AG angeschlossen haben, weiterentwickelt und ausgebaut. Technisch erfolgt die Weiterentwicklung auf Basis der Energy Web Chain, einer öffentlichen Blockchain, die als Konsensmechanismus einen Proof-of-Authority verwendet.[91]

4.1.2 Blockchainbasierter Stromhandel

Weitere Anwendungsgebiete verschiedener Blockchain-(Pilot-)Projekte in der Energiewirtschaft sind unterschiedliche Varianten des Stromhandels. Drei von ihnen werden im Folgenden kurz vorgestellt:

a) Peer-to-Peer Stromhandel zwischen einzelnen Haushalten

Das vermutlich bekannteste Blockchain-Projekt der Energiewirtschaft ist das „Brooklyn-Microgrid"-Projekt. Es wurde im Jahr 2016 in Brooklyn, New York von Transactive-Grid, einem Joint-Venture der beiden Technologieunternehmen LO3 Energy und ConsenSys, realisiert.[92]

Im Rahmen des Brooklyn Microgrid Projekts wurde erstmals getestet, wie einzelne Haushalte selbst erzeugten Strom aus Photovoltaik-Anlagen auf Basis einer Blockchain-Lösung an ihre Nachbarn verkaufen können. Die zehn teilnehmenden Haushalte (fünf Erzeuger und fünf Verbraucher) wurden dazu mit Smart Metern ausgestattet, die die jeweilige Erzeugung bzw. den Verbrauch in regelmäßigen Abständen gemessen haben. Die Bedingungen, zu denen Erzeuger bereit waren, ihren selbst erzeugten Strom zu veräußern bzw. ihre Nachbarn bereit waren, ihn zu erwerben, wurden in Smart Contracts implementiert und die jeweiligen Transaktionen anschließend über die Blockchain automatisiert abgewickelt.

Für den energieliefernden Haushalt könnte der Anreiz zur Teilnahme an einem solchen direkten Peer-to-Peer Handel insbesondere darin bestehen, eine aktivere Rolle im Energiemarkt einzunehmen und durch den Verkauf des selbst erzeugten Stroms eine weitere Einnahmequelle zu generieren. Anreize für Käufer des Stroms könnten zum einen die Gewissheit über dessen Herkunft sowie die Erwartung günstigerer Strompreise als durch eine Belieferung durch den klassischen Energieversorger sein.

Aus energiewirtschaftlicher Sicht ergibt sich bei einem solchen Peer-to-Peer Stromhandel, der unmittelbar zwischen zwei Parteien ohne einen Intermediär abgewickelt wird, eine Reihe von Herausforderungen, die in solche unterteilt werden können, die „nur" eine Änderung der bestehenden Rechtsnormen erfordern und solche, die relevante Risiken für die Stabilität des Gesamtsystems zur Folge haben können.

Der energieliefernde Haushalt wäre gemäß § 3 Nr. 18 Energiewirtschaftsgesetz (EnWG) ein Energieversorgungsunternehmen, das seine Tätigkeit gemäß § 5 EnWG der Regulierungsbehörde anzeigen und dabei auch den Nachweis der personellen, technischen und wirtschaftlichen Leistungsfähigkeit sowie der Zuverlässigkeit der Geschäftsleitung erbringen müsste. Damit wäre eine Reihe von zusätzlichen Vorgaben des Energiewirtschaftsgesetzes verbunden. Gemäß § 41 EnWG müssen Verträge über die Belieferung von Energie an Haushaltskunden weitere Bestimmungen enthalten z. B. bzgl. der Vertragsdauer, zu Möglichkeiten der Preisanpassung, zu Kündigungsterminen und Kündigungsfristen, zu Rücktrittsrechten des Kunden etc. Wenn

---

[91] Siehe dazu: https://www.energyweb.org/.

[92] Ähnliche Projekte in Deutschland sind bzw. waren das Landau Microgrid Projekt sowie das das Allgäu Microgrid Projekt. Das Allgäu Microgrid Projekt wird mittlerweile im Rahmen des Projekts „pebbles" (Peer-to-Peer-Energiehandel auf Basis von Blockchains) weiterentwickelt und auch um netztechnische Aspekte ergänzt, siehe dazu zum Beispiel EMW (2018).

der Verbraucher hinreichend über die finanziellen Risiken aufgeklärt wird, die mit dem Verzicht auf die genannten Regelungen verbunden sind, könnte man hier über Änderungen des Rechtsrahmens nachdenken.

Zudem dürften einige dieser Regelungen im Rahmen eines Smart Contract basierten Peer-to-Peer-Stromhandels nicht relevant sein, weil hierbei in der Regel keine längerfristigen Lieferbeziehungen eingegangen werden; bei einem vollautomatisierten Prozess, bei dem über einen bestimmten Zeitraum unter bestimmten (Preis-) Bedingungen Strom vermarktet wird, sollte diesem Lieferprozess aber vermutlich dennoch eine Art Rahmenvertrag zwischen den Haushalten zugrunde liegen, auf dessen Basis die Smart Contracts vergleichbar mit Einzellieferverträgen abgeschlossen werden. Für diese Rahmenverträge dürften die Regelungen des § 41 EnWG dann wieder sinnvoll sein.[93]

Zur Kategorie der nicht verzichtbaren Regelungen gehört dagegen die für ein stabiles Stromversorgungssystem entscheidende, jederzeitige Gewährleistung des Gleichgewichts von Erzeugung und Verbrauch. Daher muss der energieliefernde Haushalt wie jeder Erzeuger verpflichtet bleiben, Prognosedaten an Netzbetreiber zu melden und einen Bilanzkreisverantwortlichen nach § 4 Stromnetzzugangsverordnung zu benennen, der für eine ausgeglichene Bilanz zwischen Einspeisungen und Entnahmen in seinem Bilanzkreis in jeder Viertelstunde wirtschaftlich verantwortlich ist. Diese Bilanzkreisverpflichtung ist eine systemnotwendige Vorgabe für den Betrieb des Stromnetzes.

Auch wirtschaftliche Rahmenbedingungen für das Gesamtsystem sind weiterhin zu gewährleisten: Steuerzahlungen gemäß § 5 Stromsteuergesetz müssen jedenfalls von einem der beiden Vertragspartner sichergestellt werden, Verpflichtungen nach § 60 des Erneuerbare-Energien-Gesetzes zur Zahlung der EEG-Umlage an die Übertragungsnetzbetreiber müssen ebenso erfüllt werden wie die Verpflichtung zur Zahlung von Netzentgelten an die jeweiligen Netzbetreiber. Diese Ausführungen verdeutlichen, dass ein unmittelbarer Peer-to-Peer Stromhandel wie er im Brooklyn-Microgrid-Projekt erprobt wurde, einen einzelnen energieliefernden Haushalt aufgrund wichtiger, aber komplexer regulatorischer Vorgaben mit hoher Wahrscheinlichkeit überfordern würde.

b) Peer-to-Peer Stromhandel zwischen Kunden eines Energieversorgungsunternehmens

Eine Alternative zum zuvor beschriebenen direkten Peer-to-Peer Stromhandel zwischen verschiedenen Haushalten sind Konstellationen, in denen ein klassisches Energieversorgungsunternehmen als zusätzliche Dienstleistung seinen Kunden eine blockchainbasierte Peer-to-Peer Stromhandelsplattform bereitstellt.[94] Auf dieser Plattform können Kunden des Energieversorgers, die eigene Erzeugungsanlagen besitzen, ihren selbst erzeugten Strom anderen Kunden auf Basis von Smart Contracts automatisiert zum Verkauf anbieten. Diese wiederum können durch die Auswahl zwischen verschiedenen Erzeugern die Zusammensetzung ihres bezogenen Stroms selbst bestimmen und ggfs. von günstigen Strompreisen profitieren. In allen Fällen, in denen auf der Plattform kein oder kein ausreichender Handel zustande kommt, übernimmt das Energieversorgungsunternehmen die Energiebelieferung, sodass eine jederzeitige Versorgung der Kunden gewährleistet bleibt.

---

[93] Vgl. dazu Scholtka / Martin (2017).

[94] Dieser Anwendungsfall wird in Deutschland in unterschiedlichen Varianten zum Beispiel von der WSW Wuppertaler Stadtwerke GmbH und der Lition Energy GmbH erprobt bzw. angeboten.

Das Energieversorgungsunternehmen tritt in dieser Konstellation als klassischer Intermediär auf, der Angebot und Nachfrage der Prosumer auf der Handelsplattform zusammenbringt und als ergänzende Dienstleistung die im vorherigen Abschnitt genannten regulatorischen Anforderungen für seine Kunden erfüllt. Der Energieversorger übernimmt dabei insbesondere das Bilanzkreismanagement und die weiteren bürokratischen Verpflichtungen, die mit der Belieferung von Energie verbunden sind (Anmeldung des Prosumers als Energieversorgungsunternehmen, Zahlung der EEG-Umlage, stromsteuerliche Verpflichtungen etc.). Innerhalb des Bilanzkreises des Energieversorgungsunternehmens können die Kunden untereinander ihren Strom frei handeln. Der Netzbetreiber ist in diesem Modell nicht involviert.

Ein solches Modell ist regulatorisch einfacher realisierbar als der direkte Peer-to-Peer Stromhandel, weil das Energieversorgungsunternehmen als Dienstleister die Verantwortung für die Einhaltung der relevanten regulatorischen Bestimmungen übernimmt. Dieses Geschäftsmodell ermöglicht dem Prosumer eine relativ unkomplizierte aktive Teilnahme am Strommarkt, um seinen selbst erzeugten Strom zu veräußern. Perspektivisch könnten solche Geschäftsmodelle für Prosumer insbesondere dann an Attraktivität gewinnen, wenn der EEG-Förderzeitraum ihrer Erzeugungsanlagen abläuft und sie auf neue Vermarktungsmöglichkeiten angewiesen sind.[95] Stromnachfrager haben bei einem solchen Geschäftsmodell die Möglichkeit, ihren Strommix selbst zusammenzustellen und können ggfs. von einem günstigeren Energiebezug profitieren. Energieversorgungsunternehmen bietet ein solches Geschäftsmodell die Möglichkeit, sich als Anbieter komplexer Dienstleistungen im Markt zu positionieren, um zum Beispiel die Kundenbindung zu stärken oder etwaige sinkende Margen aus dem klassischen Versorgungsgeschäft zu kompensieren. Die Peer-to-Peer Handelsplattform könnte darüber hinaus durch die Entwicklung weiterer blockchainbasierter Dienstleistungen wie etwa die Zertifizierung von Herkunftsnachweisen[96] erweitert und damit für die Kunden attraktiver gemacht werden.

c) Peer-to-Peer Großhandelsplattformen

Weitere mögliche Anwendungsfälle im Bereich des Stromhandels sind blockchainbasierte Peer-to-Peer-Großhandelsplattformen, auf denen Handelsgeschäfte außerhalb der Börse direkt zwischen zwei Parteien abgeschlossen werden (sog. „OTC"-Geschäfte).[97] Die Ponton GmbH hat seit 2016 für die Brancheninitiative Enerchain[98] eine solche blockchainbasierte OTC-Großhandelsplattform für Strom- und Gasprodukte entwickelt. Die Plattform, die als zugangsbeschränkte private Blockchain aufgebaut ist, ist seit Mai 2019 in einer ersten Version in Betrieb.[99]

Die verschiedenen Parteien können ihre Gebote zunächst anonym in einem blockchain-basierten Orderbuch abgeben. Über Smart Contracts werden Angebot und Nachfrage zusammengebracht. Anschließend erfolgt die Offenlegung der beiden Parteien und der Eintrag der Transaktion in die Blockchain. Dritte können die konkreten Transaktionsdaten der beiden Handelspartner nicht einsehen. Die beteiligten Parteien können

---

[95] Solange Anlagenbetreiber die Einspeisevergütung gemäß EEG erhalten ist eine Vermarktung wirtschaftlich in der Regel nicht sinnvoll. Eine Doppel-Vermarktung ist gemäß dem EEG nicht möglich.

[96] Siehe dazu z. B. dena (2019) oder FfE (2018a).

[97] OTC steht für Over-the-Counter.

[98] Enerchain gehören 44 europäische Unternehmen an, die im Energiehandel tätig sind (darunter zum Beispiel E.ON, EnBW, RWE, Statoil, Statkraft, Vattenfall, Iberdrola).

[99] Für weitere Informationen dazu siehe: https://enerchain.ponton.de/.

Großhandelsgeschäfte im Rahmen dieses Anwendungsfalls direkt auf der Blockchain-Plattform ohne einen dazwischengeschalteten Broker abschließen. Laut der Ponton GmbH sind durch den Wegfall der klassischen Broker-Gebühren Kosteneinsparungen von bis zu 90 Prozent im Vergleich zum klassischen OTC-Handel möglich.[100] Die Blockchain dient in diesem Anwendungsfall ausschließlich der Abrechnung der jeweiligen Handelsgeschäfte. Die Erfüllung der Geschäfte (Lieferung, Verbuchung, Verbrauch) wird nicht über die Blockchain abgewickelt.

Aus regulatorischer Sicht ist insbesondere zu beachten, dass der Anwendungsbereich der REMIT-Verordnung[101] eröffnet ist, wenn ein Energiegroßhandelsprodukt auf der Plattform gehandelt wird.[102] Aus aufsichtsrechtlicher Perspektive könnte eine solche blockchainbasierte OTC-Großhandelsplattform den Vorteil bieten, dass die zuständigen Aufsichtsbehörden jederzeit einen umfassenden Überblick über die Handelsaktivitäten der Marktakteure erhalten, da sämtliche Transaktionen zwischen den Handelspartnern unveränderbar in der Blockchain eingetragen werden.[103]

4.1.3 Einbindung dezentraler Kleinspeicher im Netzengpassmanagement

Im Bereich der Netzführung und des Netzbetriebs gibt es bisher nur wenige Blockchain-Pilotprojekte. Ein Beispiel ist das zwischen 2017 und 2019 durchgeführte Pilotprojekt zwischen dem Übertragungsnetzbetreiber TenneT TSO GmbH und der sonnen GmbH, in dem untersucht wurde, inwieweit dezentrale, vernetzte Kleinanlagen (Heimspeicher) in der Lage sind, netzdienliche Leistungen für die TenneT zu erbringen. Die sonnen GmbH stellte der TenneT dazu Leistung von vernetzten Heimspeichern ihrer Kunden zur Verfügung, die innerhalb von Sekunden Strom aus dem Netz aufnehmen bzw. eingespeicherten Strom in das Netz abgeben können. Ziel des Projekts war es, zu untersuchen, ob diese Flexibilitäten bei einer rückläufigen Anzahl von Großerzeugern als Engpassmanagementinstrument sinnvoll eingesetzt werden können.

Die der sonnen GmbH vorliegenden Informationen darüber, wieviel Kapazität die Heimspeicher für netzdienliche Maßnahmen bereitstellen können, wurden kontinuierlich in die Blockchain eingetragen. Im Falle von Engpässen konnte die TenneT die Heimspeicherkapazitäten abrufen, indem das Angebot der Heimspeicher zur Erbringung von netzdienlichen Leistungen und dessen Nachfrage durch die TenneT blockchainbasiert auf Basis von Smart Contracts zusammengebracht wurden. Die durchgeführten Transaktionen wurden mit einem Zeitstempel und einer kryptographischen Signatur versehen und anschließend in der Blockchain abgelegt. Auf dieser Basis konnten die einzelnen Transaktionen von den beteiligten Akteuren jederzeit eingesehen werden und die Abrechnungen der Transaktionen erfolgen. Die Blockchain-Lösung wurde von IBM entwickelt und basierte auf Hyperledger Fabric.[104]

---

[100] Vgl. dena (2019).

[101] Verordnung (EU) Nr. 1227/2011 über die Integrität und Transparenz des Energiegroßhandelsmarkts (Regulation on Wholesale Energy Market Integrity and Transparency, kurz „REMIT“). Die Bundesnetzagentur ist die in Deutschland zuständige Behörde zur Überwachung des Verbots von Insiderhandel und Marktmanipulationen nach der REMIT.

[102] Eine detailliertere Analyse zu den regulatorischen Implikationen dieses Anwendungsfalls findet sich bei dena (2019).

[103] Vgl. FfE (2018b), dena (2019).

[104] Hyperledger ist ein Blockchain-Dachprojekt auf Open-Source Basis, das im Jahr 2015 von der Linux Foundation gegründet wurde. Dem Projekt haben sich eine Vielzahl von internationalen Unternehmen und Forschungseinrichtungen angeschlossen, die gemeinsam

Laut den Aussagen der TenneT und der sonnen GmbH wurde das Pilotprojekt im Mai 2019 erfolgreich abgeschlossen. Im Rahmen des Projekts habe sich herausgestellt, dass die vernetzten Heimspeicher in technischer Hinsicht grundsätzlich in der Lage seien, für Redispatchzwecke eingesetzt zu werden.[105] Mehrwerte einer solchen Blockchain-Lösung könnten auch in diesem Anwendungsfall vor allem die Manipulationssicherheit der Einträge sowie die Möglichkeit der jederzeitigen Einsicht der beteiligten Akteure in die durchgeführten Transaktionen sein. Möglicherweise besitzt die Technologie darüber hinaus auch das technische Potenzial, Kleinsttransaktionen wirtschaftlich abzubilden, sodass dezentrale Kleinanlagen zukünftig ihr Flexibilitätspotenzial effizienter ausschöpfen können.

Allerdings sind alle Anlagen- bzw. Kraftwerksbetreiber heute verpflichtet, sich an der Aufrechterhaltung der Systemsicherheit zu beteiligen. Sie erhalten daher keine Vergütung für eine im Wettbewerb erbrachte Dienstleistung einschließlich eines entsprechenden Gewinns, sondern lediglich eine die entstandenen Nachteile kompensierende Entschädigung, wenn sie zum Redispatch angewiesen werden. Geschäftsmodelle, die auf der Bereitstellung netzdienlicher Flexibilitäten beruhen, können sich nach geltender Rechtslage daher nicht rechnen. Dies wäre auch nicht sinnvoll, denn bei einer marktlichen Beschaffung von Redispatch besteht die Gefahr strategischen Verhaltens (sog. Increase-Decrease-Gaming) und damit höherer Gesamtkosten. Denn die vom Netzbetreiber benötigten Dienstleistungen sind typischerweise sehr lokal begrenzt und nur von sehr wenigen Akteuren anbietbar. Liquide Märkte mit entsprechendem Wettbewerbsdruck, die den administrierten Kostenerstattungen überlegene Ergebnisse produzieren könnten, sind daher nicht oder allenfalls in besonderen Fallkonstellationen zu erwarten.

4.2 Zwischenfazit

Die Blockchain-Technologie steht wie in anderen Sektoren auch im Energiesektor noch am Anfang ihrer Entwicklung. In verschiedenen Studien wird eine Vielzahl von konzeptionellen Ansätzen für den Einsatz der Blockchain-Technologie in allen Wertschöpfungsstufen der Energiewirtschaft vorgestellt. Gemäß dem EDNA Bundesverband Energiemarkt & Kommunikation werden in Deutschland derzeit (Stand Juni 2019) 35 konkrete Blockchain-Pilotprojekte in der Energiewirtschaft getestet.[106] Der größte Teil dieser Projekte ist den Wertschöpfungsstufen Erzeugung und Vertrieb zuzurechnen. Dazu gehören vor allem Nachbarschaftsmodelle und Microgrids, wie sie in diesem Kapitel beispielhaft vorgestellt wurden und verschiedene Projekte im Bereich der Zertifizierung von „Grün-“ und „Regionalstrom“ sowie für handelbare Emissions- bzw. CO2-Produkte. Die übrigen der derzeit erprobten Projekte sind im Wesentlichen den Bereichen Stromgroßhandel, E-Mobilität und Netzengpassmanagement zuzuordnen, von denen auch jeweils ein Beispiel im Papier dargestellt wurde. Einige wenige Blockchain-Anwendungen sind wie beschrieben bereits am Markt verfügbar. Sobald mittels der Blockchain-Technologie Anwendungen im regulierten Netzbereich tangiert sind, müssen die dahinterliegenden Prozesse für die Regulierunsgbehörde nachvollziehbar sein. Ob diese Voraussetzung in

---

an der Weiterentwicklung von Distributed-Ledger Technologien arbeiten. Hyperledger-Fabric ist eine zugangsbeschränkte Blockchain-Infrastruktur, die insbesondere die Verwendung von Smart Contracts ermöglicht (hier „chaincode“ genannt).

[105] Unter Redispatch versteht man Eingriffe in die Erzeugungsleistung von Kraftwerken, um Leitungsabschnitte vor einer Überlastung zu schützen. Droht an einer bestimmten Stelle im Netz ein Engpass, werden Kraftwerke diesseits des Engpasses angewiesen, ihre Einspeisung zu drosseln, während Anlagen jenseits des Engpasses ihre Einspeiseleistung erhöhen müssen. Auf diese Weise wird ein Lastfluss erzeugt, der dem Engpass entgegenwirkt.

[106] Vgl. EDNA (2019).

den Anwendungsbeispielen erfüllt ist, kann nicht abschließend geklärt werden. Hier besteht weiterer Diskussionsbedarf.

Derzeit ist noch nicht absehbar, welche konkreten Blockchain-Lösungen sich in der Energiewirtschaft gegenüber bereits etablierten und funktionierenden Prozessen durchsetzen werden und welchen Mehrwert sie tatsächlich aufweisen. Ein breiter Einsatz der Blockchain-Technologie wird derzeit noch durch verschiedene Umstände erschwert. Dazu gehört u. a., dass die Technologie sehr komplex ist und noch eine Reihe von technischen Restriktionen aufweist (siehe dazu die Ausführungen in Kapitel 3). Für viele der angedachten Anwendungsfälle in der Energiewirtschaft sind intelligente Messsysteme erforderlich, die heute noch nicht vollumfänglich zur Verfügung stehen. Die Kombination von intelligenten Messsystemen und Blockchain-Anwendungen verspricht grundsätzlich Potenziale, weil intelligente Messsysteme, die die Anforderungen gem. §§ 21, 22 Messstellenbetriebsgesetz erfüllen, auf Basis einer hochsicheren Dateninfrastruktur vertrauenswürdige, abrechnungsrelevante und geeichte Messwerte in hoher Granularität bereitstellen können. Ein wesentliches Erfolgskriterium für den vermehrten Einsatz der Technologie in der Energiewirtschaft dürfte außerdem die noch zu schaffende Interoperabilität sowohl zwischen einzelnen Blockchain-Anwendungen als auch zwischen Blockchains und bestehenden energiewirtschaftlichen Prozessen sein.

Aus rechtlicher Perspektive ist zu beachten, dass bei der konkreten Umsetzung von Blockchain-Anwendungen in der Energiewirtschaft neben den allgemeinen zivil- und datenschutzrechtlichen Vorgaben (siehe Abschnitt 3.3) auch die sektorspezifischen Regelungen des Energierechts berücksichtigt werden müssen. Im Bereich des Peer-to-Peer-Handels unter Haushalten sind dies zum Beispiel die Verpflichtungen, die mit der Belieferung von Energie als Energieversorgungsunternehmen an Haushaltskunden verbunden sind wie das Bilanzkreismanagement, das Abführen von Steuern, Umlagen und Netzentgelten, oder die ergänzenden Bestimmungen zu den Inhalten von Energielieferverträgen gemäß § 41 EnWG. Sobald die Netzebene involviert ist, sind die Unbundlingvorschriften zu berücksichtigen. Noch nicht geklärt ist zudem, wie Smart Contracts regulatorisch einzuordnen sind.

Insgesamt kann festgestellt werden, dass die Blockchain-Technologie mittlerweile im Wesentlichen in Form von Pilotprojekten in der Energiewirtschaft angekommen ist. Neue blockchainbasierte Geschäftsmodelle und Anwendungen werden derzeit getestet und deuten das Automatisierungspotenzial der Technologie für energiewirtschaftliche Prozesse an. Nicht immer ist jedoch klar ersichtlich, ob durch blockchainbasierte Anwendungen tatsächlich komplexe energiewirtschaftliche Prozesse vereinfacht und Effizienzpotenziale gehoben werden.

Die Blockchain-Technologie besitzt vor allem bei der Vernetzung einer Vielzahl von Akteuren und Geräten das Potenzial, Mehrwerte zu schaffen, indem sie in Echtzeit automatisierte Transaktionen zwischen unterschiedlichen Akteuren der Energiewirtschaft ermöglicht, diese manipulationssicher dokumentiert und anschließend für weitergehende Prozesse bereitstellt. Damit könnte sie neben anderen Technologien wie Big-Data-Analytics und Künstlicher Intelligenz einen Baustein zur Bewältigung des digitalen Transformationsprozesses des Energiesektors bilden. Disruptive Veränderungen, die der Technologie häufig nachgesagt werden, wird sie in naher Zukunft im Energiesektor vermutlich nicht auslösen. Auch ist der Mehrwert insbesondere für mögliche Anwendungen im regulierten Netzbereich noch nicht offenkundig dargelegt worden. Sollten sich hier perspektivisch Anwendungsfelder ergeben, kommen neue

Herausforderungen auf die Regulierungsbehörden zu, z. B. dahingehend, dass die regulatorischen Prozesse in der Blockchain transparent, für den Regulierer nachvollziehbar und gerichtsfest abgewickelt werden müssen.

5 Die Blockchain-Technologie im Telekommunikationssektor

Der Telekommunikationssektor nimmt im Zuge des digitalen Transformationsprozesses von Wirtschaft und Gesellschaft eine fundamental wichtige Rolle ein, denn gut ausgebaute, flächendeckend verfügbare Telekommunikationsinfrastrukturen sind die grundlegende Voraussetzung für alle Digitalisierungs- und Vernetzungsprozesse.

Gleichzeitig ist auch der Telekommunikationssektor selbst im Zuge der Digitalisierung einem tiefgreifenden Wandel unterworfen. Wie die anderen Netzsektoren ist auch der Telekommunikationssektor geprägt durch das Auftreten neuer Marktakteure und die Entwicklung neuer innovativer Geschäftsmodelle. Dies umfasst vor allem sogenannte Over-The-Top Anbieter („OTT-Anbieter"), die über das offene Internet eine Vielzahl kommunikativer Dienste wie Messaging- oder Internettelefoniedienste anbieten und damit in Konkurrenz zu den klassischen Telekommunikationsanbietern treten. Eng damit verknüpft ist die Tatsache, dass auch im Telekommunikationssektor die Bedeutung von Daten als einem wesentlichen Wettbewerbs- und Wertschöpfungsfaktor zunimmt. Dies zeigt sich nicht nur an der Vielzahl innovativer datenbasierter Geschäftsmodelle der OTT-Anbieter, sondern auch daran, dass zahlreiche klassische Telekommunikationsanbieter in den vergangenen Jahren Kooperationen mit Unternehmen aus anderen Sektoren (zum Beispiel aus den Bereichen Mobilität, Gesundheit und Energie) eingegangen sind, um sektorübergreifend Daten zu sammeln, auszuwerten und wertschöpfend einzusetzen.[107] Durch die Entwicklung solcher innovativer datenbasierter Geschäftsmodelle und die Einbindung einer Vielzahl neuer Datenquellen – wie zum Beispiel vernetzten Geräten im Internet der Dinge – werden immer mehr Daten generiert und zwischen den Akteuren sowohl innerhalb des Telekommunikationssektors, aber auch im Rahmen von sektorübergreifenden Anwendungen und Geschäftsmodellen übermittelt.

Vor diesem Hintergrund ergeben sich auch im Telekommunikationssektor mögliche Blockchain-Anwendungsbereiche, weil hier ebenfalls die zentralen Potenziale der Technologie – Daten automatisiert, direkt, sicher und transparent zwischen den beteiligten Akteuren auszutauschen, diesen Datenaustausch manipulationssicher zu dokumentieren und die Daten anschließend für weitergehende Prozesse bereitzustellen – an Bedeutung gewinnen. Beispielhaft dazu wird in Abschnitt 5.1.2 ein potenzieller Blockchain-Abrechnungsprozess im Bereich des Roamings dargestellt.

Weitere potenzielle Anwendungsgebiete der Blockchain-Technologie im Telekommunikationssektor ergeben sich im Bereich des Ressourcenmanagements wie der Rufnummernverwaltung. Da die Blockchain-Technologie Informationsflüsse transparent machen und Nutzungsrechte an Ressourcen wie Rufnummern bestimmten Akteuren eindeutig zuweisen kann, könnte sie zukünftig zum Beispiel im Bereich der Rufnummernzuteilung an Endkunden, im Bereich der Portierung von Rufnummern zu anderen Anbietern und möglicherweise auch im Bereich der Bekämpfung von Rufnummernmissbräuchen eingesetzt werden. Entsprechende Überlegungen dazu wurden zum Beispiel von der britischen Regulierungsbehörde Ofcom angestoßen.[108]

---

[107] Für eine detaillierte Darstellung des digitalen Transformationsprozesses des Telekommunikationssektors und zur zunehmenden Bedeutung von Daten im Telekommunikationssektor siehe BNetzA (2017) und BNetzA (2018).

[108] Vgl. Ofcom (2018).

Denkbar erscheint außerdem, dass die Technologie nicht nur im klassischen Telekommunikationssektor, sondern zusätzlich auch im Bereich angrenzender Dienstleistungen, die nicht unmittelbar zum eigentlichen Kerngeschäft der Telekommunikationsanbieter gehören, eingesetzt werden könnte. Telekommunikationsanbieter könnten zum Beispiel versuchen, auf Basis ihrer vorhandenen Kundenschnittstellen eine Vielzahl unterschiedlicher blockchainbasierter Dienstleistungen gebündelt anzubieten (siehe dazu exemplarisch Abschnitt 5.1.3).

5.1 Exemplarische Anwendungsfälle

5.1.1 IMEI-Sperrliste der Deutschen Telekom

Ein konkretes Blockchain-Projekt wird derzeit von der Deutschen Telekom AG im Zusammenhang mit sog. IMEI-Nummern durchgeführt. Bei der IMEI (International Mobile Station Equipment Identity) handelt es sich um eine 15-stellige Nummer, mit der mobilfunkfähige Endgeräte weltweit eindeutig identifiziert werden können. IMEI-Nummern werden vor allem dazu genutzt, um Endgeräte im Falle eines Diebstahls als gestohlen zu melden oder um einen SIM-Lock[109] zu entfernen. Die Telekom stellt bereits heute eine interne IMEI-Sperrliste zur Verfügung, über die gestohlene Endgeräte unter Angabe der IMEI-Nummer im Netz der Deutschen Telekom gesperrt werden können. Es ist aber weiterhin möglich, das gestohlene Endgerät in anderen Mobilfunknetzen zu nutzen.

Die Telekom testet derzeit zusammen mit SAP und dem Camelot ITLab eine blockchainbasierte, dezentral geführte Sperrliste („Global IMEI Storage and Services“). Der Vorteil der Blockchain-Lösung besteht laut den Angaben der Telekom vor allem darin, dass die Blockchain auch für weitere Akteure (z. B. andere Mobilfunkbetreiber) einsehbar ist. Sobald ein neuer Eintrag in der Blockchain vorgenommen wird, haben alle berechtigen Akteure Kenntnis von diesem Eintrag und können die Endgeräte automatisiert auch in ihren Netzen sperren lassen. Kaufinteressenten eines gebrauchten Gerätes biete die Lösung außerdem den Vorteil, dass sie durch Einsicht in die Liste vor dem Kauf anbieterübergreifend prüfen könnten, ob es sich um ein gestohlenes Gerät handelt (sofern ihnen die IMEI bekannt ist).

5.1.2 Roaming-Abrechnungen

Ein potenzieller Anwendungsfall für die Blockchain-Technologie im Telekommunikationssektor besteht darin, Roaming-Abrechnungen blockchainbasiert durchzuführen. Beim Roaming befindet sich ein Kunde außerhalb des Netzgebiets seines Netzbetreibers (dem sogenannten Host Public Mobile Network Operator, „HPMN“) und nimmt deshalb das Netz eines anderen Netzbetreibers (dem sogenannten Visited Public Mobile Network Operator, „VPMN“) in Anspruch. Zwischen den beiden Netzbetreibern wird für die notwendige Abrechnung des Telekommunikationsvorgangs eine entsprechende Roamingvereinbarung abgeschlossen. Die Abrechnung zwischen den Netzbetreibern erfolgt heute in der Regel über Data Clearing Houses, die als Intermediäre agieren und die die für die Abrechnung notwendigen Informationen, die sogenannten „Call Detail Records“, zwischen den Netzbetreibern übermitteln. Nimmt ein Kunde des HPMN das Netz eines anderen Netzbetreibers in Anspruch, geht der HPMN gegenüber dem VPMN für die entstandenen Kosten

[109] Ein SIM-Lock ist eine Sperrung des Endgeräts, die verhindert, dass das Endgerät (innerhalb eines bestimmten Zeitraums) mit SIM-Karten anderer Netzbetreiber genutzt werden kann.

zunächst in Vorleistung und stellt die Kosten für die Nutzung des fremden Netzes seinem eigenen Kunden anschließend in Rechnung.

Für den Abrechnungsvorgang zwischen den Netzbetreibern ist zukünftig eine Blockchain-Lösung denkbar: Die zwischen den Netzbetreibern abgeschlossene Roaming-Vereinbarung könnte als Smart Contract in einer konsortialen Blockchain, an der die beiden beteiligten Netzbetreiber teilnehmen, implementiert werden. Jeder der beiden Netzbetreiber würde im Blockchain-Netzwerk entsprechende Knoten bereitstellen, die in der Lage sind, eingehende Informationen zu überprüfen und in der Blockchain zu hinterlegen. Sobald ein Nutzer die Dienste eines fremden Netzbetreibers in Anspruch genommen hat, würde der Abrechnungsvorgang entsprechend der zwischen den Netzbetreibern vereinbarten Roaming-Vereinbarung über Smart Contracts automatisiert abgewickelt. Im Anschluss an die Ausführung des Smart Contracts könnte der HPMN unmittelbar die Rechnung gegenüber seinem Kunden, der die Dienste des VPMN genutzt hat, ausstellen.

Ein wesentlicher Vorteil dieser Blockchain-Lösung könnte darin bestehen, dass sie kostengünstiger ist als die derzeitige Lösung, weil auf die Data Clearing Houses als Intermediäre verzichtet werden könnte. Außerdem wäre eine solche blockchainbasierte Abrechnung vermutlich schneller als das bisherige Verfahren über die Data Clearing Houses, weil der notwendige Informationsaustausch direkt zwischen den beteiligten Netzbetreibern abgewickelt würde. Schließlich könnte die Blockchain-Lösung auch dazu beitragen, dass strittige Abrechnungsfälle (zum Beispiel zwischen dem HPMN und dem Kunden) zügiger geklärt werden könnten, weil der HMPN die zum Zwecke der Rechnungserstellung notwendigen Informationen durch Einblick in die Blockchain ohne Zeitverzug einholen könnte.

5.1.3 Identity-as-a-Service und Datenmanagement

Zusätzlich zu den in den vorherigen Abschnitten beschriebenen Anwendungen ist es denkbar, dass Telekommunikationsunternehmen zukünftig weitere blockchainbasierte Dienstleistungen anbieten, die über das klassische Telekommunikationsgeschäft hinausgehen. Sie könnten zum Beispiel ihre häufig bereits vorhandenen Kundenschnittstellen dazu nutzen, um blockchainbasierte Identity-as-a-Service-Dienstleistungen (für Dritte) zu erbringen. Auf dieser Basis könnten darüber hinaus weitere blockchainbasierte Dienste wie zum Beispiel Dokumentenzertifizierungen und Datenmanagement angeboten werden.

Identity-as-a-Service-Dienste könnten vor allem auf dem im Abschnitt 2.2.2 beschriebenen Public-Key-Verfahren basieren. Zunächst würden für die Kunden des Telekommunikationsunternehmens (beispielsweise auf Basis offizieller Dokumente wie dem Personalausweis) digitale Identitäten erstellt (Name, Anschrift, Wohnort etc.). Darüber hinaus könnte der Kunde dieser digitalen Identität beliebige weitere Daten (persönliche Präferenzen etc.) hinzufügen. Ein privater Schlüssel würde auf der eSIM[110] des Endgeräts des Kunden abgespeichert. Mit Hilfe des privaten Schlüssels könnte der Kunde persönliche Informationen seiner digitalen Identität bestätigen.

Das Telekommunikationsunternehmen würde eine Blockchain als Datenbank verwenden, in der ein Hinweis darüber abgespeichert würde, dass der Kunde an dem Identitätsservice teilnimmt. Die personenbezogenen

[110] Die eSIM (embedded subscriber identity module) ist ein Chip, der im jeweiligen Endgerät verbaut ist. Mit den darauf abgespeicherten Informationen wird der Nutzer u. a. im Mobilfunknetz identifiziert.

Daten des Kunden könnten, müssten aber nicht in der Blockchain abgelegt werden. Drittunternehmen, die Interesse an dem vom Telekommunikationsunternehmen angebotenen blockchainbasierten Identitätsmanagement haben, würden Zugang zur Blockchain erhalten.

Würde ein Kunde nun über sein Endgerät eine Bestellung bei einem an dem Identity-as-a-Service-Dienst teilnehmenden Online-Händler in dessen E-Commerce-App aufgeben, könnte der Kunde während des Bestellvorgangs dem Online-Händler über die Blockchain Zugang zu den für die Bestellung notwendigen persönlichen Informationen einräumen. Der Online-Händler könnte diese Daten dann zweifelsfrei auf ihre Korrektheit überprüfen, indem er mit Hilfe des öffentlichen Schlüssels (mit dessen Hilfe ein Teilnehmer im Blockchain-Netzwerk identifiziert wird) ein kryptographisches Rätsel an den Bestellenden sendet. Dieses Rätsel kann nur mit Hilfe des zu dem öffentlichen Schlüssel gehörenden privaten Schlüssel, der auf dem Endgerät des Kunden gespeichert ist, gelöst werden. Kann der Bestellende das Rätsel lösen, kann der Online-Händler sicher sein, dass die Bestellung tatsächlich von demjenigen aufgegeben wurde, dessen digitale Identität in der Blockchain hinterlegt wurde und der Bestellvorgang könnte fortgesetzt werden. Dieses Verfahren könnte zum einen betrügerisches Verhalten erschweren; zum anderen könnte es genutzt werden, um bestimmte gesetzliche Anforderungen des Bestellvorgangs (zum Beispiel die Überprüfung einer bestimmten Altersvorgabe) zu erfüllen.

Da die digitalen Identitäten um zusätzliche Informationen ergänzt werden können, könnte der Identity-as-a-Service Dienst um beliebige weitere Anwendungen zum Beispiel im Bereich der Dokumentenzertifizierung bzw. des Datenmanagements erweitert werden. Ein möglicher Anwendungsfall im Bereich der Dokumentenzertifizierung besteht darin, dass sich Hochschulen bereit erklären würden, Hash-Werte von Abschlusszeugnissen in der Blockchain abzulegen. In Kombination mit der Identitätsfeststellung könnten Kunden des Telekommunikationsunternehmens gegenüber potenziellen Arbeitgebern damit sowohl ihre Identität als auch ihre Studienabschlüsse digital nachweisen. Im Bereich des Datenmanagements könnte Kunden angeboten werden, zusätzliche Informationen bzw. Dokumente wie etwa Reisepräferenzen, Bahncards, Flugtickets, Hotelreservierungen etc. in der Blockchain abzuspeichern (bzw. statt der Originaldokumente die entsprechenden Hash-Werte), um sie anschließend für Reisezwecke zu verwenden.

Für Telekommunikationsunternehmen böte ein solches blockchainbasiertes Identitätsmanagement in Verbindung mit den beschriebenen Diensten im Bereich der Dokumentenzertifizierung und des Datenmanagements die Möglichkeit, auf Basis der bereits existierenden Kundenschnittstellen weitere digitale, blockchainbasierte Dienstleistungen anzubieten. Für Kunden könnten diese Dienste zu einer höheren Datensouveränität führen, weil für Telekommunikationsunternehmen die strengen sektorspezifischen Datenschutzregeln des Telekommunikationsgesetzes gelten[111] und jeweils nur die Daten mit Dritten geteilt werden müssten, die für den jeweiligen Anwendungsfall benötigt würden. Drittparteien könnten keine personenbezogenen Daten umfassend einsehen und verwerten.

5.2 Zwischenfazit

Nach Erkenntnissen der Bundesnetzagentur gibt es im Telekommunikationssektor im Vergleich zum Energiesektor in Deutschland derzeit nur wenige konkrete Blockchain-Projekte. Bei den in diesem Kapitel

[111] Für Einzelheiten zum sektorspezifischen Datenschutzrecht im Telekommunikationsgesetz siehe zum Beispiel BNetzA (2018).

beschriebenen potenziellen Anwendungsfällen handelt es sich mit Ausnahme der blockchainbasierten IMEI-Sperrliste der Deutschen Telekom noch um erste konzeptionelle Überlegungen, wie die Blockchain-Technologie zukünftig sinnvoll im Telekommunikationssektor eingesetzt werden könnte.[112] Die Tatsache, dass sich mittlerweile eine Vielzahl von Marktakteuren im Telekommunikationssektor mit der Technologie befasst, zeigt aber, dass auch hier grundsätzlich große Potenziale gesehen werden.

Die Deutsche Telekom AG beschäftigt sich beispielsweise in ihrer Forschungs- und Innovationseinheit „T-Labs“ mit der Blockchain-Technologie und ist in diesem Zusammenhang verschiedene Kooperationen und Mitgliedschaften (u. a. mit der Bosch Software Innovations GmbH, der Camelot ITLab GmbH, der Hyperledger Community und verschiedenen Universitäten) eingegangen, um potenzielle Blockchain-Anwendungsbereiche zu analysieren.[113] Beim Europäischen Institut für Telekommunikations-Normen (ETSI) wurde eine Arbeitsgruppe gegründet, die sich insbesondere mit Standardisierungs- und Interoperabilitätsfragen im Zusammenhang mit Distributed-Ledger-Technologien befasst.[114] Die Telefónica S.A. ist Ende 2018 eine Kooperation mit IBM eingegangen, um Geschäftsprozesse im Telekommunikationssektor auf Basis der Blockchain–Technologie zu optimieren.[115] Im Bereich der Unternehmensfinanzierung hat die Telefónica Deutschland Holding AG als zweites Unternehmen in Deutschland im Jahr 2018 Schuldscheine in Höhe von 75 Millionen Euro auf Basis einer Blockchain-Lösung ausgegeben.[116]

Bei der Implementierung konkreter Anwendungen ist davon auszugehen, dass die in Kapitel 3 beschriebenen technischen und rechtlichen Herausforderungen auch im Telekommunikationssektor von Bedeutung sind. Die Gründung der ETSI-Arbeitsgruppe, die sich mit Standardisierungs- und Interoperabilitätsfragen von Distributed-Ledger-Technologien befasst, deutet darauf hin, dass für einen breiteren Einsatz der Blockchain-Technologie auch im Telekommunikationssektor die Interoperabilität zwischen einzelnen Blockchain-Anwendungen, aber auch zwischen Blockchain-Anwendungen und bestehenden Prozessen im Telekommunikationssektor von Bedeutung ist.

Die Blockchain-Technologie könnte möglicherweise wichtige Mehrwerte bei der Vernetzung von Akteuren, Maschinen und Ressourcen im Internet der Dinge bieten. Es wird angenommen, dass bis zum Jahr 2030 bis zu drei Billionen Geräte mit dem Internet verbunden sein werden.[117] Auf Basis der bei Blockchains eingesetzten Public-Key-Kryptographien (siehe beispielhaft dazu den beschriebenen potenziellen Anwendungsfall in Abschnitt 5.1.3) könnte die Blockchain-Technologie eine eindeutige und manipulationssichere Identifizierung der vernetzten Akteure, Maschinen und Ressourcen gewährleisten und damit eine wesentliche Grundlage für den sicheren Informationsaustausch im Internet der Dinge bilden.

Darüber hinaus könnte sie auch im Telekommunikationssektor Geschäftsprozesse effizienter machen, indem sie einen sicheren, direkten und transparenten Informationsaustausch sowie eine automatisierte Abwicklung

---

[112] Die in den Abschnitten 5.1.2 und 5.1.3 dargestellten potenziellen Anwendungsfälle basieren im Wesentlichen auf Deloitte (2017).

[113] Vgl. Camelot ITLab (2018), Telekom (2018), Telekom (2019).

[114] Vgl. ETSI (2018).

[115] Vgl. Telefónica (2018a).

[116] Vgl. Telefónica (2018b).

[117] Vgl. General Electric (2017).

von Transaktionen auf Basis von Smart Contracts ermöglicht (vgl. beispielhaft den potenziellen Anwendungsfall im Bereich des Roamings in Abschnitt 5.1.2). Die Telefónica S.A. hat nach eigenen Angaben in diesem Zusammenhang beispielsweise erfolgreich eine umfassende Blockchain-Lösung im Bereich des Supply-Chain-Managements implementiert.

Möglicherweise könnte die Technologie zukünftig auch dazu beitragen, bestimmte regulatorische Aufgaben effizienter abzuwickeln. Die britische Regulierungsbehörde Ofcom testet derzeit beispielsweise, inwieweit die Blockchain-Technologie im Bereich der Rufnummernverwaltung Mehrwerte liefern kann.[118] Die L'agence nationale des fréquences aus Frankreich erprobt seit 2018 eine blockchainbasierte Zuordnung verschiedener Frequenzbänder.[119]

[118] Vgl. Ofcom (2018).

[119] Vgl. ANFR (2018).

6 Schlussbemerkungen

Die Blockchain-Technologie ist eine noch junge Technologie, die sich in den vergangenen Jahren rasant entwickelt hat. Sie baut auf verschiedenen bereits seit Längerem existierenden technologischen Bausteinen wie Public-Key-Kryptographien, Peer-to-Peer Prinzipien und kryptographischen Hash-Funktionen auf und schafft durch deren intelligente Kombination eine verteilte Datenbankstruktur, die vor allem durch ein hohes Maß an Ausfallsicherheit, Datenintegrität und Transparenz gekennzeichnet ist. Insbesondere die Möglichkeit, Geschäftsprozesse über Smart Contracts abzuwickeln, hat signifikantes Automatisierungspotenzial geschaffen und den potenziellen Anwendungsbereich der Technologie auch im Energie- und Telekommunikationssektor deutlich erweitert.

In technischer Hinsicht sind wesentliche Herausforderungen der Blockchain-Technologie die Erhöhung der Transaktionsgeschwindigkeit, die dauerhafte Gewährleistung der IT-Sicherheit und Datenintegrität, die Schaffung von Interoperabilität sowie die Reduzierung des Stromverbrauchs. In rechtlicher Hinsicht ergibt sich vor allem die Herausforderung, allgemeine zivil- und datenschutzrechtliche Grundsätze in Blockchain-Netzwerken zu implementieren. Insbesondere das Recht auf Löschung der eigenen personenbezogenen Daten und das Recht auf „Vergessenwerden“ stehen im klaren Widerspruch zu den Grundprinzipien der Unveränderbarkeit und der jederzeitigen vollständigen Transparenz der Daten in einer Blockchain. Derzeit diskutierte Lösungsansätze zur Bewältigung dieser Herausforderungen wurden im Papier skizziert.

Bei der technischen und rechtlichen Bewertung der Technologie ist stets zu berücksichtigen, dass es Blockchains in sehr vielen unterschiedlichen Ausprägungen gibt. Grundsätzlich gilt: je offener eine Blockchain-Architektur aufgebaut ist und je mehr Akteure daran teilnehmen, deren Identität nicht bekannt ist, desto höher sind die technischen und rechtlichen Herausforderungen. Umgekehrt gilt: Je eingeschränkter und bekannter der Teilnehmerkreis und je größer das Vertrauen zwischen den Akteuren bereits ausgeprägt ist, desto geringer sind diese Herausforderungen. In solchen Fällen kann die Komplexität des Konsensmechanismus reduziert und die Regeln des Netzwerks flexibler ausgestaltet oder verändert werden. Außerdem wird die Rechtsdurchsetzung aufgrund der bekannten bzw. identifizierbaren Identitäten der Teilnehmer erleichtert.

Soweit der Bundesnetzagentur bekannt, werden in den Netzsektoren heute praktisch keine klassischen öffentlich zugänglichen Blockchain-Architekturen mehr genutzt oder getestet, die den energieintensiven Proof-of-Work als Konsensmechanismus verwenden. Eingesetzt oder erprobt werden vor allem private und konsortiale Blockchain-Architekturen oder öffentliche Blockchains, die andere Konsensmechanismen wie den Proof-of-Authority verwenden. Verantwortlichkeiten können hier klar zugewiesen und die jeweiligen Rechte und Aufgaben der teilnehmenden Akteure individuell festgelegt werden. Aus regulatorischer Sicht ist dies insbesondere in der Energiewirtschaft, in der mit bestimmten Marktrollen eindeutig festgelegte Verantwortlichkeiten verbunden sind, von großer Bedeutung.

Im Energiesektor ist die Blockchain-Technologie mittlerweile in Form von Pilotprojekten angekommen. Möglichen Anwendungsfälle der Technologie werden hier bereits seit einigen Jahren diskutiert und mittlerweile in allen Wertschöpfungsstufen erprobt. Ein breiter Einsatz der Technologie ist bislang nicht in Sicht. Im regulierten Netzbereich mangelt es an Anwendungsfällen, bei denen die Blockchain-Technologie echte Mehrwerte gegenüber etablierten Prozessen liefert. Für eine Vielzahl der angedachten Anwendungen in den wettbewerblichen Wertschöpfungsstufen sind intelligente Messsysteme erforderlich, die heute noch nicht verbreitet sind. Ein wesentliches Erfolgskriterium für die Technologie in der Energiewirtschaft dürfte

darüber hinaus die noch zu schaffende Interoperabilität sowohl zwischen einzelnen Blockchain-Anwendungen als auch zwischen Blockchains und bestehenden energiewirtschaftlichen Prozessen sein. Disruptive Veränderungen, die der Technologie in der Energiewirtschaft häufig nachgesagt werden, wird sie in naher Zukunft vermutlich nicht auslösen.

Im Telekommunikationssektor finden sich bisher nur wenige konkrete Anwendungen der Blockchain-Technologie. Neben einigen blockchainbasierten (Pilot)-Projekten wie der IMEI-Liste der Deutschen Telekom existieren hier bisher im Wesentlichen erste konzeptionelle Überlegungen, wie die Technologie sinnvoll eingesetzt werden könnte. Verschiedene Akteure aus dem Telekommunikationssektor beschäftigen sich mittlerweile mit der Blockchain-Technologie, um denkbare Anwendungsbereiche zu analysieren. Die im Papier dargestellten potenziellen Anwendungsfälle im Bereich des Roamings und des Identitätsmanagements machen sich vor allem zu Nutze, dass mit Hilfe der Blockchain-Technologie eine eindeutige Identifizierung von Akteuren, Maschinen und Ressourcen sowie transparente, manipulationssichere Abrechnungsprozesse möglich sind. Die Gründung einer Arbeitsgruppe beim Europäischen Institut für Telekommunikationsnormen, die sich mit Fragen der Interoperabilität und Standardisierung von Distributed-Ledger-Technologien beschäftigt, deutet darauf hin, dass diesen Themen auch im Telekommunikationssektor eine hohe Bedeutung für einen breiteren Einsatz der Blockchain-Technologie beigemessen wird.

In den vergangenen Jahren war häufig zu beobachten, dass die Erwartungen an die Blockchain-Technologie entweder deutlich überzogen waren oder sie als bloße Modeerscheinung abgetan wurde. Beides wird der Technologie nicht gerecht. Sinnvoll erscheint es, sie pragmatisch in den Bereichen, in denen sie konkrete Mehrwerte liefern kann, zu erproben und weiterzuentwickeln. Dann könnte sie in den regulierten Netzsektoren neben anderen Technologien ein Baustein des digitalen Transformationsprozesses werden.

Die Bundesnetzagentur hat im Rahmen der Erstellung des Papiers mit folgenden Akteuren über ihre konkreten Blockchain-Projekte bzw. die Potenziale und Herausforderungen der Blockchain-Technologie gesprochen:

- Allgäu Netz GmbH & Co. KG
- Allgäuer Überlandwerk GmbH
- Karlsruher Institut für Technologie
- sonnen GmbH
- Stiftung Neue Verantwortung e.V.
- Telefónica Germany GmbH & Co. OHG
- Telefónica S.A.
- TenneT TSO GmbH
- The Share&Charge Foundation
- T-Systems Multimedia Solutions GmbH

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

ANFR [L'Agence nationale des fréquences] (2018): https://www.anfr.fr/innovation/innovation/blockchain-des-frequences/ [abgerufen am 07.08.2019].

Badev, A., and Chen, M. (2014): Bitcoin: Technical Background and Data Analysis, https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf [abgerufen am 26.08.2019].

BDEW [Bundesverband der Energie-und Wasserwirtschaft e.V.] (2017): Blockchain in der Energiewirtschaft – Potenziale für Energieversorger, Berlin.

BEE [Bundesverband Erneuerbare Energie e.V.] (2019): Smarte Sektorkopplung, Digitalisierung und Distributed Ledger Technologien, Berlin.

Blocher, W. (2018): Stellungnahme zur öffentlichen Anhörung des Ausschusses Digitale Agenda zum Thema „Blockchain, https://www.bundestag.de/ausschuesse/a23_digital/anhoerungen/anhoerung-576604 [abgerufen am 28.08.2019].

BMVI [Bundesministerium für Verkehr und digitale Infrastruktur] (2019): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. Gutachten des Fraunhofer-Institut für angewandte Informationstechnik FIT im Auftrag des Bundesministeriums für Verkehr und digitale Infrastruktur.

BNetzA [Bundesnetzagentur] (2017): Digitale Transformation in den Netzsektoren – Aktuelle Entwicklungen und regulatorische Herausforderungen, Bonn.

BNetzA [Bundesnetzagentur] (2018): Daten als Wettbewerbs- und Wertschöpfungsfaktor in den Netzsektoren – Eine Analyse vor dem Hintergrund der digitalen Transformation, Bonn.

BSI [Bundesamt für Sicherheit in der Informationstechnik] (2019): Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen.

Camelot ITLab (2018): https://www.camelot-itlab.com/de/press/camelot-itlab-stellt-blockchain-accelerator-paket-fuer-die-verwaltung-von-mobilgeraeten-vor/ [abgerufen am 16.09.2019].

Deloitte [Deloitte Touche Tohmatsu Limited] (2017): Blockchain @ Telco – How blockchain can impact the telecommunications industry and its relevance to the C-Suite.

dena / ESMT [Deutsche Energie-Agentur GmbH / European School of Management and Technology] (2016): Blockchain in der Energiewende. Eine Umfrage unter Führungskräften der deutschen Energiewirtschaft, Berlin.

dena [Deutsche Energie-Agentur GmbH] (2019): Blockchain in der integrierten Energiewende.

EDNA [Bundesverband Energiemarkt und Kommunikation e.V.] (2019): Die Landkarte der Blockchain-Projekte in der Energiewirtschaft., https://edna-bundesverband.de/news/die-landkarte-der-blockchain-projekte-in-der-energiewirtschaft/ [abgerufen am 07.08.2019].

EMW [Energie.Markt.Wettbewerb.Trends] (2018): Blockchain-Projekte bei AÜW, in: EMW.Trends, Heft 2, 2018.

ETSI [European Telecommunications Standards Institut] (2018): https://www.etsi.org/newsroom/press-releases/1473-2018-12-press-etsi-launches-new-industry-specification-group-on-blockchain, [abgerufen am 04.09.2019].

FfE [Forschungsstelle für Energiewirtschaft e.V.] (2018a): Die Blockchain Technologie Chance zur Transformation der Energieversorgung – Berichtsteil Technologiebeschreibung.

FfE [Forschungsstelle für Energiewirtschaft e.V.] (2018b): Die Blockchain Technologie Chance zur Transformation der Energieversorgung – Berichtsteil Anwendungsfälle.

Fraunhofer FIT [Fraunhofer-Institut für angewandte Informationstechnik] (2017): Blockchain und Smart Contracts – Technologien, Forschungsfragen und Anwendungen.

Fridgen, G. (2018): Stellungnahme zu den Fragen für das Fachgespräch zum Thema Blockchain im Ausschuss für Digitale Agenda am 28. November 2018, https://www.bundestag.de/ausschuesse/a23_digital/anhoerungen/anhoerung-576604 [abgerufen am 21.08.2019].

General Electric [General Electric Company] (2017): Electricity Value Network – Digital Solutions for Power and Utilities, https://www.ge.com/digital/sites/default/files/EVN-Solutions-for-Power-and-Utilities-from-GE-Digital.pdf [abgerufen am 09.08.2019].

Kaulartz, M, Heckmann, J. (2016): Smart Contracts – Anwendungen der Blockchain-Technologie, in: Computer und Recht, Ausgabe 9, S. 618-624, 2016.

Martini, M., Weinzierl, Q. (2017): Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: Neue Zeitschrift für Verwaltungsrecht, Heft 17, S. 1251-1259, 2017, C.H. Beck.

McKinsey [McKinsey & Company] (2017): What's new with the Internet of Things?, https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things [abgerufen am 04.09.2019].

Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016): Bitcoin and Cryptocurrency Technologies. A comprehensive introduction. Princeton, New Jersey: Princeton University Press.

Ofcom [Office of Communications] (2018): https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/blockchain-technology-uk-telephone-numbers [abgerufen am 17.07.2019].

ÖFIT [Kompetenzzentrum Öffentliche Informationstechnologie] (2017): Mythos Blockchain: Herausforderung für den öffentlichen Sektor, Berlin.

PwC / BDEW [PricewaterhouseCoopers AG / Bundesverband der Energie- und Wasserwirtschaft e.V.] (2018): Blockchain Radar – Energie und Mobilität.

PwC [PricewaterhouseCoopers AG] (2016): Blockchain – Chance für Energieverbraucher?, Kurzstudie für die Verbraucherzentrale NRW.

Reetz, F. (2019): Blockchain und das Klima – Warum die nationale Blockchain-Strategie Innovations- und Klimapolitik zusammenbringen sollte, Stiftung Neue Verantwortung, Berlin.

Rübe, I. (2018): Stellungnahme zu den Fragen für das Fachgespräch zum Thema Blockchain im Ausschuss Digitale Agenda am 28. November 2018, https://www.bundestag.de/ausschuesse/a23_digital/anhoerungen/anhoerung-576604 [abgerufen am 28.08.2019].

Schlatt, V., Schweizer, A., Urbach, N., Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth.

Schoder, D., Fischbach, K., (2002). Peer-to-Peer. Wirtschaftsinformatik: Band. 44, Nr. 6. Springer. (S. 587-589).

Scholtka, B., Martin, J. (2017): Blockchain - ein neues Modell für den Strommarkt der Zukunft?, in: Recht der Energiewirtschaft, Heft 3, S. 113-119, 2017.

Stallings, W. (2011) Network Security Essentials: Applications and Standards, 4th ed., Pearson Education, Upper Saddle River, NJ.

Telefónica [Telefónica S.A.] (2018a): https://www.telefonica.com/en/web/press-office/-/telefonica-and-ibm-collaborate-to-apply-blockchain-to-streamline-telco-processes [abgerufen am 17.07.2019].

Telefónica [Telefónica Deutschland Holding AG] (2018b): https://www.telefonica.de/news-telefonica-deutschland/pressemitteilung/news/6581/schuldscheintransaktion-mit-blockchain-tranche-telefonica-deutschland-erloest-250-mio-euro-in-innovativer-finanzierung.html [abgerufen am 19.08.2019].

Telekom [Deutsche Telekom AG] (2018): https://www.telekom.com/de/medien/medieninformationen/detail/blockchain-telekom-mitglied-globalen-hyperledger-community-555584 [abgerufen am 17.09.2019].

Telekom [Deutsche Telekom AG] (2019): https://laboratories.telekom.com/de/#layerslider-container [abgerufen am 17.09.2019].

T-Systems [T-Systems Multimedia Solutions GmbH] (2018): Whitepaper Blockchain: Die Zukunft der Industrie – Sichere Prozesse. Intelligente Verträge. Transparente Geschäftsbeziehungen.

Vries, A. d. (2018): Bitcoin's Growing Energy Problem. Joule 2, S. 801-805.

Xethalis, G. E., Moriarty, K. H., Claassen, R., Levy, J. B. (2016): An Introduction to Bitcoin and Blockchain Technology, https://files.arnoldporter.com//docs/IntrotoBitcoinandBlockchainTechnology.pdf [abgerufen am 03.06.2019].

Impressum

Herausgeber

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn

Bezugsquelle | Ansprechpartner

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Referat 119 - Digitalisierung und Vernetzung; Internetplattformen

Tulpenfeld 4

53113 Bonn

119-postfach@bnetza.de

www.bundesnetzagentur.de

Stand

November 2019

Druck

Bundesnetzagentur