Bundesnetzagentur

Die Blockchain-Technologie

Grundlagen, Potenziale und Herausforderungen

Die Blockchain-Technologie

Grundlagen, Potenziale und Herausforderungen

Stand: Juli 2021

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen

Referat 121 - Digitalisierung und Vernetzung; Internetplattformen

Tulpenfeld 4
53113 Bonn
Tel.: +49 228 14-0
E-Mail: 121-postfach@bnetza.de

Inhaltsverzeichnis

Einführung

Spätestens seitdem die Kryptowährung Bitcoin im Fokus der Öffentlichkeit steht, erhält die ihr zugrundeliegende Blockchain-Technologie große Aufmerksamkeit. Wirtschaft, Wissenschaft, Politik, und Verwaltung setzen sich seit einigen Jahren intensiv mit der Bedeutung der Technologie auseinander und treiben ihre Entwicklung und Verbreitung voran. In den vergangenen Jahren wurden in ganz unterschiedlichen Wirtschaftsbereichen und auch im öffentlichen Sektor konzeptionelle Überlegungen zum Einsatz der Technologie erarbeitet und zahlreiche Blockchain-Anwendungen entwickelt.

Auch die Bundesregierung befasst sich intensiv mit der Blockchain-Technologie und hat in diesem Zusammenhang im September 2019 eine eigene Blockchain-Strategie veröffentlicht, in der sie ihre wesentlichen Ziele und Grundsätze im Hinblick auf die Technologie vorgestellt hat. Seit zwei Jahren wird auf europäischer Ebene im Rahmen der European Blockchain Partnership, einem Gemeinschaftsprojekt von ca. 30 europäischen Ländern und der EU-Kommission, eine europaweite Blockchain-Infrastruktur aufgebaut, auf der ab dem Jahr 2021 eine Vielzahl von grenzüberschreitenden digitalen (Verwaltungs-) Diensten angeboten werden sollen.

Die genannten Entwicklungen machen deutlich, dass die Blockchain-Technologie wesentlich mehr Potenziale bietet als die Schaffung und Verwaltung von Kryptowährungen. Sie ermöglicht es vor allem, Transaktionen zwischen verschiedenen Akteuren direkt, transparent und manipulationssicher durchzuführen und einzelne Arbeitsprozesse auf Basis sog. Smart Contracts automatisiert abzuwickeln. Da die Blockchain-Technologie eine unmittelbare Interaktion zwischen den beteiligten Akteuren ermöglicht, besitzt sie außerdem das Potenzial, klassische Aufgaben von Intermediären ganz oder teilweise zu ersetzen.

In Kapitel 1 dieses Dokuments werden zunächst die technologischen Grundlagen der Blockchain-Technologie erläutert. In Kapitel 2 werden die wesentlichen Potenziale und die Herausforderungen, die bei der Implementierung konkreter Blockchain-Anwendungen bewältigt werden müssen, beschrieben. Kapitel 3 enthält einen Blockchain-Leitfaden, der eine Hilfestellung für die Frage bietet, ob die Blockchain-Technologie in einem konkret geplanten Anwendungsfall Mehrwerte bieten kann und in Kapitel 4 wird erläutert, in welchem Zusammenhang die Blockchain-Technologie aus Sicht der Bundesnetzagentur zu anderen wichtigen digitalen Technologien und Trends wie Künstlicher Intelligenz, Cloud Computing, Data-Analytics oder dem Internet der Dinge steht.

1 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.

1.1 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]

1.2 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 (vgl. dazu die Ausführungen in Kapitel 3).

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.

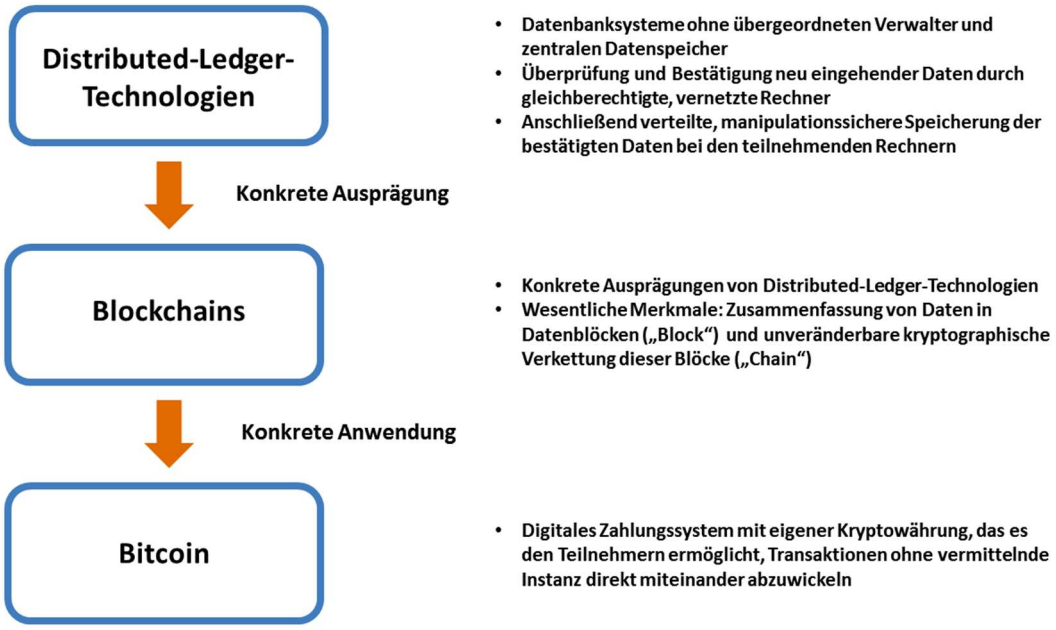

Abbildung 1: Zusammenhang Distributed-Ledger-Technologien, Blockchains, Bitcoin
Quelle: Eigene Darstellung

[5] Nakamoto (2008).

1.2.1 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.

1.2.2 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 ihm 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).

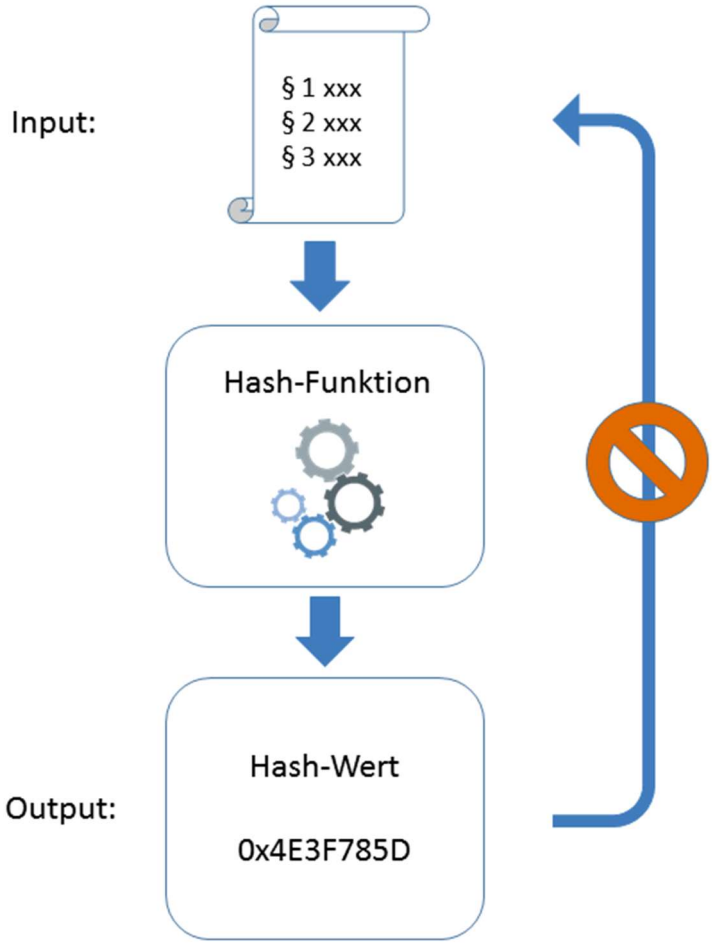

Abbildung 2: Schematischer Ablauf eines Hash-Vorgangs
Quelle: Eigene Darstellung, in Anlehnung an FfE (2018a).

1.2.3 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. 70 Millionen Teilnehmer angemeldet.[15] Im Vergleich zu den Nodes

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

(ca. 9.500)[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 6,25 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 1.2.2 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.io/

[17] Vgl. BDEW (2017).

[18] Diese Transaktionshistorie umfasst im Bitcoin-Netzwerk ca. 350 GB (Stand Juli 2021), vgl. https://www.blockchain.com/charts/blocks-size.

[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.

1.2.4 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).

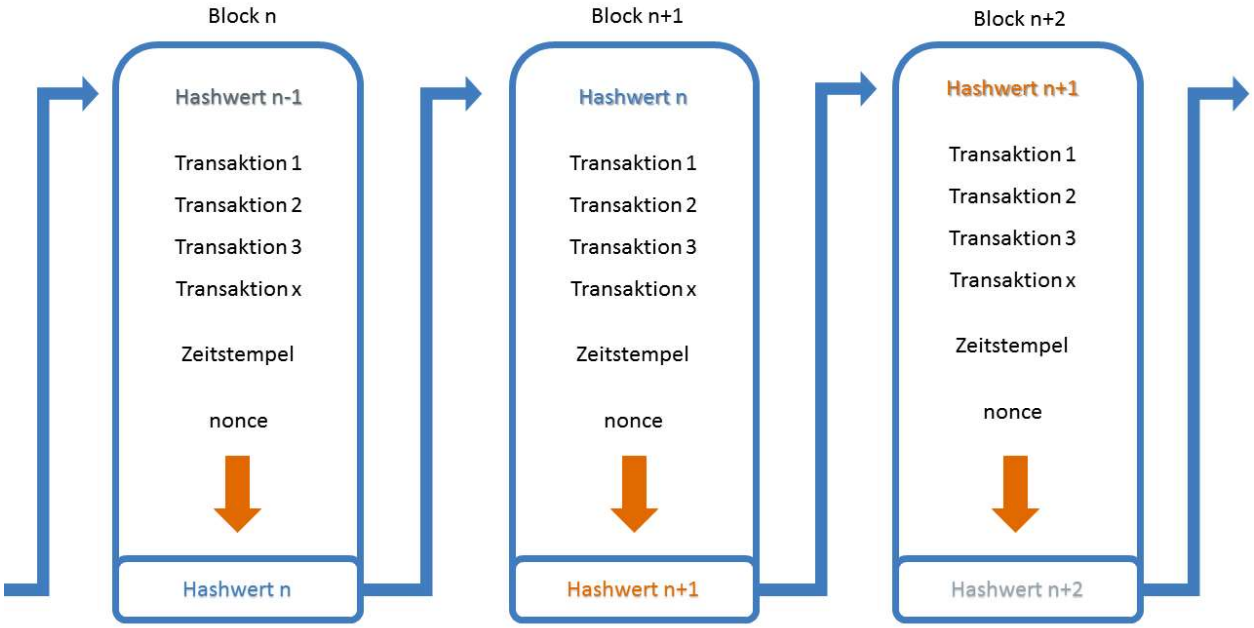

Abbildung 3: Struktur einer Blockchain - Verkettung über Hash-Werte
Quelle: Eigene Darstellung, in Anlehnung an BMVI (2019).

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 2.2.4.

[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 1.2.5) 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.

1.2.5 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 1.2.6.

[35] Vgl. dazu die Erläuterungen zu Minern in Abschnitt 1.2.3.

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

1.2.6 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 Ware eingegangen ist, dann Rechnungsbetrag begleichen.“.

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.

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. 200 Mrd. Dollar (Stand 20. Juli 2021) 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 blockchainbasierten 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].

1.2.7 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).

2 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.

2.1 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]

2.2 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.

2.2.1 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 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.

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.[51] 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.[52]

---

[49] Vgl. BDEW (2017).

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

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

[52] 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.

2.2.2 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.[53]

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.[54] 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.[55] Viele der heutigen Blockchains erfüllen diese Anforderung aber noch nicht.[56]

Eine weitere wichtige Herausforderung besteht darin, auch die Schnittstellen zu anderen Informationssystemen sicher auszugestalten. Dies gilt vor allem für die in Abschnitt 1.2.7 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.[57]

2.2.3 Interoperabilität

Als ein weiterer zentraler Erfolgsfaktor für die Blockchain-Technologie wird die Schaffung von Interoperabilität zwischen unterschiedlichen Blockchain-Architekturen angesehen.[58] Als interoperabel gelten Informationssysteme, wenn Informationen zwischen ihnen geteilt und Operationen systemübergreifend

---

[53] Vgl. Blocher (2018).

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

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

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

[57] Vgl. dena (2019), ÖFIT (2017).

[58] Vgl. BDEW (2017).

durchgeführt werden können.[59] 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 von der Bundesnetzagentur regulierten Netzsektoren dürfte ein solche Interoperabilität insbesondere bei sektorübergreifenden Anwendungen – im Energiebereich zum Beispiel im Rahmen von Sektorkopplungen – von Relevanz 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[60], Plasma[61] und MultiChain[62]. 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.

2.2.4 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.[63] Zwar ist der Stromverbrauch nicht exakt ermittelbar, weil zum Mining weltweit unterschiedliche Rechner eingesetzt werden, deren Stromverbrauch nicht zentral erfasst wird. Der Cambridge Bitcoin Electricity Index, in den verschiedene Schätzungen einfließen, geht aber davon aus, dass allein der jährliche Stromverbrauch der Bitcoin-Blockchain derzeit ca. 140 TWh beträgt.[64] . 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.[65]

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

---

[59] Vgl. dena (2019).

[60] https://polkadot.network.

[61] https://plasma.io.

[62] https://multichain.com.

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

[64] https://cbeci.org/.

[65] 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.[66]

2.3 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.

2.3.1 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.[67] 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.[68]

---

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

[67] Vgl. Blocher (2018).

[68] Vgl. Blocher (2018).

2.3.2 Datenschutzrechtliche Herausforderungen

Sofern im Rahmen einer Blockchain personenbezogene Daten verarbeitet (z. B. gespeichert) werden, müssen die einschlägigen datenschutzrechtlichen Bestimmungen, insbesondere die Datenschutzgrundverordnung[69], beachtet werden. Wesentliche Rechte, die sich aus der Datenschutzgrundverordnung für Verbraucher ergeben, sind das Recht auf Löschung der eigenen personenbezogenen Daten[70], das Recht auf „Vergessenwerden“[71] sowie das Recht auf Datenportabilität.[72] 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.[73] Problematisch ist darüber hinaus auch das Erfordernis der Datenschutzgrundverordnung, die Datenverarbeitung einem greifbaren Verantwortlichen zurechnen zu müssen.[74]

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.[75]

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.[76] 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.[77] 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.[78]

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

---

[69] 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).

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

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

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

[73] Vgl. dena (2019).

[74] Vgl. Blocher (2018).

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

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

[77] Vgl. dena (2019).

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

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

2.3.3 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.[79] 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.[80] Aufgrund der Vielzahl möglicher Anwendungsfälle kann eine belastbare juristische Einordnung von Smart Contracts vermutlich nur im Einzelfall erfolgen.[81]

Darüber hinaus gelten für Smart Contracts die gleichen zivilrechtlichen Herausforderungen wie sie in Abschnitt 2.3.1 beschrieben wurden. Zu beachten ist außerdem, dass Smart Contracts nur vergleichsweise triviale Regelungen (Wenn-dann-Beziehungen) abbilden können.[82] 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.[83]

---

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

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

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

[82] Vgl. ÖFIT (2017).

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

3 Leitfaden für den Einsatz der Blockchain-Technologie

In den vergangenen Jahren sind eine Reihe von Entscheidungsbäumen bzw. Fragenkatalogen entwickelt worden, die Anhaltspunkte dazu liefern können, ob in einem konkret geplanten Anwendungsfall der Einsatz der Blockchain-Technologie Mehrwerte bieten kann.[84] Bei den Entscheidungsbäumen wird der Anwender durch inhaltlich aufeinander aufbauende Fragen zu einem Ergebnis geleitet. Bei den entwickelten Fragenkatalogen muss eine Reihe von unabhängigen Fragen beantwortet werden. Je mehr Fragen bejaht werden, desto wahrscheinlicher ist es, dass der Einsatz der Blockchain-Technologie im konkret geplanten Anwendungsfall Sinn machen kann. Inhaltlich ähneln sich praktisch aller der bisher entwickelten Entscheidungshilfen. Ein Fragenkatalog bzw. Leitfaden, der die wichtigsten Fragestellungen bzgl. eines möglichen Einsatzes der Blockchain-Technologie zusammenfasst, ist der Folgende[85]:

Leitfaden zur Blockchain-Technologie	
1.	Ist eine unternehmens- bzw. organisationsübergreifende Kooperation zwischen mehreren Akteuren geplant?
2.	Wird (dabei) eine gemeinsame Datengrundlage für die beteiligten Akteure benötigt?
3.	Ist eine manipulationssichere Speicherung der Daten / Transaktionen von besonderer Bedeutung?
4.	Ist eine transparente Nachverfolgbarkeit der Daten / Transaktionen zwischen den beteiligten Akteuren von Bedeutung?
5.	Sollen bestimmte Arbeitsprozesse bzw. Transaktionen automatisiert abgewickelt bzw. angestoßen werden können?
6.	Sollen die jeweiligen Aufgaben und Rechte der beteiligten Akteure (Einsichtsrechte in die Daten, Schreibrechte) individuell konfiguriert werden können?
7.	Ist eine hohe Ausfallsicherheit des Systems von Bedeutung?
8.	Sind Vertrauensdefizite zwischen den beteiligten Akteuren zu erwarten, für deren Abbau bisher keine anderweitige Lösung gefunden werden konnte?
9.	Soll oder kann auf einen zentralen Akteur, der für die Überprüfung, Abwicklung und Speicherung von Informationen bzw. Transaktionen verantwortlich ist, verzichtet werden?
10.	Sind der gemeinsame Betrieb und die gemeinsame Weiterentwicklung des Systems / der Anwendung durch die beteiligten Akteure gewünscht?

Quelle: Eigene Darstellung.

Wie oben dargestellt gilt, dass die Wahrscheinlichkeit für einen nutzenbringenden Einsatz der Blockchain-Technologie umso höher ist, je mehr Fragen dieses Leitfadens bejaht werden. Dieser Leitfaden ist grundsätzlich anwendungsübergreifend nutzbar. Er kann also unabhängig davon, ob eine Blockchain-Anwendung etwa in den Netzsektoren, im öffentlichen Sektor oder in der mittelständischen Wirtschaft

[84] Eine gute Übersicht findet sich bei Meunier (2019).

implementiert werden soll, verwendet werden. Für bestimmte Anwendungsgebiete sind mittlerweile auch etwas spezifischere bzw. erweiterte Fragenkataloge entwickelt worden.[86]

Für mögliche Blockchain-Anwendungsbereiche in den von der Bundesnetzagentur regulierten Netzsektoren kann die Bundesnetzagentur bestätigen, dass der obige Fragenkatalog den "Praxistest" besteht. Die Bundesnetzagentur hat im Jahr 2020 eine Anhörung zur Blockchain-Technologie in den Netzsektoren durchgeführt, an der sich knapp 30 Akteure beteiligt haben. Ein wesentliches Ergebnis der Anhörung war, dass auch aus Sicht der Marktakteure der Einsatz der Blockchain-Technologie vor allem dann in Betracht kommt, wenn klassische Lösungen (mit zentralen Datenbanken und Intermediären) im Hinblick auf Manipulationssicherheit, Datenintegrität und Transparenz keine geeigneten Lösungen bieten, wenn ein Bedarf für automatisierte Abwicklungen von unternehmerischen Prozessen und Transaktionen besteht und wenn bestehende Vertrauensdefizite mit herkömmlichen Lösungen voraussichtlich nicht abgebaut werden können.

Zu berücksichtigen ist aber, dass Entscheidungshilfen wie der oben aufgeführte Fragenkatalog die Vielfalt der möglichen Blockchain- bzw. DLT-Architekturen und auch deren enorm schnelle technische Weiterentwicklung nicht oder kaum berücksichtigen können. Das Kapitel 1 hat verdeutlicht, dass es Blockchains bzw. DLTs in ganz unterschiedlichen Ausprägungen und insbesondere auch mit sehr unterschiedlichen Governance-Strukturen gibt und dass für den jeweiligen Anwendungsfall eine individuelle Blockchain-Lösung gefunden werden muss. Blockchain-Entscheidungshilfen können insofern erste wichtige Anhaltspunkte dazu liefern, ob die Blockchain-Technologie grundsätzlich geeignet sein kann, in einem bestimmten Anwendungsfall Mehrwerte zu bieten. Wenn dies bejaht wird, muss sich daran aber stets eine detaillierte individuelle Prüfung anschließen, die neben den konkreten technischen Anforderungen (etwa an die benötigte Transaktionsgeschwindigkeit oder an die Interoperabilität mit bestehenden Systemen) insbesondere auch die wirtschaftlichen Mehrwerte und die im jeweiligen Anwendungsfall konkret zu lösenden rechtlichen Fragen (z. B. im Hinblick auf Datenschutzvorgaben) analysiert.

[86] Ein Fragenkatalog, der auf die besonderen Anforderungen des Blockchain-Einsatzes in der öffentlichen Verwaltung zugeschnitten ist, findet sich in IT Planungsrat (2020). Ein Fragenkatalog, der etwas stärker auf die Bedürfnisse mittelständischer Unternehmen eingeht, findet sich in Andersch (2020).

4 Die Blockchain-Technologie im Kontext der Digitalen Transformation

Aus Sicht der Bundesnetzagentur ist es wichtig, die Blockchain-Technologie stets im breiten Kontext der Digitalisierung zu betrachten. Sowohl aus der Anhörung der Bundesnetzagentur zur Blockchain-Technologie als auch aus diversen Gesprächen, die die Bundesnetzagentur in den vergangenen Jahren mit verschiedenen Blockchain-Akteuren geführt hat, wurde deutlich, dass mittlerweile häufig nicht mehr in erster Linie versucht wird, ganze Geschäftsmodelle oder Anwendungen auf Basis der Blockchain-Technologie zu realisieren, sondern dass die Blockchain-Technologie zunehmend in den Teilprozessen eingesetzt oder erprobt wird, in denen sie unmittelbare Mehrwerte verspricht. Wie andere innovative digitale Technologien besitzt sie meist das Potenzial, bestimmte Teilprozesse einer Anwendung bzw. eines Geschäftsmodells zu verbessern oder erst zu ermöglichen. Die größten digitalen Wertschöpfungs- bzw. Effizienzpotenziale entstehen deshalb vermutlich durch die intelligente Verknüpfung verschiedener digitaler Technologien wie Blockchain, Data-Analytics, Künstliche Intelligenz, Cloud-Computing oder dem Internet der Dinge.

Insbesondere die Kombination von Künstlicher Intelligenz und Blockchain verspricht große Potenziale. Moderne KI-Systeme zeichnen sich vor allem durch ihre Fähigkeit zur Analyse enorm großer Datenmengen und durch die Lern- und Anpassungsfähigkeit der ihr zugrundeliegenden Algorithmen aus. KI-Systeme können auf dieser Basis zunehmend autonome oder zumindest teilautonome Entscheidungen treffen. Ein Problem moderner KI-Anwendungen ist aber, dass ihre Entscheidungsfindung für Außenstehende häufig nicht mehr nachvollziehbar ist. Dies kann zum Beispiel in Fällen, in denen mehrere KI-Systeme miteinander interagieren (etwa im Bereich des Autonomen Fahrens oder bei vernetzten und aufeinander aufbauenden industriellen Produktionsprozessen) problematisch sein, denn im Falle einer Störung oder eines Unfalls kann häufig nicht ohne Weiteres geklärt werden, wie es zu der Störung kam und ob und welches KI-System die Verantwortung dafür trägt. Die Blockchain-Technologie kann hier Lösungen bieten, weil sie es sowohl ermöglicht, die Arbeitsschritte und die darauf basierenden Entscheidungen von KI-Systemen als auch den Informationsaustausch zwischen verschiedenen KI-Systemen transparent und manipulationssicher zu protokollieren.

Das bedeutet konkret, dass in einer Blockchain zum Beispiel festgehalten werden kann, ob ein KI-System zu einem bestimmten Zeitpunkt eine Warnmeldung an ein anderes System verschickt hat, ob diese Meldung zur weiteren Verarbeitung beim anderen KI-System eingegangen ist und wenn ja, welche Prozesse das andere KI-System daraufhin angestoßen hat. Die Blockchain-Technologie kann damit dazu beitragen, das Vertrauen in KI-Systeme zu stärken, weil sie eine sichere Datenbasis bieten kann, um Fehler, Unfälle oder auch Betrugs- oder Manipulationsversuche an KI-Systemen zu rekonstruieren und aufzuklären.[87]

Auch die Kombination der Blockchain-Technologie mit IoT-Anwendungen kann Mehrwerte bieten. Im Bereich des Internets der Dinge könnten auf Basis der Blockchain-Technologie zukünftig zum Beispiel Abrechnungsprozesse zwischen autonom agierenden Maschinen, die über das Internet der Dinge miteinander vernetzt sind, abgewickelt werden. Eine konkreter Anwendungsbereich in diesem Zusammenhang sind sog. Pay-per-use Geschäftsmodelle, bei denen die Bereitstellung von mit IoT-Sensoren ausgestatteten Maschinen

[87] Vgl. BMVI (2019).

über eine Blockchain-Lösung in Abhängigkeit der Häufigkeit oder der Dauer der Nutzung automatisiert abgerechnet wird.[88]

Die Blockchain-Technologie könnte außerdem in unternehmensübergreifenden (z. B. cloudbasierten) Datenkooperationen Mehrwerte bieten. Blockchains können hier zum Beispiel eingesetzt werden, um den Zugang auf die Datenbestände für die einzelnen Akteure zu konfigurieren, die Verwendung der Daten transparent zu machen und etwaige Nutzungsentgelte für die Verarbeitung von Daten automatisiert abzuführen.

[88] Vgl. Bitkom (2019).

5 Schlussbemerkungen

Die Blockchain-Technologie ist eine noch relativ 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 in praktisch allen Wirtschaftssektoren und auch im öffentlichen Sektor 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.

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 insbesondere in Kombination mit anderen innovativen Technologien ein wichtiger Baustein der digitalen Transformation von Wirtschaft, Gesellschaft und Verwaltung werden.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

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

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.

Bitkom (2019): Blockchain in Deutschland - Einsatz, Potenziale, Herausforderungen, https://www.bitkom.org/Bitkom/Publikationen/Blockchain-in-Deutschland-Einsatz-Potenziale-Herausforderungen.

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

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.

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

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

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.

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.

IT-Planungsrat (2020): Koordinierungsprojekt Blockchain - Sachstandsbericht Mai 2020, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/32_Sitzung/TOP_15_Anlage_Blockchain.pdf?__blob=publicationFile&v=3.

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.

Meunier, S. (2019): When do you need a blockchain? Decision Models, https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1.

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.

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

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

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).

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

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

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.

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 121 - Digitalisierung und Vernetzung; Internetplattformen

Tulpenfeld 4

53113 Bonn

121-postfach@bnetza.de

www.bundesnetzagentur.de

Stand

Juli 2021

Druck

Bundesnetzagentur