B 3 Blockchain

B 3-1 Blockchain-Technologien: Mehr Sicherheit für dezentrale Anwendungen

Blockchain ist eine junge Technologie für das unveränderbare und fälschungssichere digitale Speichern und Übertragen von Daten.[355] Daten werden dabei nicht von einer einzelnen Institution gespeichert, sondern von vielen Akteuren gleichzeitig. Es gibt also keine zentrale Instanz, die die Kontrolle über die gespeicherten Daten hat (vgl. Abbildung B 3-2).

Box B 3-1 veranschaulicht die Bedeutung dieser Errungenschaft am Beispiel internationaler Lieferketten.

Neben Transaktionen von Gütern entlang von Lieferketten können Blockchains viele andere Arten von Transaktionen fälschungssicher speichern. Derzeit werden die Blockchain-Technologien u. a. dazu genutzt, finanzielle Transaktionen abzuwickeln, Stromhandel dezentral zu organisieren, digitale Identitäten zu verwalten, den Informationsfluss zwischen Behörden zu unterstützen oder Regulierungsbehörden und Unternehmen die Einhaltung von Berichtspflichten zu erleichtern.

Blockchain-Technologien und die darauf basierenden Anwendungen befinden sich derzeit noch in einem frühen Entwicklungsstadium. Die meisten Anwendungsbeispiele gehen aktuell nicht über den Status von Pilotprojekten hinaus. Fachleute rechnen aber mit einer erfolgreichen Weiterentwicklung der Technologie und ihrer Anwendungen. Mit der Weiterentwicklung von Blockchain-Technologien können erhebliche Kostensenkungen und Vereinfachungen von Transaktionsabläufen einhergehen. Daraus ergibt sich ein großes Potenzial weiterer Innovationen und Umwälzungen bisheriger Wirtschaftsstrukturen. Ein Grund dafür liegt in der großen Bedeutung von Daten für Wirtschaft und Gesellschaft und der neuen Art und Weise, wie Daten mit Hilfe von Blockchain-Technologien gespeichert werden. Auf eine zentrale, vermittelnde Instanz kann dabei verzichtet werden.

Hürden für die weitere Entwicklung von Blockchain-Technologien ergeben sich aus offenen technologischen Fragen und aus Unsicherheit in Bezug auf rechtliche und regulatorische Rahmenbedingungen sowie auf politische und gesellschaftliche Akzeptanz. Deutschland befindet sich in einer aussichtsreichen Position, um die Entwicklung von Blockchain-Technologien mitgestalten sowie wirtschaftliche und gesellschaftliche Potenziale realisieren zu können. Insbesondere Berlin ist für die Blockchain-Entwicklergemeinschaft ein Standort von globaler Bedeutung. Dieser aktuelle Standortvorteil sollte von der Politik als Hebel verwendet werden, um die weitere Entwicklung und Anwendung von Blockchain-Technologien zu befördern.

B 3-2 Wichtige Eigenschaften von Blockchain-Technologien

Aus der Funktionsweise und dem Aufbau von Blockchain-Technologien ergeben sich eine Reihe von Eigenschaften, die Einfluss auf den Erfolg und die Verbreitung dieser Technologie haben können. Zu diesen Eigenschaften gehören die Governance von Blockchains, die Sicherheit, die Unterscheidung zwischen Blockchains als Infrastruktur und als Anwendung sowie die ökonomischen Anreize der verschiedenen Akteure des Blockchain-Ökosystems.

Der Verzicht auf eine zentrale Instanz ist nicht nur das Ziel von Anwendungen der Blockchain-Technologien, sondern oft auch Leitmotiv für ihren weiteren Entwicklungsprozess.[356] Für Richtungsentscheidungen in der Entwicklung muss sich entweder ein informeller Prozess herausbilden oder ein formeller Prozess definiert werden. Informell kann sich beispielsweise ergeben, dass die aktivsten Entwicklerinnen und

Entwickler Richtungsentscheidungen treffen, die von den anderen Beteiligten mitgetragen werden. Ein formeller Prozess kann dagegen vorsehen, dass jede Nutzerin bzw. jeder Nutzer der Blockchain-Technologie eine Stimme bei Richtungsentscheidungen abgeben kann. Diese Optionen werden unter dem Stichwort der Governance von Blockchains diskutiert (für weitere Aspekte der Governance von Blockchains vgl. Box B 3-4). Die Governance kann demzufolge u. a. Einfluss auf die Qualität und Geschwindigkeit der Weiterentwicklung von Blockchain-Technologien haben.

Blockchain-Technologien sind durch die beschriebenen technischen Eigenschaften und ökonomischen Anreize (vgl. Box B 3-3) sehr sicher. Eine absolute Sicherheit kann es aber nicht geben. So kam es in der Vergangenheit beispielsweise wiederholt zu

Box B 3-1

Blockchain-Anwendungen für Lieferketten

Jährlich werden Güter mit einem Warenwert von fast 16.000 Milliarden Euro international versandt. 80 Prozent der Waren, die täglich konsumiert werden, werden international gehandelt.[357] Die Lieferketten sind sehr komplex. So können in den Transport einer Ladung Avocados von Mombasa nach Rotterdam 30 Institutionen und über 100 Personen mit über 200 Informationsaustauschen involviert sein.[358] Die hohe Komplexität solcher Lieferketten führt zu hohen administrativen Kosten entlang einer Lieferkette. Diese können die physischen Kosten der reinen Lieferung deutlich übersteigen. Darüber hinaus sind diese Lieferketten als Ganzes nur schwer nachvollziehbar. Tests mit abgepacktem Obst zeigen, dass es mehrere Tage dauern kann, eine Lieferkette nachzuverfolgen und den Ursprung eines Produkts zu bestimmen. Dabei machen Lebensmittelskandale deutlich, wie wichtig es ist, Lieferketten zurückverfolgen zu können. Nur so kann im Fall von Verunreinigungen, beispielsweise durch Krankheitserreger, die Quelle ausfindig gemacht werden. Ziel muss also sein, internationale Lieferketten mit vielen Akteuren ebenso leicht nachvollziehen zu können wie die Paketlieferung eines einzelnen Logistikanbieters durch die Sendungsverfolgung.

Um eine Lieferkette über Akteure hinweg zu dokumentieren, müssten alle Ereignisse der Lieferung an einem Ort erfasst und gespeichert werden.[359] Bisher schrecken Unternehmen allerdings vor einer gemeinsamen Erfassung der Lieferkette zurück, weil es bedeutet, dass sie Informationen zu ihren Geschäftsprozessen einem anderen Unternehmen anvertrauen und sich auf dessen Sicherheitsvorkehrungen verlassen müssten. Ein einzelnes Unternehmen als zentrale Institution für Informationen aus Lieferketten hätte zudem tiefe Einblicke in die Geschäfte der handelnden Unternehmen und könnte versuchen, aus diesem Informationsvorsprung Profit zu schlagen.

Blockchain-Technologien können eine solche zentrale Institution überflüssig machen. Anstatt die Daten durch eine zentrale Institution sammeln und speichern zu lassen, speichern beteiligte Unternehmen die Informationen zu Prozessen der Lieferkette in einem digitalen Kassenbuch, der Blockchain. Die beteiligten Unternehmen können dabei selbst eine Kopie der Blockchain speichern, sodass die Daten nicht in einer zentralen Institution konzentriert sind. Gleichzeitig können die Zugriffsrechte der Blockchain klar geregelt werden, sodass für jede Lieferung nur beteiligte Unternehmen Einträge in der Blockchain speichern oder lesen können. Darüber hinaus verhindern technische Eigenschaften der Blockchain, dass Daten im Nachhinein manipuliert werden (vgl. Box B 3-3).

So ermöglichen die Blockchain-Technologien ein hohes Maß an Transparenz und Sicherheit der gespeicherten Daten und helfen, Hürden für eine bessere Nachverfolgung von Lieferketten abzubauen. In einem Pilotprojekt konnte gezeigt werden, dass nach Einführung einer Blockchain zur Nachverfolgung von Lieferketten die Herkunft abgepackten Obstes innerhalb von Sekunden anstatt von Tagen ermittelt werden konnte. Ein anderer Fall zeigte, wie erhöhte Transparenz die Transportzeit einer Sendung von Verpackungsmaterial zu einer Produktionslinie in den USA um 40 Prozent reduzieren konnte.[360]

Im August 2018 haben der Technologiekonzern IBM und die Containerschiffsreederei Maersk nach einem zwölfmonatigen Test eine Blockchain für Lieferketten vorgestellt. Zu diesem Zeitpunkt waren 94 Organisationen in das Projekt involviert, darunter verschiedene Hafenbetreiber, Reedereien, Zollbehörden und Logistikdienstleister.[361]

Abb B 3-2

Download Daten

So funktioniert eine Transaktion mit und ohne Blockchain-Technologie

Anton und Anna möchten eine Transaktion an Kim veranlassen

Anton

Anna

ohne Blockchain

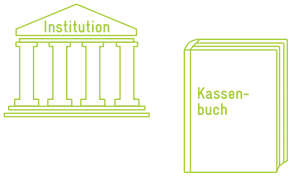
Anton sendet den Auftrag an eine zentrale Institution, z. B. eine Bank.

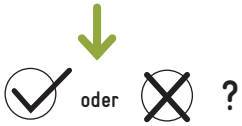
mit Blockchain

Anna sendet den Auftrag an ein Blockchain-Netzwerk.

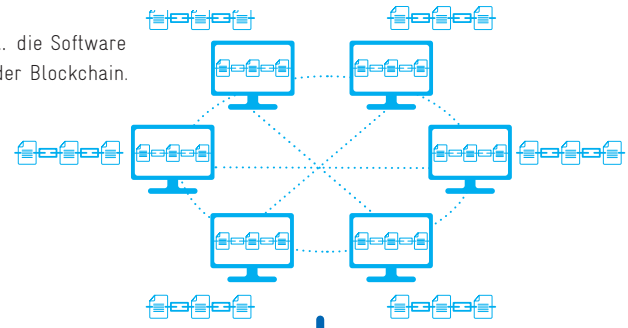
Ob die Transaktion zulässig ist, wird geprüft durch …

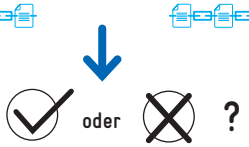
… die zentrale Institution anhand ihres zentral geführten Kassenbuchs.





… die Software der Blockchain.



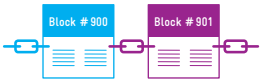


Falls die Transaktion zulässig ist, wird …

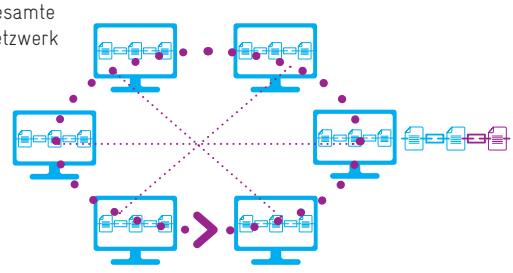
… dem zentralen Kassenbuch ein Eintrag hinzugefügt.

… die Transaktion zusammen mit anderen legitimen Transaktionen in einem sogenannten Block gebündelt,

kryptografisch mit dem vorherigen Block verkettet

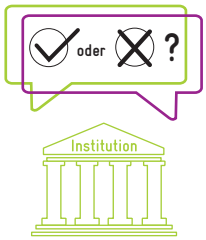


und an das gesamte Blockchain-Netzwerk kommuniziert.



Um zu überprüfen, ob die Transaktion ausgeführt wurde, …

Anton



Kim

… können Anton und Kim bei der zentralen Institution nachfragen.

Anna

Kim

… können Anna und Kim in der Blockchain nachsehen.

Ablauf der Transaktionen	Unterschiede zwischen den Transaktionen
Anton und Anna einigen sich jeweils mit Kim auf ein Geschäft, für das Kim 50 Euro bekommt. Anna führt die Transaktion über eine Blockchain aus, Anton über eine zentrale Instanz wie eine Bank.	Bei Transaktionen ohne Blockchain-Technologie muss man darauf vertrauen, dass die zentrale Institution die Transaktion verlässlich durchführt, Daten sicher verwahrt und nur für Zwecke verwendet, denen zugestimmt wurde. Für diese Dienste fallen mitunter hohe Gebühren an. Bei der Verwendung von Blockchain-Technologien muss man darauf vertrauen, dass die Technik der Blockchain einwandfrei funktioniert.
Anton beauftragt die Bank, 50 Euro an Kim zu überweisen. Die Bank prüft anhand ihres zentralen Kassenbuchs, ob die Transaktion zulässig ist. Anna sendet den Wert von 50 Euro über die Blockchain. Dort überprüfen Teilnehmende des Netzwerks, ob die Transaktion zulässig ist.	Bei Blockchain-Technologien ist klar festgelegt und einsehbar, welche Transaktionen zulässig sind. Bei Transaktionen ohne Blockchain-Technologie müssen die Nutzungsbedingungen der zentralen Institution interpretiert werden, um zu verstehen, welche Transaktionen legitim sind. Die zentrale Institution kann diese Bedingungen aber anders interpretieren und einseitig ändern. Die Computer des Blockchain-Netzwerks müssen einen Konsens bilden. Die dafür nötigen Konsensmechanismen können aber, wie im Fall der Bitcoin-Blockchain, sehr viel Energie verbrauchen.
Die Bank führt Antons Transaktion aus, belastet Antons Konto mit 50 Euro und schreibt Kim 50 Euro gut. Diese Transaktion wird im Kassenbuch verbucht. Annas Transaktion wird mit anderen Transaktionen in einem Block zusammengefasst, erhält einen digitalen Fingerabdruck, den sogenannten Hash, und wird dann an das gesamte Blockchain-Netzwerk kommuniziert. Der neue Block wird mit dem vorherigen Block verkettet, indem auf den Hash des Vorgängers verwiesen wird.	In einer Blockchain gespeicherte Transaktionen können später praktisch nicht verändert werden. Eine zentrale Institution hat dagegen die Möglichkeit, Transaktionen zu ändern oder zu löschen. Zudem kann ein erfolgreicher Cyberangriff auf eine zentrale Institution dazu führen, dass ihre Dienste nicht verfügbar sind. In einer Blockchain ist das Kassenbuch auf vielen verschiedenen Computern gespeichert, sodass die Daten auch dann verfügbar sind, wenn einige Computer ausfallen. Das Speichern einer Transaktion in einem zentralen Kassenbuch ist schnell und benötigt wenig Ressourcen. Das Speichern einer Transaktion in einer Blockchain benötigt mehr Ressourcen, weil die Transaktion an alle Computer im Netzwerk gesendet und von ihnen gespeichert wird. Hieraus entsteht u. a. ein höherer Speicherbedarf.
Um die Transaktion mit Anton zu prüfen, kann Kim in ihrem Bankkonto nachsehen. Um die Transaktion mit Anna zu prüfen, kann Kim den Block mit ihrer Transaktion einsehen.	Um den aktuellen Stand gespeicherter Transaktionen zu erfahren, muss erst eine Anfrage an die zentrale Institution gestellt werden. Die in einer Blockchain gespeicherten Transaktionen sind für die Teilnehmenden der Blockchain direkt einsehbar. Neben Transaktionen speichert eine zentrale Institution auch Daten ihrer Nutzerinnen und Nutzer wie Namen, Passwörter oder Kreditkartendaten. Zwar treffen diese Institutionen Vorkehrungen gegen Datendiebstahl, aber diverse Hacks zeigen, dass diese Vorkehrungen keine vollständige Sicherheit bieten.

Glossar:

Ein **Kassenbuch** erfasst und speichert (unter Umständen digital) Transaktionen. **Transaktionen** sind eine Abfolge von Schritten, die eine logische Einheit bilden. Sie können dabei ganz unterschiedliche Dinge umfassen: das Überweisen von Geld von einer Person an eine andere, aber auch Posts in sozialen Medien oder das Teilen von Informationen zwischen Unternehmen oder Behörden.

Eine **zentrale Institution** führt das Kassenbuch. Die zentrale Institution besitzt dabei die alleinige Kontrolle über das Erfassen und Speichern von Transaktionen. Beispiele sind Banken, Rechtsbeistände oder soziale Medien.

Ein **Netzwerk** besteht aus Computern, die miteinander verbunden sind und so Informationen austauschen können.

Eine **Blockchain** ist ein digitales Kassenbuch, das gleichzeitig auf vielen verschiedenen Computern gespeichert wird. Eine Blockchain besteht aus miteinander verketteten Blöcken.

Blöcke bündeln Transaktionen ähnlich wie auf einer Seite in einem Kassenbuch. Zusätzlich enthält jeder Block Informationen, um ihn unveränderbar mit dem vorherigen Block zu verbinden. Unveränderbar sind dabei sowohl die Transaktionen innerhalb eines Blocks als auch die Reihenfolge der Blöcke.

Konsens beschreibt eine Situation, in der sich alle Computer in Bezug auf den korrekten Stand der Blockchain und der in ihr gespeicherten Transaktionen einig sind.

Konsensmechanismen stellen sicher, dass Konsens zwischen den Computern hergestellt wird, selbst dann, wenn es Computer gibt, die das Netzwerk beispielsweise durch das Versenden falscher Informationen stören wollen.

Box B 3-3

Funktionsweise von Blockchain-Technologien

Blockchain ist eine Technologie für das digitale Speichern und Übertragen von Daten. Alle Transaktionen werden von vielen Computern[362] gespeichert und Informationen über neue Transaktionen werden zwischen den Computern des Blockchain-Netzwerks geteilt. Neue Transaktionen werden dabei in einem Block fester Größe zusammengefasst und kryptografisch mit allen vorherigen Blöcken zu einer Kette verknüpft (vgl. Abbildung B 3-2).[363]

In diesem Prozess gibt es keine zentrale Instanz, wie z.B. eine Bank, die die Korrektheit von Transaktionen prüft. Es wird damit ex-ante kein Vertrauen zwischen den Beteiligten vorausgesetzt. Dafür sorgen technische Funktionen und ökonomische Anreize.

Blockchains können entweder für jeden oder nur für einen bestimmten Teilnehmerkreis offen stehen. Beispiele für öffentliche (public) Blockchains sind die Ethereum- oder die Bitcoin-Blockchain.[364] In Konsortium-Blockchains hat nur eine bestimmte Gruppe von Personen die Berechtigung, Transaktionen zu speichern oder zu lesen. Hierzu können verschiedene Unternehmen zählen, die gemeinsam Transaktionen erfassen wollen, die nicht unbedingt für jeden öffentlich einsehbar sein sollen. In einer privaten Blockchain werden die Zugriffsrechte weiter eingeschränkt, sodass beispielsweise nur noch ein einzelnes Unternehmen Transaktionen in der Blockchain speichert.

Die hohe Sicherheit von Blockchains basiert u.a. auf der konsequenten Nutzung kryptografischer Verfahren. Sie werden genutzt, um sicherzustellen, dass die Identität der Transaktionspartner und die Transaktion selbst korrekt, d.h. nicht gefälscht sind, und um sicherzustellen, dass vergangene Transaktionen nicht geändert werden können.[365] Bei der Prüfung der Legitimität einer Transaktion wird u.a. sichergestellt, dass nur neue Transaktionen zur Blockchain hinzugefügt werden und die zu transferierenden Ressourcen vorhanden sind. Bereits gespeicherte Transaktionen können nicht manipuliert werden. Dadurch sind die Einträge in einer Blockchain unveränderbar. Dafür sorgen kryptografische Hashfunktionen, die den Transaktionen innerhalb eines Blocks einen Fingerabdruck, genannt Hash, zuweisen, der leicht zu verifizieren ist. Sollte nur ein Zeichen innerhalb der Transaktionen geändert werden, wäre offensichtlich, dass der Hash nicht korrekt ist. Die folgende Transaktion

Anna sendet 50 Euro an Kim.

erhält durch die Hashfunktion SHA-256 den Hash

e9b0e3904ff051f9e0810919afdd0a4ef963cfd79eaa2521b182e47531c2ec31.

Dieser Hash ist im originalen Block mit der Transaktion von Anna und Kim gespeichert. Sollte Anna die Transaktion nachträglich ändern und stattdessen Anne belasten wollen, bekäme

Anne sendet 50 Euro an Kim.

durch dieselbe Hashfunktion den Hash

f8aeab70bc377cea5af3916c70643cd2da3d81869965a14a9837f240f9d9a518.

Damit würde ein offensichtlicher Konflikt zu dem Hash entstehen, der in dem originalen Block gespeichert ist. Darüber hinaus enthält der nachfolgende Block den Hash seines Vorgängers als Referenz – das ist die sogenannte Verkettung der Blöcke. Deshalb kann die Manipulation einer Transaktion nur erfolgreich sein, wenn alle nachfolgenden Blöcke ebenfalls geändert werden können.

Aus diesem Grund ist die Legitimierung neuer Blöcke durch die Computer des Blockchain-Netzwerks von besonderer Bedeutung. Die Regeln dafür fassen sogenannte Konsensmechanismen zusammen. Die Wahl des Konsensmechanismus hängt vor allem auch von den Zugriffsrechten der Computer des Netzwerks ab. In einer Konsortium-Blockchain, in der sich die Teilnehmenden kennen, kann die Sicherheit und Verlässlichkeit auch außerhalb der Blockchain durchgesetzt werden. Das ermöglicht den Einsatz von Konsensmechanismen, die beispielsweise auf Mehrheitswahl basieren. Im Gegensatz dazu agieren die Nutzerinnen und Nutzer öffentlicher Blockchains weitgehend anonym. Dadurch kann die Sicherheit einer solchen Blockchain nicht außerhalb der Blockchain durchgesetzt werden, sondern muss

integriert sein. Auch hierfür gibt es unterschiedliche Ansätze wie zum Beispiel Proof-of-Work (PoW) oder Proof-of-Stake (PoS). Sie vereint, dass ökonomische Anreize genutzt werden, um Fehlverhalten, wie das Bestätigen nicht legitimer Blöcke, finanziell zu bestrafen.

Um einen neuen Block zu erstellen, muss bei PoW eine rechenintensive kryptografische Aufgabe gelöst werden. Dieser Prozess wird Mining genannt. Die Aufgabe besteht darin, eine Zahl, genannt Nonce, zu finden, sodass der Hash des Blocks mit einer bestimmten Anzahl von Nullen beginnt. Die Nonce wird, genauso wie der Zielwert für die Anzahl von Nullen, ebenfalls im Block gespeichert. So kann direkt nachgeprüft werden, ob die Arbeit zur Erstellung des Blocks tatsächlich geleistet wurde – daher der Name Proof-of-Work (Nachweis geleisteter Arbeit). Der Miner, der als Erster einen korrekten Block erstellt und eine passende Nonce gefunden hat, bekommt als Belohnung einen Betrag der entsprechenden Blockchain-Währung, zum Beispiel Bitcoin.

Der Rechenaufwand zur Lösung dieser kryptografischen Aufgabe führt zu einem hohen Stromverbrauch. Die Stromkosten bilden einen ökonomischen Anreiz, der verhindert, dass viele neue Blöcke der Blockchain generiert werden, um eine frühere Transaktion in der Blockchain zu manipulieren. Der Anreiz zur Manipulation ergibt sich dabei aus dem Abwägen des Profits einer Manipulation und den damit einhergehenden Kosten – hier den Kosten für Strom und Computer – für das Mining.

PoW ist ein sehr sicherer Konsensmechanismus, der die Regeln einer Blockchain auch durchsetzen kann, wenn die Teilnahme am Netzwerk nicht eingeschränkt ist und somit auch fehlerhafte Computer oder Teilnehmende mit betrügerischen Absichten Teil des Netzwerks sein können. Allerdings ist der damit einhergehende Stromverbrauch so hoch, dass die Bitcoin-Blockchain 2018 etwa so viel Energie verbrauchte wie das Land Österreich.[366]

Eine Alternative zu PoW in öffentlichen Blockchains besteht im Konsensmechanismus PoS. PoS verbraucht deutlich weniger Energie als PoW und schafft Anreize gegen Fehlverhalten, indem für das Validieren von Blöcken ein Pfand hinterlegt werden muss.

Nachdem ein neuer Block erstellt wurde, muss er an das gesamte Netzwerk gesendet und von den teilnehmenden Computern gespeichert werden. Dieser Prozess ist deutlich aufwendiger als das Speichern einer Transaktion in einem zentralen Kassenbuch, weil er bei allen Computern im Netzwerk wiederholt werden muss. Durch den Verzicht auf einen zentralen Speicher ist die Blockchain dann allerdings auch weniger anfällig für eine Störung.

Neben der grundlegenden Funktionsweise von Blockchain-Technologien existieren diverse Erweiterungen mit unterschiedlichem Reifegrad. Ziele aktueller Entwicklungen sind beispielsweise die Erhöhung des Transaktionsdurchsatzes[367] oder die Herstellung einer Verbindung zwischen verschiedenen Blockchains. Eine andere Erweiterung hat mit der Einführung der Ethereum-Blockchain bereits Einzug gehalten: die automatische Ausführung von Prozessen auf der Blockchain durch sogenannte Smart Contracts. Smart Contracts sind Computerprogramme, die ebenfalls in der Blockchain gespeichert sind.[368] Sie ermöglichen beispielsweise die Ausführung von Wenn-Dann-Beziehungen wie „Wenn Kim den Einkauf beim Gummibärenwerksverkauf an Anna liefert, dann werden 50 Euro von Anna an Kim transferiert". Smart Contracts haben das Potenzial, Transaktionskosten zu reduzieren, indem sie die Bedingungen für Transaktionen formalisieren und bei Erfüllung automatisch durchführen. Daraus ergibt sich eine weitere Motivation, auf zentrale Institutionen zu verzichten.

Diebstählen von Kryptowährungen, die sich im ersten Halbjahr 2018 auf fast eine Milliarde Euro belaufen haben sollen.[369] Die Sicherheitsvorkehrungen der Blockchain-Technologien werden bei diesen Diebstählen allerdings meist nicht überwunden. Diese Diebstähle erfolgen häufig auf zentralen Börsen für Kryptowährungen.[370] Dennoch gab es in der Vergangenheit wiederholt Fälle, in denen kleine Blockchain-Netzwerke, also Blockchains, in der die Miner (vgl. Box B 3-3) relativ wenig Rechenleistung besitzen, Opfer von sogenannten 51-Prozent-Angriffen wurden.[371] Blockchains, die über Netzwerke mit hoher Rechenleistung verfügen, haben eine deutlich geringere Wahrscheinlichkeit, Opfer eines 51-Prozent-Angriffs zu werden. Die Sicherheit von Blockchain-Anwendungen (vgl. auch Box B 3-3) ist ein wichtiger Grund für ihre Nutzung. Der Eindruck, Blockchain-Technologien seien nicht sicher, kann deshalb einen negativen Einfluss auf ihre Verbreitung haben.

Eine wichtige Unterscheidung muss zwischen einer Blockchain wie Ethereum als Infrastruktur und den Anwendungen, die auf ihr aufbauen, getroffen werden. Dieser Unterschied ist vergleichbar mit dem Unterschied zwischen den Internetprotokollen TCP/IP und Anwendungen, wie dem World Wide Web mit seinen Internetseiten oder E-Mail, die diese Infrastruktur nutzen. Dezentrale Anwendungen, die auf einer Blockchain aufbauen, werden dApps (Decentralized Applications) genannt. dApps ermöglichen beispielsweise als Browser oder Wallet die Interaktion mit einer Blockchain. Darüber hinaus stellen sie Anwendungen wie soziale Netzwerke, Handelsplattformen oder Identitätsmanagement zur Verfügung. dApps ermöglichen so die Nutzung von Blockchain-Technologien auch ohne tiefgehende technische Kenntnisse, generieren zusätzliche Funktionalität für Nutzerinnen und Nutzer und können damit die Verbreitung der Technologie unterstützen.

Zu den wichtigsten Akteuren des Blockchain-Ökosystems gehören: Institutionen, die hinter bestimmten Blockchains stehen, wie z. B. die Ethereum Foundation; Miner, die bei Proof-of-Work-Blockchains das Validieren neuer Blöcke übernehmen; Unternehmen, die Anwendungen auf der Basis von Blockchain-Technologien anbieten; sowie Unternehmen, die komplette Blockchain-Lösungen bereitstellen. Zu letztgenannter Gruppe gehören große Technologiekonzerne wie IBM, Amazon, SAP oder Microsoft, die Blockchain-Lösungen als Software-as-a-Service anbieten.

Start-ups, die Blockchain-Anwendungen oder Blockchain-Infrastruktur entwickeln, haben in der Vergangenheit häufig ein neues Finanzierungsinstrument genutzt, das sogenannte Initial Coin Offering (ICO). Bei einem ICO werden digitale Wertmarken, sogenannte Token, verkauft, die später zum Beispiel genutzt werden können, um die Dienste der Blockchain-Anwendung in Anspruch zu nehmen. Daneben ergänzen klassische Finanzierungsrunden über Wagniskapital die Finanzierung von Blockchain-Unternehmen.

Blockchain-Anwendungen generieren Einnahmen über Nutzungsgebühren, sogenannte Freemium-Modelle oder Abonnements für Nutzerinnen und Nutzer. Miner erhalten für ihre Arbeit einen Erlös in der Kryptowährung der Blockchain, für die sie einen Block bestätigt haben.

Anwendungen und Potenziale von Blockchain-Technologien B 3–3

Blockchain-Anwendungen finden sich in vielen Bereichen. Die Motivation für den Einsatz oder die Erprobung von Blockchain-Technologien ist häufig eine Kombination aus drei verschiedenen Beweggründen: i) Absicherung von Transaktionen, ii) Automatisierung von Transaktionen, iii) dezentrale Datenhaltung und Zugriffsmanagement.

Der Einsatz von Blockchain-Technologien in internationalen Lieferketten (vgl. Box B 3-1) ist ein Beispiel für unternehmensübergreifende und damit dezentrale Datenhaltung. Auch Behörden können durch Blockchain-Technologien den Informationsaustausch intensivieren, Prozessschritte automatisieren und dadurch die behördliche Zusammenarbeit verbessern. Ein erfolgreiches Beispiel für den Einsatz im Rahmen des Asylprozesses wird in Box B 3-5 beschrieben.

Die Nutzung von Blockchain-Technologien durch Aufsichtsbehörden und Unternehmen kann auch zu höherer Transparenz und niedrigeren Kosten für die Erfüllung der Transparenzanforderungen führen. Das hat ein Pilotprojekt der britischen Finanzmarktaufsicht FCA in Zusammenarbeit mit zwei global agierenden Banken[372] gezeigt. Die beteiligten Banken konnten den Berichtspflichten bei Immobilienkrediten deutlich einfacher nachkommen als zuvor.[373] So wendeten Banken und Aufsichtsbehörde bisher

bis zu vier Wochen für die Datenaufbereitung und -bereitstellung auf. Durch den Einsatz von Blockchain-Technologien konnte der zeitliche Aufwand des Berichtswesens deutlich reduziert werden. Darüber hinaus ermöglicht dieser neue Ansatz Berichte nahezu in Echtzeit, wohingegen bisherige Berichte höchstens quartalsweise zur Verfügung standen.[374]

Daten, die in Blockchains gespeichert werden, können nicht gelöscht oder verändert werden. Deshalb eignen sich Blockchain-Technologien, um Informationen beweisbar und somit vertrauenswürdig zu machen.[374] So wird der Aspekt der Unveränderbarkeit von Daten eingesetzt, um steuerrelevante Informationen, wie z. B. Rechnungen im Onlinehandel, fälschungssicher abzulegen. In der medizinischen Forschung findet dieser Aspekt bei der Absicherung von automatisiert generierten Daten aus Analysesystemen Anwendung. Damit kann eine Manipulation der Daten ausgeschlossen werden.[376]

Box B 3-4

Governance von Blockchains

Governance beschreibt, wie eine Organisation – hier eine Blockchain und ihre Stakeholder – gesteuert oder geregelt wird. Für Blockchains umfasst die Governance das Regelwerk, das im Protokoll der Blockchain enthalten ist und oft als On-Chain-Governance beschrieben wird. Zur On-Chain-Governance gehört z. B. auch der Konsensmechanismus (vgl. Box B 3-3). Daneben enthält die Off-Chain-Governance u. a. Entscheidungsregeln für die Anpassung des Blockchain-Protokolls oder Kriterien für die Auswahl derjenigen, die Transaktionen validieren, falls diese Gruppe eingeschränkt ist. Im Gegensatz zu Elementen der On-Chain-Governance sind Elemente der Off-Chain-Governance mitunter nicht niedergeschrieben, sondern ergeben sich aus der gelebten Praxis. Im Fall von öffentlichen Blockchains etabliert sich beispielsweise oft eine Meinungsführerschaft von prominenten Personen der Blockchain-Entwicklergemeinschaft.

Für die Realisierung der Nutzenpotenziale von Blockchain-Technologien kann die Ausgestaltung der Governance eine wichtige Rolle spielen. So wird mit der Nutzung von Blockchain-Technologien häufig das Ziel verfolgt, die Abhängigkeit von einem Intermediär oder einer zentralen Instanz zu verringern. Allerdings garantiert die Nutzung von Blockchain-Technologien nicht zwangsläufig den Verzicht auf zentrale Instanzen. Diese Rezentralisierung von Blockchain-Technologien kann sich aus der Governance der Blockchain ergeben, wenn prominente Personen eine Meinungsführerschaft etablieren konnten oder in privaten Blockchains eine geschlossene Gruppe von Akteuren für das Validieren von Transaktionen zuständig ist.

Darüber hinaus besteht ein Zielkonflikt zwischen einer wenig strikten Governance On- und Off-Chain und der Sicherheit von Blockchains. Es bedarf zumindest entweder einer strikten On-Chain-Governance oder einer strikten Off-Chain-Governance. Öffentliche Blockchains, in denen alle (zumeist anonymen) Personen Transaktionen validieren dürfen, verfügen deshalb meist über Proof-of-Work als Konsensmechanismus, um für die Einhaltung der Regeln der Blockchain zu sorgen (vgl. Box B 3-3). Öffentliche Blockchains hingegen, bei denen Transaktionen nur von Teilnehmenden validiert werden, deren Identität bekannt ist, können auf andere Konsensmechanismen zurückgreifen, weil die Einhaltung der Regeln auch außerhalb der Blockchain durchgesetzt werden kann. Dadurch können Nachteile von Proof-of-Work, z. B. der hohe Energieverbrauch, vermieden werden. Öffentliche Blockchains, bei denen alle Personen Transaktionen validieren dürfen, werden öffentliche und genehmigungsfreie Blockchains genannt. Dagegen werden öffentliche Blockchains, bei denen nur bestimmte Personen Transaktionen validieren dürfen, öffentliche und genehmigungsbasierte Blockchains genannt.

Öffentliche und genehmigungsbasierte Blockchains bieten darüber hinaus die Möglichkeit, für alle validierenden Personen (oder Organisationen) offen zu sein, die bestimmte objektive Kriterien erfüllen. Zu solchen Kriterien können beispielsweise die Geschäftstätigkeit in einem bestimmten Wirtschaftsbereich gehören – wie bei der Energy Web Foundation[377] – oder die Eigenschaft, einer Organisation, nicht gewinnorientiert zu agieren – wie bei der Interplanetary Database[378] (IPDB). Eine solche Auswahl der Teilnehmenden kann transparente Governancestrukturen fördern, ohne die Rezentralisierung der Blockchain über eine geschlossene Gruppe der Validierenden nach sich zu ziehen.

Box B 3-5

Der Einsatz von Blockchain-Technologie in Asylverfahren

Blockchain-Technologie wurde bereits erfolgreich im Rahmen eines Proof-of-Concept für den zuverlässigen und zügigen Austausch von Informationen in Asylprozessen eingesetzt.[379] Dabei wird der Informationsaustausch zwischen Aufnahmeeinrichtung, Bundesamt für Migration und Flüchtlinge (BAMF) und Ausländerbehörde unterstützt. Die Evaluation zeigt „deutliche Vorteile in den Kategorien Prozesstreue, -transparenz und -effizienz".[380]

Im Asylprozess werden Asylsuchende in einer Erstaufnahmeeinrichtung registriert und einer Aufnahmeeinrichtung zugeordnet. Falls die Antragstellung rechtmäßig erfolgt, findet im Anschluss eine Anhörung durch das BAMF statt. Falls das BAMF positiv über den Asylantrag entscheidet, stellt die Ausländerbehörde eine Aufenthaltserlaubnis aus. Damit dieser Prozess zuverlässig und schnell durchlaufen werden kann, müssen die verschiedenen Behörden stets den Vorgaben für Asylverfahren folgen und über den aktuellen Informationsstand eines Asylprozesses verfügen. In beiden Aspekten sorgt die Blockchain-Technologie für eine Verbesserung gegenüber der aktuellen Situation.

Durch die dezentrale Speicherung der Daten (vgl. Box B 3-3) liegt der aktuelle Status eines Asylprozesses den beteiligten Behörden jederzeit vor. So können die Daten aus verschiedenen Systemen der Behörden – wie dem Workflow- und Dokumentenmanagementsystem des BAMF oder den Personalisierungsinfrastrukturkomponenten der Erstaufnahmeeinrichtungen – integriert und allen beteiligten Behörden zur Verfügung gestellt werden. Darüber hinaus können durch die in der Blockchain hinterlegten Smart Contracts (vgl. Box B 3-3) Prozesse automatisiert und Abweichungen von den vorgesehenen Prozessen vermieden bzw. vollständig dokumentiert werden. Wartezeiten zwischen behördlichen Arbeitsschritten werden minimiert, der Gesamtprozess wird deutlich zuverlässiger.[381]

Die im Proof-of-Concept analysierte Architektur einer Blockchain für den Asylprozess wird seit August 2018 in einem Pilotprojekt des BAMF, der Ausländerbehörde und des AnkER-Zentrums Dresden umgesetzt.

Ein Beispiel für die Automatisierung von Prozessen durch Smart Contracts ist der Bereich Versicherungen. So bietet eine große internationale Versicherungsgesellschaft auf der Basis von öffentlich zugänglichen Informationen zu Flugdaten eine Versicherung gegen Flugverspätungen an. Die Bearbeitung eines Versicherungsfalls erfolgt dabei vollkommen automatisch und anhand eines einsehbaren Smart Contract, sobald Flugverspätungen auftreten.[382] Neben Versicherungen werden die Blockchain-Technologien für weitere Anwendungen mit Bezug zu finanziellen Transaktionen verwendet, so z. B. als Zahlungsinfrastruktur zwischen Banken.[383]

Verschiedene europäische Länder[384] erproben die Nutzung Blockchain-basierter Grundbücher. Auf dieser Grundlage können Prozesse wie das Anfordern eines Grundbuchauszugs oder das Erstellen eines Grundbucheintrags automatisiert werden. Intermediäre wie Notariate oder Banken wären für diese Aufgabe dann nicht mehr im bisherigen Umfang erforderlich und der administrative Aufwand für das Führen eines Grundbuchs könnte reduziert werden. In Ländern ohne funktionierendes Grundbuch kann so ein verlässliches Immobilienregister aufgebaut werden, selbst wenn das Vertrauen in staatliche Instanzen beschädigt ist.[385]

Blockchain-Technologien können auch für digitale Schlüssel eingesetzt werden, die nicht kopiert werden können – beispielsweise zu Wohnungen, Häusern oder Fahrzeugen. Für die Anwendung als Schloss kann die Besitzerin oder der Besitzer einen Smart Contract auf der Blockchain nutzen, der Voraussetzungen für das Öffnen des Schlosses definiert. Hierzu können das Hinterlegen einer Kaution und das Begleichen der Miete gehören. Die Mieterin oder der Mieter kann sich dann per Smartphone am Schloss identifizieren und erhält Zugriff, falls in der Blockchain hinterlegt ist, dass die nötigen Bedingungen erfüllt sind.[386]

Diese Anwendungen zeigen, dass verschiedene Akteure derzeit Blockchain-Technologien entwickeln, erproben und in marktreife Produkte überführen. Sie bilden aber nur einen kleinen Teil der Bereiche ab, in denen Blockchain-Technologien angewendet werden können. Das Potenzial von Blockchains kann

über die genannten Anwendungen weit hinausgehen, weil Blockchain-Technologien zu radikalen Veränderungen in bestehenden Industrien führen. So können in der Energiewirtschaft Blockchain-Technologien genutzt werden, um die Kosten des Betriebs eines Stromnetzes transparent zu erfassen und so Netzentgelte verursachergerecht und effizient zu erheben. Box B 2-7 beschreibt diese Anwendungen von Blockchain-Technologien für die Energiewirtschaft.

Noch grundlegender ist aber, dass Blockchain-Technologien die Art und Weise verändern, wie Daten gespeichert werden. Daten können mittels Blockchain-Technologien sicher dezentral gespeichert werden. Auf dieser Grundlage entsteht die Möglichkeit, die Kontrolle über die eigenen Daten zu behalten und nicht an zentrale Institutionen wie große Internetunternehmen zu verlieren. Hieraus erwächst die Hoffnung, dass Bürgerinnen und Bürger sowie Unternehmen ihre Daten stärker als bisher zugänglich machen und kontrolliert nutzen lassen können.[387]

Mit einer dezentralen Datenhaltung wird letztlich auch die Hoffnung verbunden, die Marktkonzentration in datengetriebenen Industrien zu verringern und Markteintrittsbarrieren abzubauen. So können Blockchain-Technologien zu erheblichen Veränderungen der Marktstrukturen führen und radikale Veränderungen auslösen.

Trotz etlicher vielversprechender Anwendungen und disruptiver Potenziale ist derzeit aber noch offen, ob sich Blockchain-Technologien zukünftig als Querschnittstechnologie etablieren können. Ob die damit verbundenen Erwartungen realisierbar sind, hängt maßgeblich von der Governance der Blockchains ab (vgl. Box B 3-4).

B 3-4 Blockchain-Standort Deutschland

Deutschland verfügt über eine aktive Entwicklergemeinschaft, die an Blockchain-Technologien arbeitet. Fast die Hälfte der deutschen Blockchain-Start-ups ist in Berlin zu finden.[388] Mit dieser Konzentration an Entwicklungstätigkeit ist Deutschland und vor allem Berlin nach Einschätzung von Fachleuten ein Standort mit internationaler Bedeutung für Blockchain-Technologien.[389] In Berlin gibt es eine hohe Konzentration von Entwicklerinnen und Entwicklern, die an der Blockchain-Infrastruktur arbeiten.[390] Bedeutende Organisationen hierfür sind u. a. die Web3 Foundation, die die Entwicklung eines dezentralen Internets fördert, die Energy Web Foundation, die eine offene Blockchain-Technologie für Energiemärkte erarbeitet, oder die IOTA Foundation mit Blockchain-Technologie für IoT-Anwendungen. Eine besondere Rolle kommt der Ethereum-Foundation[391] zu, da Ethereum derzeit einen Quasi-Standard in der Blockchain-Gemeinschaft darstellt.[392]

Eine präzise Einschätzung zur Leistungsfähigkeit Deutschlands im internationalen Vergleich ist allerdings kaum möglich. Hierfür gibt es verschiedene Gründe. So sind die Entwicklungstätigkeiten und Ziele sehr heterogen. Entwicklungen der grundlegenden Infrastruktur von Blockchains, wie beispielsweise durch die Ethereum Foundation, erfolgen oft als Open Source Software durch eine Gruppe von Entwicklerinnen und Entwicklern. Die Zusammenarbeit dieser Personen findet dabei oft über Ländergrenzen hinweg statt und lässt sich dadurch nur schwer einem Standort zuschreiben. Gleichzeitig entzieht sich die Arbeit an Open Source Software aber einem Vergleich von Entwicklungsaktivitäten auf der Grundlage einer Analyse von Patentzahlen, weil Open Source Software nicht patentiert wird. In einem anderen Ansatz wird versucht, über Ländergrenzen hinweg die Anzahl von Blockchain-Start-ups zu vergleichen.[393]Allerdings sind solche Listen, insbesondere im internationalen Vergleich, oft unvollständig und ergeben so ein potenziell verzerrtes Bild über die internationale Verteilung von Blockchain-Start-ups.

Dennoch bleibt festzustellen, dass Deutschland sich in einem dynamischen Wettbewerb befindet und andere Standorte an Attraktivität gewinnen können. So erfolgten die weltweit größten Initial Coin Offerings (ICOs), ein Finanzierungsinstrument von Start-ups mit Blockchain-Bezug, nicht in Deutschland.[394] Von den 20 weltweit größten ICOs erfolgte bislang nur eines in einem europäischen Land, nämlich der Schweiz. Eines dieser Start-ups, Tezos, arbeitet beispielsweise an einer Blockchain-Technologie, bei der jede Nutzerin bzw. jeder Nutzer ein Mitspracherecht bei der weiteren Entwicklung der Technologie besitzt.

B 3-5 Hemmnisse für die Verbreitung von Blockchain-Technologien

Derzeit gibt es noch Hemmnisse für die weitere Entwicklung von Blockchain-Technologien und die Realisierung der Nutzenpotenziale in Wirtschaft und Gesellschaft. Diese Hemmnisse liegen vor allem in

den Bereichen Technologieentwicklung, Regulierung und Rechtsprechung sowie politische und gesellschaftliche Akzeptanz.

So stehen beispielsweise technologische Lösungen für eine höhere Skalierbarkeit öffentlicher Blockchains bisher noch aus. Außerdem verwenden populäre Blockchains wie Bitcoin oder Ethereum derzeit energieintensive PoW-Konsensmechanismen, die auch mit hohen negativen Klima-Externalitäten einhergehen (vgl. Box B 3-3).[395]

Deutschland hat in Zusammenhang mit rechtlichen und regulatorischen Rahmenbedingungen für den Einsatz von Blockchain-Technologien weitestgehend einen abwartenden und beobachtenden Ansatz[396] gewählt. Unsicherheit besteht derzeit insbesondere in der Anwendung der Datenschutz-Grundverordnung im Kontext von Blockchain-Technologien, der Klassifizierung von ICOs, der Besteuerung von Kryptowährungen und des Einsatzes von Blockchain-Technologien in regulierten Märkten wie der Energiewirtschaft.[397] Um diese Unsicherheit zu reduzieren, müssen qualifizierte Ansprechpersonen in Politik, Ministerien und Behörden verfügbar sein und kommunikative Hürden zwischen Politik und Verwaltung auf der einen und der Blockchain-Gemeinschaft auf der anderen Seite abgebaut werden.[398] Zusätzlich bestehen Hürden auf Seiten der potenziellen Nutzerinnen und Nutzer von Blockchain-Technologien. Zu abstrakte oder technische Darstellungen der Technologie in Verbindung mit wenigen verfügbaren Anwendungen stehen derzeit einem breiten Verständnis für das Nutzenpotenzial von Blockchain-Technologien entgegen.

B 3-6 Handlungsempfehlungen

Die Expertenkommission sieht in Blockchain-Technologien hohe Nutzenpotenziale für Unternehmen, Bevölkerung und Verwaltung. Um diese Potenziale zu realisieren, empfiehlt die Expertenkommission der Bundesregierung die folgenden Maßnahmen:

- Die geplante Blockchain-Strategie der Bundesregierung sollte eine Analyse von Stärken und Schwächen des Blockchain-Standorts Deutschland enthalten. Dazu gehören Analysen von aktuellen rechtlichen und regulatorischen Rahmenbedingungen, die innovationshemmend sind.
- Die Strategie sollte Vorschläge für Reallabore enthalten, in denen Lösungen für die identifizierten Hemmnisse getestet werden können, um nötige Anpassungen der Rechtslage vorzubereiten.
- Die Strategie sollte Schnittstellen mit anderen digitalpolitischen Strategien der Bundesregierung wie der KI-Strategie oder der Umsetzungsstrategie Digitalisierung benennen. Ebenso sind Verbundeffekte der unterschiedlichen Strategien zu identifizieren und zu nutzen.
- Weiterhin sind rechtliche Unsicherheiten für Unternehmen zu reduzieren, indem ein Kompetenzaufbau für Ansprechpersonen in Ministerien und Behörden gefördert wird. Dieser Kompetenzaufbau sollte auch genutzt werden, um Konzepte zur Nutzung von Blockchain-Technologien in der Verwaltung zu analysieren und, wo sinnvoll, Pilotprojekte zu starten.
- Schließlich sollten Bürgerinnen und Bürger sowie Unternehmen über Vor- und Nachteile von Blockchain-Technologien informiert werden, um sie zu einem souveränen Umgang mit Blockchain-Anwendungen zu befähigen.