Kompetenzzentrum Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

MYTHOS BLOCKCHAIN: HERAUSFORDERUNG FÜR DEN ÖFFENTLICHEN SEKTOR

Christian Welzel, Klaus-Peter Eckert, Fabian Kirstein, Volker Jacumeit

DIN

IMPRESSUM

Autoren:
Christian Welzel, Klaus-Peter Eckert, Fabian Kirstein, Volker Jacumeit

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9816025-6-2

1. Auflage April 2017

VORWORT

Eine Welt ohne Mittelsmänner, ohne zentrale Instanz, der alle vertrauen müssen – das ist die Vision der Blockchain. Immer wieder sind wir im täglichen Leben auf Dritte angewiesen: seien es Banken, denen wir unser Geld anvertrauen, Notare, die Verträge besiegeln oder der Staat, der Register führt, Dokumente beglaubigt oder Identitäten bestätigt. Die Hauptfunktion der Intermediäre liegt darin, Vertrauen zu schaffen und Werttransaktionen abzusichern. Die Digitalisierung verschärft den Bedarf nach vertrauensstiftenden Instanzen noch einmal. Plötzlich kaufen die Kunden nicht mehr im Laden um die Ecke, sondern sehen sich einem globalen Angebot unzähliger, oftmals unbekannter Händler gegenüber. Große Online-Plattformen sind entstanden, zu deren Kerngeschäftsfeldern es gehört, eben dieses Vertrauen zwischen Kunde und Händler zu gewährleisten.

Doch auch solche Intermediäre sind nicht unfehlbar. Die Finanzkrise 2008 hat deutlich gezeigt, wie abhängig Wirtschaft und Gesellschaft von »systemrelevanten« Institutionen sind. Aber gibt es dazu überhaupt eine Alternative? »Ja«, sagen die Anhänger der Blockchain und diskutieren deren disruptives Potenzial.

Mit der Blockchain steht eine technische Alternative zu klassischen Intermediären zur Verfügung. Durch eine geschickte Kombination aus Wettbewerb, Kryptografie und Transparenz können Werttransaktionen zwischen in der Regel unbekannten Teilnehmern durchgeführt werden, ohne dabei die Absicherung einer vertrauensstiftenden Instanz in Anspruch nehmen zu müssen.

Entstanden ist der Ansatz durch die Kryptowährung Bitcoin. Seit 2009 funktioniert sie nach eben diesen Prinzipien mit stetig wachsenden Nutzerzahlen. Doch Finanztransaktionen sind nur der Anfang. Geht es nach den Verfechtern der Blockchain-Technologie, lassen sich eine ganze Reihe von Branchen durch den Einsatz der Blockchain verändern, immer mit dem Fokus darauf, organisatorische Intermediäre durch eine technische Lösung zu ersetzen. So ist es nicht überraschend, dass sich bereits einige Staaten mit der Blockchain-Technologie befassen und eigene Strategien für deren Einsatz entwickeln.

Allerdings ist die Technologie noch jung und wirft eine Reihe technischer wie auch rechtlicher und gesellschaftlicher Fragen auf. Um sich mit den Chancen und Risiken der Blockchain-Technologie auseinandersetzen zu können, muss man zunächst deren Funktionsweise verstehen.

Mit diesem White Paper wollen wir Ihnen einen Einblick in die komplexe Materie der Blockchain geben. Sie finden hier sowohl eine detaillierte Beschreibung der Technologie als auch Anwendungsbeispiele für den öffentlichen Sektor und nicht zuletzt eine gesellschaftspolitische Bewertung.

Ihr Kompetenzzentrum Öffentliche IT

DAS KOMPETENZZENTRUM ÖFFENTLICHE IT ERFORSCHT PRAXISRELEVANTE KONZEPTE UND ENTWICKELT ANWENDUNGEN FÜR DIE BEREICHSÜBERGREIFENDE ZUSAMMENARBEIT ZWISCHEN ÖFFENTLICHER VERWALTUNG, ZIVILGESELLSCHAFT UND WIRTSCHAFT.

INHALTSVERZEICHNIS

1. THESEN

Blockchain ist ein Hype.
Derzeit taucht die Blockchain-Technologie immer häufiger in den Medien auf. Nicht selten wird ihr dabei das Potenzial zugesprochen, bestehende Geschäftsmodelle oder ganze Branchen zu revolutionieren – oder auch gleich das gesamte Internet. Ob diese Hoffnung berechtigt ist, bleibt abzuwarten. Momentan ist Blockchain noch mehr Hype als Trend.

Die Blockchain-Technologie steht noch am Anfang.
Die Blockchain-Technologie befindet sich am Anfang eines Entwicklungsprozess. Die Technologie selbst wirft viele offene Forschungsfragen wie Skalierbarkeit, Performanz, Interoperabilität oder Energieverbrauch auf. IT-Sicherheitsvorfälle haben das Vertrauen in den Ansatz beeinträchtigt. Inwieweit unter diesen Voraussetzungen ein langfristig wirtschaftlicher Betrieb gewährleistet werden kann, ist derzeit noch offen.

Die Blockchain-Technologie löst sich von ihrem ursprünglichen Anwendungsfall einer Kryptowährung.
Die Idee der Blockchain umfasst drei wesentliche Aspekte: Vermögenswerte, ein Zahlungsnetzwerk und ein technisches Transaktionsprotokoll. Diese Eigenschaften lösen primär spezifische Probleme bei der Einführung einer Kryptowährung. Aufgrund der Komplexität derartiger Systeme müssen die verwendeten Algorithmen und das Zusammenspiel aller Komponenten innerhalb anderer Einsatzgebiete erprobt werden, um allgemein eine breite und risikoarme Nutzung zu ermöglichen. Ausgehend davon soll die Blockchain schon bald nahezu beliebige transaktionsbasierte Anwendungen absichern, indem sie eine technische Lösung für eine verteilte, vertrauenswürdige, ausfallsichere IT-Infrastruktur für Transaktionen bietet. Sie garantiert die Existenz eines zu jedem Zeitpunkt nachvollziehbaren, überprüften und in sich konsistenten Systemzustands. Für transaktionsbasierte Anwendungen ist zu überprüfen, ob eine auf einem Blockchain-Netzwerk beruhende Lösung die erforderlichen nicht-funktionalen Eigenschaften wie Antwortverhalten, Durchsatz, Sicherheit, Nachhaltigkeit usw. gewährleistet.

Die Blockchain-Technologie ersetzt Intermediäre.
Wo heute vertrauenswürdige Dritte garantieren, dass transaktionsgesicherte Prozesse korrekt ablaufen, kann die Blockchain eine Alternative darstellen. Typische Intermediäre (Banken, Notare, Trusted Third Parties) unterliegen regulatorischen Vorschriften und schaffen durch organisatorische Maßnahmen Vertrauen zwischen Transaktionspartnern. Die Blockchain ersetzt diese organisatorischen Maßnahmen durch technische, kryptografische Mechanismen. Ein Intermediär ist dann nur noch für weiterführende Aufgaben, wie Informationspflichten, Beratung etc. erforderlich. Die Abhängigkeit von einem vertrauenswürdigen Dritten wird gegen die von einer algorithmenbasierten, verteilten Technik-Infrastruktur eingetauscht.

Die Blockchain-Technologie löst bestehende Abhängigkeiten auf und erzeugt neue.
Bei der Nutzung der Blockchain-Technologie entstehen neue Abhängigkeiten. Betrachtet man den ursprünglichen Anwendungsfall, so wird ein Teil der hochregulierten und kritischen Infrastruktur Finanzwesen, insbesondere der Aspekt Finanztransaktionen, »virtualisiert« und kann mit der aus der Digitalisierung bekannten Dynamik weiterentwickelt werden. Bewährte Konzepte zum Schutz der Infrastruktur oder die Regulierung greifen für die Blockchain nicht mehr und müssen neu entwickelt werden. Zur technologischen Abbildung gesellschaftlicher Prinzipien, konkret etwa der technologischen Realisierung gesellschaftlicher Prinzipien zur Konsensbildung in einer Blockchain, ist eine Blockchain-Governance erforderlich.

Die Blockchain dezentralisiert Wirtschaft und Gesellschaft
Während zahlreiche Digitalisierungstrends eher zu einer Zentralisierung führen (Plattformen, noch größere Plattformen, einheitliche Portale usw.), birgt die Blockchain das Potenzial für einen breiten Gegentrend. Mit einer gemeinsamen Zielsetzung oder einer ausgeklügelten Anreizstruktur lassen sich Angelegenheiten gestützt durch gesicherte Technologie zwischen den Betroffenen direkt regeln.

Die Blockchain ist Angriff auf und Chance für den öffentlichen Sektor zugleich.
War die Digitalisierung bisher dadurch gekennzeichnet, dass altbekannte Vorgänge beschleunigt und effizienter ausgestaltet wurden, so greift die Blockchain gewachsene öffentliche Strukturen an. Bisher staatlich organisierte Funktionen zur Interaktion können privat organisiert werden, was eine neue Positionierung des Staates erfordert. Zugleich bietet die Blockchain technologische Ansätze, die der öffentliche Sektor nutzen kann, um mehr Transparenz und Vertrauenswürdigkeit in Verwaltungsprozessen herzustellen.

2. EINFÜHRUNG

Als Hauptcharakteristikum eines Blockchain-Netzwerks kann die sichere Ausführung von Transaktionen zwischen beliebigen Teilnehmern ohne Zwischenschalten einer kontrollierenden, vertrauenswürdigen Instanz (sog. »Trusted Third Party«) angesehen werden. Überall dort, wo heute Intermediäre Vertrauen in Prozessabläufe bringen, stellt die Blockchain eine technische Alternative dar. Bei einer Überweisung überprüft beispielsweise eine Bank, ob der Absender über ausreichend Geld verfügt sowie der Empfänger existiert und sie garantiert, dass das Geld beim Empfänger ankommt und zugleich beim Absender abgebucht wird. Vertrauensstiftende Intermediäre finden sich nicht nur im Finanzwesen, sondern überall dort, wo Repräsentationen von Werten (also z. B. Geld, Eigentumsrechte) transferiert werden. Die Zwischenschaltung eines Intermediärs verlangsamt und verkompliziert zwangläufig den Prozessablauf. Damit erhöhen sich die Aufwände für eine Transaktion.

Die Blockchain stellt dazu eine Alternative dar, indem sie den organisatorischen Intermediär durch ein offenes Netzwerk ersetzt, das technisch und kryptografisch abgesichert ist. Entstanden ist die Technologie im Bereich der Kryptowährungen, konkret bei der Kryptowährung Bitcoin. Diese ist zugleich auch die erfolgreichste Implementierung einer Blockchain.

Unter einer Blockchain versteht man ein verteiltes, dezentrales Register (teilweise auch Datenbank genannt), das Transaktionen in chronologischer Reihenfolge unveränderbar und nachvollziehbar speichert und miteinander verkettet. Die klassischen Funktionen eines Intermediärs – Protokollierung, Prozessdurchführung, Transaktionsabsicherung – werden dabei durch eine geschickte Kombination vorwiegend technischer Verfahren, bestehend aus Kryptografie (digitalen Signaturen), der rechenintensiven Lösung situationsabhängiger Kodierungsaufgaben und Peer-to-Peer-(P2P)-Netzwerken, abgesichert. Ein geeignetes Anreizsystem sorgt zusätzlich dafür, dass Teilnehmer für und nicht gegen das Netzwerk arbeiten. Die Transaktionen werden in einzelnen Blöcken zusammengefasst, die in regelmäßigen Abständen zur Blockchain hinzugefügt werden. Über kryptografische Funktionen werden die Blöcke untrennbar miteinander verkettet. Alle Transaktionen sind für jeden Teilnehmer transparent, was eine nachträgliche Manipulation erschwert. Um die Privatsphäre der Teilnehmer zu schützen, treten diese nur pseudonym auf.

Vertrauen in einen zentralen Intermediär ist bei der Blockchain-Technologie nicht mehr notwendig. Dies wird teilweise auch als »trust-less trust« oder »trust-less transaction« bezeichnet[1], was jedoch insofern eingeschränkt werden muss, als dass die Nutzer einem – anonymen – Blockchain-Netzwerk sowie der darin eingesetzten Technologie und Kryptografie vertrauen müssen.

Blockchain-Netzwerke sind eine komplexe Technologie, die in weiten Teilen nur unvollständig dokumentiert ist. Um die Chancen, aber auch die Risiken dieser Technologie einschätzen zu können, ist es erforderlich, die grundlegenden Ideen zumindest grob zu kennen und ein Gefühl für die dahinter liegenden Algorithmen, deren Stabilität und Nachhaltigkeit, aber auch für die mit einem stabilen Betrieb verbundenen organisatorischen, technischen und monetären Voraussetzungen zu entwickeln.

Im Folgenden werden anhand von Bitcoin die grundlegende Funktionsweise sowie die dahinter liegenden technischen Verfahren der Blockchain genauer beschrieben. Darauf aufbauend wird ein Überblick über Einsatzszenarien und Anwendungsbeispiele für den öffentlichen Sektor gegeben, gefolgt von einer gesellschaftspolitischen Betrachtung der Rolle des Staates, aktueller Herausforderungen sowie von Chancen und Risiken der Technologie.

[1] [Blundell-Wignall, 2014].

3. TECHNISCHE MECHANISMEN DER BLOCKCHAIN

Der Begriff Blockchain steht in engem Zusammenhang mit der Kryptowährung Bitcoin[2]. Während Bitcoin bereits 2008/2009 unter dem Pseudonym »Satoshi Nakamoto«[3] entwickelt wurde und in der Zwischenzeit nicht nur in interessierten Kreisen eine hohe Popularität erlangt hat, ist die Blockchain als der technische Motor oder Algorithmus hinter Bitcoin erst in letzter Zeit in den Mittelpunkt des Interesses getreten. Der im August 2016 veröffentlichte Gartner »Hype Cycle for Emerging Technologies 2016«[4] berücksichtigt erstmalig die Blockchain und siedelt diese mit einer »Mainstream Adoption« von 5-10 Jahren bereits auf dem »Peak of Inflated Expectations« an. Diese Einordnung zeigt, dass das Potenzial der Blockchain relativ spontan erkannt wurde, ein weitflächiger, produktiver Einsatz jedoch kurzfristig nicht gesehen wird.

Vor diesem Hintergrund ist es wichtig, die grundlegenden Konzepte der Blockchain und deren Rolle als Motor der Bitcoin-Anwendung zu verstehen.

3.1 WESENTLICHE PRINZIPIEN DER BLOCKCHAIN AM BEISPIEL BITCOIN

Die Blockchain ist ein IT-Werkzeug, das verteilte Transaktionsabwicklung ohne Mittelsmann unterstützt. Die geografisch verteilten Nutzer einer Blockchain sind dafür verantwortlich, dass die durch die Blockchain verwalteten Transaktionen im Konsens genehmigt, durchgeführt und nachvollziehbar protokolliert werden (siehe 3.2).

Im Fall von Bitcoins kann der Begriff der Transaktion analog zur Bedeutung aus dem Bankenwesen interpretiert werden: Es wird ein Geldbetrag X vom Konto eines Nutzers auf das Konto eines anderen Nutzers übertragen. Dies geschieht ohne eine Bank als vertrauenswürdigem Dritten. Nehmen wir an, dass Alice einen Betrag von 25 Bitcoins – kurz: 25 BTC – an Bob überweisen möchte. Die Logik hinter einer derartigen Transaktion ist leicht verständlich: Alice darf nicht mehr überweisen, als sie auf ihrem Konto hat. Kennt man entweder den aktuellen Kontostand von Alice oder aber die Liste aller Kontobewegungen (Transaktionen) auf dem Konto von Alice, aus denen sich wiederum der aktuelle Kontostand ermitteln lässt, so kann die Zulässigkeit der Transaktion von Alice zu Bob überprüft werden.

Was einfach klingt, wird bei seiner IT-Umsetzung durchaus komplex:
Alice verwendet für die Übertragung der 25 BTC eine Anwendung (Wallet), die ihr Konto verwaltet. Die Anwendung prüft jetzt, ob die ausreichende Geldmenge vorhanden ist. In diesem Fall wird eine Überweisung an Bob angelegt.

Jede Transaktion wird von ihrem auslösenden Nutzer signiert. Alice verwendet dazu ihren privaten Schlüssel, den sie am Anfang einmalig generiert hat. Dieser gehört zu einem Schlüsselpaar, bei dem der öffentliche Schlüssel genutzt wird, um den Nutzer gegenüber anderen Nutzern zu identifizieren. Die Teilnehmer treten also nicht mit ihren Klarnamen auf, sondern mit einem Pseudonym.[5] Im Folgenden sprechen wir der Einfachheit halber daher von Nutzer A und Nutzer B.

Im nächsten Schritt kommuniziert das Wallet die Transaktion an alle ihm bekannten anderen Wallets. Diese kommunizieren die Information weiter, sodass schließlich alle Teilnehmer einschließlich B von der angelegten Transaktion informiert sind. Ob B bereits jetzt eine zugehörige Aktion auslöst, z. B. die für die 25 BTC bestellte Ware A versendet, oder aber zunächst auf eine Bestätigung der Transaktion wartet, bleibt B überlassen. Letztlich weiß zu diesem Zeitpunkt aber jeder Teilnehmer des Netzwerks, dass A eine Transaktion zu B auslösen möchte.

Jeder Teilnehmer kann sich zudem an der Buchführung beteiligen und neue Einträge in die Blockchain hinzufügen. Solche Teilnehmer werden auch Miner genannt (siehe 3.3). Sofern ein Teilnehmer Buch über die im Netzwerk offenen Transaktionen führt – also als Miner auftritt – wird dessen Liste offener Transaktionen um die betrachtete Überweisung erweitert. Miner beteiligen sich an der globalen Buchführung, indem sie Transaktionen überprüfen und in das Buchhaltungsjournal (die

[2] [bitcoin, 2016d].

[3] [Nakamoto, 2008].

[4] [Gartner, 2016].

[5] Es ist prinzipiell nicht ausgeschlossen, dass ein Nutzer mehrere Pseudonyme besitzt, die ihn in verschiedenen Kontexten identifizieren (analog zu Privatanschrift, Dienstanschrift und Postfach). In der Regel wird jedoch der öffentliche Schlüssel oder ein daraus abgeleiteter Wert als Pseudonym verwendet.

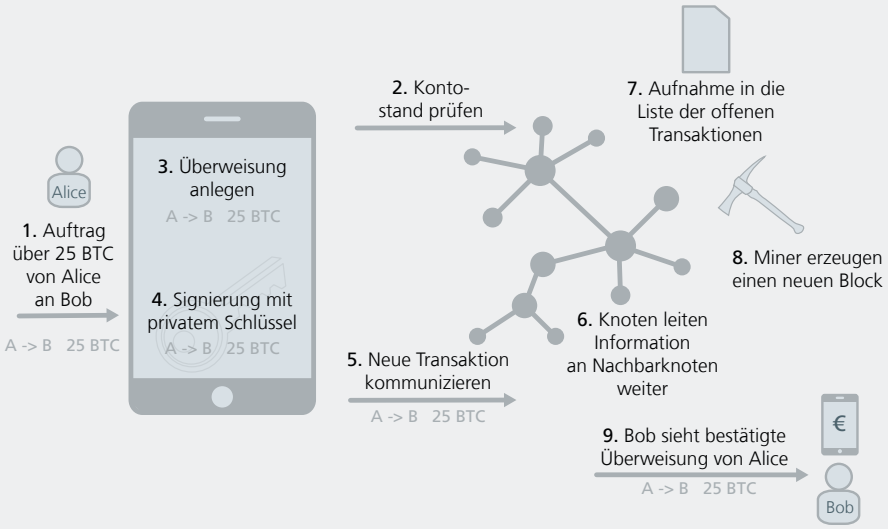

Abbildung 1: Ablauf einer Blockchain-Transaktion am Beispiel Bitcoin

Blockchain), eintragen. Dazu muss der Miner eine neue, beglaubigte Seite (in der Blockchain-Terminologie Block genannt) erzeugen. Ein Block ist eine Sammlung von Transaktionen und weist eine bestimmte Struktur auf. Über kryptografische Funktionen sind die Blöcke untrennbar miteinander verkettet, sodass eine chronologische Reihenfolge aller Transaktionen entsteht (siehe auch 3.4).

Miner, die Transaktionen Anderer auf ihre Korrektheit hin überprüfen und in einen neuen Block aufnehmen, werden für ihre Arbeit entlohnt, entweder durch Transaktionsgebühren oder durch neue Bitcoins, die automatisch mit einem neuen Block entstehen. Neue Bitcoins werden ausschließlich durch das Hinzufügen neuer Blöcke generiert (siehe 3.5).

Um die Ausgabe neuer Bitcoins zu regulieren, wird der Schwierigkeitsgrad, neue Blöcke hinzuzufügen, kontinuierlich angepasst. Die Miner müssen dazu ein kryptografisches Rätsel lösen. Das technische Protokoll der Blockchain sorgt dafür, dass statistisch gesehen in festen Zeitintervallen ein neuer Block »gefunden« wird.[6] Dieser als Mining[7] bezeichnete Vorgang ist in der Regel extrem aufwendig und verbraucht viel Rechenleistung (siehe 3.3).

Zeitgleich versuchen immer mehrere Miner dasselbe Rätsel zu lösen. Am Ende gewinnt derjenige, der es zuerst gelöst hat. Dieser fügt den neuen Block (eine neue Seite im Buchungsjournal) zur Blockchain hinzu, informiert die anderen Teilnehmer über die durchgeführte Erweiterung und löscht die Transaktionen aus seiner Liste offener Transaktionen. Andernfalls bekommt er eine Benachrichtigung über die Existenz einer neuen letzten Seite.

Sollten während dieses Prozesses durch die anderen Miner Fehler, wie ungültige oder verfälschte Transaktionen, erkannt werden, so wird der betroffene Block durch vordefinierte Regeln entfernt und die nicht betroffenen Transaktionen wieder zu den Listen der offenen Transaktionen hinzugefügt. Wird eine Seite (Block) als korrekt angesehen, so werden die in ihr aufgelisteten Transaktionen ebenfalls als korrekt angesehen. Da die Blöcke so miteinander verkettet werden, dass jede Veränderung eines Blocks auch alle nachfolgenden Blöcke betrifft, ist die Transaktion umso sicherer, je mehr Folgeseiten hinzugefügt werden, da eine erfolgreiche Manipulation automatisch auch eine Veränderung aller Folgeseiten erfordern würde.

Kann der entsprechende Block als valide angesehen werden, kann Bob davon ausgehen, dass Alice ihm und nur ihm den Betrag überwiesen hat, und eine entsprechende Gegenleistung veranlassen.

Diese vereinfachende Beschreibung erklärt die wesentlichen Prinzipien eines Blockchain-Netzwerks. Viele Schritte, wie die Erstellung und Verknüpfung neuer Blöcke, sind intuitiv verständlich und mittels kryptografischer Verfahren technisch umsetzbar. Der beschriebene Ansatz für eine verteilte Konsensbildung, d. h. die Bestätigung der Korrektheit von Transaktionen auf Basis heuristischer Ansätze mittels rechenaufwendiger Mining-Verfahren, gehört demgegenüber zu den ungewöhnlichen Konzepten einer Blockchain. Er kann in anderen Anwendungsszenarien auch durch alternative Konzepte zur Konsensbildung ersetzt werden. Der Kontostand eines Nutzers – oder genauer der seines Wallets – ergibt sich implizit aus der Folge aller sein Wallet betreffenden Transaktionen. Was unter dem Zustand eines Wallets bzw. der gesamten Blockchain zu verste-

[6] Bei Bitcoin ca. alle 10 Minuten.

[7] Im vorbereitenden Schritt validiert der Teilnehmer die letzte ihm bekannte Seite (Block) des Journals (Blockchain). Dazu muss er die Korrektheit aller in dieser Seite gesammelten Transaktionen und die interne Konsistenz der Seite überprüfen. Der Teilnehmer nimmt anschließend eine leere Seite und trägt dort kodiert die Nummer der ihm bekannten, zuvor validierten Vorgängerseite des Buchhaltungsjournals ein. Dann trägt er, ebenfalls kodiert, diejenigen Einträge aus seiner Liste offener Transaktionen ein, die er in das Journal übernehmen möchte. Ist er damit fertig, d. h., die neue Seite ist aus seiner Sicht vollständig erstellt, versucht er mittels mathematischer Rechenoperationen über diese Seite die Berechtigung zu erlangen, die so beglaubigte Seite an das Journal anzufügen.

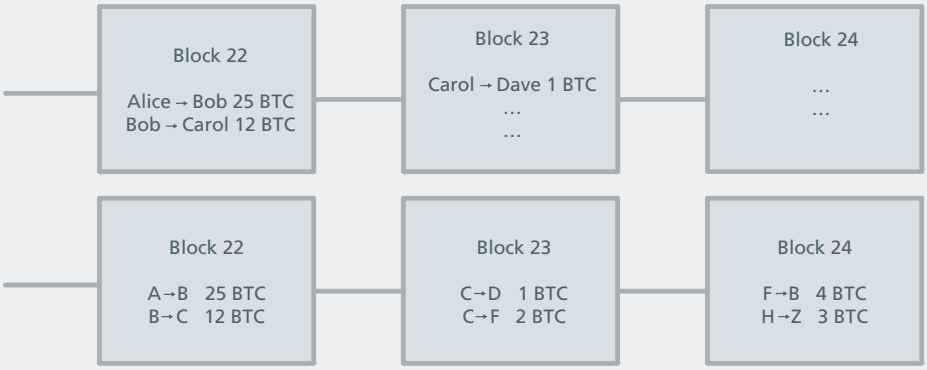

Abbildung 2: Beispielhafte Abbildung der Transaktionen in Blöcken.

hen ist, d. h., wie das verfügbare Geld zu einem gegebenen Zeitpunkt verteilt ist, ergibt sich also erst nach einer Auswertung aller Transaktionen.

Welche IT-Konzepte zur Umsetzung des gesamten Ansatzes verwendet werden und wie der Ansatz auf Transaktionen für beliebige, digitalisierbare Entitäten verallgemeinert werden kann, wird im Folgenden beschrieben.

3.2 KONSENSBILDUNG

Ein wesentliches Merkmal der Blockchain ist die verteilte Konsensbildung, was bedeutet, dass sich prinzipiell jeder Nutzer an der Konsensbildung beteiligen kann. Dazu gehören zwei Dinge: Zunächst müssen die Nutzer darüber informiert werden, dass eine Entscheidung ansteht. In dem verwendeten Beispiel muss Alice also den anderen Nutzern mitteilen, dass sie 25 BTC an Bob überweisen will. Nun ist es unwahrscheinlich, dass Alice alle anderen Nutzer kennt. Die bei Alice installierte Blockchain-Software muss jedoch zumindest eine Reihe anderer Nutzer kennen, denen sie eine Nachricht über die beabsichtigte Transaktion zukommen lässt und diese auffordert, die Transaktion zu validieren und die Nachricht an die den Adressaten bekannten Nutzer weiterzuleiten. Aus IT-Sicht werden dazu Konzepte eingesetzt, die aus Peer-to-Peer (P2P)-Systemen bekannt sind. Technisch betrachtet werden Nachrichten über die im P2P-System inhärent vorhandenen Broadcast-Mechanismen verteilt.

Wie kann eine Transaktion nun von einem Miner validiert und die durchgeführte Validierung dokumentiert werden? Wären die aktuellen Kontostände aller Nutzer zu einem gegebenen Zeitpunkt verfügbar, so könnte die Zulässigkeit einfach durch Nachsehen überprüft werden. In verteilten Systemen existiert ein derartiger, globaler Zustand jedoch nicht. Die Blockchain ist auch als verteilte, replizierte Struktur konzipiert. Dabei ist der Zustand der Blockchain zu einem beliebigen Zeitpunkt durch die Gesamtheit aller Transaktionen definiert, die bis dahin durchgeführt und bestätigt wurden. Für die Validierung einer Transaktion ist es also erforderlich, sich durch die Kette aller das fragliche Konto von Alice betreffenden Transaktionen durchzuarbeiten und zu überprüfen, ob der ermittelte Kontostand erlaubt, die Transaktion durchzuführen. Es gilt also, die Kette der zu einem Konto gehörenden Transaktionen aufzuspüren. Dazu werden alle in der Blockchain vorhanden Blöcke durchsucht und die zu Alice gehörenden Transaktionen extrahiert. Der validierende Miner benötigt also aus allen Alice betreffenden Blöcken die zugehörigen Transaktionen. Diese Beschreibung setzt implizit zwei Realisierungsdetails der Blockchain voraus: Zum einen müssen die Transaktionen erreichbar und auf ihre Validität hin überprüfbar sein. Dies wird über die in einer Kette miteinander verbundenen Blöcke erreicht. Zum anderen lassen sich einzelne Transaktionen aus einem Block extrahieren. Setzt man diese Eigenschaften voraus, so lässt sich die Zulässigkeit der Transaktion von Alice an Bob ermitteln und anschließend als überprüft in einen neuen Block eintragen, der dann seinerseits zu einem geeigneten Zeitpunkt in die Kette aufgenommen wird.

Da die meisten Nutzer einer Blockchain wegen beschränkter Ressourcen nicht die gesamte Blockchain lokal repliziert haben können[8], muss es Operationen geben, um die für die Validierung einer Transaktion erforderlichen, bereits validierten Transaktionen in ihren Blöcken zu identifizieren und zu übertragen. Um bei diesem Schritt das Replizieren ganzer Blöcke zu vermeiden, werden die Transaktionen eines Blockes nicht als Liste son-

[8] Da der Speicherbedarf einer Blockchain stetig wächst, wird es mit zunehmender Lebensdauer unpraktisch, auf allen Endgeräten eine vollständige Kopie vorzuhalten.

dern als Blätter eines binären Hash-Baums[9] gespeichert, dem sogenannten Merkle-Tree[10]. Dieser Baum erlaubt es, mittels kryptografischer Verfahren sicherzustellen, dass bei Kenntnis des Wurzelknotens Teilbäume aus beliebigen Replikaten übertragen werden können, wobei deren Korrektheit nachprüfbar ist. Das Verfahren wird allgemein in P2P-Systemen benutzt, um verteilte Dateien, die aus Datenblöcken bestehen, sicher übertragen zu können.

Was passiert, wenn mehrere Miner gleichzeitig einen neuen Block finden und wie werden die Miner kontrolliert? Um diese Frage zu beantworten, sind die folgenden Fallunterscheidungen hilfreich:

- Angenommen ein Miner hat die Transaktion korrekt validiert und nach erfolgreichem Mining einen entsprechenden Block an die Kette angehängt. Dann würde jeder weitere Miner bei der Validierung des Blocks und der zugehörigen Transaktionen erkennen, dass die Transaktion bereits berücksichtigt ist und sie nicht in seinen neuen Block einfügen. Bei einer zeitlich parallelen Berücksichtigung der Transaktion in einem alternativen Block auf Basis der alten Kette würde unter Umständen ein Abzweig der Kette erzeugt. Jetzt hätte die Kette zwei Enden. Die Wahrscheinlichkeit sagt, dass die erste Verlängerung schneller wächst als die zweite. Werden nun regelmäßig die kürzeren Kettenzweige verworfen, so setzt sich der Zweig mit der ersten Validierung durch.
- Angenommen der Miner hat eine Transaktion zu Unrecht als valide in seinem Block berücksichtigt. Neue Blöcke werden von allen Minern kontrolliert, da sie in Konkurrenz zueinander stehen. Hat ein Miner eine ungültige Transaktion mit aufgenommen, wird der Block von den anderen Minern nicht akzeptiert und verworfen.
- Angenommen der Miner hat die Transaktion zu Unrecht nicht validiert. Dieser Fall ist unkritisch, da dann andere Miner die Transaktion validieren würden.

Konsens über die Korrektheit einer Transaktion wird also durch die Tatsache erreicht, dass nach einer gewissen Zeit die Transaktion in der längsten Kette enthalten ist. Wie viele Blöcke dazu erforderlich sind, lässt sich mit statistischen Verfahren ermitteln. In der Literatur wird häufig die Zahl sechs genannt.[11] Ebenso ist es vorstellbar, dass eine bestimmte Anzahl von Minern eine Transaktion als korrekt gekennzeichnet haben muss, bevor diese als valide gilt. Prinzipiell können die Konsensregeln im Betrieb des Blockchain-Netzwerks geändert werden. Ist ein neuer Block mit validierten Transaktionen erfolgreich erzeugt und von seinem Miner in dessen lokale Kopie der Blockchain eingefügt worden, so muss im letzten Schritt dieser Block im Blockchain-Netzwerk verteilt und von anderen Minern validiert und in ihre lokalen Kopien der Blockchain eingefügt werden. Durch diese unabhängigen Überprüfungen propagierter Blöcke durch Dritte wird Konsens der Miner über die Validität der Blockchain hergestellt.

3.3 DER MINING-PROZESS

Das so beschriebene Vorgehen wirft die Frage auf, wie der neue Block gefunden wird, der die validierte Transaktion enthält? Die Antwort für die Blockchain lautet: Durch den zugehörigen Mining-Prozess.

[9] Ein Hash-Baum ist eine geordnete Baum-Struktur, wobei der Wurzelknoten den Ausgangspunkt darstellt. Durch die Folge der Knoten ergibt sich eine chronologische Reihenfolge. Da die Knoten durch sogenannte Hashwerte miteinander verkettet sind, spricht man von einem Hash-Baum. Ein Hashwert ist eine eindeutige Abbildung eines beliebig langen Ausgangstextes über eine mathematische Funktion (sog. Hashfunktion) auf eine Zeichenfolge mit fester Länge. Verändert sich ein Zeichen des Ausgangstextes, ergibt dies einen anderen Hashwert. Von einem Hashwert kann nicht auf den Ausgangstext geschlossen werden.

[10] [Merkle, 1979].

[11] Basierend auf Erfahrungswerten ist es sehr wahrscheinlich, dass sich ein Block mit mehr als 6 Nachfolgeblöcken in der längsten Blockkette befindet.

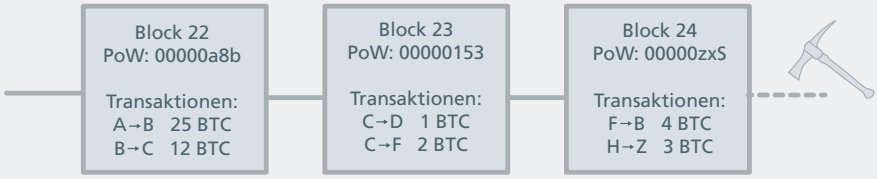

Abbildung 3: Beispielhafte Darstellung der Blöcke mit Proof of Work.

Der Mining-Prozess gehört zum Kern der Blockchain-Technik. Vereinfacht gesagt muss unter Einsatz von Rechenleistung ein »mathematisches Rätsel« gelöst werden. Dazu muss eine bestimmte Zahl erraten werden, die ausschließlich durch Ausprobieren ermittelt werden kann. Ein im Blockchain-Algorithmus implementierter Mechanismus sorgt dafür, dass die Dauer, bis eine passende Zahl gefunden wurde, im Durchschnitt immer gleich ist. Das heißt: Je mehr Teilnehmer versuchen, die passende Zahl zu erraten, desto schwieriger wird es für den einzelnen, diese zu finden. Auf diese Weise bleibt das Zeitintervall zwischen zwei Blöcken im statistischen Mittel immer etwa gleich.[12] Grundvoraussetzung bei diesem Vorgehen ist es, das Lösen des Rätsels sehr aufwendig zu gestalten. Die Überprüfung der Korrektheit der Lösung ist andererseits sehr einfach.

Das mathematische Rätsel, dessen Lösung die Berechtigung zum Anfügen an die Blockchain ermöglicht, nutzt den Hashwert aller Daten des neuen Blocks (Transaktionen + aller Zusatzinformationen) unter Einbeziehung eines im Block gespeicherten zusätzlichen Wertes. Technisch bedeutet das, die Miner müssen einen Hashwert (siehe Glossar) für den neuen Block finden, der eine bestimmte Struktur aufweist, also beispielsweise mit einer bestimmten Anzahl an Nullen beginnt. Die einzige Möglichkeit, diesen Hashwert zu finden, besteht darin, eine passenden zusätzlichen Wert (s. o.) zu finden.[13] Dieser Wert ist die Lösung des Rätsels und dient gleichzeitig dem im Block gespeicherte Nachweis für die erfolgreiche Bearbeitung des Rätsels, auch als »Proof of Work (PoW)« bezeichnet.

Da der Mining-Prozess basierend auf dem »Proof of Work«-Ansatz sehr rechenintensiv, und damit sehr energieaufwendig ist, werden derzeit eine Reihe von Alternativen zu diesem Mechanismus untersucht. Einer der am intensivsten diskutierten Ansätze ist der des sogenannten »Proof of Stake«. Hierbei steht nicht die Rechenleistung eines Miners im Vordergrund, sondern die Menge der Währungseinheiten (Coins), die ein Miner besitzt.

3.4 VERKETTUNG DER BLÖCKE

Damit die Blöcke nachträglich nicht manipuliert werden können, werden sie über kryptografische Verfahren miteinander verkettet. Dazu erhält jeder Block zusätzlich einen Hashwert seines Vorgängerblocks. Eine nachträgliche Manipulation einer Transaktion würde bedeuten, einen neuen Hashwert für den entsprechenden Block sowie alle nachfolgenden Blöcke zu errechnen. Da die Blockchain auf theoretisch alle Knoten im Netzwerk repliziert verteilt ist, müssten die manipulierten Blöcke zusätzlich auf allen Knoten gleichzeitig ausgetauscht werden. Da dies als sehr unwahrscheinlich angesehen wird, gelten Transaktionen in der Blockchain als sehr manipulationssicher im Vergleich zu herkömmlichen Verfahren.[14]

3.5 ANREIZSYSTEM

Für den Endnutzer, der problemlos sichere und nachvollziehbare Transaktionen zu anderen Nutzern auslösen kann, ist die Nutzung der Blockchain intuitiv sinnvoll. Bedenkt man jedoch, dass die Erzeugung von Blöcken mit dem Verbrauch elektrischer Energie in Form von Rechenleistung verbunden ist sowie eine nicht geringe Investition in Hardware erforderlich macht, so stellt sich die Frage, was die Miner bzw. die Initiatoren und Betreiber einer Blockchain zu ihrer Tätigkeit motiviert.

[12] Bei Bitcoin ist der Algorithmus so konfiguriert, dass ca. alle 10 Minuten ein neuer Block zur Blockchain hinzugefügt wird.

[13] Die einzige Variable, die ein Miner hat, um einen passenden Hashwert zu finden, ist, alle Zahlen durchzuprobieren, bis eine geeignete Zahl gefunden wurde. Diese Zahl wird Nonce bezeichnet.

[14] Siehe [Narayanan, 2016] und [Röder, 2016].

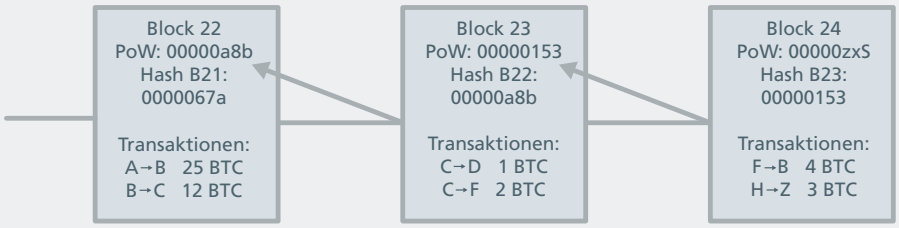

Abbildung 4: Über den Hashwert des Vorgängerblocks werden die Blöcke miteinander verkettet.

Ein Miner erhält für das erfolgreiche Einfügen eines Blocks eine »Belohnung«, im Falle der Bitcoin-Blockchain derzeit 12,5 BTC (Bitcoins). Erfolgreich bedeutet, dass der eingefügte Block Bestandteil der längsten verbleibenden Kette ist (vgl. 3.2). Diese 12,5 BTC kommen aus dem Nichts und werden mittels einer durch das Blockchain-Protokoll initiierten Transaktion mit leerem Absender generiert.[15] Weiterhin erhält der Miner Transaktionsgebühren[16], sofern diese festgelegt worden sind. Auch Trostpreise für Miner, die Transaktionen validiert haben, aber in keinen eigenen Block einfügen konnten, sind möglich. Sofern Transaktionen mit realen Vorgängen verknüpft sind, können Waren oder Dienstleistungen mittels Bitcoins wie mit herkömmlichem Geld bezahlt werden. Bitcoins erhalten dadurch einen Wert in der realen Welt. Tauschbörsen zwischen Kryptowährungen und herkömmlichen Währungen entstehen. Sobald der Wert der Kryptowährung die Kosten für das Mining neuer Blöcke übersteigt, wird die Beteiligung an einer Blockchain für Miner wirtschaftlich interessant. War es am Anfang noch möglich, mit dem privaten PC am Mining teilzunehmen, so ist mittlerweile zu beobachten, dass Rechnerfarmen, bestehend aus speziell für das Mining entwickelter Hardware, aufgebaut werden, die sich ausschließlich mit der Erzeugung neuer Blöcke beschäftigen und sich dadurch finanzieren. Übersteigen die Aufwände für das Mining den Wert der damit erzeugten neuen Bitcoins, muss der Rechenaufwand über Transaktionsgebühren finanziert werden. Je aufwendiger es ist, am Mining-Prozess teilzunehmen, desto weniger Nutzer beteiligen sich daran, was langfristig zu Zentralisierungstendenzen führen kann.[17]

In der Bitcoin-Blockchain ist die Anzahl der jemals erzeugbaren BTC auf 21 Millionen beschränkt. Aus dieser Beschränkung resultiert die Tatsache, dass im Laufe der Zeit die Belohnung für das erfolgreiche Ermitteln eines neuen Blocks abnimmt und die Haupteinnahme eines Miners auf langfristige Sicht vorrangig aus Transaktionsgebühren besteht. Geht man davon aus, dass die Zahl der Nutzer der Bitcoin-Blockchain kontinuierlich steigt und somit die Zahl der Transaktionen zunimmt, wird dies als ein nachhaltiges Geschäftsmodell angesehen.

Neben Bitcoin gibt es eine Reihe weiterer Blockchain-Realisierungen, die für unterschiedliche Anwendungsfälle genutzt werden können. Die Ethereum-Blockchain verfolgt einen besonderen Ansatz[18]. Auch hier existiert das beschriebene Belohnungssystem für gefundene Blöcke und validierte Transaktionen. Die Initiatoren haben sich jedoch zunächst 60 Millionen Ether[19] zugeteilt und 12 Millionen Ether für die Entwicklung reserviert. Für erfolgreich ermittelte Blöcke werden 5 Ether ausgeschüttet bei einer jährlichen Kappung bei 18 Millionen Ether. Bei dieser »gesteuerten Inflation« geht man davon aus, dass sich ein Gleichgewicht zwischen neu erzeugten Ether und verloren gegangenen Ether (bspw. durch verlorene private Schlüssel) einspielen wird.

3.6 SMART CONTRACTS

Im Rahmen der zunehmenden Digitalisierung kann eine Blockchain auch verwendet werden, um Transaktionen mit beliebigen, digital repräsentierten Dingen durchzuführen. Die Beurkundung von Dokumenten, der Erwerb realer oder digitaler Güter, Börsentransaktionen und Ähnliches können über die Blockchain implementiert werden. Für derartige komplexere

[15] Die Belohnung für neue Blöcke wird alle 4 Jahre halbiert, perspektivisch werden daher die Transaktionsgebühren zur Haupteinnahmequelle für Miner werden.

[16] Der Umgang mit Transaktionsgebühren ist je nach Blockchain unterschiedlich. Bei Bitcoin sind Transaktionsgebühren grundsätzlich freiwillig für die Nutzer. Transaktionen mit Gebühr werden von den Minern in der Regel bevorzugt.

[17] [Lischke und Fabian, 2016].

[18] [ethereum, 2016b].

[19] Ether ist die Währungseinheit innerhalb der Ethereum Blockchain.

SMART CONTRACTS MACHEN DIE BLOCKCHAIN ZU EINEM WELTUMSPANNENDEN COMPUTER.

Transaktionen ist es erforderlich, das Ergebnis und den Validierungsprozess einer Transaktion präzise zu beschreiben – sie zu programmieren. Das Blockchain-Netzwerk wird zu einem verteilten Computer, der mittels geeigneter Sprachen programmiert wird und dabei Validierungsregeln als Verträge (Smart Contract) und Transaktionsausführungen zur Zustandsänderung als verteilte Anwendungen ausführt. In Ethereum[20] werden dazu Verträge als eigenständige, zustandsbehaftete, adressierbare Objekte betrachtet, an die Nachrichten geschickt werden können, um Zustandsänderungen des Vertrags auszulösen. Verträge müssen mit einem Budget für die notwendige Rechenleistung ausgestattet werden, d. h., Transaktionen sind in Ether als der systeminternen Kryptowährung abrechenbar. Ergänzend wird jedem Vertrag ein maximales finanzielles Volumen zugeteilt (Maßeinheit Gas)[21], das die bei der Ausführung zulässige Rechenleistung für Transaktionen limitiert. So soll sichergestellt werden, dass Transaktionen nicht willkürlich und missbräuchlich aufgerufen werden, da dieser Prozess Kosten verursacht.

Die Einführung von Smart Contracts führt zu einer Reihe neuer Herausforderungen. Ein Smart Contract wird im ersten Schritt von seinem Ersteller im Blockchain-Netzwerk verteilt, sodass alle Miner eine Kopie des Vertrags erhalten. Wird nun eine Transaktion angestoßen, die sowohl Ether transferiert als auch den Vertrag mit Parametern versorgt, so wird der Vertrag bei jedem Miner während der Validierung der Transaktion ausgeführt. Ether und Parameterwerte werden als Bestandteil der Transaktion in der Blockchain gespeichert. Wie wird jetzt aber sichergestellt, dass die verschiedenen Kopien des Vertrags gleiche Ergebnisse liefern? Verträge können neben der Ausführungslogik auch noch ein Gedächtnis, einen Zustand, beinhalten. Ethereum löst dieses Problem dadurch, dass der Zustand in einer verteilten Datenbank gehalten wird, die die Synchronisation zwischen den einzelnen Kopien sicherstellt. Nun können Anwendungen, die Verträge ausführen andere Smart Contracts aufrufen, indem sie ihnen Nachrichten zusenden. Diese Nachrichten entsprechen Transaktionen, werden im Gegensatz zu diesen jedoch nicht in der Blockchain gespeichert. Der Zustand der Blockchain ist somit nicht mehr nur durch die Verteilung der Kryptowährung Ether auf die Menge aller Nutzer definiert, sondern auch durch den in der Datenbank für jeden Zeitpunkt explizit gespeicherten Zustand aller Verträge. Gleiches gilt für den Zustand einzelner Smart Contracts oder Nutzer (Wallets).[22]

Durch die Einführung einer maximalen Anzahl von Ausführungsschritten einer Transaktion durch das Gas-Limit sollen der missbräuchliche Aufruf von Transaktionen verhindert und die Kosten eines Transaktionsaufrufs überschaubar gehalten werden.

Die verallgemeinerte Interpretation des Begriffs Transaktion impliziert, dass auch deren Beschreibung innerhalb der Blockchain erweitert werden muss und sich ggf. die Struktur der Blöcke innerhalb der Blockchain ändert. Während in Bitcoin-artigen Netzwerken ein Block aus Header, Referenz auf Vorgänger, Proof of Work/Hash des Blocks und den validierten Transaktionen besteht, enthalten Blöcke in Ethereum weitergehende Informationen wie den Systemzustand bzw. genauer die durch die gespeicherten Transaktionen bewirkten Änderungen am Systemzustand als Baum (Merkle-Tree). Die durch eine Blockchain erzwungene Sequenzialisierung der Transaktionen erlaubt es, auch in einem verteilten System von einem (validierten) Systemzustand zu sprechen. Die Blöcke der Blockchain fungieren

[20] [ethereum, 2016a].

[21] Da jede Operation (Addition, Daten speichern, Daten lesen, etc…) eines Smart Contract Rechenleistung der Blockchain verbraucht, wird dem Smart Contract ein maximales Volumen in Gas zugeordnet. Um den Unterschied zwischen Gas und Ether anschaulicher zu machen kann man sich ein Auto vorstellen. Damit es fährt, muss es mit Sprit betankt werden (hier Gas). Der Sprit wird in Euro bezahlt. Während der Spritverbrauch des Autos konstant ist, ist der Europreis pro Liter variabel. Analog wird der Preis pro Einheit Gas in Ether berechnet.

[22] [Delmolino et al., 2016].

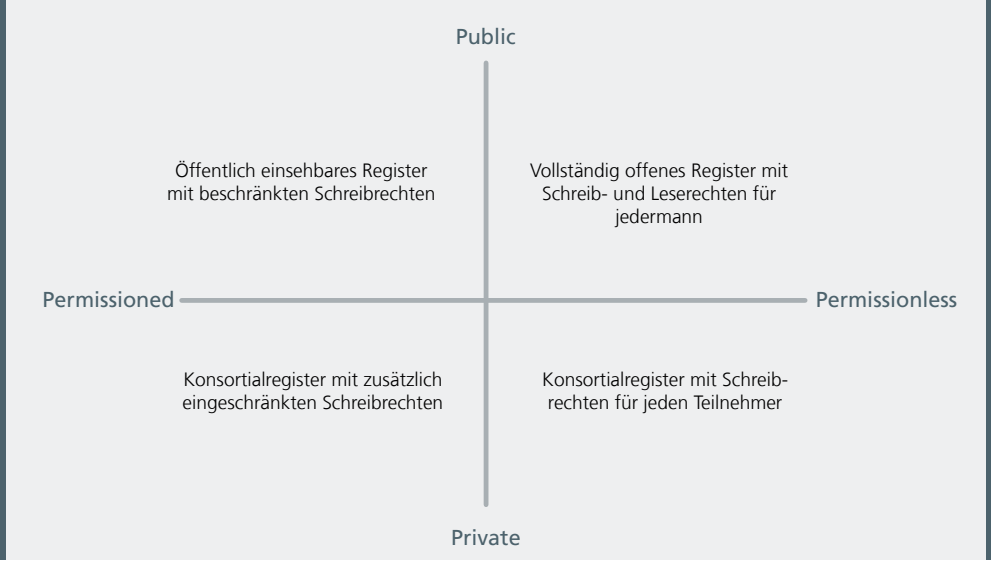

Abbildung 5: Mögliche Ausprägungen einer Blockchain

dabei als eine Art Taktgeber für die durch die Transaktionen initiierten Zustandsänderungen. Die internen Algorithmen und Protokolle der Blockchain sind entsprechend angepasst.

3.7 BLOCKCHAIN-VARIANTEN

Vergleichbar zur Unterscheidung zwischen Internet und Intranet können Blockchain-Netzwerke prinzipiell unterteilt werden in öffentliche Blockchains (public Blockchain) und geschlossene Blockchains (private Blockchain). An öffentlichen Blockchains können beliebige Nutzer teilnehmen und entsprechend den vorgestellten Ideen die vorhandenen Dienste nutzen, neue Dienste anbieten oder sich als Miner betätigen. In privaten Blockchains ist die Menge der Teilnehmer nach festgelegten Kriterien beschränkt. Je nach Anwendungsfall und Teilnehmern kann dann auf bestimmte Mechanismen wie Mining oder Konsensbildung verzichtet werden.

Befindet man sich bereits in einer »Vertrauensdomäne«, so ist der Einsatz der restriktiven Blockchain-Technologie zumindest als fraglich anzusehen, da eine der wesentlichen Zielsetzungen von Blockchains, die Vertrauensbildung, a priori erfüllt ist. Andererseits lässt sich die Eigenschaft einer Blockchain, Transaktionen nachvollziehbar und manipulationssicher zu speichern, in derartigen Umgebungen ohne aufwendiges Mining umsetzen. Der Aufwand für die Erstellung und Validierung von Blöcken lässt sich drastisch reduzieren, der Aufwand für nachträgliche Verfälschungen der Blockchain sinkt jedoch ebenso. Dieser Effekt wird in der Vertrauensdomäne allerdings als unkritisch angesehen. Im Einzelfall ist daher jeweils zu überprüfen, welcher Konsensmechanismus als angemessen betrachtet werden kann.

Orthogonal zur Unterscheidung von geschlossenen und öffentlichen Blockchains wird zwischen »permissioned« und »permissionless« Blockchains unterschieden. Dabei wird das Erfordernis von Schreibrechten in die Blockchain betrachtet. Sofern die Berechtigung in die Blockchain zu schreiben, d. h. Transaktionen veranlassen zu dürfen, eine spezielle Zulassung erfordert, spricht man von einer »permissioned blockchain«, ansonsten von einer »permissionless blockchain«.[23]

Nach diesem Schema lassen sich etwa Bitcoin oder Ethereum als public permissionless Blockchains einordnen. Darüber hinaus sind spezielle Varianten möglich, die etwa auch eine weitere Einschränkung von Leserechten ermöglichen. So gibt es beispielsweise Lösungen, bei denen Teilnehmer nur jene Transaktionen in der Blockchain einsehen können, an denen sie aktiv als Sender oder Empfänger beteiligt waren.

Die Bereitstellung lokaler Blockchain-Testnetze, wie sie für Entwicklung und Test neuer Anwendungen unabdingbar ist, steht auf der Agenda der Blockchain-Betreiber wie Ethereum. Dabei werden sowohl die Nutzung öffentlich zugreifbarer Blockchain-Testnetze als auch lokale, private Testnetze angeboten.

[23] [BitFury Group und Garzik, 2015].

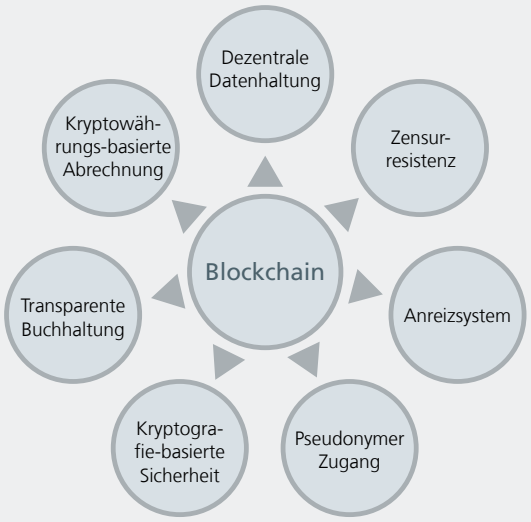

Abbildung 6: Merkmale einer Blockchain

4. DIE MERKMALE EINER BLOCKCHAIN

Eine Blockchain ist also ein verteiltes, dezentrales Register, das Transaktionen in chronologischer Reihenfolge unveränderbar und nachvollziehbar speichert und miteinander verkettet. Durch eine Kombination aus kryptografischen Funktionen, verteilten Netzwerken und komplexen technischen Mechanismen erlaubt die Blockchain eine Transaktionsabsicherung, ohne dabei auf eine vertrauenswürdige dritte Instanz zurückgreifen zu müssen.

Zu den wesentlichen Merkmalen einer Blockchain gehören:

- Verteilte redundante Datenhaltung: Daten werden nicht zentral gehalten, sondern auf alle Knoten im Netzwerk verteilt.
- Änderungsresistenz (Zensurresistenz): Durch die Verkettung der Blöcke und die eingesetzte Kryptografie ist ein nachträgliches Ändern von Transaktionen nur mit enormem Rechenaufwand möglich. Je länger eine Transaktion zurückliegt, desto aufwendiger ist eine Manipulation. Da zudem keine zentrale kontrollierende Stelle existiert, ist eine Einflussnahme von außen kaum möglich.
- Anreizsystem: Ein geeignetes Anreizsystem sorgt dafür, dass die Miner für ihre Aufwände belohnt werden. Aus wirtschaftlichen Erwägungen heraus ist es dabei attraktiver, die Rechenleistung für das Mining einzusetzen, anstatt das Netzwerk anzugreifen.
- Pseudonymer Zugang: In der Blockchain sind die Nutzer nur mit einem öffentlichen Schlüssel (öffentliche Adresse) sichtbar. Aus einer einzelnen Transaktion ist kein Rückschluss auf eine Person oder Organisation möglich. Durch eine Analyse aller Transaktionen, die von einer öffentlichen Adresse getätigt wurden, können ggf. Rückschlüsse auf Personen oder Organisationen gezogen werden.
- Kryptografie-basierte Sicherheit: Die Sicherheit einer Blockchain hängt wesentlich von der eingesetzten Kryptografie ab, daher müssen starke kryptografische Verfahren eingesetzt werden.
- Transparente Buchhaltung: Alle Einträge in einer Blockchain werden an alle Teilnehmer im Blockchain-Netzwerk verteilt. Dies schafft nicht nur Transparenz, sondern schützt zusätzlich gegen Manipulation.
- Kryptowährungsbasierte Abrechnung: Viele Blockchain-Realisierungen basieren auf Kryptowährungseinheiten, die bei einer Transaktion transferiert werden.

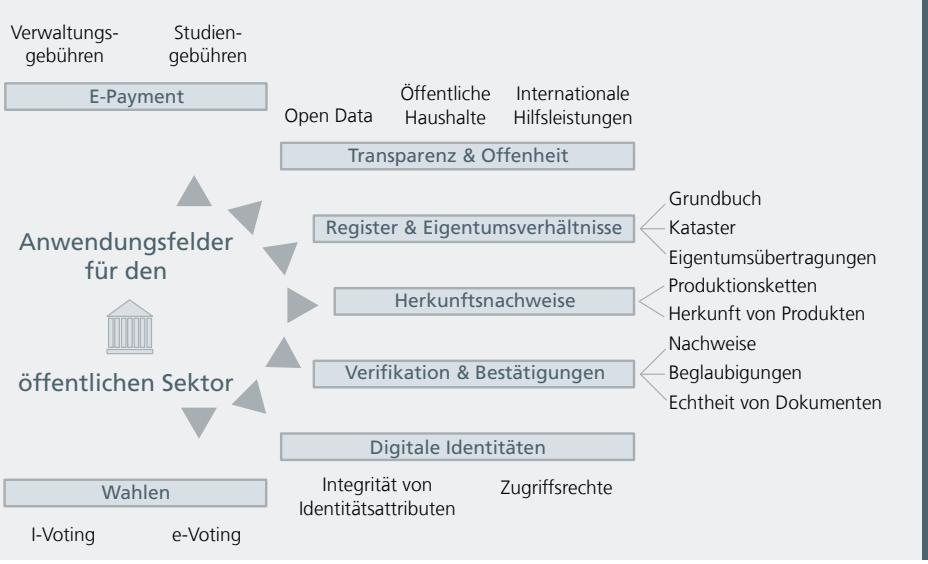

Abbildung 7: International häufig diskutierte Anwendungsfelder der Blockchain-Technologie im öffentlichen Sektor.

5. ANWENDUNGSFELDER FÜR DEN ÖFFENTLICHEN SEKTOR

Die Blockchain-Technologie setzt da an, wo derzeit zentrale Institutionen die Umsetzung von Regeln sicherstellen. Die Diskussion der Blockchain-Technologie in Verbindung mit Bitcoins hilft, ein intuitives Verständnis der umgesetzten Konzepte zu gewinnen. Ein vertrauenswürdiges globales Finanzsystem ohne Mittelsmann und Banken kann ein erstrebenswertes Ziel darstellen, auch wenn es gewohnten Konventionen zunächst widerspricht. Ein derartiges Netzwerk lebt aber nur, wenn es zum einen von einer ausreichenden Anzahl von Nutzern verwendet und betrieben wird und wenn zum anderen eine Kopplung zur realen Welt und deren Gütern und Dienstleistungen hergestellt werden kann.

Die Blockchain-Technologie wird insbesondere im Finanzsektor intensiv beobachtet und erprobt, ist jedoch auch für viele weitere Anwendungsgebiete relevant. Von besonderer Bedeutung ist sie für den öffentlichen Sektor, zu dessen wesentlichen Aufgaben es gehört, das gesellschaftliche Zusammenleben nach gemeinsamen Regeln zu gewährleisten. In vielen Anwendungsfällen fungieren Staat und Verwaltung als Intermediär, um Transaktionen und Prozessabläufe sicherzustellen. So führt der Staat etwa diverse Register, um Eigentumsverhältnisse zu regeln, etwa wenn es um Häuser, Grundstücke oder auch Autos geht. Notare gewährleisten zusätzlich eine sichere Eigentumsübertragung. An anderer Stelle übernimmt der Staat die Rolle einer vertrauenswürdigen dritten Instanz, die etwa die Echtheit von Dokumenten oder auch Identitäten bestätigt. Eine Technologie, die dritte Instanzen durch kryptografische Funktionen ersetzt, hat also direkten Einfluss auf den Staat und den öffentlichen Sektor.

Je nach Kontext kann die Blockchain-Technologie eine effektivere Prozessabwicklung ermöglichen, Teilprobleme lösen oder bisherige Abläufe grundlegend verändern. Um das Potenzial der Technologie besser einschätzen zu können, lohnt es sich, die verschiedenen Einsatzzwecke näher zu beleuchten.

Die im Folgenden dargestellten Anwendungsszenarien werden derzeit international diskutiert. Einige von ihnen werden entweder konzeptionell entwickelt oder bereits in Feldversuchen erprobt. Auf den offensichtlichen Anwendungsfall, kryptografische Währungen als Zahlungsmittel etwa bei Verwaltungsleistungen einzusetzen, wird nicht noch einmal explizit eingegangen. Hier zeigt das Beispiel der Gemeinde Zug in der Schweiz[24], wie etwa Bitcoin für die Bezahlung von Verwaltungsgebühren eingesetzt werden kann.

Die Motivation zur Nutzung der Blockchain-Technologie ist in den skizzierten Anwendungsfällen sehr unterschiedlich. Das Spektrum reicht von Korruptions- oder Missbrauchsvermeidung über das Schaffen von Transparenz bis hin zu klassischem Bürokratieabbau. Nicht alle Szenarien lassen sich direkt auf die deutsche Verwaltungslandschaft übertragen. Sie zeigen jedoch die Vielseitigkeit der Technologie auf.[25]

5.1 REGISTER & EIGENTUMSVERHÄLTNISSE

Zu den am häufigsten genannten Anwendungsbeispielen der Blockchain im öffentlichen Sektor zählen öffentlich geführte Register und die Verwaltung von Rechtstiteln, bspw. Kataster

[24] [Aschwanden, 2016].

[25] Siehe auch [Government Office for Science, 2016], [Rehfeld, 2016] und [Deloitte LLP, 2016].

DIE INTEGRITÄT VON DATEN UND DOKUMENTEN KANN DURCH DIE BLOCKCHAIN NACHGEWIESEN WERDEN.

oder Grundbücher. Die Idee ist insofern naheliegend, als dass die Blockchain mit ihrer nachweisbaren, transparenten Dokumentation von Transaktionen einer klassischen Registerführung sehr ähnelt. Als wesentliche Vorteile werden die Transparenz sowie die Unveränderbarkeit der Einträge genannt. Ziel des Blockchain-Einsatzes ist es dabei, fehlende staatliche Infrastrukturen zu ersetzen, Korruption zu erschweren oder den Prozess der Eigentumsübertragung transparenter und schneller für die Beteiligten zu gestalten.[26]

Neben öffentlichen Registern kann die Technologie auch die Zusammenarbeit zwischen Verwaltungen erleichtern, beispielsweise um herauszufinden, ob bestimmte Daten oder Dokumente bei einer Verwaltung vorliegen oder nicht. Auch der Austausch von Dokumenten zwischen Verwaltungen kann insofern vereinfacht werden, als dass der Einsatz digitaler Signaturen nicht zwingend benötigt wird, um die Herkunft und Echtheit eines Dokumentes sicherzustellen. (siehe dazu Abschnitt 6.2 Verifikation & Bestätigung) Auf diese Weise könnten etwa Anforderungen aus dem E-Government-Gesetz erfüllt werden, welches auf Ebene des Bundes die Einholung von Nachweisen innerhalb der Verwaltung erlaubt.

Dabei gilt es jedoch zu berücksichtigen, dass Vertrauen zu schaffen eine Hauptfunktion staatlicher Register ist. Das Handeln von Staat und Verwaltung muss daher stets das Ziel im Auge behalten, dieses Vertrauen zu gewährleisten, auch dann noch, wenn Kryptografie gebrochen wird oder Technologien eine disruptive Veränderung hervorbringen.

Unabhängig davon hat die Blockchain das Potenzial, Verwaltungstransaktionen zu digitalisieren und zu beschleunigen. Ein Bereich, in dem auch die deutsche Verwaltung Nachholbedarf hat, wie diverse Studien zeigen[27]. Daher ist eine differenzierte Auseinandersetzung mit der Technologie gerade im Bereich öffentlicher Register sinnvoll.

5.2 VERIFIKATION & BESTÄTIGUNG

Die Integrität von Daten und Dokumenten wird heutzutage vorrangig mithilfe digitaler Signaturen gewährleistet. Sie stellen nicht nur sicher, dass eine Person den Inhalt eines Dokumentes bestätigt (vergleichbar mit einer Unterschrift), sondern auch, dass ein Dokument seit der Unterschrift nicht verändert wurde. Viele Prozesse in der Verwaltung sind auf die Vertrauenswürdigkeit von Dokumenten angewiesen. Klassische Technologien für digitale Signaturen sind zwar erprobt und vorhanden, jedoch aufwendiger, da sie meist eine vertrauenswürdige Instanz erfordern, die digitale Signaturen ausgibt und bestätigt. Hinzu kommen Softwarekomponenten zur Signierung der Dokumente. Für Signaturen mit einem hohen bis sehr hohen Schutzniveau (beispielsweise qualifizierte elektronische Signaturen, qES) sind zusätzlich separate Hardwarekomponenten (Signaturkarten, Kartenlesegeräte) notwendig. Die eIDAS-Verordnung[28] erlaubt zukünftig auch sogenannte Server-Signaturen, bei denen das Signieren nicht mehr durch den Nutzer direkt, sondern durch einen von ihm beauftragten vertrauenswürdigen Dritten erfolgt.

Auf diese Art und Weise kann nachgewiesen werden, dass ein Dokument zu einer bestimmten Zeit bei einer bestimmten Person/Organisation in einer bestimmten Fassung vorgelegen hat Ist die Identität der Person/Organisation glaubwürdig, z. B. indem ihr öffentlicher Schlüssel in einem glaubwürdigen Verzeichnis hinterlegt ist, kann die Authentizität des Dokumentes angenommen werden.

[26] Siehe dazu [bitcoin, 2016c].

[27] Siehe: [Fromm et al., 2015], [ipima, 2016].

[28] Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt: [Europäisches Parlament, 23.07.2014].

TROTZ DER ANONYMITÄT DER NUTZER EINER BLOCKCHAIN KANN DIESE DESSEN DIGITALE IDENTITÄTEN VERWALTEN.

Dazu wird ähnlich wie bei Signaturen ein eindeutiger Fingerabdruck eines Dokumentes erstellt, ein sogenannter Hashwert. Er wird über eine mathematische Funktion berechnet und ändert sich, sobald sich auch nur minimal das Dokument ändert. Der Hashwert ist zudem unidirektional, das heißt, man kann nur mit dem originalen Dokument den Hashwert berechnen, umgekehrt kann jedoch nicht von einem Hashwert auf das ursprüngliche Dokument geschlossen werden. Hinterlegt man diesen Hashwert nun in einer Blockchain, kann auch der Hashwert selbst nicht mehr verändert werden. Auf diese Art und Weise kann nachgewiesen werden, dass ein Dokument zu einer bestimmten Zeit bei einer bestimmten Person/Organisation[29] in einer bestimmten Fassung vorgelegen hat. Das Dokument selbst kann über klassische Kanäle weitergegeben werden. Die Integrität des Dokumentes kann über die Blockchain geprüft werden. Solche Verifikationsdienste für Dokumente waren eine der ersten alternativen Anwendungen für die Blockchain, da sie recht einfach umzusetzen sind. Erste Beispiele gibt es bereits im Bildungswesen, etwa für Ausbildungs- oder Qualifikationsnachweise. Auch wenn eventuell nicht alle Anwendungsfälle, die heute eine qES benötigen, in der Verwaltung durch Blockchain-Nutzung ersetzt werden können, so kann dieser Ansatz als leichtgewichtige Alternative doch helfen, die Digitalisierung von Verwaltungsprozessen voranzutreiben.

Notwendig dafür sind jedoch einheitliche Verfahren für die Hashwertgenerierung, speicherung und -überprüfung der Dokumente sowie die Akzeptanz auf Verwaltungsseite für mittels einer Blockchain gesicherte Dokumente.

[29] Nämlich diejenige, die den Hashwert in die Blockchain geschrieben hat.

5.3 HERKUNFTSNACHWEISE

Weitere Anwendungsszenarien finden sich im Bereich der Herkunftsnachweise, wenn es etwa um die Verwendung oder die Herkunft von Produkten und Vorprodukten geht. Hierzu wird in einer Blockchain eine digitale Repräsentation der Objekte hinterlegt. Durch eine Blockchain-Transaktion kann entweder ein Eigentümerwechsel oder eine Verwendung in einem anderen Produkt dargestellt werden. Auf diese Weise können Produktions- und Wertschöpfungsketten oder Wartungszyklen nachvollzogen werden. Als Vorteile dieses Ansatzes werden vor allem Effizienzverbesserungen gesehen, besonders da, wo spezielle Dokumentationsanforderungen bestehen. Für die öffentliche Verwaltung ergeben sich Anknüpfungspunkte überall dort, wo Aufsichtspflichten über die Herkunft eingesetzter Produkte oder über Produktions- oder Wertschöpfungsketten bestehen.

Interessant ist dieser Ansatz daher vor allem für Branchen, in denen besondere Anforderungen an eingesetzte Produkte oder Produktionsketten gelten. Beispielhaft zu nennen sind hier die Luftfahrt, medizinische Geräte, Fischereifangquoten, aber auch Lebensmittelprodukte oder der Handel mit besonders wertvollen Gütern wie Diamanten oder Kunstobjekten.

5.4 DIGITALE IDENTITÄTEN

Nicht nur für Dokumente, auch für einzelne Daten kann die Integrität über eine Blockchain geprüft werden. Erste Prototypen existieren etwa für die Abbildung digitaler Identitäten. Hierbei werden Hashwerte über eine Menge von Identitätsattributen gebildet und in einer Blockchain abgelegt. Auch hierbei geht es darum, die Integrität der Identitätsattribute sicherzustellen.

Etwas weiter geht das Konzept, wenn diese Identitätsattribute zusätzlich mit Zugriffsrechten für IT-Systeme versehen werden. Auf diese Weise kann ein dezentrales Rollen- und Rechtemanagement realisiert werden. In der Blockchain werden zusätzlich zu einer Identität auch damit verbundene Zugriffsrechte auf IT-Systeme hinterlegt, die dann von den einzelnen Systemen überprüft werden. Wird ein Zugriffsrecht wieder entzogen, muss diese Information als neuer Eintrag in die Blockchain hinzugefügt werden. Wird der Ansatz konsequent über alle Organisationsanwendungen hinweg genutzt, kann darüber auch ein Single-Sign-on[30] realisiert werden. Nutzt man hierzu eine existierende Blockchain, könnten Organisationen teilweise auf ein eigenes Identitätsmanagementsystem verzichten. Dies gilt zumindest in der Theorie, in der Praxis muss trotzdem ein Rollen- und Rechtemanagement etabliert und verwaltet werden. Insbesondere organisationsübergreifende Zugriffsrechte können über einen solchen Ansatz realisiert werden, dies setzt jedoch ein standardisiertes und übergreifend akzeptiertes Vorgehen voraus.

Da alte Einträge nicht gelöscht werden können, ist automatisch eine Historie aller erteilten und widerrufenen Zugriffsrechte in einer Blockchain sichtbar, zumindest für jene Teilnehmer, die die Blockchain einsehen können. Ob dies wünschenswert ist, hängt vom Einzelfall ab.

5.5 TRANSPARENZ & OFFENHEIT

Eine wesentliche Eigenschaft von Blockchains ist ihre Transparenz bzgl. aller existierenden Transaktionen, was insbesondere bei öffentlich einsehbaren Blockchains erheblich zur Vertrauensbildung beiträgt. Auch öffentliche Hand und Politik sehen sich vermehrt der Anforderung ausgesetzt, ihre Aktivitäten transparent und damit nachvollziehbarer zu gestalten. Mit diversen Open-Data-Projekten stellen sowohl Bund als auch Länder und Kommunen der Öffentlichkeit eigene Daten zur Verfügung. Auch auf Ebene der Europäischen Union wird ein Internetportal für offene Daten bereitgestellt.

Mit der Blockchain-Technologie kann diese Transparenz auf eine neue Qualitätsstufe gehoben werden. So kann etwa die Herkunft und Echtheit von Daten durch eine Blockchain abgesichert werden, wodurch das Vertrauen in die Korrektheit, bzw. Quelle der Daten selbst gestärkt würde.[31]

Ein weiteres Anwendungsfeld in diesem Bereich sind öffentliche Haushalte. In ihrer Eigenschaft als Kassenbuch können beispielsweise die Einnahmen und Ausgaben öffentlicher Haushalte transparenter gestaltet werden. Einnahmen und Ausgaben werden wie bei einem Haushaltsbuch als Transaktion in einer Blockchain gespeichert. Dies würde einen umfassenden Einblick in die Ausgabenstruktur öffentlicher Haushalte ermöglichen – wobei der Detaillierungsgrad variieren kann – setzt jedoch die Bereitschaft zur Transparenz voraus. Ein solches Konzept wäre theoretisch auch auf internationale Hilfsleistungen oder Spendenfinanzierungen z. B. von Parteien oder Verbänden übertragbar, indem etwa hinterlegt wird, wie und wofür die Mittel verwendet werden. Dies kann helfen, Missbrauch zu verhindern und gleichzeitig Bürokratie abzubauen.

5.6 WAHLEN

Die Debatte um elektronische Wahlen wird seit Jahren sehr kontrovers geführt. Während in einigen Staaten Wahlautomaten oder gar Internetwahlen bereits etabliert sind, lehnen andere elektronische Wahlen mit Verweis auf IT-Sicherheitsvor-

[30] Unter Single-Sign-on versteht man, dass ein Benutzer sich nur einmal an einem IT-System anmelden muss, um dann alle Dienste nutzen zu können. Ein separates Anmelden pro Dienst ist dann nicht erforderlich.

[31] [Smith et al., 2016].

MIT EINER BLOCKCHAIN KANN DIE HERKUNFT UND ECHTHEIT VON DATEN ABGESICHERT WERDEN.

fälle oder grundlegende Bedenken generell ab. In die Reihe der potenziellen Technologien für sogenannte elektronische Wahlen (e-Voting) bzw. Internet-Wahlen (I-Voting) reihen sich vermehrt auch Blockchain-basierte Ansätze ein. Die Idee dahinter ist, dass jeder Kandidat eine digitales Wallet, quasi eine Art kandidatenspezifische Wahlurne, erhält. Jeder Stimmberechtigte erhält einen Token oder Coin für jede Stimme. Um die Wahl durchzuführen, transferiert der Wähler seinen Token an das Wallet des Kandidaten seiner Wahl. Die Anzahl der Token, die ein Kandidat in seinem Wallet erhalten hat, spiegelt die Anzahl der Stimmen wider, die er auf sich vereinen konnte. Die Vorteile eines solchen Verfahrens liegen in der Transparenz und Prozessoptimierung. Wie bei vielen elektronischen Wahlsystemen wäre eine manuelle Auszählung nicht erforderlich und das Ergebnis sofort nach einer Wahl vorhanden. Jeder Stimmberechtigte kann zudem nachprüfen, dass die eigene Stimme mitgezählt wurde.[32]

Der Ansatz geht jedoch auch mit Problemen einher. So ist die Wahl nicht komplett anonym, da zumindest die Stelle, die die Token für die Stimmberechtigten ausgibt, zurückverfolgen kann, wer wie abgestimmt hat. In Kombination mit weiteren Verfahren der Kryptografie, etwa sogenannten Blind Signatures, könnte trotzdem ein anonymes Wahlverfahren ermöglicht werden.[33] Darüber hinaus wäre schon während einer Wahl transparent, welcher Kandidat bereits wie viele Stimmen erhalten hat, was das sogenannte »taktische« Wählen unterstützt. Auch das »Verkaufen« einer Stimme kann durch einen solchen Ansatz befördert werden, da der Stimmberechtigte gegenüber einem Dritten nachweisen kann, wie er abgestimmt hat. Hinzu kommen, wie bei jeder technischen Lösung für elektronische Wahlen, Aspekte der IT-Sicherheit, Benutzbarkeit und Barrierefreiheit.

Für parlamentarische Wahlen in Deutschland, die höchste Ansprüche hinsichtlich Sicherheit und Vertrauenswürdigkeit einer Wahl stellen, ist der Einsatz der Technologie derzeit nicht geeignet. Für Abstimmungsprozesse mit geringeren Anforderungen, bspw. Vereinswahlen, kann der Ansatz durchaus interessant sein, muss sich jedoch mit bereits etablierten Lösungen messen.

[32] [Noizat, 2015].

[33] Erste Lösungsansätze dazu finden sich in: [Zhao und Chan, 2016].

6. TECHNISCHE ANFORDERUNGEN UND GESELLSCHAFTLICHE WIRKUNG

Ideen und Anwendungsszenarien für die Blockchain existieren viele. Nicht nur für den öffentlichen Sektor, auch für viele andere Branchen wird über Einsatzmöglichkeiten diskutiert, die eine enge Verbindung zum öffentlichen Sektor aufweisen, etwa um den Status eines Verwaltungsanliegens zu prüfen. Aber auch für die Abbildung von Nachweis- und Verantwortungsketten (Lieferketten o. Ä.) oder den Handel mit zunehmend dezentral erzeugtem Strom existieren erste konzeptionelle Ideen, die Blockchain-Technologie einzusetzen. Inwieweit diese Ansätze zu umfassenden Lösungen führen, muss sich noch zeigen.

Interessant ist der Ansatz immer dann, wenn der klassische Prozess in einer »organisationsübergreifenden mehrpoligen Kette organisiert ist, also auch organisatorisch in einer Peer-to-Peer Netzstruktur gestaltet ist«.[34]

Wesentliches Merkmal der Blockchain ist ihre Unabhängigkeit von Intermediären. Beim Einsatz der Blockchain ist kein Vertrauen in eine einzelne Institution oder Organisation notwendig. Stattdessen muss einem dezentralen Netzwerk und kryptografischen Verfahren vertraut werden. Wie viele neue Technologien der öffentlichen IT steht auch die Blockchain dabei in einem Spannungsfeld zwischen Sicherheit, Akzeptanz (Nutzbarkeit) und Wirkkraft (Effektivität).

Da mit der Nutzung der Blockchain der Einfluss von Intermediären zurückgeht, stellen sich einige grundsätzliche Fragen. Etwa: Sind wir als Gesellschaft bereit, einer dezentral ausgerichteten Technologie eher zu vertrauen als etablierten Institutionen? Wo liegen die Chancen und Risiken? Und welche Rolle übernimmt der Staat?

6.1 DIE ROLLE DES STAATES

Für staatliche Strukturen ist die Blockchain-Technologie in vielerlei Hinsicht relevant. Auf der einen Seite tritt der Staat als Regulierer auf, beispielsweise wenn es um kryptografische Währungen wie Bitcoin geht. Die Besonderheit für die Regulierung liegt dabei in der Dezentralität des Blockchain-Ansatzes. Klassische Regulierungsmechanismen stoßen an ihre Grenzen, wenn Ansprechpartner und Verantwortlichkeiten fehlen. In der Diskussion um die Blockchain wird daher oft von Regulierungsresistenz gesprochen. Ob dies wirklich der Fall ist, darf jedoch bezweifelt werden. Auch in Blockchain-Netzwerken gibt es Teilnehmer, die eine Schlüsselrolle übernehmen. Miner sind hier ebenso zu nennen wie Händler, die klassische und kryptografische Währungen tauschen. Es lassen sich also durchaus Adressaten der Regulierung identifizieren. Der globale Charakter des Netzwerkes erschwert jedoch eine nationalstaatliche Regulierung.

Neben dem Aspekt der Regulierung werden Staat und Politik sich vor allem mit der Frage befassen müssen, wie man praktisch mit der Technologie umgeht. Die Spanne der Möglichkeiten reicht dabei von Verbot (was vermutlich kaum umsetzbar wäre) über Duldung, Akzeptanz, bis hin zu Förderung und Nutzung. Dazu sind qualifizierte Einschätzungen notwendig, etwa bei der Frage: »Wie und in welcher Form bildet die Technologie bestehendes Recht ab und wie erkennt das Recht die Technologie an?«[35] Dies erfordert eine intensive Zusammenarbeit zwischen Juristen und Informatikern. Auch in Deutschland hat der Diskurs dazu in Fachkreisen bereits begonnen.[36]

Darüber hinaus kann der Staat die Entwicklung der Technologie gestalten und vorantreiben, etwa mithilfe staatlicher Förderinstrumente, Unterstützung der Standardisierung oder durch die Nutzung der Technologie für eigene Prozesse. Der dezentrale Ansatz der Blockchain könnte durchaus gut zum föderalen System der deutschen Verwaltungslandschaft passen. Dabei stellt sich die Frage, an welchen Stellen der Einsatz der Blockchain-Technologie bestehende Prozesse verbessern und optimieren kann, wobei die Betrachtung primär von der fachlichen Notwendigkeit und weniger von den technologischen Möglichkeiten ausgehen muss.

6.2 WIRTSCHAFTLICHE DYNAMISIERUNG

Die offenen Fragen hinsichtlich der Regulierung der Blockchain-Technologie respektive der von ihr beeinflussten Wirtschaftssektoren verweist auf die beträchtlichen Veränderungspotenzi-

[34] [Rehfeld, 2016].

[35] Siehe auch [Kaulartz, 2016] und [Blocher Prof. Dr. Dr., 2016].

[36] Siehe auch: [Bitkom, 2016].

Abbildung 8: Wie viele neue Technologien der öffentlichen IT steht auch die Blockchain in einem Spannungsfeld zwischen Sicherheit, Akzeptanz und Wirkkraft.

ale, die ihr für etablierte Branchen nachgesagt werden. Davon sind nicht nur Professionen betroffen, die klassischerweise die Funktion des vertrauenswürdigen Dritten übernehmen. Während die Funktionsweise der Blockchain Aufgaben, die von Notaren wahrgenommen werden, direkt angreift, weisen zwei technische Möglichkeiten weit über diesen wirtschaftlichen Kernbereich hinaus: Smarte Verträge und die vertrauensvolle Abwicklung auch kleinster Transaktionen.

Smarte Verträge (vgl. Kapitel 3.6) bieten die Möglichkeit, definierte Vereinbarungen elektronisch abzubilden und ihre Einhaltung in Teilen automatisiert zu kontrollieren. Als Beispiel hierfür wird gerne das Auto herangezogen, das sich bei Ausbleiben der letzten Leasingrate nicht mehr starten lässt. Mit der Ausgestaltung solcher Verträge sind zahlreiche konzeptionelle, technische und vertragliche Probleme verbunden. Die in jedem Vertragswerk erforderliche Flexibilität geht bei deterministischer Auslegung beispielsweise verloren, weshalb sich grundsätzlich nur vergleichsweise triviale Regelungen abbilden lassen. Unvollständige Verträge, die auch über längere Zeiträume hinreichende Flexibilität gewährleisten sollen, verbieten sich etwa für die automatisierte Abbildung vollständig. Aber auch bei trivialen, deterministischen Zusammenhängen ergeben sich Schwierigkeiten, auf der einen Seite die für die festgelegten Wirkungen erforderlichen Informationen in die Blockchain einzuspeisen und auf der anderen Seite diese Wirkungen beim Vertragsgegenstand auch durchzusetzen. Während die Blockchain gegenüber Beeinflussungen weitgehend geschützt ist, bleiben an den Schnittstellen beträchtliche Umsetzungs- und Sicherheitsrisiken. Bleiben smarte Verträge also absehbar auf wenige Anwendungsfälle beschränkt, zeigt sich doch ihr beträchtliches Potenzial, Mechanismen der Kontrolle und Streitschlichtung zu ergänzen oder auch abzulösen.

Die Möglichkeit, auch kleinste Transaktionen effizient und effektiv abzusichern, stellt einen Angriff auf gewachsene Strukturen dar. Bei vielen alltäglichen Transaktionen übernehmen oftmals digitale Plattformen die Funktion des vertrauenswürdigen Dritten. Die Blockchain erlaubt es nun, diese Funktion von Plattformen zu ersetzen. Solange die Transaktionsgebühren niedrig sind, wird ein kleinteiliger Markt von Mikroanbietern und -nachfragern möglich, die sich für eine vertrauensvolle Abwicklung von Online-Geschäften nicht mehr kennen müssen und auch keiner Absicherung durch Intermediäre bedürfen. Zusammen mit dem Trend zur Eigenproduktion[37] entstehen so möglicherweise völlig neue Marktstrukturen, die sich in Ansätzen bereits am Elektrizitätsmarkt und bei Fahrdienstleistungen abzeichnen. Selbst bei nur zurückhaltender Durchsetzung dürften sich dadurch beträchtliche Verschiebungen der Marktmacht in einzelnen Branchen ergeben.

6.3 CHANCEN UND RISIKEN DER TECHNOLOGIE

Neben der Dezentralität werden vor allem in der Transparenz und der hohen Fälschungsresistenz die wesentlichen Vorteile des Blockchain-Ansatzes gesehen. Die Unabhängigkeit von Intermediären vermeidet nicht nur kostenintensive Mittelsmänner, sondern ermöglicht völlig neue dezentrale Transaktionsmodelle. Insbesondere dort, wo zentrale Infrastrukturen fehlen, bietet die Technologie ein großes Potenzial, etwa in Regionen, in denen ein Bankensystem oder auch ein vertrauenswürdiges Registerwesen fehlen. Nicht zuletzt kann eine direkte Durchführung von Transaktionen zwischen zwei Transaktionspartnern schlankere und damit effizientere Prozesse schaffen.

Die Nutzung einer Kryptowährung wie Bitcoin ermöglicht zudem ein schnelles Bezahlen, ohne dabei eigene Finanzdaten wie etwa Kreditkartennummer oder Ähnliches preisgeben zu müssen. Die Pseudonymität der Transaktionen senkt zusätzlich die Gefahr eines umfassenden Identitätsdiebstahls.

[37] Siehe dazu Trendthema Prosument in [Mike Weber et al., 2016].

JE GRÖSSER EIN BLOCKCHAIN-NETZWERK IST, DESTO SCHWIERIGER IST EINE MANIPULATION.

In einer public Blockchain sind alle Transaktionen für jeden Teilnehmer einsehbar. Sofern die Teilnehmer für jede Transaktion eine andere Adresse verwenden, kann jedoch durch Kenntnis der an einer Transaktion beteiligten Partner nicht direkt auf weitere Transaktionen dieser Partner geschlossen werden.

Die Transparenz der Blockchain und ein fehlender Ansprechpartner bzw. Betreiber erschweren Willkür und Einflussnahme. Informationen, die in einer Blockchain abgelegt werden, können von keiner, insbesondere keiner zentralen Instanz verändert oder gelöscht werden. Damit ist die Blockchain in hohem Maße resistent gegen Zensur und Kontrolle. Zugleich erschwert diese Eigenschaft jedoch auch die Regulierung (siehe 6.1).

Heutige Blockchain-Lösungen basieren auf dem Prinzip, dass der Mehrheit der Rechenleistung im Netzwerk vertraut wird. Durch massive Rechenkapazität ist theoretisch eine Einflussnahme möglich. Je größer ein Blockchain-Netzwerk ist, desto unwahrscheinlicher wird diese Möglichkeit. Insbesondere beim Aufbau einer neuen öffentlichen Blockchain mit wenigen Teilnehmern muss dieser Aspekt berücksichtigt werden.

Das Vertrauen in die Blockchain ist stark von der Sicherheit der eingesetzten Kryptografie abhängig. Die kryptografischen Mechanismen sind zwar änderbar, da jedoch eine steuernde Instanz fehlt, ist für eine technische Änderung ein Konsens aller Teilnehmer (oder zumindest der Mehrheit der Teilnehmer) erforderlich.

Kritisch zu betrachten ist auch der enorme Energieverbrauch, der für die Berechnung neuer Blöcke (siehe 3.3) aufgebracht werden muss[38]. Außerdem ist ein dauerhaftes Anreizsystem notwendig, um eine Blockchain-Infrastruktur lauffähig zu halten.

[38] [O'Dwyer und Malone, 2014].

All diese Punkte müssen für einen potenziellen Einsatz der Blockchain-Technologie in die Betrachtung einbezogen werden.

6.4 POTENZIELLE ANGRIFFSVEKTOREN

Die Blockchain bietet durch ihre Transparenz eine hohe Fälschungssicherheit. Das Fehlen eines zentralen Betreibers macht sie robust gegen eine Vielzahl klassischer Angriffsmethoden. Nichtsdestotrotz gibt es auch bei diesem Ansatz Angriffspunkte. Ein wesentliches Prinzip der Blockchain liegt darin, dass jeder Nutzer für seine IT-Sicherheit eigenständig verantwortlich ist. Jeder Nutzer muss seine privaten Schlüssel für die Kryptografie, mit denen Transaktionen signiert werden, selbst verwalten. Er muss sie gegen Verlust und Ausspähen schützen. Gelingt es einem Angreifer, die privaten Schlüssel zu erlangen bzw. zu kopieren, kann er Transaktionen damit signieren und beispielsweise im Fall einer Kryptowährung das Geld stehlen.

Für das Hinzufügen neuer Blöcke, das Mining, ist die Rechenleistung der Miner sehr entscheidend. In aktuellen Blockchain-Netzwerken geht man von der Annahme aus, dass die Mehrheit der Rechenleistung vertrauenswürdig ist. Schafft es ein Angreifer, mehr als die Hälfte der Rechenleistung unter seine Kontrolle zu bringen, kann er statistisch betrachtet langfristig eigene Transaktionen in der Blockchain bestätigen. Diese Methode ist vor allem bei kleineren Blockchain-Netzwerken realistisch und wird als 51-Prozent-Angriff bezeichnet. Typische Angreifer sind beispielsweise Betreiber von Botnetzen, die über eine große Rechenleistung verfügen. Je größer das Blockchain-Netzwerk, desto aufwendiger wird diese Methode für den Angreifer.

Ein weiteres Angriffsszenario ist gegeben, wenn Sicherheitslücken im Code der Blockchain-Software vorhanden sind. Ein Beispiel hierfür ist ein Angriff auf eine Ethereum Blockchain, der in

der Presse auch als DAO-Hack[39] bezeichnet wird. Hier gelang es einem Angreifer, einen Teil des über eine Blockchain gesammelten Investitionskapitals durch eine Schwachstelle im Code abzuzweigen.

Darüber hinaus existiert die Möglichkeit, durch eine sogenannte Denial-of-Service-Attacke das Blockchain-Netzwerk zu überlasten. Bei dieser Angriffsmethode wird das Netzwerk mit massenhaften Kleinsttransaktionen quasi überflutet, sodass es für andere Teilnehmer nicht mehr nutzbar ist.

In Abhängigkeit von der Ausgestaltung einer Blockchain – öffentlich einsehbar (public) oder nicht (private), Beschränkungen bei der Teilnahme (permissioned) bzw. offene Teilnahme (permissionless) – ergibt sich das Risiko für die dargestellten Angriffsvektoren. Für öffentlich einsehbare unbeschränkte Blockchains müssen alle Angriffsvektoren einer Risikoanalyse unterzogen werden.

6.5 FORSCHUNGSFRAGEN

Aus der Betrachtung der Chancen und Risiken sowie bestehender Angriffsvektoren ergibt sich bereits eine Reihe von offenen Fragen, denen sich die Forschung aktuell widmet bzw. in den kommenden Jahren widmen muss. Darüber hinaus sind auch grundsätzliche Fragen der Technologiegestaltung zu beantworten. Im Wesentlichen zählen dazu gesellschaftliche, politische, technische und wirtschaftliche Aspekte. Die folgenden Fragen werden derzeit in Fachkreisen sowie im öffentlichen Diskurs behandelt:

- Welche Alternativen zum energieaufwendigen Prozess des Mining (siehe 3.3) sind möglich? Wie kann der Energieaufwand für das Mining reduziert werden?
- Wie können die Zeiten bis zur Validierung einer Transaktion verkürzt werden?
- Wie können Performanz und Skalierung der Technologie verbessert werden?
- Wie können technologische Anpassungen vorgenommen werden, wenn es keinen zentralen Ansprechpartner gibt?
- Wie ertüchtigt man Nutzer im Umgang mit der Kryptografie, insbesondere der Absicherung der privaten Schlüssel?
- Wie verträgt sich die Unveränderbarkeit der Blockchain mit dem Recht auf Vergessen? Wie geht man mit irrtümlichen Falschbuchungen um?
- Welche weiteren Angriffsmuster sind denkbar und wie kann man sich dagegen absichern?
- Wie können Anwendungen von einer Blockchain zu einer anderen migrieren?
- Wie und welche Daten sollten in einer Blockchain gespeichert werden?
- Wie werden Datenhaltung und Blockchain miteinander verbunden?
- Die Absicherung durch rein technische und sehr komplexe Mechanismen, die nur von Experten nachvollzogen werden können, kann den Eindruck erwecken, bzw. verstärken, einer Technologie ausgeliefert zu sein. Wie geht man mit den damit entstehenden Ängsten und Vorbehalten um?

6.6 NORMUNG UND STANDARDISIERUNG

Auch wenn die Technologie in vielen Punkten nicht ausgereift ist und der Einsatz von Blockchains und elektronischen verteilten Journalen für Branchen und Geschäftsfelder noch nicht eindeutig definiert ist, sollte dennoch an Normung und Standardisierung auch zu Blockchains gedacht werden. Ein sehr wichtiger Punkt von Normung und Standardisierung, ist Terminologie und

[39] Siehe [Kannenberg, 2016].

Governance. Immer dann, wenn Experten aus unterschiedlichen Bereichen zusammenarbeiten, ist die Verständigung auf gemeinsame Definitionen, Begriffe und eine Ontologie wichtig. Hinzu kommt bei Lösungen, bei denen viele Systeme integriert werden müssen, die Notwendigkeit der Verständigung auf einen Technologierahmen (Technology Framework) und eine Referenzachitektur, in denen auch Schnittstellen definiert werden, um sowohl die Interoperabilität nach außen wie nach innen zu gewährleisten. Bei Blockchains bedeutet dies, z. B. festzulegen, wie private Blockchains interagieren, oder wie Blockchains in bestehende Systeme integriert werden können. Der Technologierahmen beschreibt aber auch welche Normen und Standards vorhanden sind und ggf. ergänzt werden müssen. Hier sind insbesondere ISO-IEC JTC 1 Normen im Bereich IT-Sicherheit, Skalierbarkeit, Webservices und IoT zu referenzieren.

Bei ISO wurde die Gründung eines neues Technical Committee (TC) für »Blockchain and distributed ledger technologies« beschlossen, um diese Aspekte von Anfang an zu berücksichtigen. Das deutsche Spiegelgremium bei DIN zum ISO/TC 307 »Blockchain and distributed ledger technologies« befasst sich daher unter anderem mit folgenden Punkten:

- Terminologie
- Governance
- Blockchain für diverse Branchen/Sektoren wie
  - Industrie 4.0
  - Finanzwirtschaft
  - Government
- Technology Framework

7. HANDLUNGSEMPFEHLUNGEN

Bislang hat nur Bitcoin als Blockchain-Anwendung einen breiten Bekanntheitsgrad. Bevor die Blockchain ein disruptives Potenzial entfalten kann, müssen noch einige Herausforderungen angegangen und die Eignung der Blockchain als technische Lösung zur dezentralen Vertrauensbildung beispielhaft gezeigt werden. Kapitel 5 zeigt dazu eine Reihe möglicher Einsatzszenarien auf. Staaten wie Schweden[40], Estland[41], Dubai[42], Großbritannien[43] oder auch einige Bundesstaaten in den USA haben sich bereits intensiv mit dem Thema befasst und teilweise eigene Blockchain-Strategien entwickelt. Die Blockchain wird früher oder später auch die deutsche Verwaltungslandschaft erreichen, sodass eine frühzeitige Auseinandersetzung lohnend erscheint.

Blockchain-Technologie beobachten und regulatorische Bedarfe identifizieren.
Deutschland steht bei der Beobachtung der Blockchain-Technologie, bis auf Ausnahmen wie das Finanzwesen, noch am Anfang. Fragen der Haftung für die (unerwünschten) Folgen automatisiert durchgesetzter Verträge oder der Ausgestaltung der Technologie aufgrund rechtlicher Vorgaben erfordern umfassende Untersuchungen. Da nationalstaatliche Regulierung hier nur bedingt wirkt, ist, wie bei anderen Digitalisierungsfragen auch, eine internationale und europäische Auseinandersetzung mit dem Thema notwendig.

Blockchain-Technologie selbst nutzen und Best-Practice-Beispiele entwickeln.
Erfahrung kann nur durch Ausprobieren gesammelt werden. Die Verwaltung sollte daher die eigenen Prozesse analysieren und hinsichtlich einer sinnvollen Umsetzbarkeit mit Blockchain-Technologie prüfen. Dazu müssen Experimentierräume geschaffen werden, die mit Pilotprojekten oder Feldversuchen einzelne Anwendungsfälle eruieren und dabei Erfahrung aufbauen und Best Practice-Beispiele entwickeln.

Mögliche Beispiele sind Kryptowährungen als E-Payment für Verwaltungsverfahren, wie in Zug (Schweiz)[44], öffentlich geführte Register oder die Absicherung digitaler Dokumente wie Ausbildungsnachweise oder Ähnliches.

Verwaltungsinterne Zusammenarbeit bei organisations- oder ebenenübergreifenden Prozessen kann ein geeignetes Einsatzgebiet sein. Der dezentrale Ansatz der Blockchain kommt der föderalen Verwaltungsstruktur zupass. Es wäre denkbar, dass Bund und Länder mit ihren Rechenzentren eine gemeinsame Blockchain-Infrastruktur für Verwaltungsdienste aufbauen.

Standardisierung vorantreiben
Derzeit ist die Entwicklung der Blockchain von proprietären Schnittstellen geprägt. Ein einheitlicher Standard existiert nicht. Dies erhöht die Abhängigkeit von einer proprietären Implementierung und wirkt sich negativ auf die Nachhaltigkeit aus. Die dringend notwendige Standardisierung hat gerade erst begonnen. Dieser Umstand bietet die Chance, von Beginn an bei der Standardisierung mitzuwirken und so die Weiterentwicklung beeinflussen zu können. Dabei müssen zunächst einheitliche Terminologien erarbeitet werden. Darüber hinaus sind Kriterien notwendig, nach denen Blockchain-Realisierungen kategorisiert oder gar zertifiziert werden können.

Hierfür müssen die entsprechenden Ressourcen und das notwendige technische Wissen vorhanden sein und ein gemeinsames Verständnis über Ziele und Ausgestaltung der Technologie entwickelt werden. Aus der Perspektive der öffentlichen Hand sind hierbei insbesondere Anforderungen für eigene Anwendungen und technische Möglichkeiten zur Umsetzung von Regulierungserfordernissen zu betrachten.

Die Weiterentwicklung aktiv gestalten
In Abschnitt 6.6 sind zahlreiche offene Fragen identifiziert worden, denen sich die Forschung in den kommenden Jahren widmen muss. Hierbei stehen nicht nur technische, sondern auch ethische Fragestellungen wie die gesellschaftlichen Auswirkungen der Blockchain-Technologie im Raum. Mit seinen Förderinstrumenten kann der Staat die Forschung in diesem Bereich vorantreiben. Hierfür ist jedoch ein über Ressorts und Ebenen hinweg abgestimmtes Vorgehen notwendig.

[40] [Chavez-Dreyfuss, 2016].

[41] [e-Estonia.com, 2015], [Buldas et al., 2013], [Buldas et al., 2014].

[42] [Kerr, 2016].

[43] [Government Office for Science, 2016], [Plimmer, 2016].

[44] [Higgins, 2016], [Condos et al., 2016].

8. BEGRIFFE

An dieser Stelle werden die wichtigsten Begriffe im Umfeld von Blockchains kurz beschrieben. Ausführlichere Beschreibungen und Diskussionen findet man beispielsweise in [ethereum, 2016c], [bitcoin, 2016a] oder [bitcoin, 2016b].

Account: Ein Account verbindet einen Nutzer der ➞ Blockchain (oder einen Vertrag/➞ Smart Contract) mit einer Adresse in der Blockchain. Sie gehört zu einem kryptografischen Schlüsselpaar, wobei der öffentliche Schlüssel die Adresse des Nutzers repräsentiert. Accounts können einen Zustand besitzen und sind in der Lage, Nachrichten zu empfangen oder zu versenden. Der Zustand (balance) wird in der Regel bei der Ausführung von ➞ Transaktionen modifiziert.

Bitcoin: Bitcoin ist eine Kryptowährung, d. h. eine digitale Währung basierend auf kryptografischen Prinzipien. Bitcoin basiert auf einem Blockchain-Ansatz.

Block: Ein Block ist eine Datenstruktur zur Speicherung validierter ➞ Transaktionen. Neben den Transaktionen beinhaltet ein Block u. a. den ➞ Hashwert seines Vorgängers.

Blockchain: Die Liste aller ➞ Blöcke wird als Blockchain bezeichnet. Sie beinhaltet die Historie und somit den Zustand des durch sie verwalteten Netzwerks.

Hash/Hashwert: Eine Hash-Funktion berechnet aus Daten, z. B. einem Dokument, Dateiinhalt oder auch ➞ Block, auf reproduzierbare Art und Weise eine zufällig wirkende Zeichenkette mit fester Größe (bspw. 32 Bytes). Aus diesem Hashwert ist kein Rückschluss auf das ursprüngliche Datum möglich. Andererseits verursachen bereits kleinste Änderungen an dem ursprünglichen Datum einen vollständig neuen Hash-Wert.

Konsens/Consensus: Zustand des ➞ Blockchain-Netzwerks, bei dem eine relevante Anzahl von Teilnehmern die gleichen ➞ Blöcke in ihre lokal validierte Blockchain eingefügt haben und dadurch die Korrektheit der in den Blöcken enthaltenen ➞ Transaktionen bestätigen.

Mining: Als Mining wird der Prozess bezeichnet, regelmäßig ➞ Transaktionen zu validieren, in ➞ Blöcken zusammenzufassen und mittels eines ➞ Proof of Work oder alternativen Mechanismus (bspw. ➞ Proof of Stake) in die ➞ Blockchain einfügen zu können. Er wird von Minern ausgeführt, wobei jeder Nutzer der Blockchain sich am Mining beteiligen kann.

Proof of Work: Eigenschaft eines ➞ Blocks, mit der nachvollziehbar sichergestellt werden kann, dass die ➞ Blockchain nicht beliebig mit Blöcken geflutet werden kann, sondern die Erzeugung eines Blocks statistisch gesehen nach einer konfigurierbaren Zeitspanne und durch unterschiedliche ➞ Miner erfolgt.

Proof of Stake[45]**:** Vergleichbar dem ➞ Proof of Work dient der Proof of Stake der Kontrolle des Wachstums der ➞ Blockchain. Dabei wird Nutzern, die sich als ➞ Miner »bewährt« haben, ermöglicht, die mathematischen Rätsel in einem beschränkten Lösungsraum zu lösen und somit weniger Rechenleistung zu verbrauchen.

Smart Contract[46]**:** Ein Smart Contract ist eine Software, »die rechtlich relevante Handlungen (insbesondere einen tatsächlichen Leistungsaustausch) in Abhängigkeit von digital prüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert, mit dessen Hilfe aber unter Umständen auch […] dingliche und/oder schuldrechtliche Verträge geschlossen werden können.«[47]

Transaktion: Eine Transaktion bezeichnet eine durch die ➞ Blockchain verwaltete Aktion. Die Aktionen müssen durch die Blockchain ausführbar sein (Anwendung, App) und validiert werden können. Transaktionen sind digital signiert. Sie besitzen in der Regel Angaben über eine Gebühr für die Validierung bzw. Ausführung.

Verteilte Anwendung (Decentralized Application kurz: DApp): Anwendungen definieren eine Art anwendungsspezifisches Overlay in einer ➞ Blockchain. Sie können von beteiligten Nutzern ausgeführt werden. Durch das Versenden von ➞ Nachrichten lösen sie ➞ Transaktionen aus. DApps sind in der Regel mit einem oder mehreren Kontrakten (➞ Smart Contracts) verbunden.

Verteiltes Register/Distributed Ledger: Distributed Ledger ist ein Sammelbegriff für verteilte elektronische Registerführung. Dabei kommen Konzepte für verteilte Datenbanken und Peer-to-Peer-Systeme zum Einsatz. Blockchain kann als eine technische Lösung für ein Distributed Ledger gesehen werden.[48]

Wallet: Als Wallet, d. h. als elektronische Brieftasche oder Börse, wird ein Blockchain-Client bezeichnet. Er ermöglicht den Zugang zum Blockchain-Netzwerk und erlaubt es dem Nutzer, einen Überblick über seine digitalen Güter zu erhalten und sie betreffende ➞ Transaktionen auszulösen.

---

[45] Für eine Diskussion des Begriffs »Proof of Stake« vergleiche man [Chan, 2016].

[46] Für eine Diskussion über Kontrakte vergleiche man [Burgwinkel, 2016] und [ethereum, 2016d].

[47] [Kaulartz und Heckmann, 2016].

[48] Siehe auch [Mainelli und Milne, 2015] und [Bitkom, 2016].

9. REFERENZEN

Aschwanden, Erich (2016): Stadt Zug wird weltweit zum Bitcoin-Pionier. Als international erste staatliche Behörde akzeptiert die Stadt Zug eine Kryptowährung. In: Neue Züricher Zeitung, 10.05.2016. http://www.nzz.ch/schweiz/crypto-valley-zukunftsmodell-oder-marketing-gag-ld.22911.

bitcoin (2016a): Developer Documentation. https://bitcoin.org/en/developer-documentation.

bitcoin (2016b): Einige Wörter, die Sie im Zusammenhang mit Bitcoin hören könnten. https://bitcoin.org/de/glossar.

bitcoin (2016c): Smart Property. https://en.bitcoin.it/wiki/Smart_Property.

bitcoin (2016d): Welcome to the Bitcoin Wiki. https://en.bitcoin.it/wiki/Main_Page.

BitFury Group; Garzik, Jeff (2015): Public versus Private Blockchains. Part 1: Permissioned Blockchains. White Paper. http://www.the-blockchain.com/docs/Jeff%20Garzik%20Public%20vs%20Private%20Blockchain%20pt1.pdf.

Bitkom (2016): Blockchain #Banking. Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien. Bitkom. https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Blockchain/161104-LF-Blockchain-final.pdf.

Blocher, Walter (2016): The next big thing: Blockchain – Bitcoin – Smart Contracts. Wie das disruptive Potential der Distributed Ledger Technology (nicht nur) das Recht fordern wird. In: Anwaltsblatt 2016 (8+9), S. 612-618.

Blundell-Wignall, A. (2014): The Bitcoin Question: Currency versus Trust-less Transfer Technology: OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing. http://dx.doi.org/10.1787/5jz2pwjd9t20-en.

Buldas, Ahto; Kroonmaa, Andres; Laanoja, Risto (2013): Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Secure IT Systems, Bd. 8208. Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 313-320. https://eprint.iacr.org/2013/834.pdf.

Buldas, Ahto; Laanoja, Risto; Truu, Ahto (2014): Efficient Quantum-Immune Keyless Signatures with Identity. https://eprint.iacr.org/2014/321.pdf.

Burgwinkel, Daniel (2016): Blockchains und Smart Contracts – Grundlage für neue disruptive Geschäftsmodelle? http://blockchain.jetzt/intro-de.

Chan, Ronald (2016): Consensus Mechanisms used in Blockchain. https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-chan.

Chavez-Dreyfuss, Gertrude (2016): Sweden tests blockchain technology for land registry, 16.06.2016. http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV.

Condos, James; Sorrell, William H.; Donegan, Susan L. (2016): Blockchain Technology: Opportunities and Risks. Vermont. http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf.

Delmolino, Kevin; Arnett, Mitchell; Kosba, Ahmed; Miller, Andrew; Shi, Elaine (2016): Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In: Jeremy Clark, Sarah Meiklejohn, Peter Y.A Ryan, Dan Wallach, Michael Brenner und Kurt Rohloff (Hg.): Financial Cryptography and Data Security, Bd. 9604. Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 79-94.

Deloitte LLP (2016): Blockchain applications in the public sector. Deloitte LLP. London. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf.

e-Estonia.com (2015): Keyless Signature Infrastructure. e-Estonia. https://e-estonia.com/component/keyless-signature-infrastructure/.

ethereum (2016a): A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper.

ethereum (2016b): Ether – The crypto-fuel for the Ethereum network. https://www.ethereum.org/ether.

ethereum (2016c): Glossary. https://github.com/ethereum/wiki/wiki/Glossary, zuletzt aktualisiert am 01.01.2016.

ethereum (2016d): The Greeter - Building a smart contract using the command line. https://www.ethereum.org/greeter.

Europäisches Parlament (23.07.2014): Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. eIDAS. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32014R0910.

Fromm, Jens; Welzel, Christian; Nentwig, Lutz; Weber, Mike (2015): E-Government in Deutschland: Vom Abstieg zum Aufstieg. Kompetenzzentrum Öffentliche IT. Fraunhofer FOKUS. http://www.oeffentliche-it.de/publikationen.

Gartner (2016): Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage. http://www.gartner.com/newsroom/id/3412017.

Government Office for Science (2016): Distributed Ledger Technology: beyond block chain. London. Online verfügbar unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Higgins, Stan (2016): Delaware to Seek Legal Classification for Blockchain Shares. CoinDesk. http://www.coindesk.com/delaware-government-blockchain-shares/.

ipima (2016): eGovernment MONITOR 2016. Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich. Initiative D21. http://www.egovernment-monitor.de/fileadmin/uploads/Studien/2016/160915_eGovMon2016_WEB.pdf.

Kannenberg, Axel (2016): Nach dem DAO-Hack: Ethereum glückt der harte Fork. heise.de. https://heise.de/-3273618.

Kaulartz, Markus (2016): Die Blockchain-Technologie. Hintergründe zur Distributed Ledger Technology und zu Blockchains. In: Computer und Recht 2016 (7), S. 474-480.

Kaulartz, Markus; Heckmann, Jörn (2016): Smart Contracts – Anwendungen der Blockchain-Technologie. In: Computer und Recht (9), 15.09.2016, S. 618-624.

Kerr, Simeon (2016): Dubai turns to blockchain for domestic challenges. The emirate is challenging tech developers to solve expensive problems. In: Financial Times, 06.10.2016.

Lischke, Matthias; Fabian, Benjamin (2016): Analyzing the Bitcoin Network. The First Four Years. In: Future Internet 8 (1), S. 7. DOI: 10.3390/fi8010007.

Mainelli, Michael; Milne, Alistair (2015): The Impact and Potential of Blockchain on the Securities Transaction Lifecycle. SWIFT Institute (SWIFT Institute Working Paper, 2015-007). https://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf.

Merkle, Ralph C. (1979): A Certified Digital Signature. Palo Alto. http://www.merkle.com/papers/Certified1979.pdf.

Weber, Mike et al. (2016): Prosument. In: Jens Fromm und Mike Weber (Hg.): ÖFIT-Trendschau. Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. https://www.oeffentliche-it.de/-/prosument

Nakamoto, Satoshi (2008): Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf.

Narayanan, Arvind (2016): Bitcoin and cryptocurrency technologies. A comprehensive introduction. Princeton, New Jersey: Princeton University Press.

Noizat, Pierre (2015): Blockchain Electronic Vote. In: David Lee Kuo Chuen (Hg.): Handbook of digital currency. Bitcoin, innovation, financial instruments, and big data. Academic Press S. 453-461.

O'Dwyer, K. J.; Malone, D. (2014): Bitcoin Mining and its Energy Footprint. In: IET Irish Signals and Systems Conference // Proceedings of the Joint 25th IET Irish Signals & Systems Conference 2014 & 2014 China-Ireland International Conference on Information and Communications Technologies. 26th-27th June 2014. University of Limerick. https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf.

Plimmer, Gill (2016): Use of bitcoin tech to pay UK benefits sparks privacy concerns. In: Financial Times, 12.07.2016.

Rehfeld, Dieter (2016): Die Blockchain. Hat sie das Potenzial, Gesellschaft und Wirtschaft neu zu gestalten? In: Benjamin Fadavian (Hg.): Transparente Staatstätigkeit. tredition, S. 25-42.

Röder, Dirk (2016): Netzwerk des Vertrauens: Blockchain. In: OBJEKTspektrum, 01.01.2016 (05/2016), S. 14-17.

Smith, James; Tennison, Jeni; Wells, Peter; Fawcett, Jamie; Harrison, Stuart (2016): Applying blockchain technology in global data infrastructure. Open Data Institute. http://theodi.org/technical-report-blockchain-technology-in-global-data-infrastructure.

Zhao, Zhichao; Chan, T.-H. Hubert (2016): How to Vote Privately Using Bitcoin. In: Sihan Qing, Eiji Okamoto, Kwangjo Kim und Dongmei Liu (Hg.): Information and Communications Security, Bd. 9543. Springer International Publishing (Lecture Notes in Computer Science), S. 82-96.

GEFÖRDERT VOM

Bundesministerium
des Innern

Fraunhofer
FOKUS

KONTAKT

Christian Welzel
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

ISBN: 978-3-9816025-6-2

kre | 1703 (Fotos: Fraunhofer FOKUS)