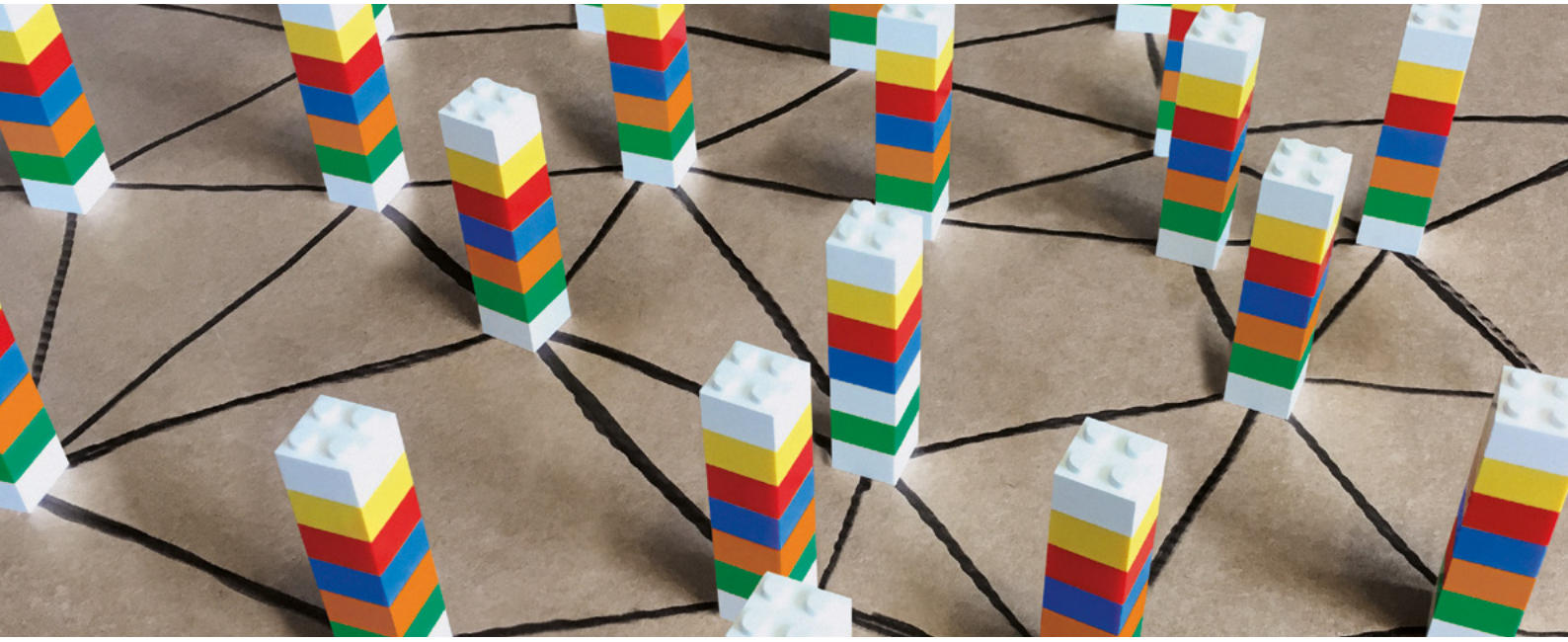
VDI Technologiezentrum

GESELLSCHAFT FÜR INFORMATIK



BLOCKCHAIN – EINE TECHNOLOGIE MIT DISRUPTIVEM CHARAKTER

01

Potenziale und Herausforderungen

März 2018
Version: 1.0

IMPRESSUM

Herausgeber:
VDI Technologiezentrum GmbH
VDI Platz 1
40468 Düsseldorf

Deckblatt und Design:
dombek design

Düsseldorf, im März 2018

INHALT

VORWORT

01

Liebe Leserin, lieber Leser,

Vertrauen ist gut, Blockchain ist besser – so könnte man die aktuelle Diskussion um diese Technologie beschreiben, die nicht weniger verspricht, als unbestechliche Konstante digitaler (Wert-)Transaktionen zu sein. Die wohl bekannteste Blockchain-Anwendung ist das digitale Zahlungssystem Bitcoin, doch die Anwendungsbereiche der Technologie sind vielfältig: Mobilität, Energie, Identitätswesen – Anwendungen sind in nahezu allen auf vertragliche Regelungen angewiesenen Bereichen denkbar. Ganz nebenbei könnte die Technologie neue sozio-ökonomische Standards setzen – etwa bei demokratischer Selbstverwaltung oder der Dezentralisierung im Produktions- und Dienstleistungssektor. Mit anderen Worten: Das mit Blockchain verbundene Potenzial ist enorm.

Unser Anliegen ist es, Ihnen einen einfachen und kompakten Einstieg in die Technologie zu ermöglichen. Was ist Blockchain? Was kann die Technologie schon heute – was ist in Zukunft denkbar? Welche zentralen Handlungsfelder ergeben sich aus sozialer, welche aus ökonomischer Sicht? Aber auch: Welche rechtlichen oder technischen Herausforderungen bestehen – z. B. bezüglich des Datenschutzes oder einer stabilen digitalen Infrastruktur? Anhand praktischer Fallbeispiele zu dezentralen Energiesystemen, Identitätsmanagement und autonomer Mobilität werden einige schon heute wirksame Anwendungsbereiche skizziert – inklusive der damit verbundenen Veränderungen und der existierenden Potenziale.

Die digitale Transformation erfasst mittlerweile sämtliche Lebensbereiche. Digitale Innovationen stoßen wichtige Veränderungen entscheidend an. Innovationszyklen werden immer kürzer. Um tiefgreifenden Wandel von Anfang an gestalten zu können, ist es essenziell, sich frühzeitig mit digitalen Neuerungen und deren Potenzialen zu befassen. Dazu gehört nicht zuletzt auch die Blockchain-Technologie.

Wir wünschen Ihnen eine anregende Lektüre!

Sascha Hermann
Geschäftsführer der
VDI Technologiezentrum GmbH

Prof. Dr.-Ing. Peter Liggesmeyer
Past President der
Gesellschaft für Informatik e.V.

VON BLOCKCHAIN, SMART CONTRACTS, TOKEN UND DAO - ERSTE BEGRIFFSBESTIMMUNGEN

02

Über dezentrale Datenbanken, Computer-Protokolle mit „Wenn… Dann…"-Logik, digitale Verbriefungen und Organisationsbindungen ohne Verträge

Was ist Blockchain? - Eine Blockchain ist eine dezentrale Datenbank.

Technisch gesehen ist eine Blockchain eine dezentrale, auf vielen Computern verteilte Datenbank, mit der Aufzeichnungen von Transaktionen hinterlegt werden, die für jeden Teilnehmer dieser Blockchain einsehbar sind. Die Computer, die an einer Blockchain teilnehmen, sind über das Internet vernetzt und bilden damit ein Blockchain-Netzwerk.

In jeden neuen Datensatz („block") wird eine kryptografische Prüfsumme (Hashwert) der bisherigen Kette („chain") von Datensätzen geschrieben, sodass eine Manipulation der Daten durch einzelne Teilnehmer im Prinzip unmöglich ist. Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt, durch das die Reihenfolge der Datensätze in der Blockchain festgelegt wird. Das Verfahren zum Erstellen und Anfügen der Blöcke wird als Blockchain-Protokoll bezeichnet. Es gibt verschiedene Varianten von Blockchain-Protokollen, in denen der Konsensmechanismus unterschiedlich umgesetzt ist.

Aufgrund des dezentralen Konsensmechanismus wird eine Blockchain zu einer dezentralen und unveränderlichen Aufzeichnung von Datensätzen, die für jeden Teilnehmer dieser Blockchain einsehbar ist. Um einen Datensatz in einer Blockchain zu fälschen, müssten der Block mit dem Datensatz und alle nachfolgenden Blöcke neu berechnet und auf der Mehrzahl der Rechner in diesem Blockchain-Netzwerk weltweit verändert werden. Ein solcher Angriff kann für lange Blockchains ausgeschlossen werden, auch weil er nicht ökonomische Mengen an Zeit, Rechenleistung und Energie kostet.

In einer Blockchain sind also die Daten und die Reihenfolge, in der sie in diese geschrieben wurden, gegen Veränderungen gesichert. Damit eignen sie sich, um Transaktionen von digitalen Informationen oder physischen Gütern zu speichern.
Durch die Manipulationssicherheit der Daten über einzelne Transaktionen und ihre Reihenfolge können digitale Daten nicht von einem Netzwerkteilnehmer mehrfach und an unterschiedliche andere Netzwerkteilnehmer transferiert werden (double spending problem).

Blockchains sind in Teilen einem Buchführungsjournal (Grundbuch der Buchführung) ähnlich.
Das dezentrale Konsensverfahren verbessert die Sicherheit von Transaktionsdaten gegen Manipulationen im Vergleich zu einem zentralen System, sodass mit dem Verfahren keine vertrauenswürdige dritte Instanz mehr benötigt wird, die die Integrität eines Datensatzes bestätigt. Man könnte auch sagen: „Viele Zeugen ersetzen den Notar."

Die Aufzeichnung der Ereignisse wird von vielen Parteien geteilt und Informationen, die einmal eingegeben wurden, können nicht verändert werden, da die nachgelagerte Kette Upstream-Transaktionen verstärkt. Der dezentrale Konsensmechanismus wird nicht unbedingt für alle Anwendungen benötigt, stellt aber eine sehr sichere Verwahrung der Daten dar. Insbesondere für andere Verfahren sollte jeder Nutzer der Blockchain mit einer digitalen Signatur identifiziert und authentifiziert sein.

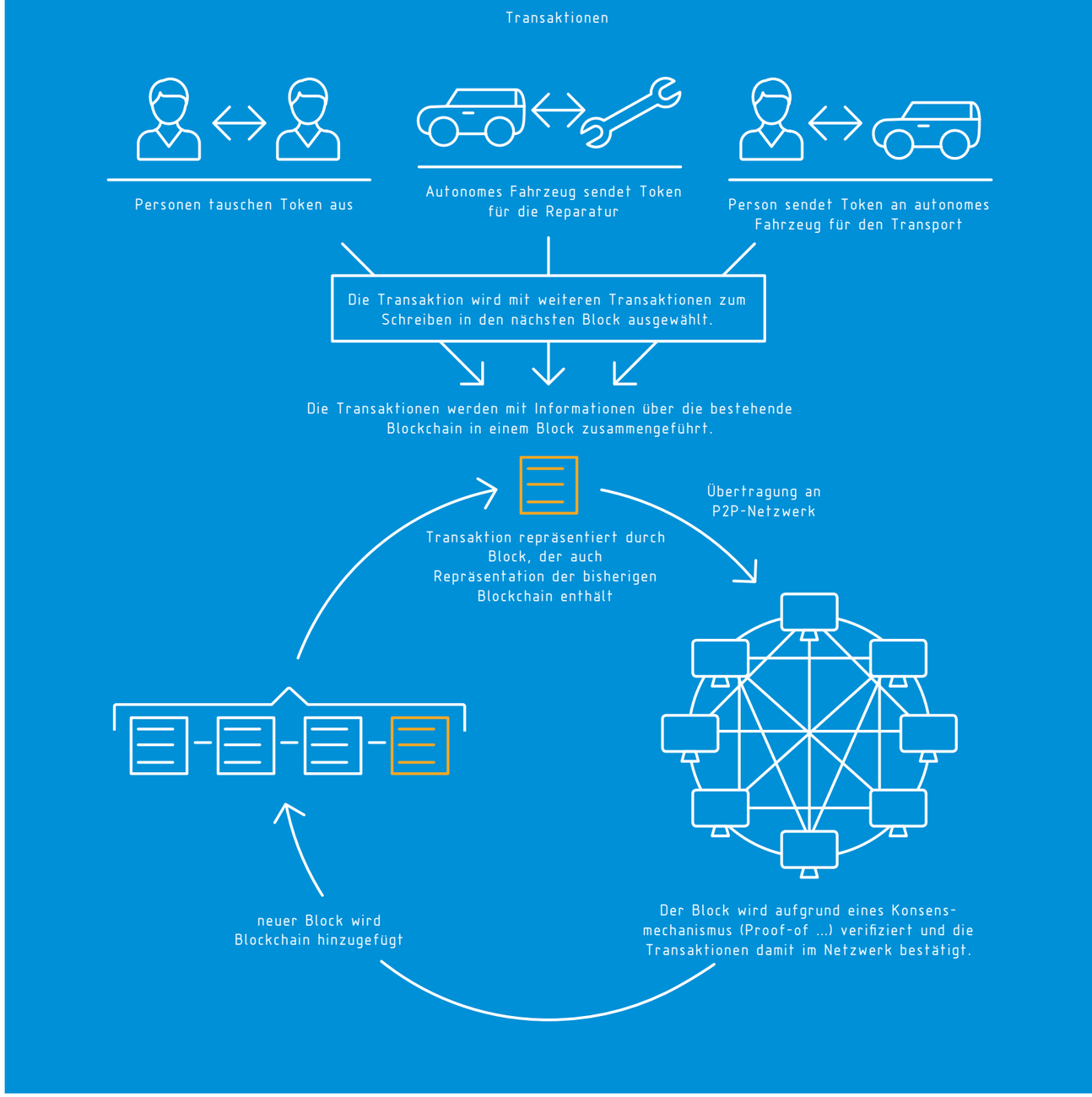


Abbildung 1: Die Blockchain ist eine dezentrale Datenbank, mit der Aufzeichnungen von Transaktionen hinterlegt werden.

Die erste weitverbreitete und mittlerweile sehr bekannte Anwendung, die seit 2009 auf einer Blockchain basiert, ist das dank Internet weltweit verwendbare, dezentrale und staatlich nicht regulierte Zahlungssystem „Bitcoin". Der Zahlungsverkehr wird simultan von unterschiedlichen Computern abgewickelt und gespeichert, sodass kein Kreditinstitut als übergeordnete Institution nötig ist. Ebenso wird sichergestellt, dass die virtuellen Geldeinheiten nicht mehrfach ausgegeben werden können – die im Internetzeitalter ansonsten mühelose Kopierbarkeit von Information ist also nicht gegeben. Die Erzeugung von neuen Geldeinheiten geschieht innerhalb des Bitcoin-Systems durch die Bereitstellung von Rechenleistung für die aufwendigen kryptografischen Berechnungen beim Mining, die den Akteuren vergütet wird.

Und was ist ein Smart Contract?

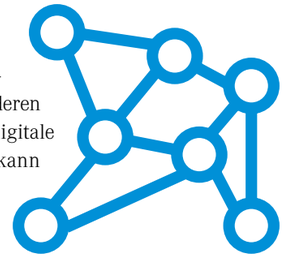
Mittels Blockchain-Technologie lassen sich neben Transaktionsdaten auch sogenannte Smart Contracts und deren Ausführung manipulationssicher dokumentieren. Solche Smart Contracts könnten beispielsweise die Beurkundung von Dokumenten und Transaktionen oder elektronische Stimmabgaben abwickeln, ohne Beteiligung von Intermediären wie Notaren oder behördlichen Institutionen. Smart Contracts stellen regelbasierte Systeme dar, die die Umsetzung der Rechte aller Vertragspartner automatisch durchsetzen. Die Idee von Smart Contracts ist gute 20 Jahre älter als die von Blockchains. Im Prinzip handelt es sich um Computerprotokolle, die Verträge in „Wenn ...-Dann ...“-Logiken abbilden oder in diesem Sinne Vertragserfüllungen überprüfen. Solche Computerprotokolle sind damit auch in der Lage, einfache Verhandlungen und Abwicklungen von Verträgen technisch zu unterstützen oder selbst abzuwickeln, denn diese „Wenn ...-Dann ...“-Schleifen können weitgehend beliebige Geschäftskonstellationen aus allen wirtschaftlichen Bereichen abdecken.

Mit der zunehmenden Digitalisierung von Geschäftsprozessen ist die Komplexität der eingesetzten Smart Contracts und insbesondere die Notwendigkeit der sicheren Dokumentation der Abwicklung der Smart Contracts gewachsen. Dafür bietet die Blockchain-Technologie die Lösung und hat damit erst ein schnell wachsendes Interesse an der Idee der Smart Contracts ausgelöst. Denn mit der Blockchain wird der Smart Contract selbst und die Dokumentation von dessen Abwicklung nicht veränderbar und für jeden Teilnehmer transparent.

Da Smart Contracts eben nicht „Smart“ sind, sondern nur die Dinge abwickeln, die im Sinne der „Wenn ...-Dann ...“-Logik vorgegeben sind, sind auch nicht alle Eventualitäten geregelt und machen unter Umständen auch den menschlichen Eingriff erforderlich. Das liegt auch daran, dass man zwar in einem Smart Contract bestimmte Eventualitäten berücksichtigen kann, die vollständige Berücksichtigung geltenden Rechts in „Wenn...-Dann...“ Logiken eines Smart Contracts aber als zu komplex gilt.

Token - die Verbriefung in der Blockchain

Ein Token in einer Blockchain ist letztlich ein Eintrag in der Blockchain. Der Besitz des Tokens ergibt sich dadurch, dass der Besitzer den Schlüssel hat, mit dem er einen neuen Eintrag in der Blockchain erzeugen und damit den Besitz an jemand anderen übertragen kann. Der Token kann als eine digitale Verbriefung verstanden werden. Der Token kann intrinsisch oder asset-backed sein. Native Token von Blockchains wie Bitcoin oder Ethereum sind Teil des Anreizsystems, um eine heterogene Gruppe von Personen, die sich weder kennen noch vertrauen, dazu zu bringen, gemeinsam das Blockchain-Netzwerk zu bilden. So verfügt der native Token des Bitcoin-Netzwerks, der sogenannte Bitcoin, über Token-Governance-Regeln, die auf einem Anreizmechanismus bestimmen, unter welchen Umständen Bitcoin-Transaktionen validiert und neue Blöcke erstellt werden.



DAO - dezentrale autonome Organisation

Klassische zentralisierte Organisationen besitzen üblicherweise hierarchische Managementebenen, entlang derer ein Regelsystem festgelegt und umgesetzt werden soll. Letztlich verantwortet die Geschäftsführung zentral den Geschäftsbetrieb. Dagegen können mit einem Blockchain-Netzwerk derartige Top-down-Governance-Strukturen aufgelöst und dezentrale autonome Organisationen (DAOs) entwickelt werden. In einer DAO sind Personen nicht durch klassische Verträge gebunden, sondern durch Tokens mit einem transparenten Anreizmechanismus.

Über die Autoren

◀ Dr. Jan Christopher Brandt
ist Leiter des Kompetenzteams Digitale Transformation bei der VDI Technologiezentrum GmbH. Er berät nationale und internationale Kunden aus Politik und Verwaltung zu digitalen Innovationstrends und der Gestaltung der digitalen Transformation. Er war und ist an zahlreichen Leuchtturmprojekten wie der „Plattform Industrie 4.0“ oder der nordrhein-westfälischen Plattform „Wirtschaft und Arbeit 4.0“ beteiligt. Er ist Autor und Co-Autor verschiedener Studien zu digitalen Innovationen und Geschäftsmodellen und deren Finanzierung sowie zum digitalen Wandel in Wirtschaft und Arbeit.

◀ Thomas Werner
ist seit 2004 Technologieberater in der Abteilung Innovationsbegleitung und Innovationsberatung der VDI Technologiezentrum GmbH. Zu den Arbeitsschwerpunkten zählen die Methodenweiterentwicklung und Umsetzung in softwarebasierte Lösungen, insbesondere im Bereich Wissensmanagement und Wissenstransfer. Fachliche Schwerpunkte liegen bei Informationstechnologien, Algorithmentheorie, semantischen Technologien, der explorativen Datenanalyse, Information Retrieval sowie der Szenario-Technik als Methode der Zukunftsforschung. Herr Werner hat zahlreiche Zukunftsprospektionsprojekte mit der Szenario-Technik für Institutionen und Unternehmen durchgeführt und ist Autor und Co-Autor verschiedener Studien zu digitalen Innovationen unter anderem im Auftrag des Bundesministeriums für Bildung und Forschung.

MOBILITÄT NACH UBER & CO. 03

Wie Blockchain die Basis autonomer Mobilität bilden kann - und gleichzeitig auf eine direktdemokratische Ebene hebt

Weltweit kämpfen Städte gegen Schadstoffbelastung und verstopfte Straßen - beides Ergebnis eines Fokus auf das Automobil. Ökonomisch ist das unsinnig, denn die meisten Autos eines Verkehrsraums fahren nur durchschnittlich 50 Kilometer pro Tag. Etwa 23 Stunden am Tag verbrauchen sie Platz beim Parken und verlieren an Wert. In Uber & Co. manifestiert sich ein gesellschaftliches Umdenken: Die Plattformen vernetzen weltweit Fahrer und Mitfahrer - die Anzahl der Fahrzeuge sinkt. Doch die nächste Disruption für die Uber-schüttelte Taxi-Branche steht unmittelbar vor der Tür: Autonom fahrende Robo-Taxis werden den Markt von hinten aufrollen.

Erst Blockchain schafft die Infrastruktur für eine Mobilitätswende

Mit der Blockchain-Technologie frisst die Digitalisierung ihre Kinder. Open-Source verbündet sich mit urdemokratischen Abstimmungsverfahren zum Frontalangriff auf neue Mobilitätsplattformen wie Uber, Lyft, blablacar oder Didi. Mobilität wird zum Allgemeingut, der Preis wird deutlich sinken. Die technologischen Voraussetzungen gibt es bereits oder sie sind in absehbarer Zeit verfügbar: Elektrofahrzeuge mit genügend Reichweite für den Stadtverkehr, autonom fahrende Autos - und die Blockchain-Technologie als technische Grundlage eines Netzwerks von Fahrzeugen, das sich selbst gehört und verwaltet.

Mit autonom fahrenden Autos sinkt der Preis für eine gefahrene Meile von circa 2 US-Dollar bei einem Uber-Fahrzeug auf etwa 0,30 US-Dollar. In Kombination mit dem öffentlichen Nahverkehr sorgt der Preisverfall für eine permanente Verfügbarkeit von individueller oder gemeinsamer Mobilität in Städten und bald auch im Umland. Diese Rundumversorgung macht das eigene Auto für viele Bürger immer uninteressanter.

Von den genannten 30 US-Cent pro Meile zweigt ein Plattform-Betreiber für autonom fahrende Autos

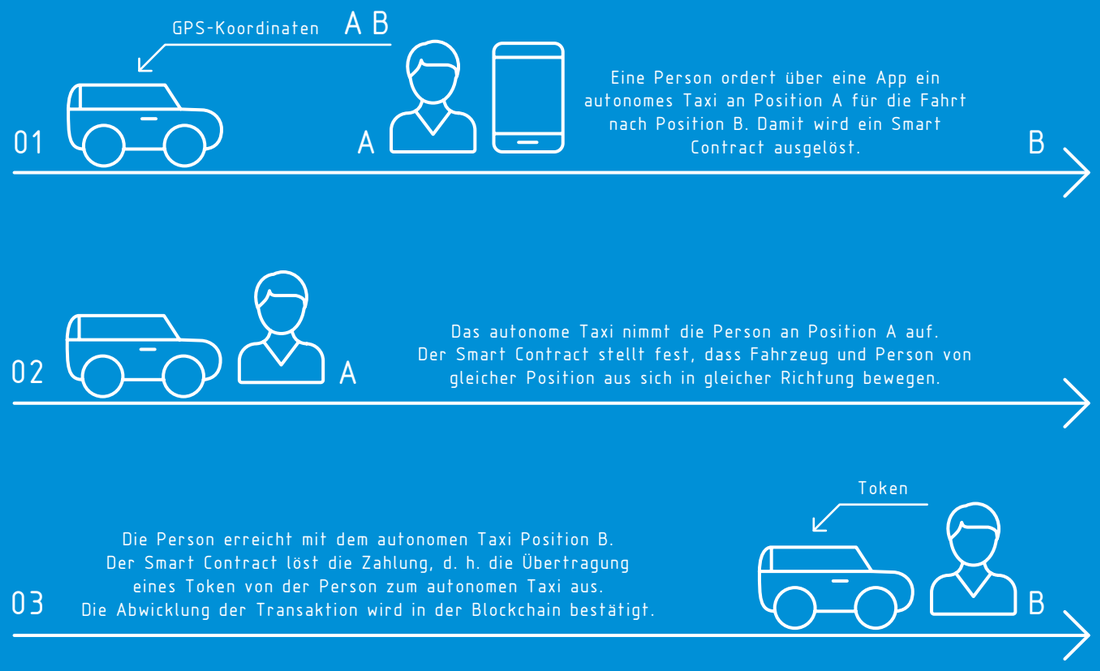
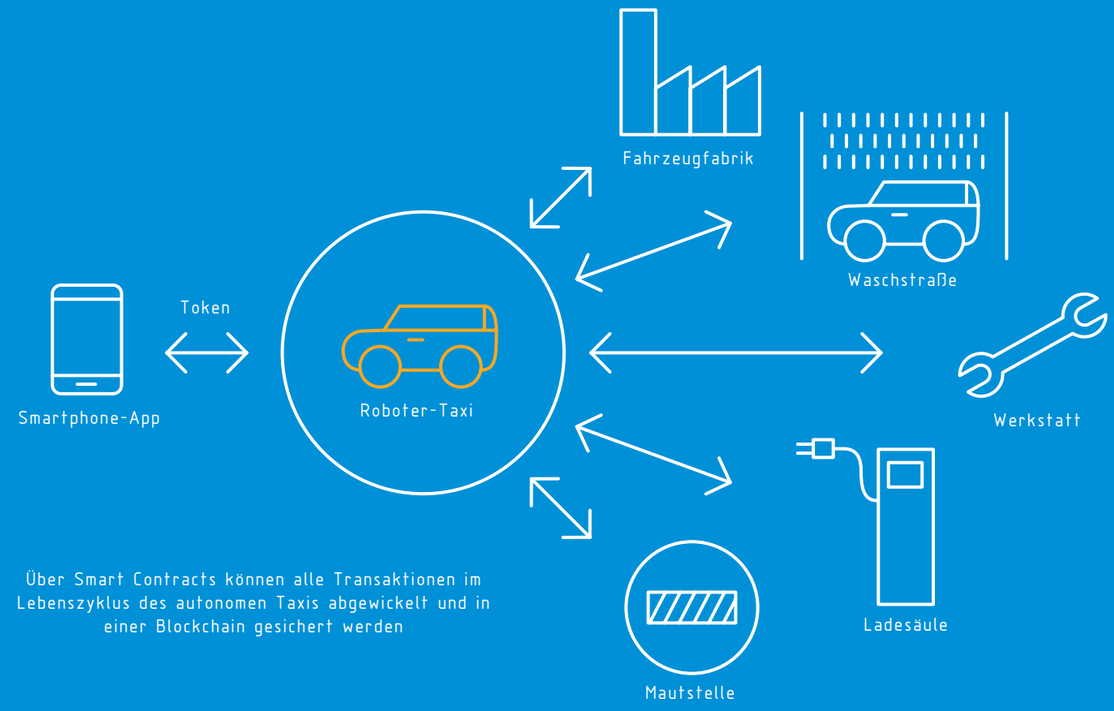


Abbildung 2: Blockchain als Unterbau für eine autonom fahrende Robo-Taxi-Flotte



Über Smart Contracts können alle Transaktionen im Lebenszyklus des autonomen Taxis abgewickelt und in einer Blockchain gesichert werden

Abbildung 3: Dokumentation aller Transaktionen über Smart Contracts

seine Provision ab. Den Aufschlag verdient er für die Vermittlung zwischen Fahrgast und Auto und der Abwicklung der Transaktion inklusive einer „Garantie“, dass der Fahrgast abgeholt und zum Ziel gebracht wird. In der Regel arbeitet der Vermittler nicht kostendeckend, sondern mit Gewinnabsicht. Was wäre, wenn es keinen Betreiber gibt, der Geld verdienen muss?

Mobilität zum Selbstkostenpreis

Hier grätscht die Blockchain-Technologie in naher Zukunft in die Geschäftsmodelle der neuen Mobility-Anbieter. Sie eignet sich als Unterbau für den Betrieb einer autonom fahrenden Robo-Taxi-Flotte. Mit Smart Contracts sinken die Transaktionskosten erheblich. Eine Robo-Taxi-Flotte könnte sich mit der unbestechlichen und manipulationssicheren Technologie selbst managen und muss dabei „nur“ kostendeckend arbeiten. Kurz: Robo-Taxis machen Mobilität mit niedrigen Transaktionskosten und ohne Gewinnabsicht verfügbar.

Eine mobilityDAO organisiert die Robo-Taxis einer Stadt unter festgelegten Parametern. „DAO“ steht für „Decentralised Autonomous Organisation“. Dahinter verbirgt sich eine Organisationseinheit, die sich selbst verwaltet und nach den Regeln der Teilhaber funktioniert. Als Teilhaber kommen z. B. alle Bürger einer Stadt infrage – sie können demokratisch über die Rahmenbedingungen für ihr Mobilitätsangebot abstimmen. Mit diesen Regeln ausgestattet ist die mobilityDAO ein sich selbst verwaltender Algorithmus, der Robo-Taxis an Interessenten vermittelt, die Fahrzeuge regelmäßig warten lässt und natürlich deren Bedarf kontinuierlich der Anfrage anpasst. Die Fahrzeuge gehören sich quasi selbst und verfolgen keinerlei Gewinnabsichten.

Da Maschinen das Konzept „Vertrauen“ nicht verstehen, muss eine andere Instanz ein Äquivalent für die Maschinen herstellen. Hier kommt die Blockchain ins Spiel: „Vertrauen“ ist Teil ihrer DNA, sie garantiert gegenüber anderen Teilnehmern die Vertrauenswürdigkeit der Robo-Taxis im allgemeinen Wirtschaftsverkehr. Die Transaktion zwischen Robo-Taxi und Mitfahrer – bestehend aus Buchung und Abrechnung – wird automatisch, das bedeutet: ohne Zwischeninstanz, über die Blockchain abgewickelt.
Über die Tokens der mobilityDAO wird der Preis vor der Fahrt beim Mitfahrer reserviert und beim Erreichen der vereinbarten GPS-Koordinate automatisch durch einen Smart Contract abgebucht. Die reservierten Tokens stellen für das Robo-Taxi sicher, dass der Fahrgast die Fahrt bezahlen wird. Der Fahrgast hat die Garantie, seinen gewünschten Zielort zum vereinbarten Preis zu erreichen. Das Protokoll auf der Blockchain mit den dazugehörigen Smart Contracts dokumentiert Zielwunsch, GPS-Koordinaten der Fahrt und Preis nachvollziehbar und transparent auf der Blockchain. Damit lassen sich bei Beschwerden Fakten schaffen.

Die Interaktion mit einem Fahrgast ist nur eine von vielen Transaktionen, die ein Robo-Taxi täglich abschließt. Mit anderen sichert es seinen Unterhalt: Es macht selbsttätig Geschäfte mit Waschstraßen, Werkstätten, Mautstellen oder Stromtankstellen. Alle diese Vorgänge sind Beispiele für Maschine-zu-Maschine-Kommunikation. Hier stehen sich zwei Apparate im Wirtschaftsleben gegenüber, die Entscheidungen treffen müssen und dafür zuverlässige Daten brauchen. Die Blockchain schafft diese Basis – und damit das Äquivalent zu Vertrauen zwischen Maschinen.

Mobilität als Vorreiter für „liquid democracy“

Eine Grundanlage der Blockchain ist, dass sie dezentral ist. Das könnte in einer Stadt durch die Bürger sichergestellt werden: Jeder Einwohner stellt seinen Computer für das Netzwerk bereit und unterstützt so die verteilte Struktur der Blockchain. Die Kosten für den Betrieb der DAO sind auf viele Schultern verteilt und das unternehmerische Ziel der schwarzen Null sorgt für niedrige Gebühren des Mobilitätsangebots. Darüber hinaus bietet es sich an, jedem teilnehmenden Bürger eine Stimme zu geben. Sie werden zu Teilnehmern einer DAO und stimmen über Entscheidungen ab bzw. geben die Rahmenbedingungen vor. So beeinflussen die Bürger direkt die Fortentwicklung der für sie bereitgestellten Mobilitätsgüter. Dieses Verfahren der direkten Demokratie nennt sich „liquid democracy“.

Für Plattformen wie Uber & Co. ist in diesem Szenario kein Platz mehr – durch ihre Gewinnabsicht können sie nicht mit den Preisen eines gemeinnützigen Angebots konkurrieren.

Über den Autor

◀ **Dirk Röder**
von MaibornWolff berät Unternehmen bei Blockchain- und Transformationsprojekten. Mit spielerischen Mitteln, wie dem Digital Venture Game oder Blockchain Game, entwirft er neue Geschäftsmodelle, digitalisiert Produkte oder passt bestehende an neue Gegebenheiten an.

ENERGIEMARKT AUF AUGENHÖHE 04

Wie die Blockchain-Technologie eine diskriminierungsfreie Energie-Marktkommunikation schafft und das Rückgrat des künftigen Energiesystems werden kann

Vertrauen ist gut, Vertrauensmaschinen sind besser

Die Energiewirtschaft befindet sich in einem radikalen Umbruch. Die Digitalisierung und das Internet der Dinge (IoT) sollen neue Geschäftsmodelle ermöglichen und Anlagenoptimierungen effizienter gestalten. Treiber dieses Umbruchs sind jedoch weder die Digitalisierung noch das IoT, sondern die Dezentralisierung und die damit verbundene Demokratisierung der Produktionsmittel – kurz: die Energiewende. Vor dem Hintergrund dieses Produktionsmodellwechsels, weg von der brennstoffkostenbasierten Erzeugung hin zu Energie-Investition, entsteht das Problem der Skalierung und Synchronisation dieser verteilten Produktionsmittel. Die Transaktionskosten wirken sich aufgrund der vielen kleinen, dezentralen Kraftwerke mit spezifisch geringerer Stromerzeugung verhältnismäßig stärker aus. Die relative Erhöhung der Wertschöpfungskosten wirkt sich wiederum auf das bisherige Modell der institutionalisierten Marktkommunikation über den Austausch von Nachrichten im edi@energy-Datenformat aus. Da eine diskriminierungsfreie Marktkommunikation jedoch die Grundlage für gegenseitiges Vertrauen der Marktakteure ist, eröffnet die Blockchain-Technologie allen Marktakteuren die Möglichkeit, Kraftwerksprojekte überhaupt umzusetzen und die erzeugte Strommenge gewinnbringend zu vermarkten. Somit ermöglicht die Blockchain-Technologie als dezentral verwaltetes Register zum Speichern, zur Auslesung und zum Verarbeiten von Transaktionen bei gleichzeitiger systemimmanenter Verifizierung – kurz: als „Vertrauensmaschine" – nicht nur eine revolutionäre Art der Marktkommunikation, sondern auch eine echte Marktintegration Erneuerbarer Energien.[1)]

Die Blockchain-Technologie – Rückgrat der Energiewirtschaft 2.0

„Mit Ablauf des Jahres 2020 werden [...] etwa 6.000 Windenergieanlagen mit einer Leistung von rund 4,5 Gigawatt aus der EEG-Vergütung fallen."[2)] Diese Prognose der deutschen WindGuard verdeutlicht, wie groß die Welle der Dezentralisierung und damit die Notwendigkeit einer kostengünstigen Marktkommunikation für die energetische Versorgungssicherheit und den Klimaschutz sind. Bei einem durchschnittlichen Spotmarktpreis von knapp unter 3ct/kWh und Betriebskosten von rund 3,5 ct/kWh ist ein wirtschaftlicher Weiterbetrieb der Anlagen unmöglich.[3)] Da eine ähnliche Entwicklung auch bei PV-Anlagen zu erwarten ist, sind alternative Vermarktungsmöglichkeiten zum Handel an der Strombörse für die Anlagenbetreiber unabdingbar. Aus Sicht der Regulierung ist es hierbei wichtig, dass die Marktregeln so geschaffen sind, dass eine Versorgungssicherheit mit hoher Güte möglich ist. Dies kann bei einem Punkt-zu-Punkt-Austausch von Nachrichten nicht gelingen. Es wird also notwendig, eine Methode zu finden, die einen zentralen Marktkonsens herstellt, die Durchführung der Marktaktivität jedoch dezentral und möglichst feingranular vornimmt.

In der bestehenden Praxis wurde durch Aggregation der Prognosen bei den EEG vergüteten Anlagen ein Konsens hergestellt und die Anzahl der miteinander zu kommunizierenden Akteure möglichst gering gehalten. Spätestens mit dem vermehrten Auslaufen der EEG-Vergütung in einer Post-2020-Ära müssen jedoch neue Mechanismen greifen, um Versorgungssicherheit auch bei einem offenen Markt zu garantieren.

1) Seffinga; Lyons; Bachmann (2017) 2) Wallasch; Lüers; Rehfeldt (2016) 3) Ebd.

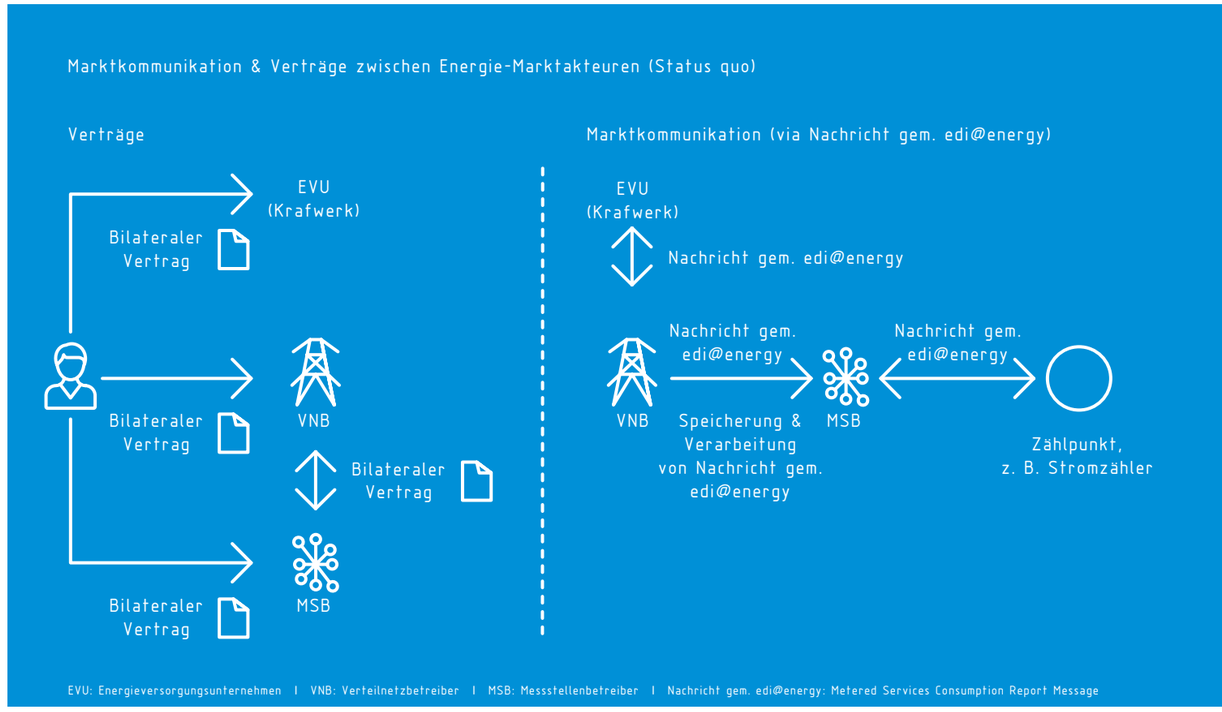


Abbildung 4: Marktkommunikation via Nachricht gem. edi@energy

Ich kommuniziere, also bin ich

„Ein wichtiger Schlüssel für das Gelingen der Digitalisierung der Energiewirtschaft ist eine funktionierende und zukunftsfähige Marktkommunikation".[4)] Doch wie funktioniert das derzeitige, standardisierte Nachrichtenformat zur Übertragung von Energiedaten und wie zukunftsfähig ist es? Um allen Akteuren entlang der energiewirtschaftlichen Wertschöpfungskette einen einheitlichen Informationsstand und effiziente Geschäftsprozesse zu ermöglichen, wurde das edi@energy-Datenformat, welches auf dem EDIFACT Standard zur Übertragung elektronischer Daten im Geschäftsverkehr basiert, eingeführt. Die drei Hauptakteure, Messstellenbetreiber (MSB), Verteilnetzbetreiber (VNB) und Energieversorgungsunternehmen (EVU), mit welchen der Stromkunde jeweils bilaterale Verträge abschließt, können somit Energiemarktdaten kommunizieren und die Bilanzkreise bewirtschaften (siehe Abbildung 4).

Dreht ein Stromzähler nun um eine Kilowattstunde weiter, so wird dieser Vorgang über eine Nachricht gem. edi@energy-Format an den MSB gesendet. Dieser wiederum ist dazu verpflichtet, diese Nachricht an den VNB zu kommunizieren. Bei jedem Prozessschritt muss sichergestellt werden, dass die Daten richtig verarbeitet und versandt werden. Die damit verbundenen Hard- und Softwarekosten machen es Betreibern kleiner Anlagen wirtschaftlich beinahe unmöglich, beispielsweise die Verfügbarkeit von Anlagen im Markt zu kommunizieren. Es lässt sich festhalten: Für die derzeit 2.361 beim Bundesverband der deutschen Energie- und Wasserwirtschaft (BDEW) gemeldeten Unternehmen[5)] der Energiewirtschaft funktioniert diese Marktkommunikation – wenn auch zu hohen Infrastrukturkosten. Für Millionen dezentraler Marktakteure ist diese Art der Kommunikation weder diskriminierungsfrei noch zukunftsfähig. Es ist diesen schlicht nicht möglich, zu wettbewerbsfähigen Preisen energetische Leistungsverfügbarkeiten in den Markt zu kommunizieren. Mehr noch: Es wäre grob fahrlässig, das bestehende Verfahren auf eine größere Akteursanzahl auszubilden, da zu jedem Zeitpunkt Konsens darüber bestehen muss, dass Angebot und Nachfrage auf gleicher Höhe sind. Ansonsten ist die Versorgungssicherheit massiv gefährdet.

4) BDEW (2017) 5) Ebd.

Die Autonomisierung der Marktkommunikation – der Stromkunde als vollwertiger Marktakteur

Im Energiemarkt der Zukunft gilt es also, die Kommunikation einer signifikant höheren Anzahl von Marktakteuren in immer komplexeren Wertschöpfungsketten zu tatsächlich diskriminierungsfrei niedrigen Transaktionskosten zu organisieren. Und genau hierfür ist die Blockchain-Technologie ideal geeignet. Sie ermöglicht nicht nur einen Datenaustausch ohne zentrale Steuerungs- und Regulierungsinstanz auf Basis schlüssiger, nachvollziehbarer Handlungen der Marktakteure, sondern auch die Transparenz und Verifikation desselben. Die Transaktionskosten und damit auch die Kosten der Prozesssicherheit sind gegenüber der edi@energy-Kommunikationsarchitektur signifikant geringer. Der Hauptgrund hierfür ist der gegenseitige Nachweis der Teilnehmer des Blockchain-Netzwerks, dass jeder Prozessschritt genauso wie spezifiziert auch durchgeführt wurde. Der bis dato mehrstufige Prozess der Akkumulation, Verarbeitung und Weitergabe unter der Prämisse der Datensicherheit wird damit nicht nur schneller, sicherer und transparenter, sondern faktisch autonomisiert (siehe Abbildung 5).

Autonomisiert deshalb, weil nun nicht mehr die Instanzen MSB, VNB und EVU im Mittelpunkt der Kommunikation stehen, sondern der Stromkunde (ggf. Prosumer) selbst. Durch den Abschluss eines den BDEW-Vorgaben zur Marktkommunikation entsprechenden Vertrags mit dem VNB und dem MSB ist der Stromkunde „gridborne“. Da VNB- und MSB-Vertrag „on-chain“ vorliegen, also über eine Schnittstelle zur Blockchain-Technologie verfügen, kann der Energie-Service-Provider über einen sogenannten „Role-Look-up“ sicherstellen, dass diese Verträge tatsächlich vorliegen.[6)] Der Wandel vom EVU hin zum Energie-Service-Provider zeigt deutlich, dass nun der Stromkunde selbst zum geschäftsfähigen Marktakteur emanzipiert wird (siehe Abbildung 5). Er ist es, der im Role-Look-up die notwendigen Verträge (VNB & MSB) für den Energie-Service-Provider zur Verfügung stellt und der erstmalig zu wirtschaftlichen Transaktionskosten seinen Bedarf oder sein Angebot an elektrischer Energie kommunizieren kann. Waren es früher Zentralbibliotheken mit hunderten von Büchern, so ist es heute Google. War es früher die edi@energybasierte Marktkommunikation, so ist es heute die „energychain” der STROMDAO UG. Doch was bedeutet das für die Dezentralisierung und Digitalisierung der Energiewirtschaft?

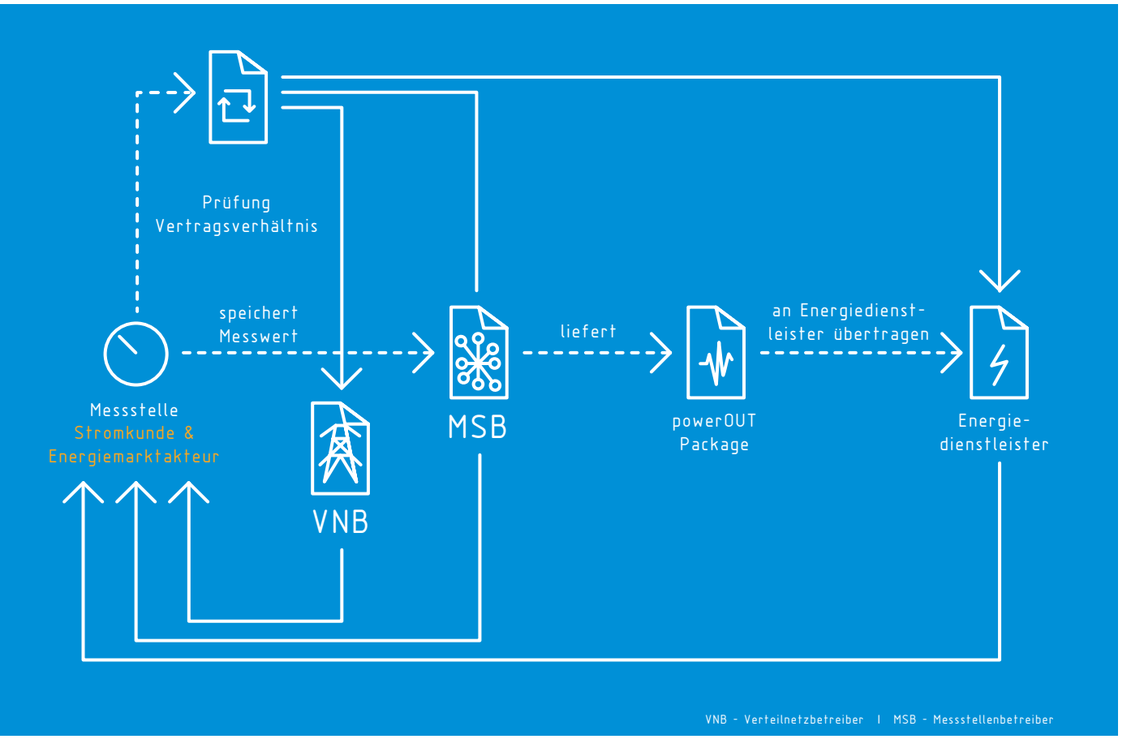


Abbildung 5: Autonomisierte Marktkommunikation via Blockchain

6) Ebd.

Das Ende der Kilowattstunde

Ein weiterer Grund für die „Welle der Dezentralisierung“ ist, neben dem Auslaufen der EEG-Vergütung, auch der Wandel von operativen Kosten hin zu Investitionskosten der Kraftwerke. Während konventionelle Kraftwerke vergleichsweise hohe Betriebskosten (unter anderem Brennstoffkosten, Zertifikatskosten für CO_2-Emissionen) aufweisen, sind bei EE-Anlagen die Investitionskosten entscheidend.[7)] Letztere jedoch spielen am Terminmarkt, also dem Verkauf von Energiemengen auf einen Zeitpunkt in der Zukunft, kaum eine Rolle.[8)] Das liegt im Wesentlichen daran, dass ein Großteil des Stroms aus EE-Anlagen, welche gem. Erneuerbarem-Energien-Gesetz (EEG) einspeisen, über den Spotmarkt, also kurzfristig, verkauft werden muss.[9)] Der Planungssicherheit – und damit auch der Bereitschaft von Investoren, zukünftig in EE-Anlagen zu investieren – läuft das entgegen. Hier ist ein grundsätzliches Umdenken erforderlich. Was würde passieren, wenn anstelle der Kilowattstunden zukünftig Anteilsscheine an EE-Anlagen verkauft werden? Private und gewerbliche Stromkunden könnten sich dann Anteile an einem Portfolio und damit einen gewissen Grad an energetischer Autarkie sichern. Die erzeugten Kilowattstunden des Anlagenportfolios können über die Marktkommunikation via Blockchain zweifelsfrei dem jeweiligen Eigner zugewiesen werden. Der aufgrund der fluktuierenden Einspeisung zu beschaffende Reststrom wird von konventionellen Kraftwerken bereitgestellt. Investoren von EE-Anlagen haben in diesem Hybridstrom-Markt einerseits eine deutlich verbesserte Prognostizierbarkeit der Rentabilität. Andererseits wird die Direktvermarktung zu wirtschaftlichen Prei-

7) transentis consulting (2017) 8) Gorgs (2017) 9) Agentur für Erneuerbare Energien (2017)

sen auch für Altanlagenbesitzer möglich. Schlussendlich profitiert der Stromkunde sowohl durch eine Emanzipation zum vollwertigen Marktakteur als auch durch vergleichsweise günstige und vor allem langfristig stabile Strompreise.[10] Das EVU wird zum Energie-Service-Provider, dessen Hauptaufgabe in der Konfektionierung, d. h. der Anpassung des Energie-Erzeugungsportfolios auf das Verbrauchsprofil des Stromkunden, besteht. Die Kilowattstunde als Vermarktungsinstrument weicht dem Anteilsschein an individuell zugeschnittenen Anlagenportfolios.

Zu gut, um wahr zu sein

Die „Vertrauensmaschine“ Blockchain kann in Ihrer Funktion als „Marktkommunikationsmittel” und „Herkunftsnachweiser von Kilowattstunden” zum Bindeglied der Marktakteure werden und den Stromkunden emanzipieren. Ein allumfänglicher Problemlöser ist sie deshalb nicht. Die oftmals beschworene Botschaft, dass im Strommarkt der Zukunft EVUs keine Rolle mehr spielen, ist nicht absehbar. Dass sich deren Rolle innerhalb des Energiemarktes jedoch radikal wandeln wird, liegt auf der Hand. Und um oft angebrachte Kritik hinsichtlich der Legalität des Einsatzes der Blockchain-Technologie im Energiemarkt vorwegzunehmen: Die Marktkommunikation via Blockchain ist nicht illegal. Die vom BDEW festgelegten Kriterien können eins zu eins in übliche Papierverträge oder Smart Contracts gefasst und anschließend genau wie spezifiziert ausgeführt werden. Will man eine tatsächliche Digitalisierung und Dezentralisierung der Energiewende erreichen, ist die Nutzung der Blockchain-Technologie derzeit alternativlos.

Über die Autoren

◀ Stefan Thon
ist Experte für anwenderorientierte Gestaltung interaktiver Systeme und Dienstleistungen. Er war 4 Jahre als Interaction Designer bei Intel tätig und an der Entwicklung und Erforschung neuer Technologien und Geschäftsfelder in den Sparten Gesundheitsforschung, Diagnostik und Gesundheitspflege beteiligt. Seit Ende 2014 ist er Mitgründer/Geschäftsführer bei Sunride GmbH, mit Schwerpunkt auf der Entwicklung und Vermarktung von Softwarelösungen für dezentrale Versorgungsmodelle, wie z. B. Mieterstrom. Als Mitgründer und Kurator der STROMDAO beschäftigt er sich seit Ende 2016 mit der Entwicklung und Vermarktung von Blockchainanwendungen im Energiesektor.

Manuel Utz ▶
beschäftigte sich nach dem Studium des Wirtschaftsingenieurwesens intensiv mit Fragen innovativer Energieeffizienz-Technologien, die ihn zu seiner Position als Energiemanager in einem Großkonzern führten. Zweieinhalb Jahre lang leitete er dort das Energieeffizienzteam, bevor er 2017 die STROMDAO UG mitbegründete. Zusätzlich promoviert Manuel Utz derzeit im Bereich der Anwendungen der Blockchain-Technologie in der Energiewirtschaft.

◀ Thorsten Zoerner
ist Experte für Datenanalyse und IT-Systemarchitekturen und hat bereits frühzeitig begonnen, die datentechnischen Grundlagen der Stromversorgung zu analysieren. 2007 entstand „blog.stromhaltig“ als Sammlung von Anekdoten aus der täglichen Praxis zwischen Marktdaten und Netzbetrieb. 2015 wurde von ihm maßgeblich der Hybridstrommarkt entwickelt, welcher als Blaupause für den Strommarkt 2.0 und die Digitalwende angesehen werden kann. Bei der STROMDAO wurden diese theoretisch entwickelten Szenarien in die Praxis umgesetzt: ein neues Modell für einen Stromversorger.

10) Zörner (2015)

IDENTITÄTSMANAGEMENT ALS BLOCKCHAIN-ANWENDUNGSFELD

05

Dieser Beitrag erörtert die Rolle von Identitätssystemen in einer vernetzten Welt, aktuelle Herausforderungen und wie blockchainbasierte Technologien Lösungsansätze liefern können

Blockchain ist ein Protokoll, das auf dem herkömmlichen Internet aufbaut und den Werteaustausch revolutioniert. Es ermöglicht zum ersten Mal echte P2P-Transaktionen ohne intermediäre Clearingstelle. Menschen, die sich nicht kennen und nicht vertrauen, können in Zukunft basierend auf Blockchain und anderen dezentralen Protokollen Geld überweisen (Bitcoin), Strom handeln (Smart Grids), Gebrauchsgegenstände des Alltags vermieten – von Autos bis Waschmaschinen und Rasenmähern (Slock.it) – um hier nur einige wenige Beispiele zu nennen. Die Rolle, die früher Banken, Stromkonzerne oder Autovermieter innehatten, kann nun durch Blockchains und Smart Contracts ersetzt werden. Bürokratie und Vertrauen wird durch Code ersetzt.

Bedeutung von Identitätsmanagement im Internet

Die Basis solcher P2P-Transaktionen – ob zwischen Mensch und Maschine oder Maschine und Maschine – ist eine vertrauenswürdige Identität. Historisch wurden Identitäten durch zentrale hoheitliche Instanzen vergeben: staatliche oder semi-staatliche Behörden, die Identitäten von Menschen und Gegenständen feststellen, zertifizieren und dokumentieren.

In einer zunehmend internationalen, technologisierten und vernetzten Welt ist es notwendig, dass wir herkömmliche Standards, wie Identitäten ausgestellt und zertifiziert werden, überdenken. Es gibt noch wenige, die sich mit diesem Thema auseinandergesetzt haben. Federführend ist hier die Initiative „Rebooting Web of Trust“[1] und insbesondere dessen Initiator Christopher Allen, der auch einiges zu dem Thema geschrieben hat[2].

Mit diesem Grundverständnis ermöglichen Blockchain und andere dezentrale Technologien neue Formen des Identitätsmanagements, die nicht nur effizienter sind, sondern auch die Privatsphäre von Individuen besser schützen und somit Gesetzgebungen wie der Europäischen Datenschutzgrundverordnung[3] (GDPR)[4] gerecht werden.

Aktuelle Herausforderungen

Seit dem Einzug des Internets in den 1990er Jahren bestimmen Onlinedienste in zunehmendem Maße unsere täglichen Interaktionen - im Privaten, in der Arbeit und mit den Behörden. Damit Menschen diese nutzen können, benötigen sie eine digitale Identität, die allerdings derzeit noch viele Probleme aufweist.

Als das Web ursprünglich entwickelt wurde, dachte man noch nicht an die Notwendigkeit von digitalen Identitäten. Daher schien es am einfachsten, das Konzept hoheitlicher Identitäten aus der analogen Welt in die digitale Welt zu übernehmen. Doch wie sich in den vergangenen 25 Jahren gezeigt hat, werden diese traditionellen Identitätskonzepte den Herausforderungen einer vernetzten Welt nicht gerecht, da viele nationalstaatliche Instanzen keine oder sehr schwer durchsetzbare Hoheitsgewalt auf viele Akteure in einem globalen Internet haben.

Außerdem mussten wir erst lernen, dass digitale Identitäten uns vor neue Herausforderungen stellen, wie etwa die Frage: Wie kann ich im digitalen Raum beweisen, dass ich wirklich die Person bin, die ich angebe zu sein? Betrug und Identitätsdiebstahl im Internet stellen Unternehmen wie auch Privatperso-

1) weboftrust.info/ 2) Allen (2016) 3) dsgvo-gesetz.de/ 4) Datenschutz-Grundverordnung: de.wikipedia.org/wiki/Datenschutz-Grundverordnung

© panthermedia.net / Jakub Krechowicz

nen vor große Probleme. 33 Prozent der Internetnutzer waren schon einmal in der einen oder anderen Form davon betroffen. Der durchschnittliche Schaden liegt bei € 1.366. Das erklärt auch, warum viele staatliche Institutionen und Unternehmen darauf bestehen, ihr eigenes, vermeintlich sicheres Identitätssystem zu unterhalten.

In einer zunehmend vernetzten Welt, in der wir nun auch alle Geräte miteinander vernetzen (Internet der Dinge) und mit Blockchain neue Formen von automatisierten Interaktionen einführen, bedarf es eines neuen Identitätssystems, das auch den Anforderungen einer vernetzten und durch dezentrale Instanzen gesteuerten Welt gerecht wird.

Dies ist jedoch nicht trivial. Um ein dezentrales Identitätssystem zu bauen, das höhere Sicherheit und zusätzliche Vorteile gegenüber den bisherigen Lösungen aufweist, müssen sowohl Betrug und Identitätsdiebstahl verhindert werden als auch die Netzwerkeffekte jenseits der heutigen liegen. Und genau diese Vorteile versprechen dezentrale Technologien mit Blockchain zu ermöglichen. Gleich ob staatliche Identitäten oder bisherige Online-Identitäten, beide sind aktuell in ihrer Interoperabilität, der Sicherheit und damit auch in ihrer Anwendung beschränkt. Blockchain und andere dezentrale Zukunftstechnologien können dem Abhilfe schaffen. Der Nutzer kann in Zukunft seine eigene Identität schaffen und sie in vertrauenswürdiger Form anderen Nutzern mitteilen. Hat der Nutzer einmal bewiesen, wer er ist, kann er diese Information immer wieder verwenden, ohne seine Daten erneut bei einem Dienstleistungsanbieter verifizieren, registrieren und somit speichern zu müssen.

Herkömmliche Identifikationssysteme

Der Staat kann an jemanden eine eindeutige Identifikationsnummer ausgeben. Aber die Zahl selber sagt kaum etwas aus. Wenn Sie allerdings mit einem Namen und dem Geburtsdatum einer Person verbunden wird, weiß man schon mehr. Fügt man ein Foto, biometrische Merkmale[6], eine Telefonnummer, Adresse oder Zeugnisse hinzu, kann man diese Informationen sinnvoll in einer Vielzahl von Anwendungsfällen nutzen, um zu beweisen, wer man ist. Nun sind Menschen nicht die Einzigen, die Identitäten haben. Juristische Personen wie Unternehmen (Handelsregisternummer) oder Organe der öffentlichen Hand oder Gegenstände (Eigentum) können auch eine Identität haben (z. B. Seriennummer). Die Attribute, die in der Identität festgehalten werden, helfen anderen zu entscheiden, ob die Information für eine Transaktion (Geschäft) ausreicht - z. B. zur Eröffnung eines Bankkontos, zum Verkauf einer Flasche Wein und so weiter. Gleiches gilt für juristische Personen und Vermögenswerte. Identitäten, oder eher bestimmte Attribute, die mit der Identität verknüpft sind, helfen anderen zu entscheiden, ob ein Geschäft mit dem entsprechenden Eigentümer, Vertreter oder Verwalter eingegangen werden kann.

Jedes Mal, wenn eine Person oder ein Unternehmen in Interaktion mit einer anderen Person oder Unternehmen tritt, müssen für alle Akteure Identitäten in zentral gespeicherten Datenbanken angelegt werden. Dies führt zu (a) Datenredundanzen, verursacht (b) hohe administrative Kosten sowie eine (c) Einschränkung der Datensouveränität für den Einzelnen.

Nun erstellt nicht nur jeder Staat und jedes Unternehmen ein eigenes System (Datenbank in der Identitätsdaten gespeichert sind), sie gehen auch davon aus, dass sie Eigentümer der Systeme und Daten sind, woraus wiederum ein Eigentumsanspruch auf die Identitäten, und somit aller damit verbundenen Daten, abgeleitet wird. Bislang haben wir das so akzeptiert, vor allem auch deswegen, weil wir in der analogen Welt Organe brauchten, denen wir vertrauten, um unsere Identitäten zu verwalten.

Neue Lösungsansätze für verteilte Identitätssysteme

Es gibt ein zunehmendes Verständnis dafür, dass wir uns weg von zentralen – und somit geschlossenen – Identitätslösungen hin zu verteilten Identitätslösungen bewegen müssen, die mehr Interoperabilität aufweisen. Derzeit stehen verschiedene Ansätze für eine Blaupause für ein neues digitales Identitätsmanagement zur Diskussion.

Das World Economic Forum[7] favorisiert hierfür Banken. Als Vorteil wird hier gesehen: (a) Banken als vertrauenswürdige Instanzen, (b) international verteiltes Netzwerk, (c) unterliegen in den meisten Ländern strenger staatlicher Regulierung (KYC)[8].

Auf der anderen Seite gibt es die Mobilfunkanbieter, die einen Standard für digitale Identitäten entwickelt

5) PWC (2016) 6) oeffentliche-it.de/trendsonar

7) WEF (2016) 8) wirtschaftslexikon.gabler.de/Definition/know-your-customer-prinzip-kyc.html

haben. Dieser Standard - Mobile Connect - soll dabei helfen, die Barriere zu reduzieren, eine vertrauenswürdige digitale Identität erwerben zu können[9]. Dies ist insbesondere deswegen wichtig weil es weltweit 2,4 Milliarden undokumentierte Menschen gibt, die keine staatlich anerkannten Dokumente haben, um sich für ein Bankkonto zu registrieren.

Als dritte Gruppe positionieren sich die marktbeherrschenden sozialen Netzwerke wie Google, Amazon, Facebook, Apple (auch GAFA genannt) als Identitätsanbieter, die sich in den letzten 15 Jahren im Internet als neue Identitätsanbieter positioniert haben. Ihre Vorteile sind weite Verbreitung international und hohe Netzwerkeffekte durch single-sign-on[10]-Lösungen für Drittanbieter. Diese Firmen unterliegen aber weniger strengen Regularien – KYC und Datenschutz – als Banken und Mobilfunkanbieter, insbesondere in Ländern wie beispielsweise China oder den USA.

Alle diese Lösungen bieten sich an, können jedoch den bestehenden Herausforderungen (Datenredundanzen, hohe administrative Kosten, Einschränkung der Datensouveränität und Privatsphäre) nicht ausreichend gerecht werden, da sie alle eins gemeinsam haben: Es sind in sich geschlossene Systeme, die miteinander konkurrieren und die Daten der betroffenen Individuen und Organisationen besitzen.

Eine weit sinnvollere Lösung wäre ein komplettes Umdenken: Die wichtigste Rolle, die Identitätsanbieter von heute erfüllen, ist das vertrauenswürdige Verifizieren von personenbezogenen Daten. Diese Rollen sollen und können sie auch in Zukunft weiterhin einnehmen. Um aber den angesprochen Herausforderungen gerecht zu werden, müssen wir das Besitzen der personenbezogenen Daten vom Verifizieren der Daten trennen. Blockchain in Kombination mit anderen dezentralen Standards und Protokollen bieten hierzu eine Grundlage. Die Identitätsanbieter von heute könnten sich mit so einem System in Zukunft auf ihre Kernkompetenz konzentrieren: das Verifizieren von personenbezogenen Daten.

Selbst-souveräne Identität: Verifizieren statt Identifizieren

Eine verteilte und selbst-souveräne Lösung sollte daher nach einem gemeinsamen Rahmen aufgebaut werden, damit die Interoperabilität[11] von Merkmalen, Attributen und Anforderungen der Identitäten sichergestellt ist. eIDAS hat die Notwendigkeiten für Interoperabilität von Identitätsdaten bereits definiert. Dies muss nur noch im Kontext von selbst-souveränen Identitäten technisch umgesetzt werden.
Entscheidend ist dann, ob die Attribute, die dieser Identität zugeschrieben werden, auch in einer Weise geprüft und verifiziert werden können, die es Dritten ermöglicht, dieser Information zu vertrauen.
Exakt der gleiche Prozess wie bei konventionellen Identitätsmanagementsystemen heute, nur mit entscheidenden Vorteilen:

- **Vollständige Souveränität & Privatsphäre**
  Die Identität gehört einer Person. Identität mit einer Identifikationsnummer wird von einer Person selbst generiert und gehört nur ihr, ähnlich wie bei einer staatlichen Identifikationsnummer. Da die Daten in der Kontrolle der Nutzer liegen, ist das Prinzip von Privacy-by-Design automatisch berücksichtigt (GDPR).

- **Verifizierung statt Identifizierung**
  Statt Identitäten auszustellen, verifizieren Staat und Firmen Attribute, die zu einer Identität gehören, und zwar so, dass sie nicht verfälscht werden können; dazu kann auch die Zuteilung einer weiteren Identifikationsnummer gehören.

- **Interoperabilität**
  Die Identitäten und Daten können plattformübergreifend genutzt werden. Um Interoperabilität zu erreichen, ist die eIDAS-Verordnung 31 der EU[12] ein gutes Beispiel. Sie bildet einen Rahmen für die gegenseitige Anerkennung unter den nach ihren Normen festgelegten und verwalteten digitalen Identitäten der Mitgliedstaaten. Während die nationalen Regierungen immer noch das Vorrecht haben, die elektronische Identifizierung zu ermitteln, sind die anderen europäischen Mitgliedsstaaten verpflichtet, sie anzuerkennen. Herausforderung hierbei ist, dass Interoperabilität global gedacht werden muss, um die Benutzererfahrung tatsächlich zu vereinfachen und viele Anwendungsfälle erst zu ermöglichen. Eine eigene Identität zu besitzen, muss allen Menschen, Firmen und Institutionen gleichermaßen ermöglicht werden. Nur dies kann zu einer Gesellschaft des Miteinanders und einem gemeinsamen Markt führen.

9) GSMA (2016) 10) Single Sign-on: de.wikipedia.org/wiki/Single_Sign-on 11) Kubicek; Noack (2010) 12) Durchführungsverordnung (EU) 2015/1501 des Rates vom 8. September 2015 über den Interoperabilitätsrahmen gemaß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifikations- und Treuhanddienste für elektronische Transaktionen im Binnenmarkt

Vorteile von selbst-souveränen Identitäten

- Verwandlung von Identitätsdiensten (kostenintensiv) hin zu Verifikationsdiensten (kostensparend). Dies fördert auch Innovation und Wirtschaftswachstum.

- Einbindung und Integration aller Menschen in gesellschaftliche Aktivitäten, die einer Identität bedürfen. Dies ist insbesondere in Anbetracht der Flüchtlingsproblematik ein Thema. Laut UN müssen 2,4 Mrd. Menschen ohne jegliche Identität auskommen[13].

- Auflösen von Identitäts-Monopolen: Durch Sicher-stellung der Interoperabilität und die konsequente Nutzung von technischen Spezifikationen, Standards und Verfahren würde man die Wettbewerbsprobleme und Monopolbildungen im Identitätsbereich auflösen, bei denen bislang dominante Spieler den Zugang zu einem bestimmten digitalen Identitätssystem kontrollieren oder (aus-)nutzen. Konkret ist hier GAFA (Google-Amazon-Facebook-Apple) gemeint, wobei allein Facebook 2 Milliarden (Stand Juli 2017)[14] Nutzer angibt, die eine Facebook-Identität nutzen und diese Identität zum Authentifizieren bei Drittanbietern verwenden.

Die Implementierung von dezentralen und souveränen digitalen Identitäten wird ein globales dezentrales digitales Identitätsnetzwerk ermöglichen, welches kulturelle und rechtliche Faktoren sowie die individuellen Bedürfnisse der Nutzer berücksichtigt und Langlebigkeit und Interoperabilität sicherstellt. Diese vollkommen souveränen Identitäten, welche unter verschiedenen Identitätssystemen entstehen können, erlauben es von anderen Systemen erkannt und genutzt werden zu können.

Voraussetzungen

- Die Identität muss der Person gehören, also souverän sein; dadurch entsteht eine Identität, die nicht nur ein nutzer-zentrisches Gefühl vermittelt, sondern auch so aufgebaut ist.

- Es muss eine offene und robuste neue Identitätslösung geschaffen werden, d. h. sie muss langlebig und verlässlich sein.

- Interoperabilität ist fester Bestandteil einer dezentralen und souveränen Identität.

- Unterstützung von Regierungsbehörden, um rechtliche Grundlagen für die Neuausrichtung bestehender und neuer Identitätsdienste aufzubauen.

- Respekt der Privatsphäre von Personen, einschließlich der Einbettung von Privacy-by-Design-Prinzipien im Sinne von GDPR.

Anwendungsbeispiele, die in die richtige Richtung gehen

Die unten aufgeführten Beispiele setzen bereits teilweise Interoperabilität so um, dass unterschiedliche Identitätssysteme Daten untereinander erkennen.

(a) Mobile Connect ist ein digitales Identitätssystem, dass die Benutzer über ihr Gerät authentifiziert, sodass Benutzer auf eine Vielzahl von Diensten zugreifen können. Dies beseitigt die Notwendigkeit für Benutzer, viele Benutzernamen und Passwörter zu haben, um auf Online-Dienste zuzugreifen. Mobile Connect ist ein Standard, der auf OpenID Connect aufbaut.

(b) TUPAS ist ein finnisches Identitätssystem, in dem über zehn Banken als Identitätsanbieter agieren. Einzelpersonen können sich in eine breite Palette von Online-Dienstleistern mit den Anmeldeinformationen von ihrer Bank anmelden. Die vollständigen Namen und die nationalen ID-Nummern der Benutzer werden vom Identitätsanbieter zum Online-Dienstleister übertragen.

Über die Autoren

◀ Joachim Lohkamp
ist Unternehmer und Tech-Enthusiast. Derzeit ist er Gründer und CEO von Jolocom, einem Berliner Start-up, das dezentralisierte Tools entwickelt, mit denen Personen ihre eigene digitale Identität generieren können, um die Verknüpfung und Zuordnung von Daten zu unterstützen. Außerdem ist Joachim ein Konnektor für Ouishare, Mitgründer und Vorstandsmitglied des Blockchain Bundesverband e.V. sowie Advisor für den Blockchain Hub.

◀ Dr. Shermin Voshmgir
ist die Direktorin des Instituts für Kyptoökonomie an der Wirtschaftsuniversität Wien und Gründerin des BlockchainHubs, einem Informations-Hub und Thinktank in Berlin, der weltweit interdisziplinär die Entwicklung der Blockchain-Technologie vorantreibt, kommuniziert und diskutiert. Die promovierte Wirtschaftsinformatikerin ist eine gefragte Vortragende, berät Unternehmen zu relevanten Blockchain-Anwendungen sowie Regierungsorganisationen bezüglich notwendiger Neugestaltung der Gesetzgebung. Zusätzlich zu ihrem Wirtschaftsinformatik-Studium hat Shermin die Filmschule in Madrid besucht. Ihre langjährige Arbeitserfahrung reicht von Consulting bis Internet-Start-ups und der Kreativindustrie. Als gebürtige Wienerin mit iranischen Wurzeln pendelt sie zwischen Wien und Berlin.

13) Weltbank (2015) 14) allfacebook.de/toll/state-of-facebook

BLOCKCHAIN – SICHERE IDENTITÄTEN FÜR DIE GESELLSCHAFT 4.0? 06

Individual perSonal data Auditable addrEss Number (ISAEN) als Beispiel für die Anwendung der Blockchain-Technologie

Die Blockchain ist die Technologie, die derzeit wohl die größten Hoffnungen auf eine sichere, zuverlässige und gerechte Digitalisierung schürt. Sie wird als eine zentrale Schlüsseltechnologie der Zukunft gehandelt. Das Weltwirtschaftsforum prognostiziert, dass bis 2027 mindestens zehn Prozent des gesamten Weltbruttoinlandsprodukts in einer Blockchain abgespeichert sein werden. Ob im Finanzsektor, im Energiebereich oder im Handel – es gibt kaum eine Branche, die sich keine Gedanken macht, wie sie die Blockchain-Technologie sinnvoll nutzen kann. Dabei ist das Prinzip der Blockchain denkbar einfach: Jede Transaktion – sei es eine Überweisung, ein Grundstücksverkauf oder ein Vorgang bei einer Versicherung – wird in einem Datenblock gespeichert. Die Speicherung erfolgt nicht zentral, keine Bank, Behörde oder anderer Intermediär ist involviert. Dafür übernimmt ein Netzwerk aus zahlreichen Rechnern diese Aufgabe und jeder Knoten dieses Netzwerks enthält eine Kopie aller Datenblöcke. Die Computer innerhalb des Netzwerks sind miteinander verbunden und agieren gleichberechtigt. Gespeichert werden die Datenblöcke damit dezentral auf allen Rechnern des Netzwerks.

Security by Design – Sicherheit als Grundlage der Technologie

Um Manipulationen zu vermeiden, sind im Blockchain-Code verschiedene Sicherheitsmechanismen eingebaut. So wird die Rechtmäßigkeit jeder Transaktion im Vorhinein automatisch geprüft, etwa ob eine Person, die Geld überweisen möchte, überhaupt über den entsprechenden Betrag verfügt. Dazu muss die Mehrheit der Rechner im Netzwerk der Transaktion zustimmen. Ist die Zustimmung erteilt, erfolgt die Transaktion. Verwehren die Computer jedoch ihre Zustimmung, kann auch die Transaktion nicht erfolgen. Das heißt umgekehrt auch, eine Manipulation der Blockchain ist nur mit enormer Rechnerleistung möglich. Zusätzlich sind die Erstellung und die Verschlüsselung des Datenblocks geschützt: Im Falle der Bitcoins wird ein schweres mathematisches Rätsel generiert und den im Netzwerk verfügbaren Rechnern gestellt. Der Rechner, der das Rätsel als erstes lösen kann, erstellt den Datenblock und erhält für die (enorme) erbrachte Rechenleistung eine Aufwandsentschädigung in Form von Bitcoin.

Die Anwendung des persönlichen Identifiers ISÆN

Eine sinnvolle Anwendung der Blockchain ist die Datenschutz- und Verschlüsselungstechnologie ISÆN – Individual perSonal data Auditable addrEss Number. Sie soll es Bürgerinnen und Bürgern ermöglichen, die Kontrolle über ihre personenbezogenen Daten im Internet zu behalten und die Datenspeicherung bzw. -verarbeitung transparent und nachvollziehbar zu gestalten. Mit ISÆN können betroffene Personen jederzeit feststellen, wer welche personenbezogenen Daten über sie verarbeitet und darüber hinaus die erteilte Zustimmung zur Verarbeitung und Weitergabe auch jederzeit einschränken. Das Konzept wurde in Frankreich entwickelt und seine Anwendbarkeit im Rahmen der Begleitforschung des Technologieprogramms „Smart Data - Innovationen aus Daten“ des Bundesministeriums für Wirtschaft und Energie (BMWi) untersucht.

Werden beim Einkauf in einem Webshop beispielsweise Angaben des Käufers wie Name, Liefer- und Rechnungsadresse sowie Informationen zur Abrechnung erfasst, dann muss vom Käufer eine Einwilligung zur Nutzung und Verarbeitung seiner personenbezogenen Daten eingeholt werden. Doch wer erhält welche persönlichen Daten bei einer solchen

Transaktion? Und wie kann sichergestellt werden, dass der digitale Einkäufer tatsächlich mit seiner echten Identität auftritt? Wie können also persönliche Daten vor Missbrauch geschützt werden?

Das ISÆN-Konzept schlägt vor, die persönlichen Nutzerdaten in einem elektronischen Safe (z. B. in einem abgesicherten Bereich eines Mobiltelefons) zu speichern. Die Identität des Nutzers wird vorab sichergestellt und geeignet zertifiziert, z. B. durch biometrische Verfahren wie Fingerabdruckscan oder Gesichtserkennung. Dann wird aus diesen Identitätsmerkmalen eine Art digitale Adresse berechnet, mit der zwar die Transaktionen oder Geschäftsvorgänge des Nutzers gespeichert und geprüft werden können, mit der aber wiederum keine Identifizierung des Nutzers möglich ist.

Ein persönlicher Identifier wird über Blockchain-Technologie verwaltet

Das Konzept von ISÆN sieht die Einführung eines eindeutigen Bezeichners (ISÆN-Identifier) vor. Dieser Identifier wird aus den personenbezogenen Daten des Benutzers gebildet und ist als Erweiterung von eIDAS konzipiert. Bei der Identifikation gegenüber Internet-Dienstanbietern werden nicht die Daten des Nutzers verwendet, sondern stattdessen ein aus dem ISÆN-Identifier generierter Hashwert, der keinen unmittelbaren Rückschluss auf die tatsächliche Identität des Nutzers zulässt.

Eine mögliche Realisierung des Konzepts baut auf der Blockchain-Technologie auf: In einer Blockchain werden Einwilligungen und die Weitergabe persönlicher Daten protokolliert. Kommt es beispielsweise zu einem Kaufabschluss im Internet, wird über die Blockchain eine Anfrage an den Nutzer gestellt, ob der Internet-Händler (z. B. ein Webshop) auf die für den Kauf benötigten Daten zugreifen darf. Erst nach der Protokollierung der Einwilligung durch den Nutzer in der Blockchain erfolgt dann der Datenaustausch.

Alle Informationen über die Datenweitergabe (Transaktionen) werden inklusive rechtlicher Verarbeitungsrestriktionen und einer ggf. erteilten Zustimmung der Benutzer in der Blockchain – in Form einer Art Kassenbuch – weitgehend manipulationssicher, transparent und nachvollziehbar gespeichert.

Die Daten der Benutzer werden in einer Anwendung für mobile Endgeräte, durch biometrische Verfahren geschützt, gespeichert. Eine Weitergabe der Daten findet nur dann statt, wenn die betroffene Person dazu ihre explizite Einwilligung erteilt hat (Opt-In). Gegenüber einem Internetdienstleister können so – dem Gebot der Erforderlichkeit und Datensparsamkeit folgend – nur die tatsächlich für die Abwicklung des Geschäftsprozesses erforderlichen Daten übermittelt werden (beispielsweise nur das Alter oder ein Altersnachweis, wenn eine entsprechende Altersfreigabe erforderlich ist).

ISÆN vor dem Hintergrund der EU-Datenschutzgrundverordnung

Die mit ISÆN konzipierte Unterstützung zur Umsetzung von Datenschutzbestimmungen, insbesondere der europäischen Datenschutzgrundverordnung (DS-GVO), mittels technischer Maßnahmen ist eine vielversprechende Technologie. Der ISÆN-Identifier kann grundsätzlich als elektronisches Identifizierungsmittel nach der eIDAS-Verordnung ausgestaltet werden, sodass eine – anzustrebende – europaweite Anerkennung möglich ist.

Da Benutzer sich jederzeit darüber informieren können, an welche Dienstanbieter ihre personenbezogenen Daten weitergegeben wurden, trägt ISÆN dazu bei, die Transparenz bei der Speicherung und Verarbeitung solcher Daten zu stärken. Beispielsweise können gezielt Verantwortliche (Internet-Dienstanbieter) identifiziert werden, gegen die der Benutzer anschließend seine Betroffenenrechte gemäß DS-GVO geltend machen kann. Er kann dann entsprechend von seinem Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrecht Gebrauch machen und bei Bedarf die Daten auch zu anderen Anbietern übertragen (Datenportabilität).

Die Ablage der Informationen über die Transaktion von Daten in einer Blockchain als manipulationssicheres „Kassenbuch“ ermöglicht Dienstanbietern, ihren Dokumentations- und Informationspflichten nachzukommen. Die Benutzer können anhand dieser Information auf einfache Art und Weise Auskunft über erteilte Genehmigungen für den Zugriff und die Verarbeitung personenbezogener Daten erlangen. ISÆN besitzt das Potenzial, die elektronische Identifizierung und das Anbieten von Vertrauensdiensten für elektronische Transaktionen im EU-Binnenmarkt voranzubringen.

Ob beim Aktienhandel, im Versicherungswesen oder eben im Energiesektor: Die Blockchain hat das Potenzial, Korruption einzudämmen sowie für mehr Transparenz und Sicherheit zu sorgen. Ob sie diese großen Versprechen halten kann, wird der Praxistest zeigen müssen und vor allem das Vertrauen in die Technologie in der Bevölkerung. Grundlage, um Vertrauen herzustellen, sind sichere und zuverlässige Konzepte wie die Datenschutz- und Verschlüsselungstechnologie ISÆN.

Über die Autoren

◀ Prof. Dr.-Ing. Dr. rer. nat. h.c. Stefan Jähnichen
ist Direktor am FZI Forschungszentrum Informatik und Leiter der Begleitforschung des Technologieprogramms „Smart Data – Innovationen aus Daten“ des Bundeswirtschaftsministeriums. Er leitet das Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik FIRST, hatte seit 1991 einen Lehrstuhl für Softwaretechnik an der TU Berlin inne und war Präsident der Gesellschaft für Informatik e.V. (GI).

◀ Daniel Krupka
ist Geschäftsführer der Gesellschaft für Informatik e.V., der größten Fachgesellschaft der Informatikerinnen und Informatiker in Deutschland. Er ist Teil der Smart-Data-Begleitforschung und seit mehr als zehn Jahren im Bereich Wissens- und Technologietransfer für Forschungs- und Technologieprogramme des Bundes tätig.

◀ Dr. Jan Sürmeli
forscht in der Gruppe „Softwaretechnik” an der Technischen Universität Berlin an den Themen Identitätsmanagement und Blockchain-Technologien. Nach seiner Promotion untersuchte er die Möglichkeiten der Zusammenführung prozess- und ereignisbasierter Systeme sowie Ähnlichkeitsmaße für Prozessmodelle. Sürmeli ist Gast am FZI Forschungszentrum Informatik und unterstützt in diesem Rahmen die Begleitforschung des Technologieprogramms Smart Data.

RECHTLICHE RAHMENBEDINGUNGEN DER BLOCKCHAIN 07

Vom Vertragsrecht bis zur Finanzmarktregulierung: ein kurzer Überblick über allgemeine und spezielle Rechtsprobleme beim Einsatz der Blockchain-Technologie

Als branchen-revolutionierende Technologie stellt die Blockchain auch das Recht vor besondere Herausforderungen. Vor allem die Pseudonymität der Blockchain-Teilnehmer und die Unveränderbarkeit von in der Blockchain gespeicherten Daten scheinen im Konflikt mit wesentlichen Grundgedanken des Datenschutzrechts zu stehen. Aber auch die Frage nach der national anzuwendenden Rechtsordnung, der gerichtlichen Zuständigkeit und der Beweiskraft von Blockchain-Transaktionen werfen spannende Fragen auf. Hinzu kommt, dass aufgrund der branchenübergreifenden Anwendungsszenarien der Blockchain auch etliche sektorspezifische Regulierungskonzepte betroffen sind, unter anderem in der Finanzwirtschaft, aber auch im Energiesektor. In vielen Bereichen werden sich dabei Marktstrukturen so verändern, dass sich das Recht mit der Technologie wandeln muss, wenn es die Potenziale nicht im Keim ersticken will.

© panthermedia.net / bioraven

1. Allgemeines

Schon nach dem allgemeinen Zivilrecht stellt sich besonders die Unveränderbarkeit von in der Blockchain gespeicherten Daten als Herausforderung dar. Obgleich sie eines der tragenden Prinzipien der Technologie ist, steht sie im Widerspruch zu wesentlichen Regelungen des deutschen Zivilrechts, das beispielsweise als Rechtsfolge der Anfechtung eines Vertrages auch die Nichtigkeit eines Rechtsgeschäfts von Anfang an vorsehen kann. Eine solche Rückwirkung bzw. die damit erforderliche Rückabwicklung ist aber in einer Blockchain ohne Mitwirkung des Gegners kaum umzusetzen. Zudem stellt sich die Frage, an wen im Falle der Anfechtung einer über eine öffentliche Blockchain erfolgten Transaktion die erforderliche Anfechtungserklärung zu richten wäre.

Auch der Verstoß gegen gesetzliche Verbote oder die Sittenwidrigkeit eines Vertrages sehen die Rechtsfolge einer anfänglichen Unwirksamkeit vor. Da insbesondere die letzten beiden Umstände Wertungsfragen betreffen, lassen sie sich auch nicht in die Blockchain bzw. einen Smart Contract programmieren.

Zudem kollidiert auch beispielsweise der Minderjährigenschutz des BGB mit dem Prinzip der Unveränderlichkeit: So sieht das BGB bei Rechtsgeschäften eines Minderjährigen eine schwebende Unwirksamkeit des Geschäfts vor, bis es von seinem gesetzlichen Vertreter genehmigt wird. Die Blockchain aber kennt keinen Schwebezustand und könnte Transaktionen des Minderjährigen nur unmittelbar als gültig verzeichnen.

Letztlich besteht auch für den Fall des Rücktritts vom Vertrag die Frage, wie sich dies mit dem Prinzip der Blockchain und der damit erforderlichen Rückabwicklung verträgt. Es bestünde nur die Möglichkeit, den wirtschaftlichen Ursprungszustand wiederherzustellen, indem man eine zweite Transaktion durchführt, die den Wert zurück zum Berechtigten überträgt. Dafür muss allerdings der Vertragspartner mitspielen – ohne seine Mithilfe kann keine zweite Transaktion erzwungen werden.

Schließlich offenbaren sich auch auf der Rechtsdurchsetzungsebene systematische Schwierigkeiten. Im Rahmen der Zwangsvollstreckung stellt sich hier beispielsweise die Frage, was passiert, wenn in das in der Blockchain gespeicherte Vermögen vollstreckt werden soll. Da die Passwörter des Wallet geheim und nur dem Schuldner bekannt sind, wäre ein Gerichtsvollzieher beim Versuch, auf das Wallet zuzugreifen, auf dessen Mithilfe angewiesen. Einzige Möglichkeit, den Schuldner hierzu zu bewegen, wäre die Anordnung von Zwangsgeld oder Zwangshaft. Auch dies muss aber keinen sicheren Erfolg für die angestrebte Vollstreckung nach sich ziehen.

Hinzu kommt, dass bisher völlig unklar ist, ob in Kryptowährungen wie Bitcoin überhaupt vollstreckt werden kann. So werden Geldforderungen in der Regel durch die Pfändung in körperliche Sachen, Forderungen und in „sonstige Vermögensrechte“ beigetrieben. Inwieweit Kryptowährungen wie Bitcoin hiervon umfasst sind, ist bisher rechtlich nicht geklärt.

2. Smart Contracts

Smart Contracts sind ein besonderes Einsatzgebiet der Blockchain. Rechtlich handelt es sich bei Smart Contracts nicht um eine eigenständige Vertragsart im Sinne des BGB, sondern um eine neue Form der Aufzeichnung bekannter Vertragstypen und eine automatisierte Ausführung unter bestimmten, in den jeweiligen Code programmierten Voraussetzungen.

Grenzen zeigen sich dabei überall dort, wo keine „ja - nein“- bzw. „wenn - dann“-Ausführung eines Vertrages erfolgen kann, sondern wertende Kriterien relevant werden. Aber auch Fälle der Leistungsstörung werfen vor dem Hintergrund der Unveränderbarkeit der Blockchain durchaus Fragen auf. So ist zwar offen, wie Gewährleistungsansprüche im Falle der automatisierten Vertragsausführung geltend gemacht werden können. Andererseits bieten Smart Contracts durchaus die Möglichkeit, Gewährleistungsfälle zu reduzieren: Wenn beispielsweise die Frage der rechtzeitigen oder vollständigen Leistungserbringung bereits in einem Smart Contract angelegt und damit auf Basis der Blockchain-Technologie sicher abgebildet werden kann, werden typische Störpotenziale der Leistungsabwicklung bereits im Kern ausgeschlossen.

3. Datenschutz und Blockchain

Im Bereich des Datenschutzrechts treten die Probleme zwischen der Blockchain-Technologie und der deutschen bzw. europäischen Rechtsordnung bislang am deutlichsten zutage. Charakteristische Eigenschaften der Blockchain, wie die dezentrale Verwaltung, die Pseudonymität der Nutzer und die Unveränderbarkeit der Daten, werfen im Zusammenhang mit wesentlichen Grundprinzipien des deutschen und europäischen Datenschutzrechts viele Fragen auf.

Zunächst könnte man annehmen, dass das Datenschutzrecht bei Blockchains mangels personenbezogener Daten gar nicht anwendbar ist. Schließlich müssten dafür Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person verarbeitet werden, was zweifelhaft ist, da in der bislang bekanntesten Bitcoin-Blockchain die Nutzer nur per öffentlichem Schlüssel gegenüber dem Netzwerk auftreten, mithin also mit einem Pseudonym. Klarnamen oder andere persönliche Daten werden nicht offengelegt.

Dennoch muss in vielen Anwendungsszenarien davon ausgegangen werden, dass die Nutzer in der Blockchain bestimmbar sind. Einige Studien haben bereits die Möglichkeit der Re-Identifizierung der Bitcoin-Blockchain-Nutzer über bestimmte Heuristiken bestätigt. Häufig gelingt dies über Informationen bei mit der Blockchain verbundenen Dritteinrichtungen – wie beispielsweise Handelsplattformen –, auf denen etwa die Lieferanschrift oder die Bankverbindung eines Nutzers gespeichert werden.

Weiterhin muss geklärt werden, wer bei der Blockchain überhaupt Adressat der datenschutzrechtlichen Verpflichtungen und damit die sogenannte „Verantwortliche Stelle“ ist.
Nach dem Bundesdatenschutzgesetz ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet, nutzt oder dies durch andere im Auftrag vornehmen lässt. Eine ähnliche Definition findet sich in der ab Mai 2018 geltenden EU-Datenschutzgrundverordnung.

Da das dezentrale System der Blockchain davon geprägt ist, dass gerade nicht eine Person oder Stelle allein über die Verarbeitung der Daten entscheidet, sondern jeder Teilnehmer an allen im System ablaufenden Transaktionen gleichermaßen beteiligt ist, müsste auch jeder Teilnehmer als verantwortliche Stelle im datenschutzrechtlichen Sinne gelten. Allerdings hat nicht jeder Teilnehmer allein auch Einfluss auf die gesamte Blockchain. Vor diesem Hintergrund stellt sich die Frage, ob für die Blockchain möglicherweise ein neues Modell der datenschutzrechtlichen Verantwortlichkeit geschaffen werden muss.

Eine der größten datenschutzrechtlichen Herausforderungen der Blockchain ist indes, dass sich ihre Unveränderbarkeit und die Durchsetzung von datenschutzrechtlichen Betroffenenrechten scheinbar diametral gegenüberstehen. Da die Blockchain (ggf. nach einer Übergangsphase) faktisch nicht mehr verändert werden kann, gestaltet sich die Umsetzung des Rechts auf Löschung von Daten, das Recht auf Berichtigung und das Recht auf Vergessen schwierig. Zumindest bei einer öffentlichen Blockchain dürfte eine datenschutzkonforme Umsetzung sogar teilweise unmöglich sein, sofern dabei personenbezogene Daten europäischer Teilnehmer verarbeitet werden und man zu dem Ergebnis gelangt, dass es sich im konkreten Fall um personenbezogene Daten handelt. Zu einer anderen Beurteilung gelangt man möglicherweise bei einer privaten oder „permissioned“ Blockchain, in der ein bestimmter Betreiber die Infrastruktur bereitstellt und für die Organisation verantwortlich ist. Streng genommen fehlt es bei diesen Modellen gerade an der für die Blockchain typischen Dezentralität. In einigen Anwendungsbereichen ist dies dennoch momentan die einzige Lösung, in der durch eine individuelle Vertragsgestaltung rechtliche Hürden umschifft werden können.

4. Sektorspezifische Themen

Neben den allgemeinen Problemen in den oben angesprochenen Rechtsbereichen gerät die Blockchain besonders in hochregulierten Rechtsbereichen wie etwa der Finanz- und Versicherungsbranche oder der Energiewirtschaft in Konflikt mit bestehenden Regulierungskonzepten.

Sowohl die BaFin als auch das Bundesfinanzministerium haben Bitcoins nicht als gesetzliches Zahlungsmittel, aber als „Rechnungseinheit“ und damit als Finanzinstrument i.S.d. § 1 Abs. 11 Nr. 7 KWG eingeordnet. Dies hat zur Folge, dass das gewerbliche Mining, Kaufen bzw. Verkaufen von Bitcoins (hierzu zählt auch der Betrieb eines Mining-Pools) regelmäßig einer Erlaubnis durch die BaFin bedarf. Es gibt im KWG verschiedene Erlaubnistatbestände, die eine solche Tätigkeit möglich machen würden. Es könnte z. B. ein Finanzkommissionsgeschäft vorliegen. Ebenfalls infrage käme ein multilaterales Handelssystem oder eine Anlage- und Abschlussvermittlung. Je nach Erlaubnistatbestand würde dies aber auch bedeuten, dass der Gewerbetreibende ein bestimmtes Anfangskapital vor Geschäftsbeginn aufbringen müsste.

Auch in der Energiewirtschaft stellt sich eine Reihe von sektorspezifischen Fragen. Im Bereich der Microgrids z. B., in dem eine geschlossenen Nutzergruppe teilweise über private Anlagen Solarstrom erzeugt und über eine Blockchain-Plattform damit handelt, stellt sich nach deutschem Recht die Frage, ob jeder aktive Teilnehmer als Energieunternehmen im Sinne des Energiewirtschaftsgesetzes einzuordnen ist. Zudem sieht das deutsche Energierecht einen sogenannten Bilanzkreisverantwortlichen vor, der eine ganze Reihe von Auflagen zu erfüllen hat. Auch dieses Beispiel zeigt, dass es in regulierten Märkten hohe Hürden für die Entwicklung von blockchainbasierten Geschäftsmodellen gibt.

5. Ausblick

Das revolutionäre Potenzial, welches der Blockchain vielfach – und sicherlich nicht ganz zu Unrecht – zugeschrieben wird, kann sich nur entfalten, wenn der Gesetzgeber entsprechende Spielräume schafft. Derzeit sind viele Anwendungsszenarien zwar technisch gut vorstellbar, kollidieren aber mit bestehenden Regulierungskonzepten – oft in einer Weise, die nicht mit kosmetischen Eingriffen in die gesetzlichen Grundlagen behoben werden kann. Wenn hier durch den Gesetzgeber keine Freiräume geschaffen werden und keine rechtlichen Anpassungen erfolgen, werden viele technologische Entwicklungen bereits im Keim erstickt. Es ist erfreulich, dass dem Thema Blockchain auch in der deutschen Politik eine recht hohe Aufmerksamkeit entgegengebracht wird; dennoch kann gleichzeitig festgestellt werden, dass viele andere europäische Länder die Potenziale früher erkannt haben und schnell und entschieden die rechtliche Voraussetzungen für eine breite Anwendung – auch durch die öffentliche Hand selbst – geschaffen haben. Um Deutschland als attraktiven Standort für Blockchain-Anwendungen zu positionieren, werden die rechtlichen Rahmenbedingungen eine wichtige Rolle spielen.

Über die Autoren

◀ Oliver Süme
ist Partner im Dezernat IT & Datenschutz. Er ist seit fast 20 Jahren auf den Bereich des IT- und Internetrechts spezialisiert und berät nationale und internationale Technologieunternehmen zu allen Rechtsfragen der Digitalisierung, mit einem Fokus auf IT-Vertragsgestaltung, Datenschutz und den rechtlichen Implikationen neuer Technologien wie Blockchain.

◀ Stephan Zimprich
ist Partner im Dezernat IP & Technology. Er berät nationale und internationale Mandanten in den Bereichen Lizenzrecht, Wettbewerbsrecht, Medienregulierung und Vertragsgestaltung und vertritt seine Mandanten in technologiegetriebenen Streitigkeiten vor Gericht. Stephan Zimprich ist Leiter der Kompetenzgruppe Blockchain des eco Verbands der Internetindustrie e.V.

◀ Jan Niklas Vogt
ist Referendar am Hanseatischen Oberlandesgericht Hamburg und wissenschaftlicher Mitarbeiter bei Fieldfisher im Bereich IP & Technologie. Neben den Themen „Recht auf Vergessen“ und „Adblock“ forscht er unter anderem im Bereich Datenschutz und Blockchain und war mit diesem Thema auch bei der Herbstakademie 2017 der Deutschen Stiftung für Recht und Informatik vertreten.

BLOCKCHAIN-TECHNOLOGIE: ANWENDUNGSPOTENZIALE UND LIMITIERENDE FAKTOREN

08

Den Nutzen eines Internet der Werte wahrnehmen und dabei die Fragen für Sicherheit und Nachhaltigkeit von Wirtschaft und Gesellschaft erkennen

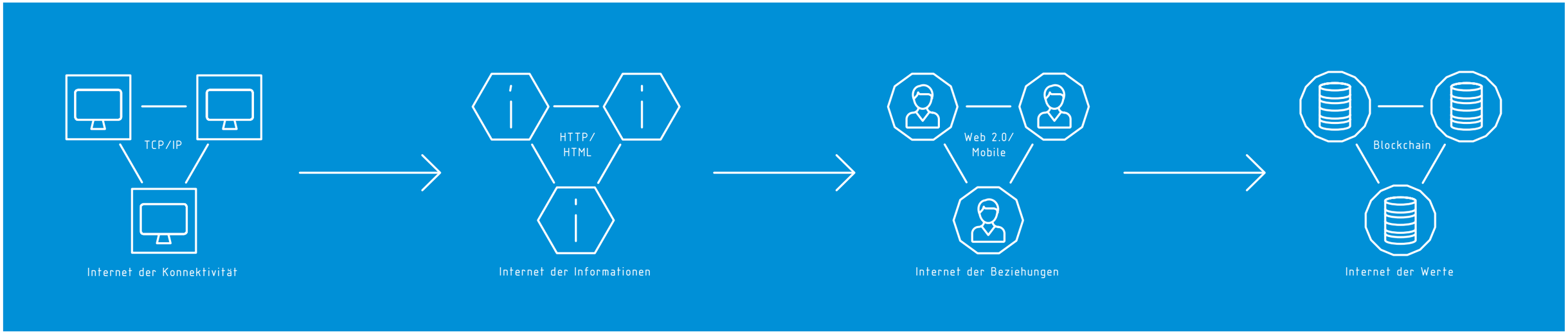


Abbildung 6: Evolution des Internets

Chancen und Potenziale der Blockchain-Technologie

Die mit der Blockchain verbundenen Potenziale werden vielfach als Weiterentwicklung des Internets der Informationen zu einem Internet der Werte gefasst, was Dan Tapscott[1)] als Paradigmenwechsel bezeichnet. Ginni Rometty formulierte es so: Was das Internet für die Kommunikation getan hat, wird Blockchain für vertrauenswürdige Transaktionen tun.[2)]

Wann kann der Einsatz einer Blockchain sinnvoll sein?

Die Blockchain-Technologie ermöglicht den Austausch von digitalen Werten, ohne eine verwertbare Kopie zu behalten (kein Mehrfachbesitz, kein Mehrfachverkauf), da die Weitergabe unveränderbar dokumentiert ist und jeder Teilnehmer diese nachvollziehen kann (sichere Transaktion zwischen unbekannten Teilnehmern). Der Einsatz einer Blockchain kommt daher insbesondere in Betracht, wenn Werte in einem Netzwerk von im Zweifel nicht vertrauenswürdigen Parteien ausgetauscht werden sollen. Die in Transaktionen hoher Werte sonst übliche vertrauenswürdige dritte Partei, wie ein Notar oder eine Bank, wird durch einen Konsensus-Mechanismus ersetzt. Ein weiteres Anwendungsfeld kommt hinzu, wenn Daten oder Werte unveränderbar archiviert und von berechtigten Stakeholdern eingesehen werden sollen, etwa bei Identitätsauskünften (Verweis auf Kapitel Lohkamp und Kapitel Krupka) oder Grundbucheinträgen.

Effizient und transparent – Blockchain in der Finanz- und Versicherungswirtschaft

In vielen Branchen wird intensiv an der Anwendung von Blockchains gearbeitet. Ausgelöst durch das erste Anwendungsbeispiel Bitcoin zählt die Finanzwirtschaft dabei zu den Vorreitern. Dazu gehört beispielsweise die Abwicklung von Wertpapiertransaktionen oder die risikolose Übertragung von Geschäftsbankgeld.[3)]

Durch die Verbindung von Blockchain und Smart Contracts steigt das Interesse der Versicherungswirtschaft. Beispielsweise könnte eine Ernteversicherung Landwirte automatisiert entschädigen, sobald nach einer Schadensmeldung Wetterdaten eine Dürre bestätigen.[4)] Im Kraftfahrzeugwesen könnte der weitverbreitete „Tachobetrug“ beim Kilometerstand wirksam bekämpft werden.[5)]

Blockchains im Internet der Dinge – Lösung für Maschinenverhandlungen?

Im Internet der Dinge werden unzählige Geräte, Sensoren und Apps, die auch geschäftliche Transaktionen abwickeln, interagieren. In der Industrie 4.0 werden Menschen, Maschinen und Produkte direkt miteinander kommunizieren und kooperieren. Dabei werden die Produktions- und Logistikprozesse zwischen Unternehmen für einen gemeinsamen Wertschöpfungsprozess intelligent vernetzt. Kooperationen sollen in dem Netzwerk von Menschen, Maschinen und Produkten flexibel ausgehandelt und vereinbart werden. Dahinter steckt letztlich eine Vielzahl von Mikrotransaktionen, die in Smart Contracts abgebildet werden könnten.

Im Energiemarkt sind Ablese- und Abrechnungsprozesse, die Dokumentation von Anlagenzuständen und Herkunftsnachweisen wie CO2- und Ökostromzertifikaten sowie der Stromhandel über Energiebörsen mittels Blockchain abbildbar.[6)] Ebenso ist die Dokumentation der Logistikkette mittels Blockchain keine Zukunftsmusik mehr und kann helfen, Betrug und Fehler zu reduzieren. Weitere Potenziale dieses Ansatzes werden in der Verkürzung der Abwicklungszeiträume und im Bestandsmanagement gesehen[7)].

1) brand eins (2016) 2) Forbes (2017)

3) Deutsche Börse (2017) 4) Munich Re Group (2016) 5) Bosch Presse (2017) 6) dena (2016) 7) IBM (2017)

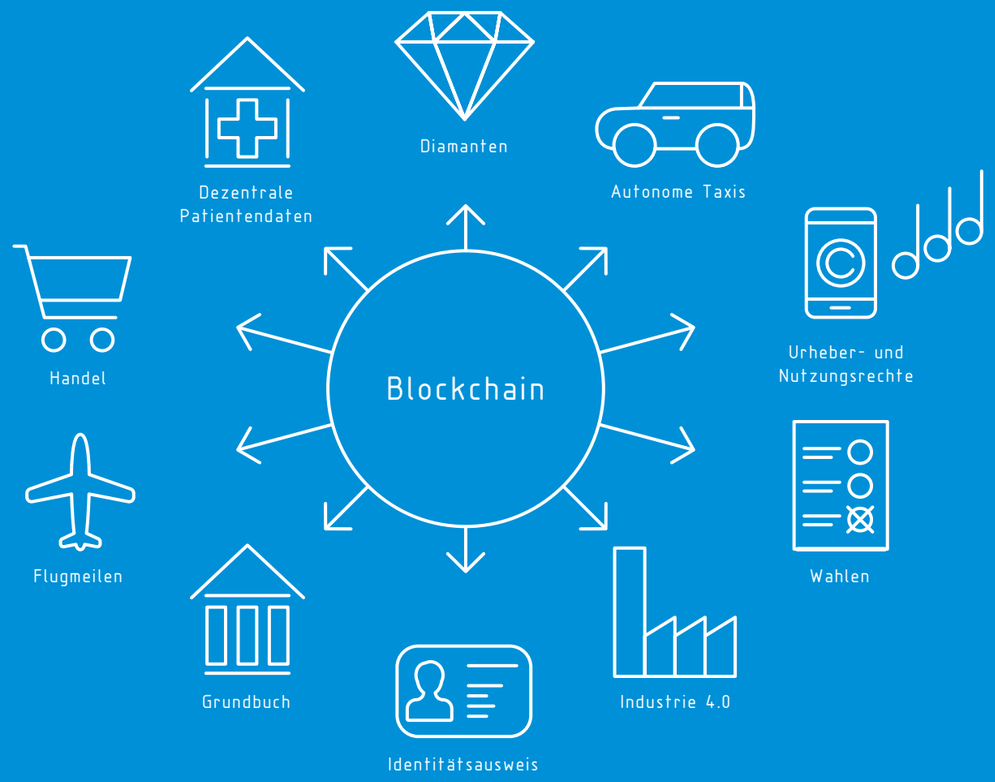


Abbildung 7: Anwendungsfelder der Blockchain-Technologie

Nutzungsrechte an Daten und Werken mit Blockchains sichern und handeln

Mithilfe der Blockchain und Smart Contracts können Rechte zur Nutzung urheberrechtlich geschützter Daten und Güter eingeräumt werden. Beispielsweise können je nach Abnehmer – Privatkunde, Radiosender, Streaming-Dienste – verschiedene Preise und Nutzungsbedingungen direkt in eine Musikdatei programmiert werden. Das Datum bzw. die Information erhält über die Abbildung in einer Blockchain einen Wert und kann nicht mehr losgelöst davon ausgetauscht werden. Dies kann insbesondere in der verteilten Produktion der Industrie 4.0 Anwendung finden, wenn Nutzungsrechte an Maschinendaten abgerechnet werden.

Limitierende Faktoren für Nutzen und Sicherheit einer Blockchain

Um die Blockchain zu fälschen, müssten die Hashwerte des Blockes mit der jeweiligen Transaktion und alle nachfolgenden Blöcke neu berechnet werden sowie alle Instanzen der (verteilten) Blockchain auf Rechnern weltweit verändert werden. Ein Manipulationsversuch wird damit bei großen Blockchain-Netzwerken – so die Erwartung – unwirtschaftlich. Bei kleineren Blockchain-Netzwerken ist allerdings nicht auszuschließen, dass es einem Angreifer gelingen könnte, die Mehrheit der Rechenleistung zu kontrollieren. Damit könnte der Angreifer eigene Transaktionen bestätigen. So hat sich beim hochkompetetiven Bitcoin-Mining ein Oligopol von dominierenden Mining-Organisationen herausgebildet,[8)] die zudem in einem Cloud-Mining-Pool kooperieren. Der vom Start-up Cex betriebene Cloud-Mining-Pool Ghash.io vereinte 2017 über 51 Prozent der gesamten Hashing-Leistung des Bitcoin-Netzwerks auf sich[9), 10)].

Wenn ein Akteur ein nicht-wirtschaftliches Interesse verfolgt, wäre er möglicherweise bereit - auch für größere Blockchain-Netzwerke - den erforderlichen Aufwand zu betreiben. Auch wenn eine solche Aktivität im Netzwerk immer auffallen wird, braucht es ein Konzept, wie ein solcher Angriff systematisch abgewehrt werden kann.

8) Der Preis für das Mining wird nicht vom Anbieter, sondern durch den Bitcoin-Algorithmus festgelegt und beträgt aktuell 12,5 BTC pro Block bzw. gelöster Aufgabe. Er wird alle 210.000 Blocks bzw. etwa alle 4 Jahre halbiert. 9) pressat.co.uk/releases/ghashio-is-open-for-discussion-93ee9eeb66b80e94bbe31705d451780e/ 10) bitcoinchain.com

Weitere Sicherheitsrisiken gehen von möglichen Bugs in der Blockchain-Software aus. So ist es Unbekannten Mitte 2016 im sogenannten DAO-Hack[11)] gelungen, 3,6 Einheiten der Kryptowährung Ethereum aus dem Crowdfunding-Projekt DAO abzuzweigen. Es ist außerdem denkbar, dass eine Blockchain durch sogenannte Denial-of-Service-Attacken überlastet wird.

Sicherheit kostet: Energie – weiterer limitierender Faktor für den Erfolg von Blockchains?

Abschätzungen zufolge setzt das Bitcoin-Netzwerk aktuell zwischen 3[12)] und 16 TWh Energie pro Jahr[9), 13)] um. Eine einzelne Transaktion verbrauchte im März 2017 etwa 26 kWh[14)]. Das ist mehr als ein durchschnittlicher 3-Personen-Haushalt in einem Mehrfamilienhaus in drei Tagen verbraucht[15)].

Der Energiehunger der Bitcoin-Blockchain ist im Wesentlichen im sogenannten proof-of-work-Ansatz begründet, bei der die „Miner“ eine mathematisch aufwendige Aufgabe lösen müssen. Der hohe Energiebedarf führt dazu, dass Miner in wenigen Ländern mit niedrigen Energiekosten hocheffiziente Rechenzentren aufsetzen. In Deutschland ist Mining aufgrund der hohen Energiekosten nicht rentabel. Die Dezentralität des Bitcoin-Netzwerks wird dadurch absehbar ausgehebelt.

Tatsächlich sind andere „proof-of“-Konzepte als Konsensmechanismus für Blockchains in der Diskussion und in Anwendungsbeispielen umgesetzt. Jeder Konsensmechanismus hat seine spezifischen Vor- und Nachteile. Ob und welche Variante der Blockchain-Technologie für eine Anwendung sinnvoll und geeignet ist, ist insofern immer für den einzelnen Anwendungsanfall zu prüfen.

Über die Autoren

◀ **Dr. Jan Christopher Brandt**
ist Leiter des Kompetenzteams Digitale Transformation bei der VDI Technologiezentrum GmbH. Er berät nationale und internationale Kunden aus Politik und Verwaltung zu digitalen Innovationstrends und der Gestaltung der digitalen Transformation. Er war und ist an zahlreichen Leuchtturmprojekten wie der „Plattform Industrie 4.0“ oder der nordrhein-westfälischen Plattform „Wirtschaft und Arbeit 4.0“ beteiligt. Er ist Autor und Co-Autor verschiedener Studien zu digitalen Innovationen und Geschäftsmodellen und deren Finanzierung sowie zum digitalen Wandel in Wirtschaft und Arbeit.

Dr. Andreas Hoffknecht ▶
ist Senior Berater bei der VDI Technologiezentrum GmbH. Der Experte für Technologiefrüherkennung und Innovationstransfer beschäftigt sich seit über 15 Jahren mit Fragen der digitalen Transformation. Unter anderem koordiniert er die Arbeitsgruppe „Referenzarchitekturen, Standards und Normung“ der Plattform Industrie 4.0. Aktuell analysiert er im Auftrag des Bundesforschungsministeriums die Potenziale der Blockchain für das deutsche Hochschulbildungssystem.

◀ **Dr. Christian Krug**
ist Technologieberater bei der VDI Technologiezentrum GmbH und mit seiner ausgewiesenen Expertise in IT-Sicherheit der industriellen Produktion Teil des Kompetenzteams Digitale Transformation. Er ist Teilprojektleiter „Sicherheit vernetzter Systemen“ der Geschäftsstelle Plattform Industrie 4.0 und ist in weiteren Projekten zu Digitalisierung und Innovation in der Industrie strategischer Berater und themenkompetenter Ansprechpartner an der Schnittstelle für Politik und Verwaltung, Wirtschaft, Wissenschaft und Gesellschaft.

11) heise.de/newsticker/meldung/Kryptowaehrung-Ethereum-Crowdfunding-Projekt-DAO-um-Millionen-beraubt-3240675.htm 12) Vranken (2017)
13) digiconomist.net/bitcoin-energy-consumption 14) securitygladiators.com/bitcoin-uses-energy-alot/ 15) Stromspiegel (2017)

EXPERIMENTIEREN, PROJEKTIEREN, STANDARDISIEREN, GESTALTEN – HANDLUNGSFELDER ZUR BLOCKCHAIN-TECHNOLOGIE

09

Die potenziellen Umwälzungen und ihre Auswirkungen verstehen und ordnen, um die Chancen zu ergreifen und Anwendungen zu schaffen

Gesellschaftliche Implikationen verstehen und gestalten

Die Blockchain-Technologie wird als wichtige Veränderung für zahlreiche Anwendungsgebiete bezeichnet. Ihr wird enormes gesellschaftliches und volkswirtschaftliches Umwälzungspotenzial zugeschrieben.

Die gesellschaftlichen und ökonomischen Auswirkungen einer Verbreitung der Blockchain-Technologie bzw. deren Anwendungen sind bisher jedoch nur wenig und nur unkonkret bekannt. Es sollte untersucht werden, ob und wie beispielsweise eine Volkswirtschaft, die auf public Blockchain-Anwendungen und -Bezahlsystemen basiert, funktionieren kann und welche Auswirkungen für Wachstum und Beschäftigung daraus resultieren. Gleichzeitig bestehen zahlreiche zivil- und datenschutzrechtliche sowie regulierungsrechtliche Fragen in Bezug auf Blockchain-Anwendungen. Nur durch die Beantwortung dieser grundsätzlichen Fragen kann ein gemeinsames Verständnis von Politik, Wissenschaft und Wirtschaft für die Blockchain-Technik entwickelt werden.

Experimentierräume schaffen und Pilotanwendungen ermöglichen

Wer die Umbrüche gestalten und von den Potenzialen profitieren will, braucht Räume mit Infrastruktur und Rahmenbedingungen, in denen rechtssicher an Anwendungen und Potenzialen der Technologie experimentiert, geprüft und weiterentwickelt werden kann. Die Experimentierräume sind technische Infrastruktur und rechtlicher (Ausnahme-)Rahmen, auf denen Blockchain-Anwendungen erprobt werden können. Um Erkenntnisse für eine mögliche zukünftige Rechtssetzung generieren zu können, sollten diese Experimentierräume so ausgestaltet werden, dass sie neben der Erprobung der Anwendungen auch die Möglichkeit schaffen, die gesetzten rechtlichen und regulatorischen Rahmenbedingungen zu erproben. Damit können Recht und Regulatorik die mit der Digitalisierung verbundenen Innovationsfelder mitgestalten.

Damit die Blockchain-Technologie in Anwendungen kommt und die Potenziale in Deutschland und Europa gehoben werden, kann die öffentliche Hand, über die Schaffung von Experimentierräumen hinaus, unterstützen: Sie kann die Vernetzung, Sichtbarkeit und Transparenz einer branchenübergreifenden Blockchain-Community in Deutschland und Europa durch die Förderung von Projekten oder Start-ups unterstützen. Sie kann Anwendungen in den eigenen Aufgabenfeldern vorantreiben und die Entwicklung und Erprobung von Anwendungen im Bereich der öffentlichen Hand befördern. Sie kann weitere Maßnahmen zur Unterstützung anwendungsorientierter Forschungs- und Entwicklungsprojekte aufsetzen.

Anforderungen an Blockchains entwickeln und erproben

Mit der Etablierung von Blockchains als dezentrale Vertrauensstrukturen in Anwendungen sind Mindestanforderungen an deren organisatorisch-technische und supernational rechtssichere Realisierung verknüpft. Die Forderung nach supernationaler Kompatibilität resultiert aus der nahezu grenzenlosen Erreichbarkeit des mit einer Blockchain verbundenen Leistungsangebots.

Aus rechtlicher Sicht muss gewährleistet werden, dass das spezifische Leistungsangebot einer Blockchain, insbesondere die Speicherung von personenbeziehbaren Daten und der bedarfsgerechte Zugang dazu, den jeweiligen Rechtsräumen genügt. Entsprechend müssen, in Konkurrenz zu dem Transparenzversprechen der Blockchain, Anforderungen für den Schutz der personenbezogenen Daten entwickelt, erprobt und etabliert werden.

Für eine breite Anwendung von Blockchain-Technologie gilt es, die Voraussetzungen für den rechtssicheren Gebrauch zu schaffen. Erst wenn beispielsweise in einer Blockchain geführte Grundbucheinträge die gleiche Rechtssicherheit gewähren wie die etablierte Dokumentation, kann Blockchain zu einer echten Alternative werden. Gleiches gilt für Dokumentation von geistigem Eigentum beispielsweise in gemeinsam bearbeiteten Publikationen, der Vertragsdokumentation oder die Abwicklung von Smart Contracts in der Industrie 4.0. Bei solchen Dokumentationsleistungen ist ein anwendungsgerechter Verfügbarkeitszeitraum zu garantieren, auch wenn die Incentives für die Netzwerkteilnehmer nicht mehr attraktiv sein sollten.

Abhängig von der Art und Implementierung der angewandten Blockchain-Technologie sind bestimmte Punkte des Vertragsrechts, wie die Rückabwicklung von Verträgen, Fehlbuchungen oder Irrtümern, nicht einfach möglich. Es sollten Lösungen technischer oder rechtlicher Art dafür entwickelt und erprobt werden.

Standardisierung von Blockchain-Technologien aus Europa heraus vorantreiben

Anwendungsfälle entstehen vielfach als nicht-standardisierte, proprietäre Blockchain-Lösungen. Das führt zu hohem Aufwand bei der Implementierung, mangelnder Kompatibilität im Betrieb und letztlich schlechter Skalierbarkeit. Damit Blockchain-Anwendungen über einzelne Anwendungs-Implementierungen hinaus anwendungsübergreifend skalieren können, ist es notwendig, internationale Normen und Standards zu erarbeiten. Dabei geht es sowohl um technische als auch organisatorische (Mindest-) Anforderungen an die Konzeption, Implementierung und den Betrieb von Blockchains. Ganz grundlegend geht es um Terminologien, Referenzarchitekturen, Datenschutz und Governance. Deutschland und Europa sollten eine prägende Rolle in der Standardisierung anstreben. Das 2017 gegründete technische Komitee bei der ISO bietet die Chance für die deutsche und europäische Wirtschaft, Wissenschaft und Verwaltung zur gemeinsamen Gestaltung.

Blockchain-Technologien anwendungsorientiert weiterentwickeln

Damit deutsche und europäische Kompetenzstandorte auch zukünftig eine relevante Rolle spielen und den Transfer aus der Forschung in die Praxis wirksam unterstützen, sollte die Erforschung und nachhaltige Weiterentwicklung von Blockchain-Netzwerken und anderer Varianten von Distributed Ledger-Technologien vorangetrieben werden. Dabei sollten der Energiebedarf, die Effizienz der Transaktionen sowie die Skalierbarkeit der Netzwerke im Fokus stehen. Gegenstand können beispielsweise Varianten von proof-of-Konsensmechanismen oder neue Datenstrukturen wie Hashgrafen sein.
Auch Ideen, im proof-of-work sinnvolle mathematische Aufgaben wie Monte Carlo-Klimamodelle, Verkehrsmodelle oder Primzahlen anstelle von Aufgaben ohne weiterverwertbares Ergebnis zu berechnen, könnten untersucht werden.

Über die Autoren

Dr. Jan Christopher Brandt
ist Leiter des Kompetenzteams Digitale Transformation bei der VDI Technologiezentrum GmbH. Er berät nationale und internationale Kunden aus Politik und Verwaltung zu digitalen Innovationstrends und der Gestaltung der digitalen Transformation. Er war und ist an zahlreichen Leuchtturmprojekten wie der „Plattform Industrie 4.0“ oder der nordrhein-westfälischen Plattform „Wirtschaft und Arbeit 4.0“ beteiligt. Er ist Autor und Co-Autor verschiedener Studien zu digitalen Innovationen und Geschäftsmodellen und deren Finanzierung sowie zum digitalen Wandel in Wirtschaft und Arbeit.

Daniel Krupka
ist Geschäftsführer der Gesellschaft für Informatik e.V., der größten Fachgesellschaft der Informatikerinnen und Informatiker in Deutschland. Er ist Teil der Smart-Data-Begleitforschung und seit mehr als zehn Jahren im Bereich Wissens- und Technologietransfer für Forschungs- und Technologieprogramme des Bundes tätig.

LITERATURVERZEICHNIS

10

Agentur für Erneuerbare Energien (2017). Homepage der Agentur für Erneuerbare Energien.
Abgerufen am 25. Juli 2017 von https://www.unendlich-viel-energie.de/.../276.AEE_RenewsKompakt_Strommarkt_de.

Allen, C. (2016). The Path to Self Sovereign Identity.
Abgerufen von www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

allfacebook.de (Website). State of Facebook.
Abgerufen von https://allfacebook.de/toll/state-of-facebook.

Bosch Presse (2017). Künstliche Intelligenz: Bosch bringt dem Auto das Lernen und kluges Handeln bei.
Abgerufen am 19. November 2017 von http://www.bosch-presse.de/pressportal/de/de/kuenstliche-intelligenz-bosch-bringt-dem-auto-das-lernen-und-kluges-handeln-bei-92352.html.

brand eins (2016). Blockchain – Durchsichtige Geschäfte.
Abgerufen am 20. Oktober 2017 von www.brandeins.de/archiv/2016/wir/bitcoin-blockchain-don-tapscott-interview/.

bitcoinchain.com (Website). Bitcoin to [Currency] Price Index.
Abgerufen am 20. November 2017 von https://bitcoinchain.com/.

Bundesverband der Deutschen Energie- und Wasserwirtschaft e.V., BDEW (2017). BDEW EDIFACT Codenummern.
Abgerufen am 3. August 2017 von Homepage des Bundesverbands der Deutschen Energie- und Wasserwirtschaft e.V.: https://bdew-codes.de/Codenumbers/BDEWCodes/CodeOverview.

Bundesverband der Deutschen Energie- und Wasserwirtschaft e.V. (2017). BDEW Marktkommunikation.
Abgerufen am 1. August 2017 von Homepage des Bundesverbands der deutschen Energie- und Wasserwirtschaft e.V. : https://www.bdew.de/internet.nsf/id/DE_Marktkommunikation.

Deutsche Börse (2017). Deutsche Börse präsentiert Blockchain-Konzept zum risikolosen Geldtransfer.
Abgerufen am 20. Oktober 2017 von deutsche-boerse.com/dbg-de/presse/pressemitteilungen/Deutsche-Boerse-praesentiert-Blockchain-Konzept-zum-risikolosen-Geldtransfer/2883238.

Deutsche Energie Agentur, dena (2016). Blockchain in der Energiewende.
Abgerufen von shop.dena.de/fileadmin/denashop/media/Downloads_Dateien/esd/9165_Blockchain_in_der_Energiewende_deutsch.pdf.

digiconomist.net (Website). Bitcoin Energy Consumption Index.
Abgerufen am 21. November 2017 von /bitcoin-energy-consumption.

DSGVO-Gesetz.
Abgerufen von dsgvo-gesetz.de/.

EU KOMM (2015). Durchführungsverordnung 2015/1501 des Rates vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifikations- und Treuhanddienste für elektronische Transaktionen im Binnenmarkt.

Forbes.com (2017). IBM Bets The Company On Cloud, AI And Blockchain.
Abgerufen am 20. Oktober 2017 von www.forbes.com/sites/jasonbloomberg/2017/03/22/ibm-bets-the-company-on-cloud-ai-and-blockchain/#455195cd776d.

Gabler Wirtschaftslexikon (Website). Know-your-Customer-Prinzip (KYC).
Abgerufen von: wirtschaftslexikon.gabler.de/Definition/know-your-customer-prinzip-kyc.html.

Gorgs, C. (2017). Warum Wind- und Solarstrom bedroht sind.
Abgerufen am 25. Juli 2017 von Homepage Manager Magazin: http://www.manager-magazin.de/unternehmen/energie/oekostrom-wind-und-solarenergie-sind-ploetzlich-zu-billig-a-1139869-2.html.

GSMA (2016). Regulatory and policy trends impacting Digital Identity and the role of mobile.
Abgerufen von www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf.

Kannenberg, A. (2016). Kryptowährung Ethereum: Crowdfunding-Projekt DAO um Millionen beraubt.
Abgerufen am 20. November 2017 von heise.de unter https://www.heise.de/newsticker/meldung/Kryptowaehrung-Ethereum-Crowdfunding-Projekt-DAO-um-Millionen-beraubt-3240675.html.

IBM (2017). Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain.
Abgerufen am 19. November 2017 von http://www-03.ibm.com/press/us/en/pressrelease/51712.wss.

Kompetenzzentrum Öffentliche IT (Homepage). Trendsonar.
Abgerufen von http://www.oeffentliche-it.de/trendsonar.

Kubicek, H. & Noack, T. (2010). "Different Countries-Different Paths Extended Comparison of the Introduction of eIDs in Eight European Countries," in: Identity in the Information Society 3 (1).

Munich Re Group (2016). Blockchain – mehr als nur Bitcoins.
Abgerufen am 20. Oktober 2017 von www.munichre.com/topics-online/de/2016/05/blockchain-more-than-just-bitcoins.

pressat.co.uk (Website). GHash.IO is open for discussion.
Abgerufen am 19. November 2017 von http://www.pressat.co.uk/releases/ghashio-is-open-for-discussion-93ee9eeb66b80e94bbe31705d451780e/.

PricewaterhouseCoopers (2016). Identitätsklau - die Gefahr aus dem Netz.
Abgerufen von www.pwc.de/de/handel-und-konsumguter/assets/cyber-security-identitaetsdiebstahl-2016.pdf.

securitygladiators.com (Website). How Much Energy Does Bitcoin Use? A Lot It Turns Out.
Abgerufen am 21. November 2017 von https://securitygladiators.com/bitcoin-uses-energy-a-lot/.

Seffinga, J., Lyons, L., & Bachmann, A. (Februar 2017). Deloitte Whitepaper - Die Blockchain (R)evolution; die Schweizer Perspektive. Zürich: Deloitte Touche Tohmatsu Limited.

Stromspiegel (2017). Stromspiegel für Deutschland 2017.
Abgerufen am 21. November 2017 von www.die-stromsparinitiative.de/fileadmin/bilder/Stromspiegel/broschuere/Stromspiegel_2017_web.pdf.

The World Bank. The Identity Target in the Post 2015 Development Agenda.
Abgerufen von www.worldbank.org/en/topic/ict/brief/the-identity-target-in-the-post-2015-development-agenda-connections-note-19.

transentis consulting (2017). Das Energiemarktmodell.
Abgerufen am 4. August 2017 von https://www.transentis.de/das-energiemarktmodell/.

Vranken, H. (2017). „Sustainability of bitcoin and blockchains", in: Current Opinion in Environmental Sustainibility 28 , S. 1-9.

Wallasch, A.-K., Lüers, S., & Rehfeldt, D.-I. K. (Dezember 2016). Weiterbetrieb von Windenergieanlagen nach 2020. Düsseldorf: Narturstrom AG.

WebOfTrustInfo (Homepage). Rebooting the Web of Trust.
Abgerufen von www.weboftrust.info/.

World Economic Forum (2016). A Blueprint for Digital Identity.
Abgerufen von www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

Zörner, T. (2015). Hybridstrommarkt - ein Strommarktdesign für die Energiewende. Mauer: StromDAO Ltd.

VDI Technologiezentrum

VDI Technologiezentrum GmbH
VDI-Platz 1
40468 Düsseldorf
Telefon: +49 211 6214-401
Telefax: +49 211 6214-484
E-Mail: vditz@vdi.de
www.vditz.de