

Blockchain

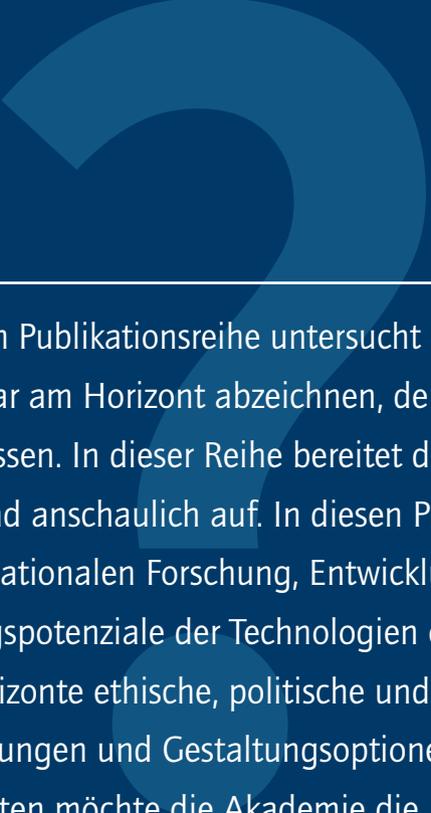
Warum Blockchain?

Wie Blockchain Wirtschaft und
Gesellschaft verändern kann

Der internationale Wettlauf um
die Blockchain – Schlaglichter

Handlungsfelder –
Gestaltungsspielräume





+++ Mit der vorliegenden Publikationsreihe untersucht acatech bedeutende Technikfelder, die sich klar am Horizont abzeichnen, deren Auswirkungen aber noch geklärt werden müssen. In dieser Reihe bereitet die Akademie solche Technikfelder fundiert und anschaulich auf. In diesen Prozess fließen der aktuelle Stand der internationalen Forschung, Entwicklung und Anwendung sowie die Wertschöpfungspotenziale der Technologien ein. Darüber hinaus nehmen die acatech Horizonte ethische, politische und gesellschaftliche Fragen sowie denkbare Entwicklungen und Gestaltungsoptionen in den Blick. Mit den acatech Horizonten möchte die Akademie die Diskussion über neue Technologien anregen, politische Gestaltungsräume aufzeigen und Handlungsoptionen formulieren. Auf diese Weise möchte acatech einen Beitrag für eine vorausschauende Innovationspolitik leisten. +++



acatech
HORIZONTE

Blockchain

Inhalt



Auf einen Blick

Seite 4

Zehn Botschaften.....	Seite 5
Deutschland und die Blockchain.....	Seite 6



Warum Blockchain?

Seite 8

1.1 Die Grundidee.....	Seite 10
1.2 Mehr als Bitcoin – Ausgestaltungsmöglichkeiten.....	Seite 14
1.3 Smart Contracts – Automatisierung von Transaktionen.....	Seite 16
1.4 Token – Bausteine für das Internet der Werte.....	Seite 19
1.5 Aktuelle technologische Herausforderungen.....	Seite 21



Wie Blockchain Wirtschaft und Gesellschaft verändern kann

Seite 24

2.1 Effiziente und transparente Lieferketten für Lebensmittel.....	Seite 26
2.2 E-Government – eine Alternative zur Zentralisierung von Registern.....	Seite 29
2.3 Facebook ohne Facebook – die Revolution der Plattformökonomie?.....	Seite 32
2.4 Eine sichere gemeinsame Sprache für intelligente Geräte und digitale Assistenten.....	Seite 34
2.5 Wann macht eine Blockchain Sinn?.....	Seite 36



Der internationale Wettlauf um die Blockchain – Schlaglichter

Seite 38

- 3.1 Blockchain-Ökosystem in DeutschlandSeite 40
- 3.2 Weltweit entstehen Blockchain-Konsortien – auch große Unternehmen sind mit dabeiSeite 42
- 3.3 ICOs und Patente zeigen: Der Wettlauf um Blockchain hat begonnen.....Seite 43
- 3.4 Akademische Blockchain-Aktivitäten.....Seite 48
- 3.5 Blockchain-Anwendungen im öffentlichen Sektor, privat-öffentliche Initiativen weltweit.....Seite 49
- 3.6 Standardisierung stellt Weichen für die MarktentwicklungSeite 51



Handlungsfelder – Gestaltungsspielräume

Seite 52

- 4.1 Eine Gestaltungsaufgabe über alle Politikfelder hinweg.....Seite 54
- 4.2 Regulierung von Token und ICOs.....Seite 55
- 4.3 Datenwirtschaft und Datenschutz.....Seite 58
- 4.4 Forschung und Fachkräfte – Was braucht es, um Blockchain zu fördern?.....Seite 59
- 4.5 Verantwortung, Sicherheit und Kontrolle.....Seite 60

Interviewpartnerinnen und Interviewpartner

Seite 61

Literaturverzeichnis

Seite 62

Mitwirkende

Seite 64

Auf einen Blick





Zehn Botschaften

1. Das Konzept der Blockchain hat das Potenzial zu einer neuen digitalen Basistechnologie.
2. Blockchain ist nicht gleich Bitcoin. Es gibt viele unterschiedliche Arten von Blockchains und zahlreiche Ideen, diese einzusetzen.
3. Die Technologie entwickelt sich rasant. Eine Garantie, dass sich die hohen Erwartungen erfüllen werden, gibt es aber nicht.
4. Blockchain ist keine Silicon-Valley-Technologie. Das Rennen um die Technologieführerschaft und die Leitmärkte ist noch offen.
5. China, Russland und eine Reihe anderer Staaten haben bereits ambitionierte Blockchain-Strategien formuliert.
6. Deutschland muss jetzt politisch aktiv werden, wenn es bei der Blockchain-Technologie nicht ins Hintertreffen geraten soll, sondern aufholen will.
7. In Deutschland ist eine international konkurrenzfähige Blockchain-Szene entstanden, insbesondere in Berlin.
8. Diese Community wünscht sich vor allem klare Ansprechpartner in Politik und Behörden. Dies ist noch wichtiger als weitere Fördermittel.
9. Der Staat wird in Zukunft selbst aktiv Blockchains anwenden. Daher ist jetzt ein Kompetenzaufbau notwendig.
10. Blockchain ist Team sport. Vordenkerinnen und Vordenker aus Politik, Wirtschaft, Wissenschaft und Gesellschaft müssen ihre Kräfte in einer nationalen Blockchain-Strategie bündeln.

Deutschland und die Blockchain



STÄRKEN:

- ▶ Lebendige und breit aufgestellte Start-up-Landschaft
- ▶ Steigendes Engagement etablierter Unternehmen und Industrien
- ▶ Hohe Anziehungskraft Berlins für weltweit führende Köpfe



SCHWÄCHEN:

- ▶ Keine nationale Blockchain-Strategie
- ▶ Einschränkung innovativer Projekte durch ungeklärte rechtliche und regulatorische Fragen
- ▶ Bislang geringe Verankerung in Forschung und Lehre



CHANCEN:

- ▶ Gewinnung von internationalen Fachkräften, Unternehmen und Kapital durch innovationsfreundliche Blockchain-Strategie
- ▶ Stärkung der digitalen Souveränität der Bürgerinnen und Bürger
- ▶ Deutsche Leitbieterschaft bei einer digitalen Basistechnologie, unter anderem für Industrie 4.0



RISIKEN:

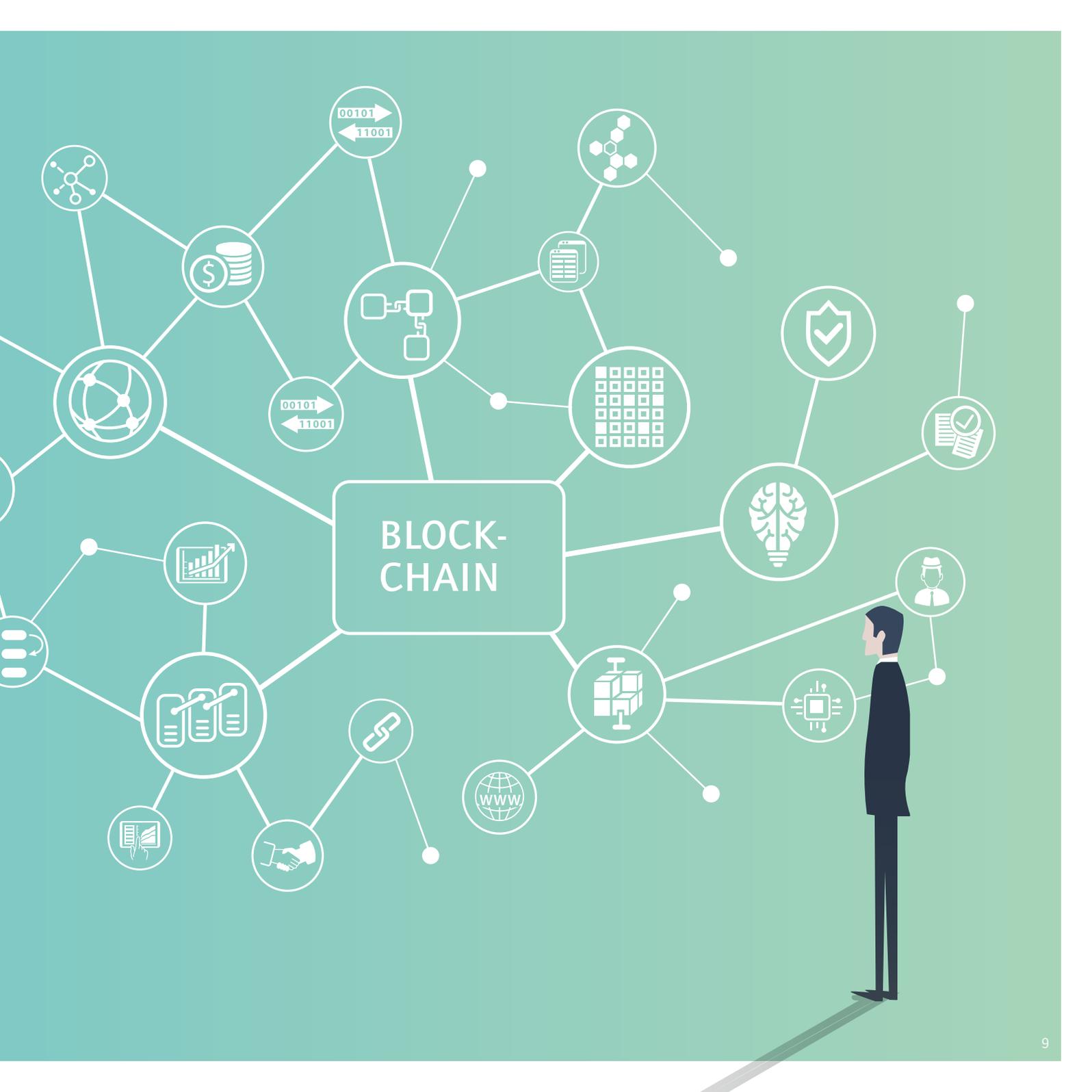
- ▶ Abwanderung des Know-hows in Wirtschaftsräume mit klaren Blockchain-Strategien
- ▶ Blockade der Anwendung von Blockchain durch nicht praxistaugliche Interpretation von Vorschriften, wie zum Beispiel der DSGVO
- ▶ Kontrolle der Technologie durch Leitanbieter und Leitmärkte außerhalb Europas

1

Warum Blockchain?

Warum sollte man sich als Politiker, Unternehmerin oder Bürger mit der Blockchain-Technologie beschäftigen? Die Blockchain erlaubt es, über innovative und bessere Lösungen für zahlreiche Problemstellungen unseres wirtschaftlichen und gesellschaftlichen Lebens nachzudenken, in denen wir Informationen, Daten und Werte austauschen. Kapitel 1 führt in die Grundlagen der Technologie und die dadurch entstehenden Gestaltungsmöglichkeiten ein. Es zeigt auf, welche technologischen Herausforderungen vor einem breiten Einsatz noch bewältigt werden müssen. ►





1.1 Die Grundidee

Wichtige Aufzeichnungen verwalten wir oft nicht selbst. Banken führen unsere Konten. Der Staat verwaltet unseren Personenstand und bei substantiellen Rechtsgeschäften beauftragen wir Notare.

Sich über Informationen, Daten und Werte zu verständigen und diese auszutauschen bedeutet heute also meist, auf Betreiber von zentralen Registern angewiesen zu sein. Diese bürgen für die Korrektheit der Einträge und Transaktionen und sichern uns bei Geschäften ab. Für ihre Leistungen bezahlen wir diese Intermediäre direkt mit Geld, indirekt mit der Abgabe der Kontrolle über unsere Daten.

Der Ansatz: Verteilte anstelle zentral geführter Register

2008 wurde unter dem Pseudonym Satoshi Nakamoto eine Technologie veröffentlicht, die alle Leistungen vertrauenswürdiger Intermediäre ohne deren Nachteile erbringen soll: Blockchain¹.

Dabei handelt es sich um ein in vielfacher Ausfertigung im Internet gespeichertes verteiltes Register, das ohne zentralen vertrauenswürdigen Betreiber auskommt. Dass Blockchain dennoch in der Lage ist, Informationen und Transaktionen zuverlässig, dauerhaft und gegen Fälschungen abgesichert zu speichern, beruht auf der innovativen technischen Konstruktion.

Blockchain kombiniert auf kreative Weise Ansätze aus akademischen Disziplinen wie der Kryptografie, dem Netzwerk- und Datenbankmanagement sowie dem Design wirtschaftlicher Anreizmechanismen. Sie ist damit ein Beispiel für konkrete Innovationen, die auf einer starken akademischen Grundlagenforschung und angewandten Forschung beruhen.

Bitcoin als erstes und bis heute funktionierendes Blockchain-Netzwerk war und ist der Nachweis für das Funktionieren von Blockchain. Experimenten und Experten sehen revolutionäre Potenziale der Technologie aber in Anwendungsfeldern jenseits der Kryptowährungen.

Das Versprechen: Datensouveränität und Effizienz

Es lohnt sich insbesondere dort über den Einsatz von Blockchains nachzudenken, wo viele Akteure Informationen oder Werte übertragen müssen, sich aber nicht persönlich kennen oder vertrauen. Der internationale Frachttransport ist hierfür ein Beispiel.

Nur wer die richtigen kryptografischen Schlüssel besitzt, kann auf die Werte zugreifen, die in einer Blockchain gespeichert sind. Weil zudem auch jeder Zugriff protokolliert wird, könnten Bürgerinnen und Bürger beispielsweise im E-Government selbst nachprüfen, welche Behörde ihre Daten zu welchem Zweck abgerufen hat. Auf einem Blockchain-basierten sozialen Netzwerk könnten tatsächlich nur die als Freundinnen und Freunde bestätigten Nutzerinnen und Nutzer etwa hochgeladene Babyfotos sehen und nicht automatisch auch immer das Unternehmen, das die zentralisierte Plattform betreibt.

Es muss sich erst noch herausstellen, ob Blockchain in diesen und anderen Anwendungsfeldern gegenüber bisherigen Lösungen überlegen ist. Auf jeden Fall befeuert die neue Technologie schon jetzt das Nachdenken über neue Geschäftsmodelle, bessere Formen der Kooperation und Wege, frei nutzbare öffentliche digitale Güter bereitzustellen.

Weitere Informationen zu den technischen Grundlagen von Blockchain finden Sie hier:



<https://www.acatech.de/horizonte/blockchain/grundidee>

Wo über den Blockchain-Einsatz nachgedacht wird



E-GOVERNMENT

- Register, z. B. Grundbücher
- Open Data
- Digitale Identitäten
- Patentregistrierung
- ...



HANDEL

- Dezentrale Marktplätze
- Sichere Übertragung von Eigentumstiteln
- Produktauthentizität von Konsumgütern
- Herkunftsnachweise und Sicherheit bei Lebensmitteln
- ...



MEDIZIN

- Sicheres Teilen von Gesundheitsdaten
- Echtheitsnachweis von Medikamenten
- Register für Implantate und Organspenden
- ...



ENERGIE

- Dezentrale Stromnetze
- Peer-to-Peer Energiemärkte
- Abrechnungssysteme für E-Mobilität
- ...



INTERNET DER DINGE/ INDUSTRIE 4.0

- Automatisierung durch Smart Contracts
- Kommunikation Maschine zu Maschine
- Manipulationssichere Updates und digitale Zwillinge
- Rechtemanagement beim Zugriff auf proprietäre Daten
- ...



LOGISTIK UND ENTERPRISE- RESOURCE-PLANNING

- Koordination firmenübergreifender Wertschöpfungsnetzwerke
- Transparente Logistik in Echtzeit
- Verhinderung von Produktfälschungen
- ...



ENTWICKLUNGSZUSAMMENARBEIT

- Transparenter Einsatz von Geldmitteln
- Identifikation von Hilfeempfängern
- Aufbau staatlicher Register
- ...



VERSICHERUNGEN

- Registrierung von Policen
- Automatisierte Schadensfallabwicklung
- Marktplätze für den Handel von Risiken
- ...



FINANZEN

- Kryptowährungen und staatliche Währungen auf Blockchains
- Kapitalisierung von Start-ups (ICOs)
- Schnelles Settlement von Wertpapiergeschäften
- Automatisierte Erfüllung von Berichtspflichten
- ...



MEDIEN/UNTERHALTUNG

- Digitales Rechtemanagement
- Crowdfunding
- Nichtvervielfältigbare digitale Originale
- ...



WISSENSCHAFT/BILDUNG

- Nachweis von erworbenen Abschlüssen und Zertifikaten
- Nachträglich unveränderbare Dokumentation klinischer Studien
- Manipulationsgeschützte Forschungsdatensätze
- ...

Lena will ihrem Neffen Ben zum 18. Geburtstag einen Bitcoin schenken. Sie öffnet ihre Wallet-App, eine Art digitale Geldbörse. Diese verbindet sich mit Danielas Knoten im Bitcoin-Netzwerk. Lena sieht, dass ihr in der Blockchain gespeichertes Guthaben aktuell 10 Bitcoin beträgt.

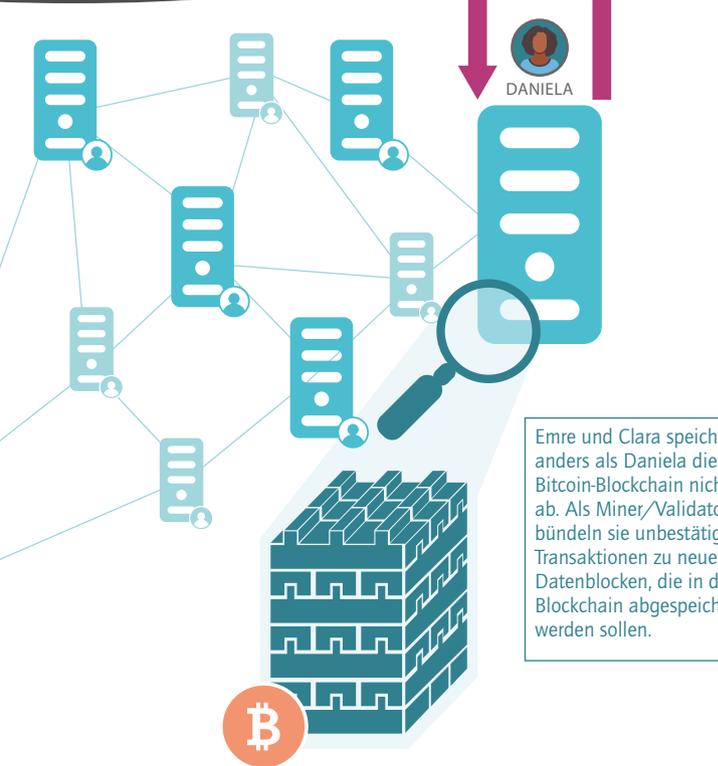
Lena erstellt eine Transaktion und unterschreibt sie mit Hilfe ihres fälschungssicheren geheimen kryptografischen Schlüssels. Die Wallet-App schickt die Transaktion an den von Daniela betriebenen Knoten.

TRANSAKTION

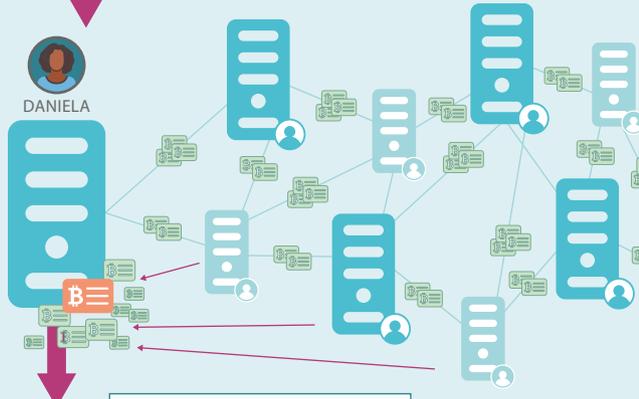
- EMPFÄNGER: Ben
- BETRAG: 1
- TRANSAKTIONSGEBÜHR: 0,00001
- SIGNATUR: *Lena*



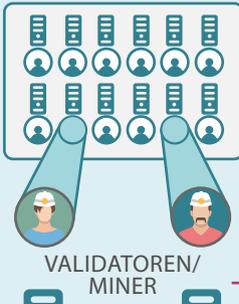
START →



Danielas Knoten schreibt Lenas Transaktion auf eine Liste, auf der schon viele andere noch unbestätigte Transaktionen stehen. Er gibt die Transaktion auch an andere Knoten des Netzwerks weiter, die diese ebenfalls auf ihre Listen nehmen.



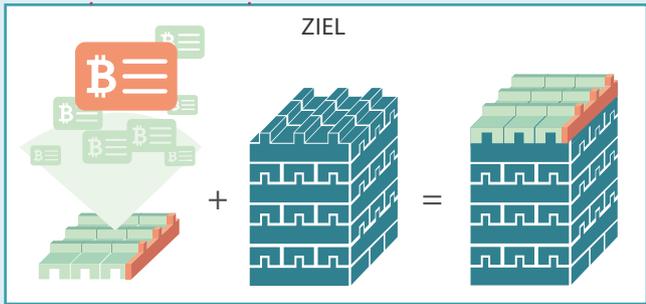
Emre und Clara speichern anders als Daniela die Bitcoin-Blockchain nicht nur ab. Als Miner/Validatoren bündeln sie unbestätigte Transaktionen zu neuen Datenblöcken, die in der Blockchain abgespeichert werden sollen.



Der Bitcoin-Konsensmechanismus „Proof-of-Work“ verlangt von Minern, dass sie eine Lösung für ein vorgegebenes kryptografisches Rätsel finden müssen, bevor sie einen neuen Block vorschlagen dürfen. Die Suche nach einer passenden Lösung verbraucht viel Rechenleistung und damit Strom.

Emre hat Glück und findet als erster eine Lösung. Er schickt den neuen Block an alle anderen Knoten. Diese prüfen ohne viel Aufwand, ob alles stimmt.

RÄTSEL



So funktioniert Blockchain



Wichtige Eigenschaften von Blockchains



Verkettungsprinzip: Eine Blockchain ist eine verkettete Folge von Datenblöcken, die über die Zeit weiter fortgeschrieben wird.



Dezentrale Speicherung: Eine Blockchain wird nicht zentral gespeichert, sondern als verteiltes Register geführt. Alle Beteiligten speichern eine eigene Kopie und schreiben diese fort.



Konsensmechanismus: Es muss sichergestellt werden, dass eine bei allen Beteiligten identische Kette entsteht. Hierfür müssen zuerst Vorschläge für neue Blöcke erarbeitet werden. Dies geschieht durch Validatoren (die bei Bitcoin „Miner“ genannt werden). Dann müssen sich die Beteiligten einig, welcher vorgeschlagene Block tatsächlich in die Kette eingefügt wird. Dies erfolgt durch ein sogenanntes Konsensprotokoll, ein algorithmisches Verfahren zur Abstimmung.



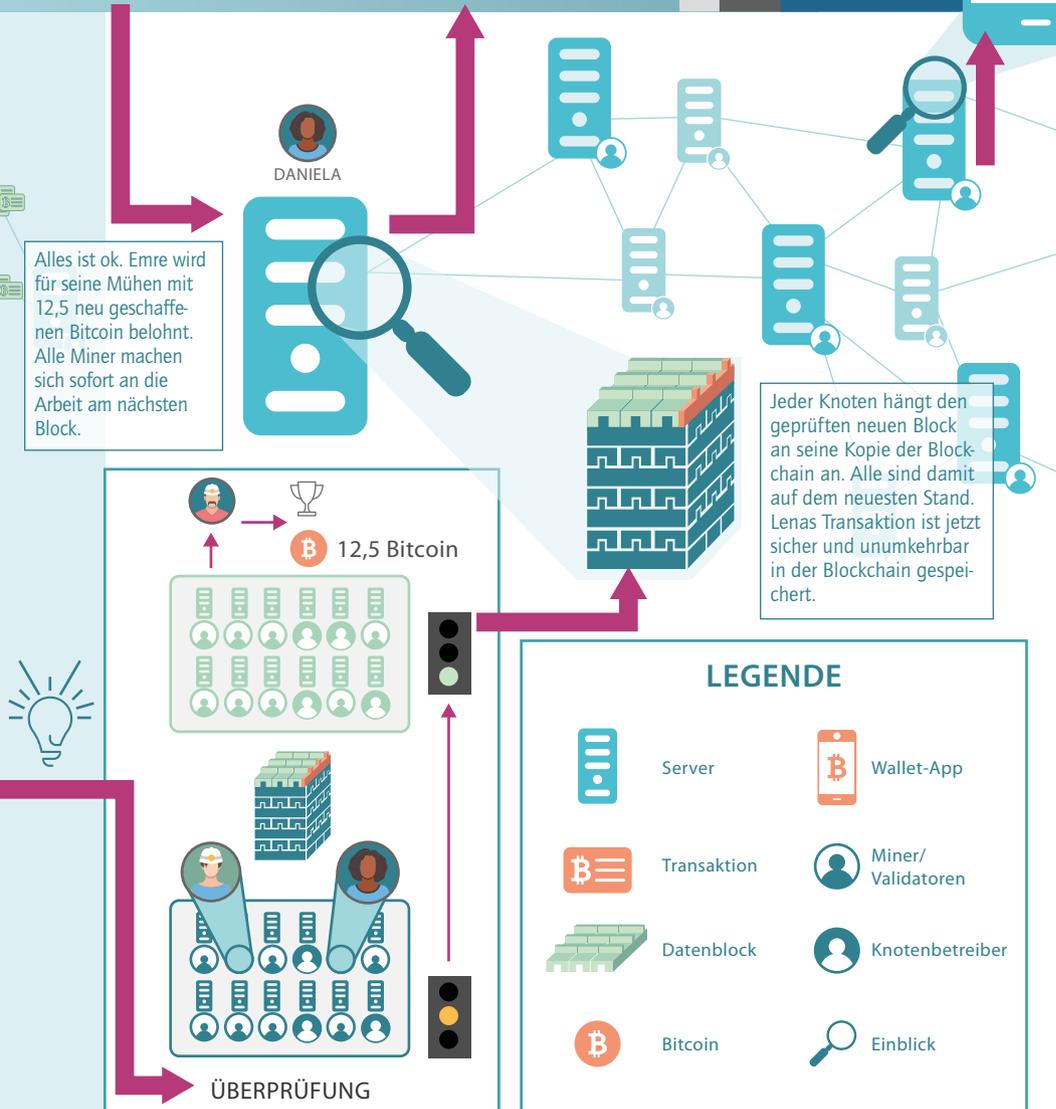
Manipulationssicherheit: Durch kryptographische Verfahren wird sichergestellt, dass die Blockchain nicht nachträglich geändert werden kann. Die Kette der Blöcke ist somit unveränderbar, fälschungs- und manipulationssicher.



Transparenz/Vertraulichkeit: Die auf der Blockchain gespeicherten Daten sind von allen Beteiligten einsehbar. Sie sind deshalb aber nicht unbedingt auch für alle sinnvoll lesbar, denn Inhalte können verschlüsselt abgespeichert werden. Blockchains erlauben so eine flexible Ausgestaltung des Vertraulichkeitsgrads.



Nichtabstreitbarkeit: Durch die Nutzung digitaler Signaturen sind Informationen in der Blockchain speicherbar, die fälschungssicher nachweisen, dass Teilnehmende unabstreitbar bestimmte Daten hinterlegt haben, etwa Transaktionen angestoßen haben.



1.2 Mehr als Bitcoin – Ausgestaltungsmöglichkeiten

Es gibt nicht nur eine Blockchain. Blockchain ist eine Technologie, die sich in den neun Jahren seit dem Start des Bitcoin-Netzwerks rasant weiterentwickelt hat. Der Begriff Blockchain dient heute – auch in dieser Publikation – als Sammelbegriff für ein breites Spektrum an verteilten Registern, die sogenannten „Distributed Ledger Technologies“ (DLTs). Diese haben jeweils ähnliche – im Vergleich zu Blockchains im engeren Sinne oft reduzierte – Eigenschaften.

Technisch unterscheiden sich viele heutige Ansätze deutlich von der Blockchain Nakamotos. Was sie leisten, ist aber generell ähnlich. So gibt es beispielsweise Verfahren zur Verkettung von Transaktionen anstelle von Blöcken, wie im „Tangle“-Ansatz des Start-ups IOTA⁶. Dies soll zu einem deutlich höheren Datendurchsatz führen. Blockchains können also gezielt an die Anforderungen des Anwendungsgebiets angepasst werden.

Anpassbarer Grad der Dezentralität

Die wichtigste Entscheidung bei der Planung einer Blockchain ist, ob sie so dezentral wie die ersten Blockchains sein soll, oder zentralisierte Elemente aufweisen kann. Die Kriterien für diese Entscheidung sind nicht primär technische Aspekte, sondern rechtlicher, sozialer und wirtschaftlicher Natur. Die dann vorgenommene Festlegung hat weitreichende Implikationen für das mit der Blockchain verbundene Geschäftsmodell und die Art und Weise, wie die Nutzerinnen und Nutzer miteinander interagieren.

Der erstrebenswerte Dezentralisierungsgrad ist oftmals Gegenstand von Grundsatzdebatten in der Blockchain-Community. Praktisch zeichnet sich aber ab, dass es für jede Ausgestaltungsoption vielversprechende wirtschaftliche und gesellschaftliche Anwendungsmöglichkeiten gibt. Diese gehen dann mit unterschiedlichen technischen und rechtlichen Herausforderungen einher.

Wer darf zugreifen?

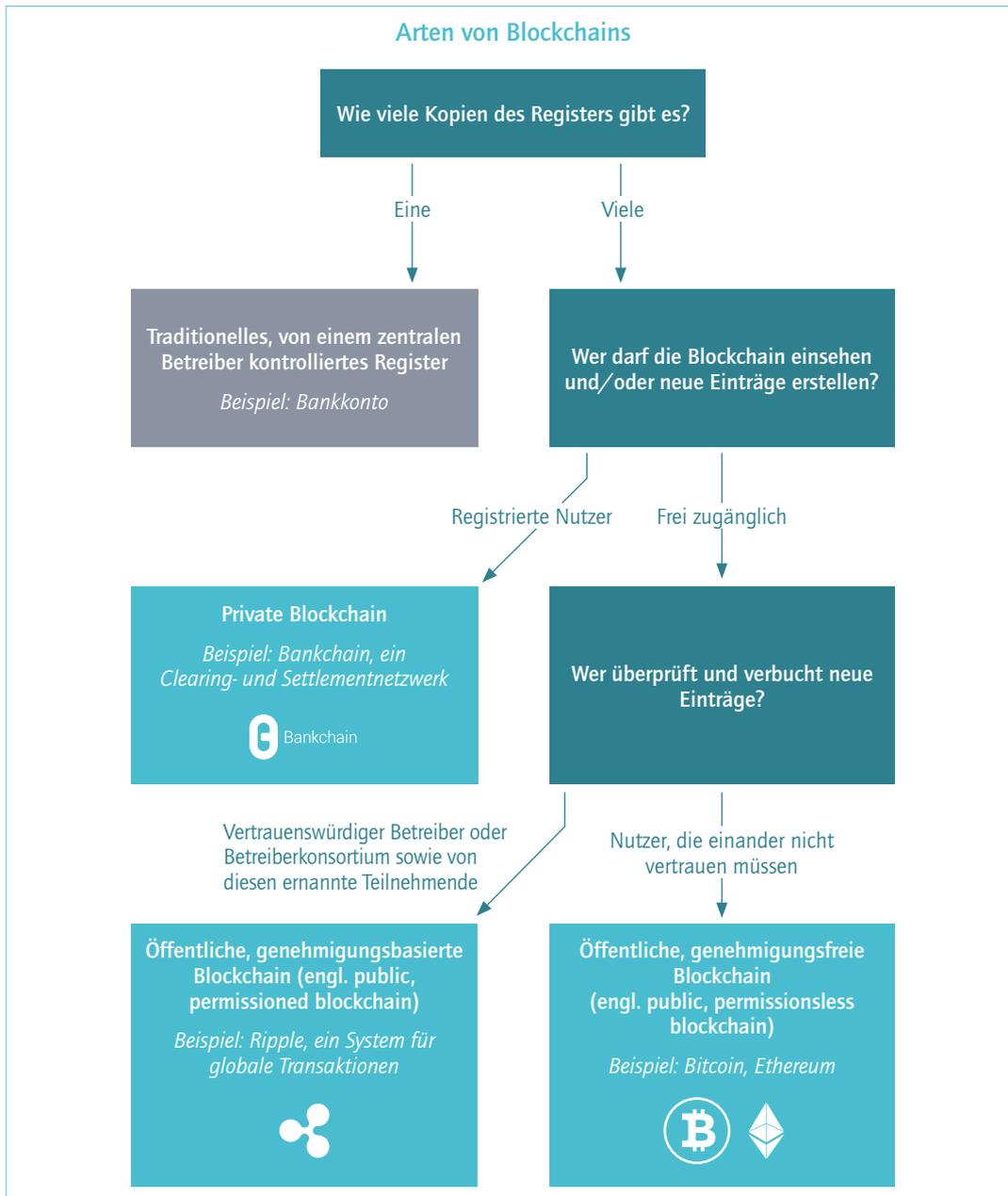
Auf eine öffentliche (englisch „public“) Blockchain darf jeder ohne Registrierung oder Preisgabe der eigenen Identität zugreifen. Niemand kann von der Nutzung ausgeschlossen werden.

An einer privaten Blockchain können nur registrierte Nutzerinnen und Nutzer teilnehmen. Eine Gruppe von Teilnehmenden erteilt und verwaltet den Zugang. Sie kann den anderen Teilnehmenden auch unterschiedliche Berechtigungsstufen zuweisen. Beispielsweise könnte Nutzer A nur ein passives Leserecht erhalten, Nutzerin B dagegen das Recht, selbst Transaktionen vorzunehmen.

Wer prüft und verbucht neue Transaktionen?

In einer genehmigungsfreien (englisch „permissionless“) Blockchain kann sich jeder an der Erzeugung neuer Blöcke beteiligen, somit auch böswillige Nutzerinnen und Nutzer. Eine solche Blockchain muss daher robust gegenüber Manipulationsversuchen sein. Gleichzeitig muss sie auch Anreizmechanismen für die Teilnahme an der Validierung von Transaktionen bieten. Der energieintensive „Proof-of-Work“-Konsensmechanismus dient heute in vielen öffentlichen Blockchains diesen Zwecken.

Bei einer genehmigungsbasierten (englisch „permissioned“) Blockchain verbuchen der Betreiber, ein Betreiberkonsortium oder von diesen autorisierte Teilnehmende Transaktionen. Die anderen Teilnehmenden müssen ihnen vertrauen. Auf einen ressourcenintensiven Konsensmechanismus kann verzichtet werden. Anreize zur Beteiligung an der Validierung können auch außerhalb der Blockchain gesetzt werden, beispielsweise durch Verträge von Konsortialpartnern untereinander.



1.3 Smart Contracts – Automatisierung von Transaktionen

In Blockchains können nicht nur Werte gespeichert werden, sondern auch Programmcodes, die unter festgelegten Bedingungen automatisch und garantiert ausgeführt werden. Somit ist es technisch möglich, „Wenn-dann...“-Prozesse in einer Blockchain umzusetzen, was auch die Möglichkeit der manipulations-sicheren Abbildung von Verträgen zwischen Teilnehmenden umfasst.

Für diese Programmcodes hat sich der Begriff „Smart Contracts“ eingebürgert. Diese bieten ein großes Potenzial zur Automatisierung und Effizienzsteigerung von Geschäftsprozessen, gerade dann, wenn es um Routineaufgaben und Transaktionen mit wenig Interpretationsspielraum und Variation geht.

Smart Contracts für Industrie 4.0 und das Internet der Dinge

Smart Contracts hätten insbesondere in Fällen einen Mehrwert, in denen es für Nutzerinnen und Nutzer zu aufwendig wäre, jede Transaktion eigenhändig zu erstellen und freizugeben. So können Smart Contracts beispielsweise auch Maschinen die Teilnahme an Blockchains ermöglichen.

Da Smart Contracts auf der Blockchain zudem manipulations-sichere Prozesse sind, erlauben sie es, Zug-um-Zug Geschäfte verbindlich umzusetzen. Durch diese Eigenschaften könnten Smart Contracts zukünftig für die Industrie 4.0 oder auch viele private Anwendungen (z. B. Smart Home) unabdingbar werden.

Rechtlich stellt sich die Frage, wie mit Smart Contracts umzugehen ist. Im juristischen Sinne stellen sie nicht zwangsläufig Verträge dar, vielmehr handelt es sich um Programme, in denen alle Arten von Konditionen und gewünschten Reaktionen einprogrammiert sind. Bisher ersetzt Computercode kein Recht. Auch ist unklar, wie effektive Rechtsdurchsetzung bezüglich der verteilten Netzwerkknoten (Rechner) innerhalb einer Blockchain erfolgen kann.

Aktueller Stand der Smart-Contract-Entwicklung

In vielen Anwendungsfeldern wird bereits erfolgreich mit Blockchain-basierten Apps (englisch, „Distributed Apps“, kurz „Dapps“) experimentiert, deren Geschäftsmodelle sich die Eigenschaften von Smart Contracts zunutze machen. Öffentliche Blockchain-Plattformen wie zum Beispiel Ethereum oder Hyperledger sind auf die Programmierung von Smart Contracts ausgelegt. In diese Plattformen sind für die Nutzerinnen und Nutzer Programmiersprachen eingebaut, auf deren Basis Smart Contracts und Dapps entwickelt werden können. Diese bieten somit eine direkte Schnittstelle zur jeweiligen öffentlichen Blockchain.

Die Qualitätssicherung von Smart Contracts gestaltet sich jedoch bisweilen noch problematisch: Programme können Schwachstellen oder Programmierfehler enthalten, die von Angreifern oder Unwissenden (teilweise absichtlich) ausgenutzt werden können⁸. Dies hat beispielsweise zum Scheitern der ersten vollständig dezentralen, autonomen Investment-Firma „The DAO“ geführt⁹ oder zum Einfrieren von Ether-Münzen auf digitalen Geldbörsen von Nutzerinnen und Nutzern des Ethereum-Wallet-Betreibers „Parity“¹⁰.

Auch ist es unklar, inwiefern Ereignisse („Trigger“) aus der realen Welt, die den Smart Contract auslösen, verlässlich in eine Blockchain gelangen können. Hierzu gibt es das Konzept der sogenannten „Oracles“: Sensoren, die reale Ereignisse messen und die Daten dann an den Smart Contract weiterleiten. Die Qualitätssicherung, der rechtliche Status sowie die Manipulierbarkeit solcher Oracles sind aber noch Herausforderungen für die Forschung.

Realisierung von Geschäftsmodellen per Smart Contract

Smart Contracts bieten die Möglichkeit, neue Geschäftsmodelle zu etablieren, die aufgrund hoher Transaktionskosten (z. B. von Intermediären wie Finanzdienstleistern) bislang unwirtschaftlich waren.

Anwendungsbeispiele

EFFIZIENZSTEIGERUNG UND VEREINFACHUNG BESTEHENDER PROZESSE:

Automatische Auszahlung einer Versicherung gegen

Flugverspätungen: Eine als Smart Contract abgeschlossene Versicherung kann dem Reisenden automatisch eine Entschädigung zahlen, wenn der Flug ausgefallen ist.

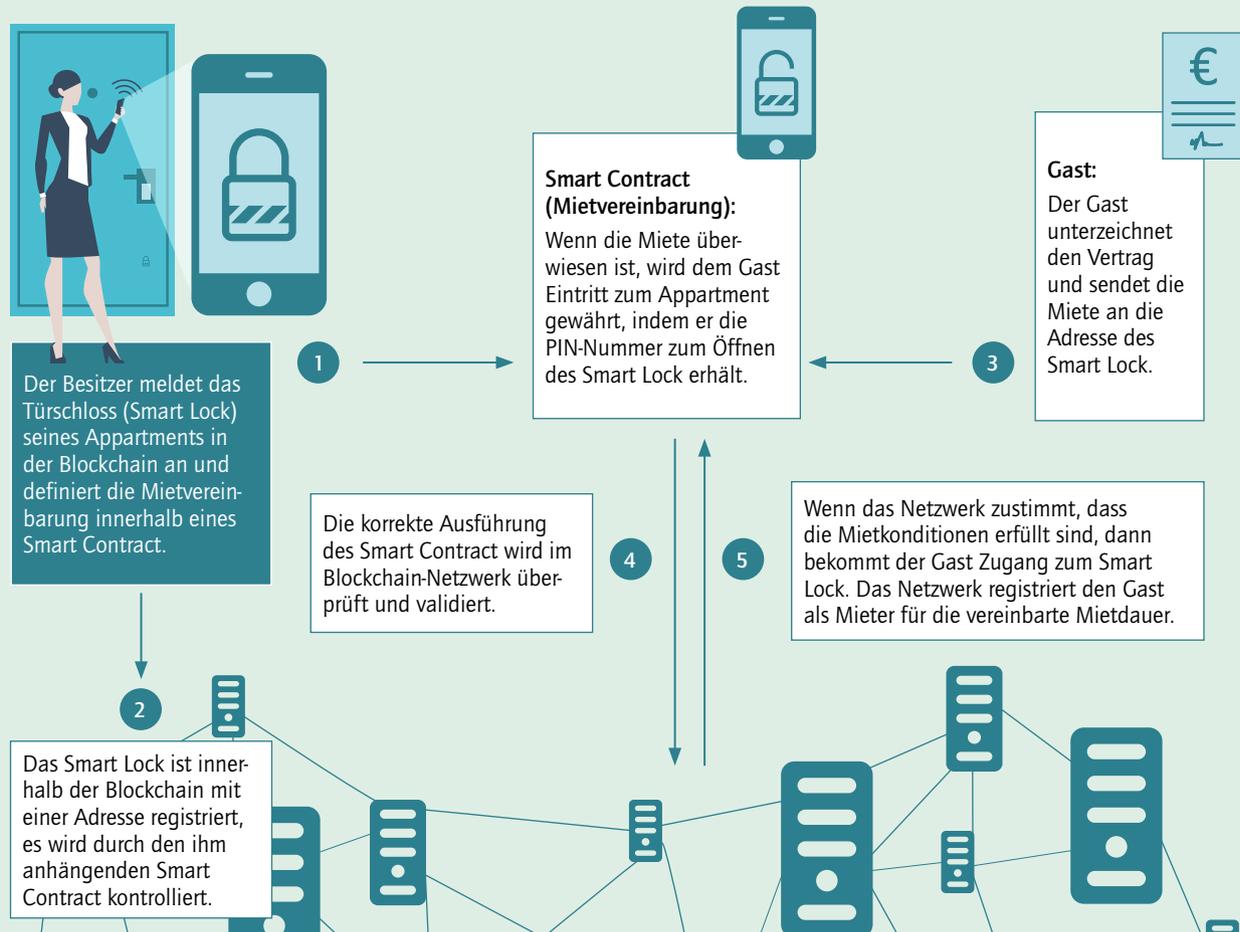
NEUE GESCHÄFTSMODELLE:

„Streaming Money“ für das Internet der Dinge:

Streaming Money bedeutet eine automatisierte und sekundengenaue Abrechnung der Nutzung einer Dienstleistung, zum Beispiel einer Ladestation oder eines Streamingdienstes durch Mikrozahlung.

„Die Verknüpfung mit der echten Welt ist eine Herkulesaufgabe.“

Anwendungsbeispiel: „Smart Lock“ – ein intelligentes Türschloss, das sich gegen Bezahlung automatisch öffnet



SMART CONTRACTS FÜR SMART HOMES

Smart Contracts können zum Beispiel im Smart Home zum Einsatz kommen. Hier bieten sie den Vorteil, dass Geräte nicht mehr der Kontrolle eines einzelnen Herstellers bzw. Anbieters unterliegen müssen. Smart Contracts sind auf der Blockchain vielfach abgesichert und es wird Anbieterneutralität ermöglicht. Dies bedeutet, es gibt keine zentralen Anbieter mehr, die ihre Server abschalten können. Die Funktionalität von Geräten bleibt so permanent erhalten, da Nutzerinnen und Nutzer auf andere Smart Contracts zur Steuerung ausweichen können.

1.4 Token – Bausteine für das Internet der Werte

Ein Grundproblem des Internets ist, dass sich durch die beliebige Kopierbarkeit von Daten die digitale Übertragung von Werten als schwierig gestaltet.

Hier bieten sogenannte „Token“ (deutsch „Wertmarken“) eine Lösung, die als eine Art digitale Urkunde oder Verbriefung Werte auf einer Blockchain festhalten. Werte können dabei nicht nur Besitztümer, sondern auch Ereignisse oder Dienstleistungen sein. Ziel der Token ist es, diese Güter aus dem Alltag im Internet abzubilden und somit zuverlässig handelbar zu machen.

Die Regeln für die Erstellung, den Transfer bis hin zur Vernichtung von Token sind in einer Blockchain fest definiert. Nicht jede Transaktion innerhalb einer Blockchain benötigt Token, aber sie sind immer dann interessant, wenn es um das Thema Wertübertragung geht.

Klassifizierung von Token-Typen nach FINMA

Es gibt verschiedene Arten von Token. Manche Typen unterstehen den Finanzaufsichten und sind deren Regeln unterworfen, andere Token hingegen nicht. Die Schweizer Behörde FINMA¹² entscheidet beispielsweise anhand folgender Klassifizierung:



1. KRYPTOWÄHRUNGEN (PAYMENT-TOKEN)

Bitcoins und andere Kryptowährungen sind die bekanntesten Token, sie dienen als Zahlungsmittel.



2. NUTZUNGS-TOKEN (UTILITY-TOKEN)

Nutzungs-Token geben Zugang zu einer digitalen Anwendung oder Dienstleistung, die in einer Blockchain-Infrastruktur erbracht wird.



3. ANLAGE-TOKEN (SECURITY-TOKEN)

Anlage-Token repräsentieren Vermögenswerte. Bei diesen Token werden der oder dem Kaufenden beispielsweise Anteile an künftigen Unternehmenserträgen oder künftige Kapitalflüsse versprochen. Token, die physische Wertgegenstände über eine Blockchain handelbar machen, gelten ebenfalls als Anlage-Token. Diese Token erlauben eine Erhöhung der Liquidität aufgrund von beliebiger granularer Stückelung der Investmentanteile.

Hybride Token

Die Token-Klassifizierungen schließen einander nicht zwingend aus, hybride Token sind möglich. Bitcoin und Ether sind Beispiele für hybride Token, da sie eine Kombination aus Kryptowährung und Nutzungs-Token sind: Beide Token fungieren zunächst als Zahlungsmittel. Darüber hinaus haben sie den Zweck, Teilnehmenden der öffentlichen Blockchains Bitcoin und Ethereum ökonomische Anreize zu bieten, um so den Betrieb der jeweiligen Infrastruktur aufrechtzuerhalten.

Initial Coin Offering (ICO) - Kapitalerhöhung durch den Verkauf von Token

Mehrere kapitalintensive ICOs haben in den letzten Jahren viel Aufmerksamkeit erfahren. Initial Coin Offerings, kurz „ICOs“, sind ein neues Fintech-Instrument zur Kapitalerhöhung, bei der Firmen Token für Geld verkaufen. Sie sind bisher hauptsächlich von Start-ups in Anspruch genommen worden, deren Geschäftsmodell auf der Entwicklung von Blockchain-Anwendungen fußt. Ähnlich wie beim Crowdfunding bieten Start-ups bei einem ICO oft nur ein Konzept mit der Geschäftsidee, aber keine gesicherten Werte oder gar ein existierendes Produkt. Es besteht daher das Risiko, dass Anlegerinnen und Anleger bei einer Investition leer ausgehen. Mit entsprechender Regulierung und rechtlicher Sicherheit, vor allem für Anleger, könnten ICOs aber zukünftig zu einer neuen Anlageklasse werden.

„Die Technologie ist noch auf einem frühen Stand, das ist alles work in progress.“

Anwendungsbeispiel für einen Nutzungs-Token

BAT-TOKEN:

Der Internetbrowser „Brave“ verfügt über ein internes Zahlungsmittel, den sogenannten „Basic Attention Token“ (BAT). Der BAT-Token dient dazu, das Gut der „Aufmerksamkeit einer Nutzerin beziehungsweise eines Nutzers“ abzubilden und handelbar zu machen.

Bisher war dies nicht möglich: Nutzerinnen und Nutzer mussten Werbung im Browser „über sich ergehen lassen“ und bekamen keine Entlohnung für ihre Aufmerksamkeit. Wenn diese jedoch Werbung im Browser „Brave“ zulassen, werden sie dafür in BAT entlohnt. Diese Token können sie dann zum Beispiel zur Freischaltung von Premiuminhalten innerhalb des Browsers nutzen. Beim ICO konnten Anlegerinnen und Anleger etablierte Kryptowährungen wie Bitcoin und Ether in BAT investieren. Der ICO generierte umgerechnet circa 35 Millionen US-Dollar¹³.

1.5 Aktuelle technologische Herausforderungen

Auf dem gegenwärtigen Entwicklungsstand kann die Blockchain-Technologie viele der großen mit ihr verknüpften Versprechen noch nicht einlösen, auch wenn sich mehr und mehr marktreife Anwendungen abzeichnen.

Vor einer breiten Nutzung sind eine Reihe technischer Herausforderungen zu bewältigen. Diese werden im Folgenden vorgestellt und relevante Unterschiede zwischen Blockchainarten aufgezeigt. Jede Problemstellung wird zudem am konkreten Beispiel des Bitcoin-Netzwerks verdeutlicht.

Es gibt keine Garantie dafür, dass diese Hürden bewältigt werden. Es ist denkbar, dass sich ein Problem als so fundamental herausstellt, dass viele potenzielle Anwendungsfelder verschlossen bleiben. Die Einschätzungen von Expertinnen und Experten tendieren aber deutlich zum Optimismus, da für jedes Problemfeld bereits vielversprechende Ideen für Lösungsansätze vorhanden sind. In jedem Fall setzt eine erfolgreiche Beseitigung der Hürden den Einsatz von Mitteln für Forschung und Entwicklung voraus.

Ein Dilemma

Für Unternehmen und Politik ergibt sich aus der unklaren Zukunft der Blockchain das klassische Dilemma innovativer digitaler Technologien. Ihr tatsächlicher Siegeszug kann nicht garantiert werden. Wartet man aber ab, bis sich die erfolgreiche Lösung der bestehenden Probleme abzeichnet, werden Unternehmen und Wirtschaftsräume, die aktiv an der Technologie arbeiten, uneinholbar in Führung gegangen sein.



ENERGIEVERBRAUCH

Der genaue Energieverbrauch von öffentlichen, genehmigungsfreien Blockchain-Netzwerken wie Bitcoin oder Ethereum ist schwer zu bestimmen, da Studien ihn nur abschätzen können. Das Bitcoin-Netzwerk verbraucht aktuell mindestens 2,5 Gigawatt. In Zukunft könnte der Energieverbrauch dem von Volkswirtschaften wie Irland (3,1 Gigawatt) oder sogar Österreich (8,2 Gigawatt) entsprechen¹⁴. Auf jeden Fall ist er aber unakzeptabel hoch.

Wichtig ist hierbei aber zweierlei: Erstens ist der wachsende Energiehunger nicht direkt durch eine zunehmende Transaktionszahl bedingt. Er resultiert vielmehr aus dem Konsensmechanismus Proof-of-Work, bei dem Nutzerinnen und Nutzer Hardware und Strom einsetzen, um neue Blöcke zu erstellen und dafür mit neuen Token der jeweiligen Kryptowährung belohnt werden.

Zweitens nutzt nicht jede Blockchain Proof-of-Work. Betreiber privater Blockchains können diese anderweitig gegen Attacken absichern, der Bedarf für einen energieintensiven Konsensmechanismus entfällt daher von Anfang an. Eine Kritik am Energieverbrauch von Blockchains muss daher zwischen Konsensmechanismen differenzieren.

Proof-of-Work wird mittlerweile nur als Übergangslösung betrachtet. Viele Entwickler arbeiten bereits an alternativen Konsensmechanismen für öffentliche, genehmigungsfreie Blockchains.



Große Hoffnungen werden aktuell in den Mechanismus „Proof-of-Stake“ gesetzt, auf den beispielsweise das Ethereum-Netzwerk langfristig umgestellt werden soll. Hier bezahlen die Validatoren ihre Chance, neue Token zu erhalten durch ein temporäres Einfrieren ihres Token-Guthabens statt mit der Stromrechnung.



Expertinnen und Experten halten es für ausgeschlossen, dass sich die Bitcoin-Community vom Proof-of-Work trennt, da dieser Konsensmechanismus einen hohen ideologischen Stellenwert für diese Gemeinschaft besitzt.



Bitcoin verarbeitet maximal zwanzig Transaktionen pro Sekunde. Kreditkartensysteme wie Visa dagegen können mit herkömmlicher Technik durchschnittlich 1.500 Transaktionen pro Sekunde verarbeiten, bei Belastungsspitzen sogar bis zu 50.000 pro Sekunde.

Mit dem „Lightning Network“ werden gegenwärtig Zahlungskanäle entwickelt, die auf dem Bitcoin-Netzwerk aufsetzen und eine deutliche Steigerung der Transaktionsrate erlauben sollen¹⁶.



NIEDRIGE MAXIMALE TRANSAKTIONSRATE



Viele Blockchains stoßen regelmäßig an ihre Kapazitätsgrenzen. Dies betrifft vor allem öffentliche Blockchains. Private Blockchains erreichen aktuell deutlich höhere maximale Transaktionsraten als öffentliche Blockchains. „Hyperledger Fabric“ verbucht beispielsweise bis zu 3.500 Transaktionen pro Sekunde¹⁵.

Wird die Verarbeitungskapazität einer Blockchain überschritten, kann eine zeitnahe Verbuchung von Transaktionen nicht garantiert werden und es können Transaktionen sogar komplett verfallen.

Viele denkbare Blockchain-Anwendungen, gerade im Internet der Dinge, setzen Transaktionsraten voraus, die heute auch von privaten Blockchains noch nicht erreicht werden.



Einerseits wird daran gearbeitet, den Durchsatz der Blockchains selbst zu steigern. Andererseits sollen möglichst viele Transaktionen nicht mehr auf der Blockchain selbst durchgeführt werden, sondern nur in aggregierter Form mit ihr verknüpft und so abgesichert werden.



HOHER SPEICHERPLATZBEDARF



An eine Blockchain werden immer nur neue Einträge angehängt, keine alten Einträge verändert oder gelöscht. Sie und damit der Speicherplatzbedarf für jede Kopie wachsen also stetig. Dies kann gerade in Anwendungsbereichen mit vielen Transaktionen wie dem Internet der Dinge schnell die vorhandenen Kapazitäten sprengen und Nutzerinnen und Nutzer daran hindern, eine eigene Kopie der Blockchain zu betreiben. Damit gerät aber die Verwirklichung der Dezentralisierungsidee in Gefahr.



Viele Projekte arbeiten daran, nicht mehr alle Daten in einer großen Blockchain zu speichern, sondern sie auf verschiedene Art und Weise aufzuteilen und nur bei Bedarf zu verknüpfen.



Im Oktober 2018 benötigt eine Kopie der Bitcoin-Blockchain circa 190 Gigabyte Speicherplatz. Im Oktober 2017 waren es noch 125 Gigabyte¹⁷.



SICHERHEIT



Die Sicherheit öffentlicher, genehmigungsfreier Blockchains basiert auf Dezentralisierung. Die aktuellen Anreizmechanismen vieler Blockchains führen aber zur Bildung von Oligopolen, die über genügend Rechenleistung verfügen, um Attacken starten zu können.

Die Sicherheit aller Blockchains beruht auf der Annahme, dass die verwendeten kryptografischen Verfahren sicher sind. Quantencomputer könnten zukünftig aber in der Lage sein, viele der aktuell eingesetzten Verschlüsselungsverfahren auszuhebeln.



In neue Konsensmechanismen müssen wirtschaftswissenschaftliche Erkenntnisse einfließen, um Anreizstrukturen zu schaffen, die einer Zentralisierung entgegenwirken.

Quantensichere Verschlüsselungsverfahren werden in der Post-Quanten-Kryptografie erforscht. Hier muss sichergestellt werden, dass die neuen Verfahren sowohl in bestehende als auch neue Blockchains integriert werden.



Obwohl es ein lohnendes Ziel darstellt, wurde das Bitcoin-Netzwerk selbst noch nicht erfolgreich attackiert. Zusammenschlüsse von Validatoren, bei Bitcoin Miner genannt, kontrollieren jedoch einen gefährlich hohen Anteil der Rechenleistung. Auch sind nicht alle eingesetzten kryptografischen Verfahren quantensicher.



KOORDINIERUNG/GOVERNANCE



Öffentliche, genehmigungsfreie Blockchains haben keinen zentralen Betreiber beziehungsweise kein betreibendes Konsortium. Dennoch braucht es auch für Blockchains dieser Art tragfähige Wege, wie sich alle Beteiligten auf technische Weiterentwicklungen und andere Anpassungen der Blockchain einigen können. Verlässliche derartige Governance-Modelle für Blockchains ohne Betreiber gibt es bislang noch nicht.

Aktuell führen Meinungsverschiedenheiten oftmals zur Lähmung oder sogar zur Aufspaltung der Netzwerke (englisch „hard fork“) in zwei unabhängig voneinander weitergeführte Versionen. Dies muss nicht in jedem Fall negativ sein, Aufspaltungen als Normalfall würden jedoch am Vertrauen in die Technologie rütteln.



Expertinnen und Experten sehen Versuche kritisch, das Koordinationsproblem rein technisch, also durch die Integration von Abstimmungsmechanismen in die jeweilige Blockchain-Software, lösen zu wollen.

Realistischer erscheint eine Kombination solcher technischer Möglichkeiten mit angepassten Modellen der Multi-Stakeholder-Governance, beispielsweise in Anlehnung an die ICANN. Die Standardisierung der Blockchain-Governance ist auch Thema einer Arbeitsgruppe bei der International Organization for Standardisation (ISO).



Unstimmigkeiten über die Weiterentwicklung führten 2017 zur Abspaltung von Bitcoin Cash und Bitcoin Gold.

„Forks als Standardereignis rütteln am Vertrauen in die Blockchain-Technologie.“

2

Wie Blockchain Wirtschaft und Gesellschaft verändern kann

Bei Blockchain geht es stets um die Gestaltung von Beziehungen: zwischen Kundinnen und Verkäufern, Bürgern und Staat oder auch Nutzerinnen und Nutzern digitaler Plattformen. Hinzu kommt die Chance, mit Blockchain auch die koordinierende Beziehung von intelligenten Geräten zu ihren Nutzerinnen und Nutzern sowie zwischen den Geräten selbst dezentral und zukunftssicher zu gestalten. Im Folgenden werden Anwendungsszenarien vorgestellt, in denen eine Blockchain einen Mehrwert bieten kann. ►



2.1 Effiziente und transparente Lieferketten für Lebensmittel

Sieben Jahre nach der EHEC-Epidemie und der aufwendigen Suche nach dem Erreger ist es auch heute noch ein langwieriger Prozess, Lebensmittel-Lieferketten nachzuvollziehen. Auch jenseits konkreter Gesundheitsgefährdungen steigt bei den Verbraucherinnen und Verbrauchern der Wunsch nach einer transparenten und einfachen Nachverfolgbarkeit von Nahrungsmitteln.

Lieferketten sind bürokratisch höchst aufwendig

Bei internationalen Lieferketten sind oftmals bis zu dreißig Institutionen und über hundert Personen beteiligt, die circa 200-mal Informationen, oftmals auf Papier, austauschen müssen¹⁸. Dies ist teuer, langsam und fehleranfällig. Die Rückverfolgung der Herkunft – beispielsweise einer Portion abgepackten Obstes – kann mehr als sechs Tage dauern. Dies ist für Verbraucher kaum nachzuvollziehen.

Schreib- und Leserechte nach Bedarf verteilen

Der Einsatz einer Blockchain, in der die Beteiligten die Transaktionen der Lieferkette gemeinsam dokumentieren, kann hier deutliche Kosten- und Zeiteinsparungen ermöglichen. Eine Blockchain könnte das Misstrauen gegenüber einem zentralen registerführenden Akteur aufheben, da ein Blockchain-Register für alle Teilnehmenden zugänglich ist.

Die Buchführungs- und Leserechte können dabei gestuft verteilt werden, angepasst an die unterschiedlichen Nutzergruppen und deren Bedürfnisse, wie zum Beispiel Hersteller, Spediteure, Zoll und verschiedene Verbraucherinnen und Verbraucher.

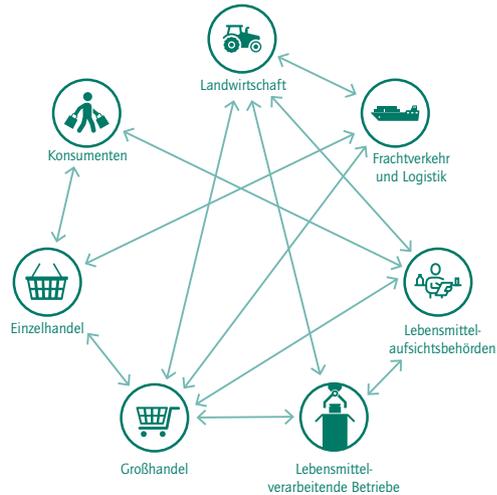
Somit herrscht keine vollständige Transparenz, die Wettbewerber ausnutzen könnten. Für Endverbraucherinnen und -verbraucher können zum Beispiel lediglich Leserechte eingeräumt werden, anhand derer die Herkunft und die gesamte Lieferkette von der Ernte über Verarbeitung, Logistik, Verzollung, Zertifizierung, Lebensmittelüberwachung, den Großhändler bis zum Einzelhandel transparent und überprüfbar nachvollzogen werden können.

Automatisierungspotenziale

Zudem gibt es Automatisierungspotenziale für die einzuhaltenen Dokumentationspflichten: So könnte beispielsweise ein im Container angebrachter Sensor die Temperatur von Lebensmitteln messen, die Messdaten in die Blockchain schreiben und so eine lückenlose Einhaltung der Kühlkette dokumentieren. Würde sie nicht eingehalten, könnte ein entsprechend aufgesetzter Smart Contract automatisch Alarm schlagen.

Chancen	Herausforderungen
<ul style="list-style-type: none">▪ Transparenz▪ Nachverfolgbarkeit▪ Zeiteinsparung▪ Automatisierungspotenziale	Bereitschaft der Lieferkettenteilnehmer zu gewisser Datentransparenz, verlässliche Übertragung von Realdaten in die Blockchain (► Kapitel 1.3)

Informationsflüsse im Lebensmittel-Lieferketten Management ohne Blockchain



Informationsaustausch im Lebensmittel-Lieferketten Management mit Blockchain-Einsatz



Vorteile einer Blockchain-Lösung für die Beteiligten

Landwirtschaft



- Dokumentation der Warengüte
- Erleichterung des Anschlusses an die Lieferkette

Frachtverkehr und Logistik



- Verbesserte Fähigkeit, rechtliche Vorgaben zu erfüllen
- Reduzierung händischer Prozesse

Lebensmittel-aufsichtsbehörden



- Reduzierung von Zertifikatsfälschungen
- Zeiteinsparung bei der Erneuerung von Zertifikaten

Lebensmittelverarbeitende Betriebe



- Vertrauensaufbau zwischen Einzelhandel, Lieferanten und Kundinnen/Kunden
- Automatisierung und Reduzierung von händischem Zertifikatsmanagement

Großhandel



- Schnelle und zielgerichtete Durchführung von Rückrufen
- Einfaches Teilen von internen Daten

Einzelhandel



- Schnelle und zielgerichtete Durchführung von Rückrufen
- Sicherstellung von Lebensmittel-Qualität für die Endkundin/den Endkunden

Konsumenten



- Schnelle Information bei eventuellen Rückrufen durch hohe Transparenz
- Verminderung von Nahrungsmittelbetrug

Quelle: Eigene, modifizierte Darstellung auf Basis von IBM-Food Trust 2018¹⁹ und IBM/Maersk open global trade digitization platform 2018²⁰



2.2 E-Government – eine Alternative zur Zentralisierung von Registern

In der Entwicklungszusammenarbeit wird die Blockchain als Chance gesehen, Grundbücher und andere Register in Staaten aufzubauen, in denen diese bislang nicht existieren oder unzuverlässig sind. Dies kann die Rechte der Bevölkerung stärken und ihr in vielen Fällen überhaupt erst die wirtschaftliche Teilhabe ermöglichen.

Der permanente und transparente Charakter der Blockchain kann helfen, dass Aufzeichnungen auch über mögliche Phasen der politischen Instabilität eines Staats hinaus erhalten bleiben und zu einer Durchsetzung von Rechtsansprüchen beitragen.

Eine zentrale Anlaufstelle auf dezentraler Basis

In Deutschland hingegen mangelt es nicht an Registern. Aktuell existieren 214. Das Problem liegt in der Fragmentierung dieser Registerlandschaft über Behörden und föderale Ebenen hinweg²¹. Der deutsche Föderalismus wird als Rahmenbedingung der Umsetzung innovativer E-Government-Ansätze oft übersehen, wenn Estland als Vorbild genannt wird.

Der mögliche Beitrag der Blockchain zu einer Modernisierung des Registerwesens liegt nicht darin, alle Daten in Zukunft auf einer zentralen, staatlich geführten Blockchain abzulegen. Sie dient stattdessen als sichere Infrastruktur für die Kommunikation zwischen den einzelnen weiterhin bestehenden Registern.

Bürgerinnen und Bürger können über die Blockchain abfragen, wo welche Daten von ihnen gespeichert sind und Aktualisierungen veranlassen. Gleichzeitig haben die einzelnen Behörden keinen freien Zugriff auf alle Daten. Die Zugriffsrechte sind transparent in der Blockchain festgelegt und die Schlüssel liegen in den Händen der Bürgerinnen und Bürger.

Richtig ausgestaltet macht eine E-Government-Blockchain die Menschen also nicht zu gläsernen Bürgerinnen und Bürgern. Sie versetzt sie stattdessen in die Lage, Behörden nur die für den jeweiligen Anlass erforderlichen Daten einmalig freizugeben.

Ein-Klick-Antrag oder sogar Kein-Klick-Antrag

Wirklich leistungsfähig wäre eine solche Blockchain-Lösung, wenn sie mit privat geführten Datenbanken kommunizieren kann und auch Open-Data-Anforderungen erfüllt.

Die Zulassung eines Autos könnte so vom Sofa aus erfolgen. Die oder der Anmeldende erteilt der Zulassungsstelle die Einwilligung, automatisch alle benötigten Informationen und Bescheide beim KFZ-Hersteller, der Versicherung und bei anderen Behörden abzurufen. Die Anmeldebestätigung wird sofort erteilt und dem gewählten Nummernschildhersteller eine einmalige Freigabe zur Aufbringung einer individualisierten Zulassungsplakette erteilt.

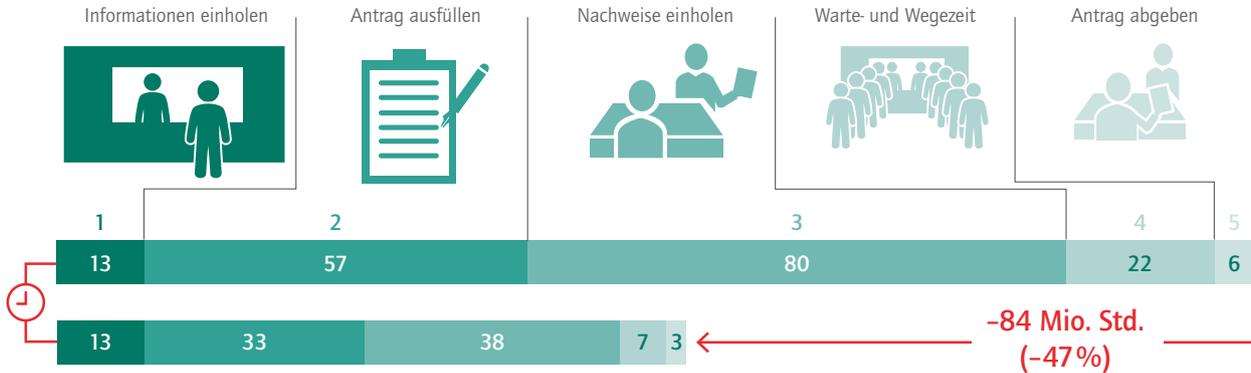
Ein weiteres Beispiel: Gerade nach der Geburt eines Kindes haben Eltern anderes im Sinn als Anträge bei Behörden auszufüllen. Staatliche Vorgänge wie die Bewilligung des Kindergelds könnten deshalb ohne vorherigen Antrag automatisch durchgeführt werden, sobald eine Geburtsurkunde digital abgelegt und mit den Daten der Eltern verknüpft wird.

Chancen	Herausforderungen
Effiziente, transparente und komfortable Verwaltungsprozesse	Einigung und Koordination aller föderaler Ebenen bei der Umsetzung

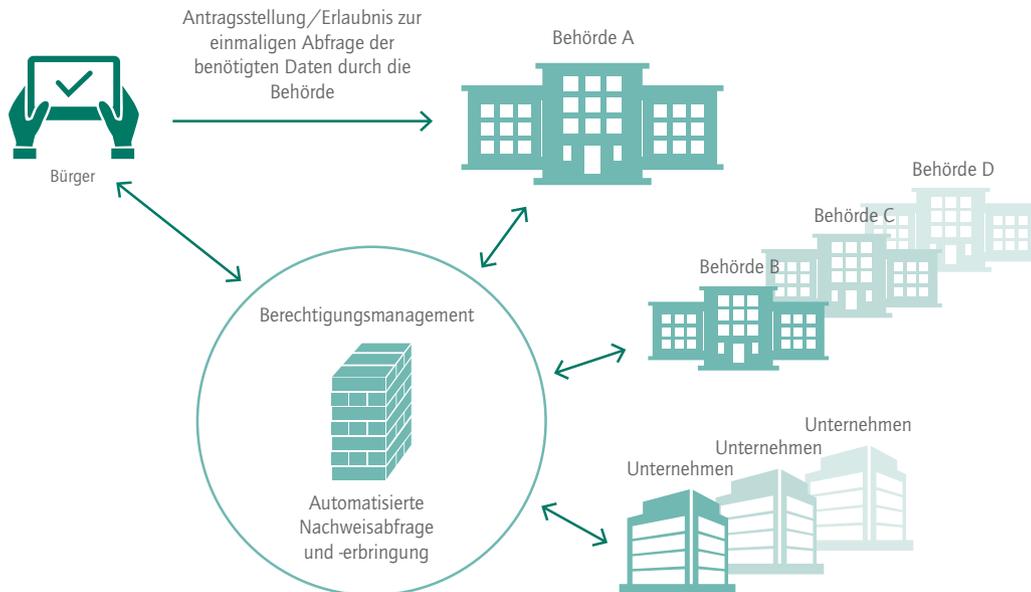
Vorteile eines modernen Registerwesens für Bürgerinnen und Bürger

in Mio. Std. pro Jahr

Ist-Zustand



Ziel-Zustand*



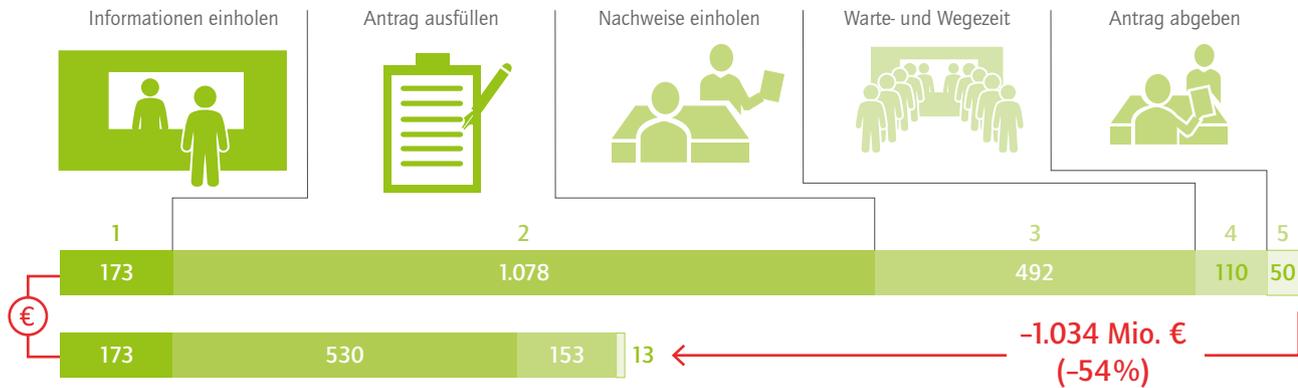
* Für Bürger wird eine 80%ige Nutzungsquote angenommen ("Opt-In")

Quelle: Eigene, modifizierte Darstellung auf Basis von Normenkontrollrat 2017²¹

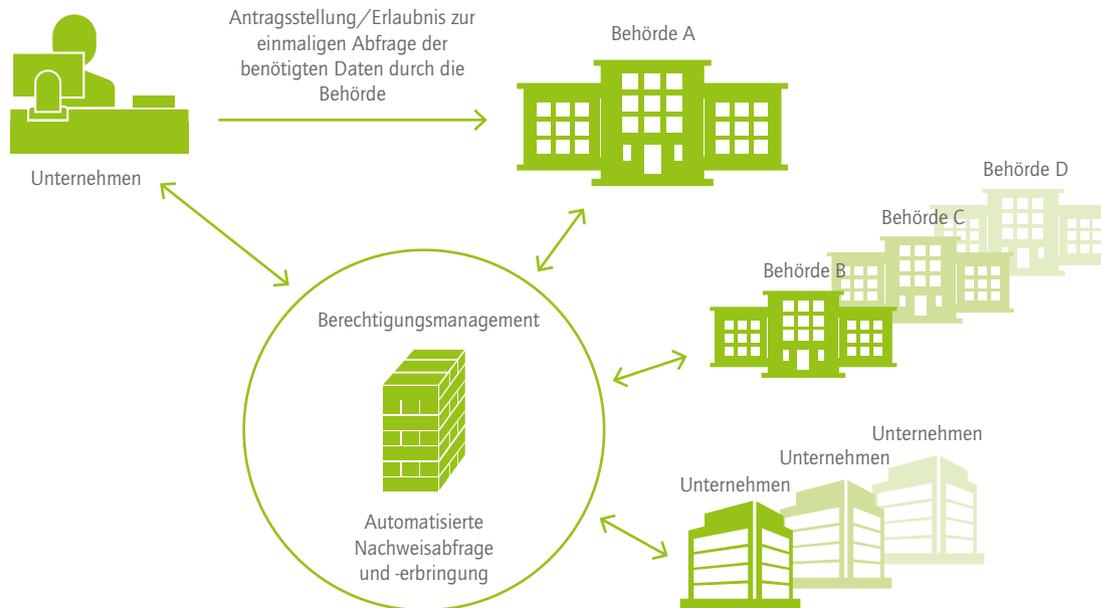
Vorteile eines modernen Registerwesens für Unternehmen

in Mio. € pro Jahr

Ist-Zustand



Ziel-Zustand



2.3 Facebook ohne Facebook – die Revolution der Plattformökonomie?

Eine breite Nutzung von Anwendungen auf Basis öffentlicher, genehmigungsfreier Blockchains steht noch von einer Reihe technologischer Herausforderungen. Gerade diese Art von Blockchains hat nach Einschätzung einiger Expertinnen und Experten aber das Potenzial, die aktuelle Plattformökonomie disruptiv zu verändern.

Das disruptive Versprechen

Öffentliche Blockchains als Kern digitaler Ökosysteme zielen darauf ab, mächtige Plattformanbieter zu ersetzen. Nutzerinnen und Nutzer profitieren von dem auf der Plattform generierten Mehrwert (z. B. über Token-Ausschüttung). Zudem behalten sie die Kontrolle über eigene Daten und entscheiden, mit wem sie diese zu welchen Konditionen teilen und erlangen somit Datensouveränität.

Blockchain ermöglicht, dass kein einzelner Konzern die Kontrolle über die erzeugten Daten besitzt und es keinen zentralen Akteur gibt, der den durch das Netzwerk geschaffenen Mehrwert abschöpfen kann. Hinter solchen Blockchain-Initiativen steckt oftmals die ideelle Motivation, Gemeingüter ohne Gewinnabsicht frei zugänglich zu machen und so dem Gemeinwohl zu dienen.

Anwendungsbeispiel: Steemit – ein soziales Netzwerk ohne zentralen Betreiber

Das Konzept: Steemit ist ein soziales Netzwerk, (ähnlich wie Reddit), bei dem Nutzerinnen und Nutzer Inhalte einstellen, bewerten („liken“) und teilen können. Steemit basiert auf einer öffentlichen, genehmigungsfreien Blockchain, der Steem-Blockchain.

Chance: Nutzerinnen und Nutzer werden mit Nutzungs-Token belohnt, wenn sie Inhalte erstellen, lesen oder bewerten. Häufig angeklickte Inhalte steigen im Ranking und sind somit mehr Token wert. Sowohl Autoren als auch Kuratoren profitieren also von Aktivität und Wachstum des Netzwerks, nicht ein zentraler Betreiber.

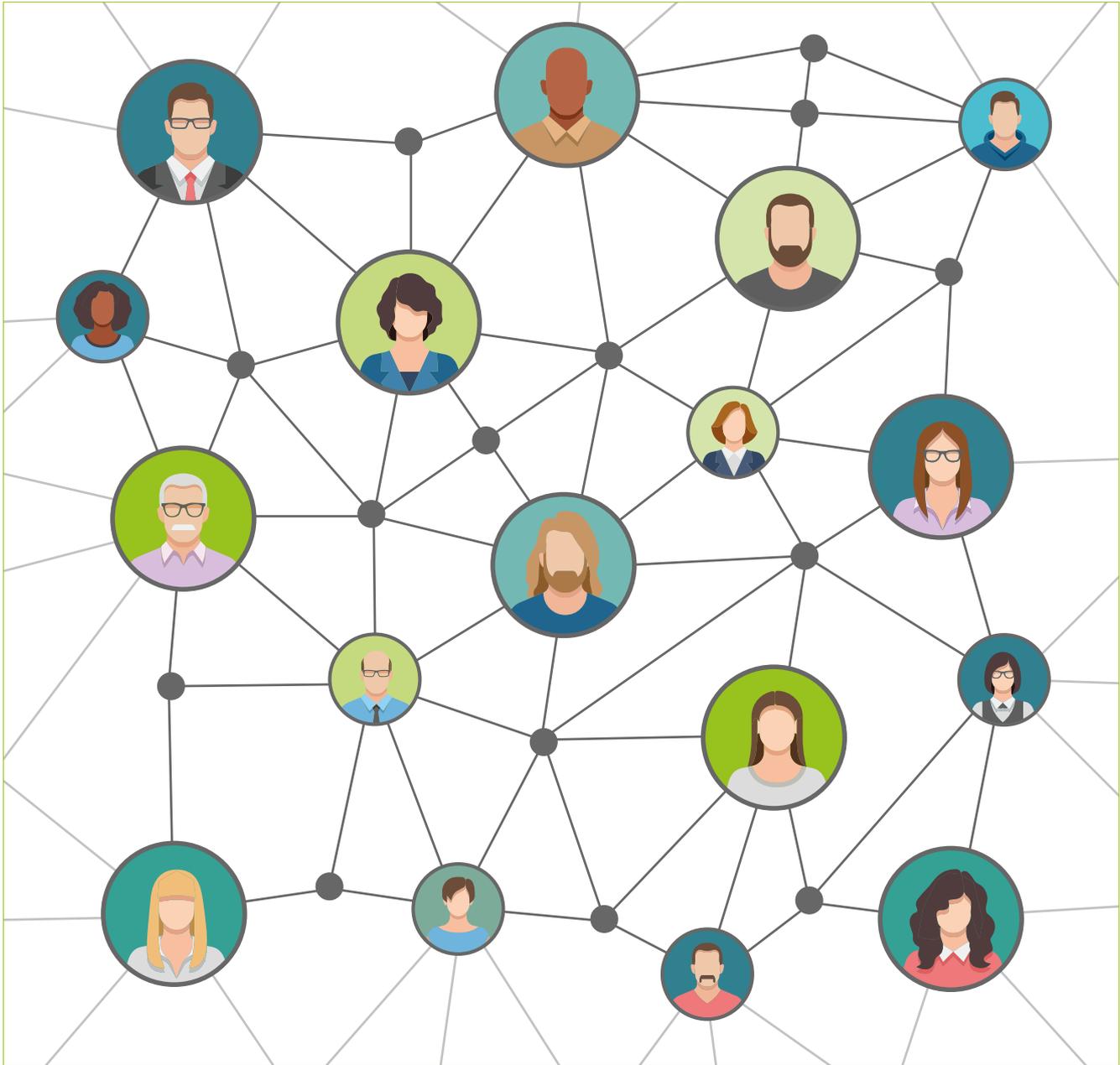
Außerdem dient der Token als Anreiz-Token für die Betreiber des Netzwerks. Token können auf Börsen gegen andere Währungen (auch Euro und US-Dollar) oder Token getauscht werden.

Konsensmechanismus: Delegated Proof-of-Stake: Nicht jene mit einem großen Anteil (englisch „Stake“) an den Token eines Netzwerks, sondern gewählte Vertreterinnen und Vertreter, sogenannte „Witnesses“, generieren Blöcke. Die Nutzerinnen und Nutzer wählen diese Personen.

Gefahr: Eine Nutzergruppe mit einer großen Menge an Netzwerkeinfluss, der über Token zu erlangen ist („Steem Power“), kann eigene Inhalte dauerhaft prominent platzieren. Zwar bleiben alle anderen Inhalte weiterhin vorhanden, unpopuläre Meinungen können jedoch so unterdrückt werden.

Zensurreistenz: Unbeliebte Inhalte können markiert („geflagged“) werden. Eine solche Markierung blendet die betreffenden Inhalte im Netzwerk aus, was sich aber negativ auf die Reputation und die Belohnung der Autorin/des Autors auswirkt. Vollständig gelöscht werden kann ein Inhalt aber nicht, auch nicht von der Autorin oder dem Autor selbst. Ausgeblendete Inhalte bleiben auf der Blockchain gespeichert. Dasselbe gilt für pseudonyme Nutzernamen und Nutzer-Accounts insgesamt.

Chancen	Herausforderungen
Disruption der Plattformökonomie, Nutzerinnen und Nutzer erhalten Datenhoheit und werden für ihre Aktivitäten im Netzwerk (z. B. Inhalte schreiben, liken) entlohnt	Rechtliche Rahmenbedingungen, Zensurreistenz, Oligarchie von Nutzerinnen und Nutzern mit hohem Netzwerkeinfluss



2.4 Eine sichere gemeinsame Sprache für intelligente Geräte und digitale Assistenten

Vernetzte Geräte wie Kameras, Werkzeugmaschinen und Tablets sind zunehmend Cyber-Angriffen ausgesetzt und benötigen deshalb regelmäßige Sicherheits-Updates. Blockchains können helfen, diesen meist über das Internet durchgeführten Update-Prozess abzusichern.

Der Hersteller hinterlegt dafür den digitalen Fingerabdruck des Updates auf einer Blockchain. Das Gerät vergleicht dann den Fingerabdruck der Update-Datei, die es heruntergeladen hat, mit dem Eintrag in der Blockchain. Unterscheiden sie sich, hat während der Übertragung eine Manipulation stattgefunden. Das Gerät verwirft diese Datei dann und lädt das Update neu herunter.

Ähnliche Verfahren können im Kontext von Industrie 4.0 eingesetzt werden, um die korrekte Übermittlung von Fertigungsdaten und Maschineneinstellungen zu prüfen. Über Smart Contracts kann zudem festgelegt werden, wie oft und zu welchem Zweck freigegebene Daten, beispielsweise Blaupausen für die additive Fertigung, vom Empfänger genutzt werden können.

Automatisierung von Transaktionen

Intelligente Geräte und digitale Assistenten tauschen Daten nicht nur mit ihren Herstellern. Um unser Leben wirklich zu erleichtern, müssen sie auch untereinander abgestimmt sein und Leistungen austauschen.

Wir wären aber schnell frustriert, müssten wir jede einzelne Einstellung und Verknüpfung von Hand vornehmen. Vielmehr soll die Koordination automatisch im Hintergrund erfolgen, ohne dabei unsere Aufmerksamkeit zu beanspruchen. Bei Geräten desselben Herstellers funktioniert dies bereits oft gut. Probleme tauchen aber spätestens dann auf, wenn irgendwann der für die Steuerung zuständige Server abgeschaltet wird. Komplikationen gibt es aber meist schon deutlich früher: wenn man versucht, das Gerät eines anderen Herstellers zu integrieren.

„Ohne Blockchain ist Industrie 4.0 nicht zu machen.“

Blockchains könnten sich zu dezentralen, herstellerunabhängigen gemeinsamen Sprachen für das Internet der Dinge und Dienste weiterentwickeln. Mit Smart Contracts und Token haben sie grundsätzlich die dafür nötigen Voraussetzungen.

Ein Elektrofahrzeug könnte so beispielsweise mit jeder beliebigen Ladestation eine auf den Cent genaue Abrechnung vornehmen, ohne dass sein Fahrer oder seine Fahrerin mehr tun muss, als die Steckerverbindung herzustellen.

Dieses und ähnliche Szenarien setzen nicht nur die Entwicklung ausreichend leistungsfähiger Blockchains voraus, sondern auch eine Bereitschaft der Hersteller, entsprechende Schnittstellen in die Geräte einzubauen und passende Geschäftsmodelle zu entwickeln.

Zwei oft diskutierte Zukunftsvisionen



SELBSTFAHRENDES UND SICH SELBST VERWALTENDES FAHRZEUG

Hier knüpfen sich hohe Erwartungen an die Künstliche Intelligenz und an die Token-Ökonomie. Das Auto der Zukunft soll nicht nur den Straßenverkehr eigenständig meistern. Es verdient durch die Beförderung von Passagieren auch seine eigenen Token. Mit diesem bezahlt es an der Tankstelle und auch die von ihm selbst in Auftrag gegebenen Reparaturen. Überschüsse führt es an seinen Besitzer ab, der nichts tun muss, außer sich über den Gewinn zu freuen.



DEZENTRALE AUTONOME ORGANISATIONEN (DAOS)

Ganze Organisationen sollen zukünftig über Blockchains gesteuert werden können. Ihre Strukturen, Regeln und Verfahren werden dabei als Geflecht von Smart Contracts realisiert. Die Eindeutigkeit ihres für alle einsehbaren Codes sorgt nicht nur für eine maximale Transparenz der Entscheidungen. Es sollen in einer DAO sogar Menschen erfolgreich miteinander kooperieren können, die keine gemeinsame Sprache außer der Programmiersprache sprechen, in der die Regeln festgeschrieben sind.



EINORDNUNG

Eine Verwirklichung dieser Zukunftsvisionen ist nach Meinung von Expertinnen und Experten nicht ausgeschlossen, liegt aber noch weit in der Zukunft.

Dennoch lohnt es sich, schon heute über derartige Szenarien nachzudenken: Es wird bereits an der Verwirklichung von Teilaspekten gearbeitet. Beim Experimentieren mit diesen Ansätzen können neue Geschäftsmodelle und Formen der Kooperation entdeckt werden, die ohne Blockchain nicht denkbar sind.

Außerdem machen gerade diese weitreichenden Zukunftsbilder rechtliche, regulatorische und ethische Fragestellungen sichtbar, die durch neue Technologien wie Blockchain und auch ihr Zusammenspiel mit der Künstlichen Intelligenz aufgeworfen werden (► Kapitel 4.5).



Quelle: Eigene Darstellung

2.5 Wann macht eine Blockchain Sinn?

Blockchains sind nicht automatisch die „bessere“ Lösung. Sie müssen für Anwendungen nicht nur technisch machbar sein, sondern bisherigen Lösungen auch in der wirtschaftlichen und/oder sozialen Dimension überlegen sein.

„Auch Blockchain ist immer ein Trade-off.“

Blockchain ist ein Werkzeug, kein Allheilmittel

Es gibt viel Hype um mögliche Blockchain-Anwendungen, oft bleibt aber unklar, worin der Mehrwert einer Umstellung auf Blockchain liegen soll. Blockchain ist eine mögliche Lösung von vielen und eine wertvolle Ergänzung der verfügbaren Datenbanktechnologien – aber diesen nicht automatisch überlegen.

„Blockchain ist mindestens fünfzig Prozent Change Management.“

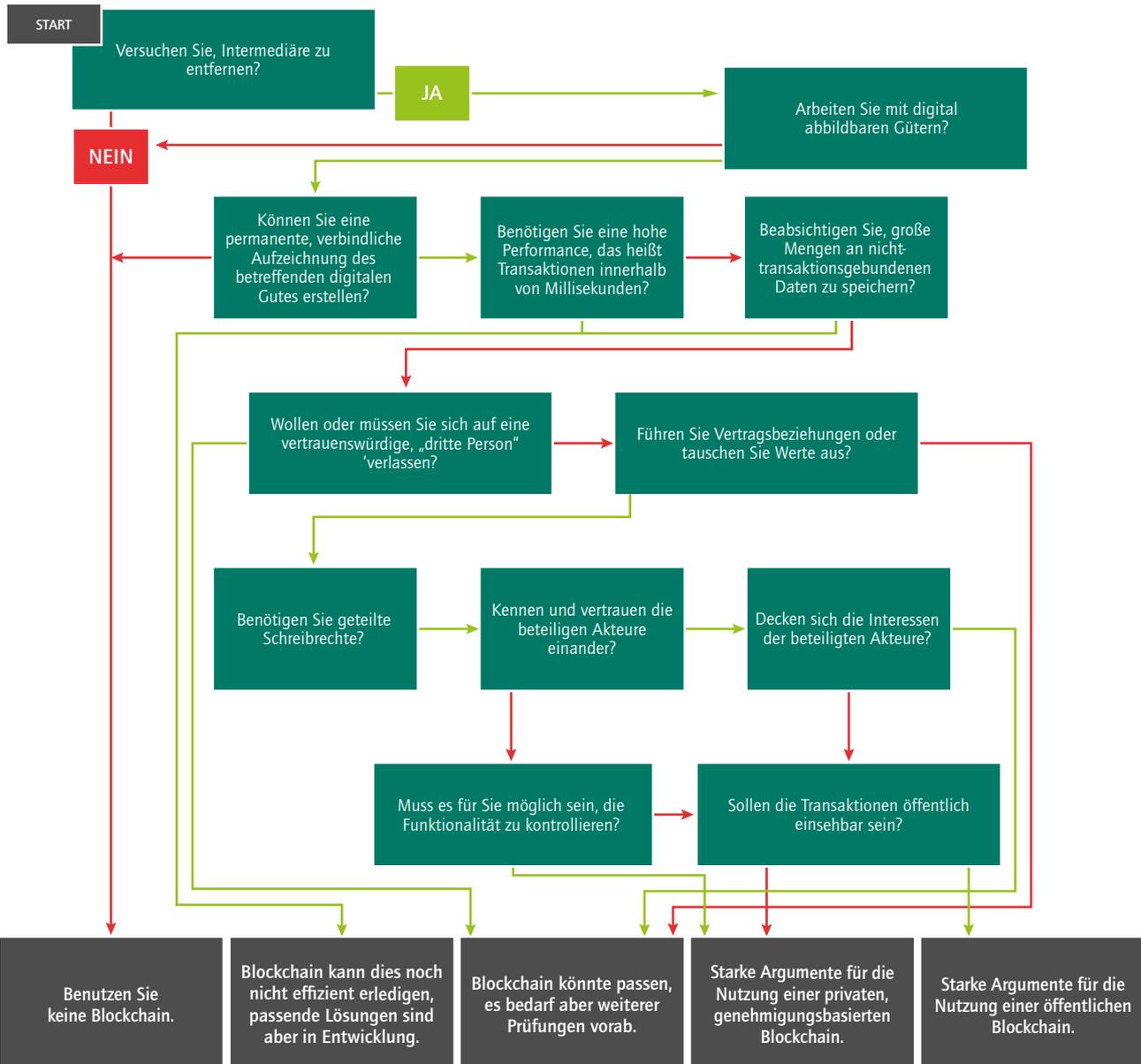
Wenn zum Beispiel nur eine vom Netzwerk akzeptierte Nutzerin beziehungsweise nur ein von diesem akzeptierter Nutzer existiert, die/der Daten registriert, bietet eine Blockchain keinen zusätzlichen Vorteil. Eine klassische Datenbank hätte in diesem Fall eine bessere Leistung bezüglich des Datendurchsatzes.

Wann brauche ich eine Blockchain und wann nicht?

Kriterien: Ob eine Blockchain-Lösung Sinn macht, entscheiden der Transparenz- und Nachvollziehbarkeitsbedarf sowie die Verfügbarkeit und die Kosten von Intermediären, aber auch die Zahl der Beteiligten und der Grad des Vertrauens dieser zueinander.

Weitreichende Implikationen: Eine Umstellung auf Blockchain ist nichts, was verborgen im Maschinenraum passiert. Soll sie tatsächlich ganzes Potenzial entfalten, bedeutet dies meist eine Umstellung von Prozessen, Organisationsstrukturen und Beziehungen in wirtschaftlichen Ökosystemen.

Wann macht eine Blockchain Sinn?



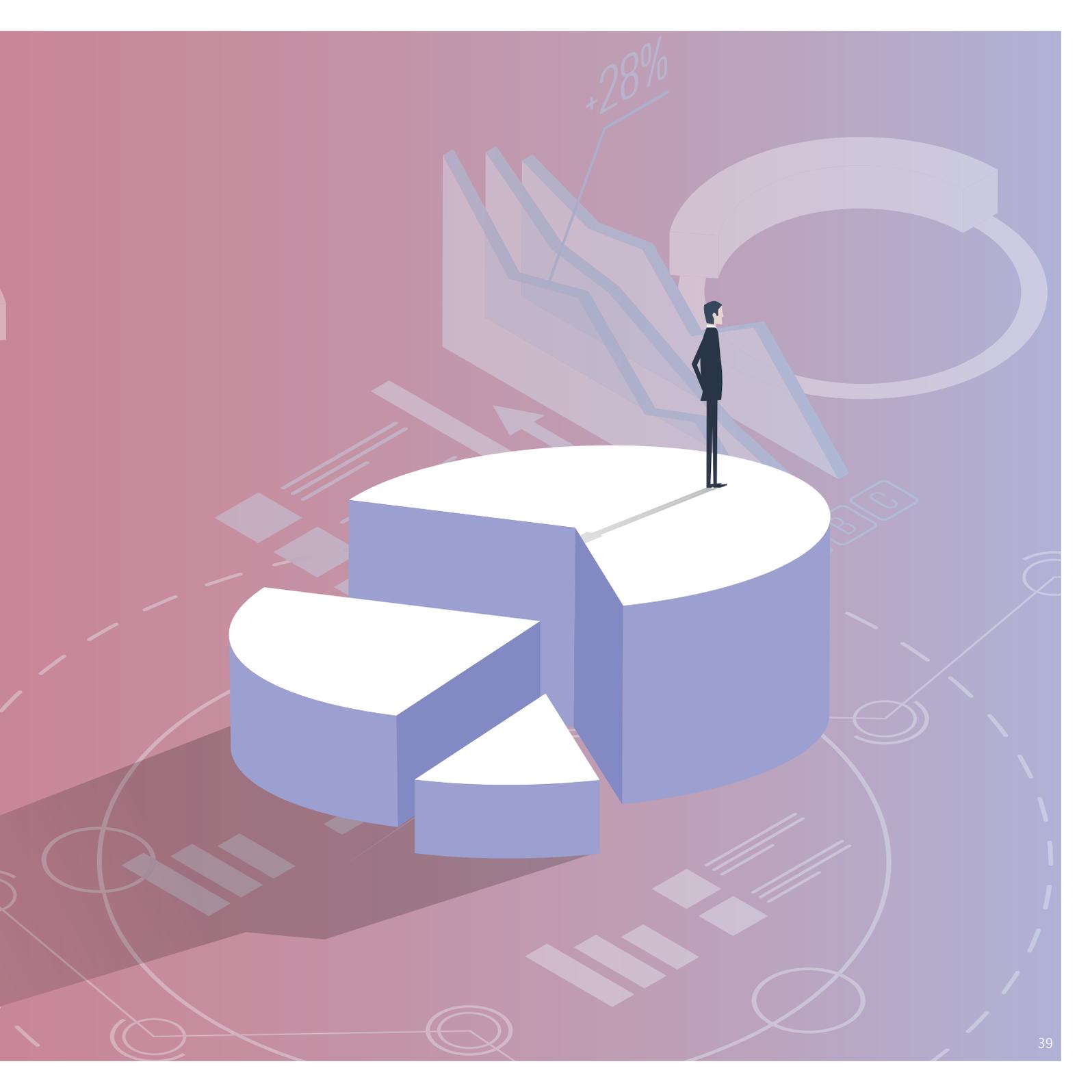
3



Der internationale Wettlauf um die Blockchain – Schlaglichter

Blockchain ist keine Silicon-Valley-Technologie, aber auch dort wächst das Interesse an ihr rasant. In China und Russland wird die Technologie in einem Atemzug mit Künstlicher Intelligenz und Quantentechnologien genannt. Umfassende und zugleich belastbare Analysen der wirtschaftlichen und wissenschaftlichen Dynamik rund um Blockchain gibt es noch nicht.

Die Schlaglichter des folgenden Kapitels zeigen aber: Deutschland und Europa besitzen durchaus Potenzial im Hinblick auf diese junge Technologie. Dies allein reicht im internationalen Wettlauf um die Technologieführerschaft aber nicht aus. Soll eine Technologie- und Marktführerschaft erreicht werden, müssen die Potenziale schnell genutzt und sinnvoll miteinander kombiniert werden. ►



3.1 Blockchain-Ökosystem in Deutschland

Blockchain ist keine Silicon-Valley-Technologie. Sie entstammt freien Entwicklercommunities und viele bedeutende Köpfe leben und arbeiten in Berlin. Es genügt aber nicht, sich auf dem Berliner Blockchain-Ökosystem auszuruhen. Dieser und andere Blockchain-Standorte mit innovativen Start-ups müssen aktiv ausgebaut und weiterentwickelt werden, was auch Aktivitäten der Politik erfordert.

Nur so könnte Deutschland diese vorhandenen guten Anlagen tatsächlich auch nutzen, um nach langer Zeit wieder eine führende Rolle bei einer digitalen Technologie einzunehmen. Aktuell sehen die Expertinnen und Experten Deutschland im internationalen Wettbewerb eher ins Hintertreffen geraten.

*„Hier sind wir nicht abgehängt,
aber der Zug fährt schnell weiter.“*



Blockchain-Ökosystem in Deutschland



3.2 Weltweit entstehen Blockchain-Konsortien – auch große Unternehmen sind mit dabei

Die Wirtschaft hat die Potenziale der Blockchain-Technologie erkannt. Nicht nur Start-ups, auch etablierte Unternehmen investieren zunehmend. Es haben sich viele Konsortien gebildet,

auch unter deutscher Beteiligung. Google, Facebook, Apple und Amazon zeigten lange wenig Interesse am Thema Blockchain, haben aber nun ebenfalls erste Aktivitäten begonnen.

Übersicht über wichtige Blockchain-Konsortien und Business-Netzwerke weltweit			
Start	Konsortienname	Mitglieder	Auswahl an Mitgliedern
Oktober 2012	Ripple	100+	Bank of England, Bank of America, BBVA, Santander, SEB, UBS, UBS, UniCredit
September 2015	Corda	70+	entwickelt von R3: u. a. Citi, Commerzbank, Credit Suisse, Deutsche Bank, UniCredit, UBS
Dezember 2015	Hyperledger	250+	Accenture, Airbus, American Express, Change Healthcare, Cisco, CME Group, Daimler, Deloitte, Deutsche Börse Group, Digital Asset, DTCC, EY, Fujitsu, Huawei, Hitachi, IBM, Intel, J. P. Morgan, NEC, Oracle, R3, Samsung SDS, SAP, Swift, Wanda Group
Oktober 2016	B3i Konsortium	15	Achmea, Aegon, Ageas, Allianz, Generali, Hannover Re, Liberty Mutual, Munich Re, RGA, SCOR, Sompo Japan Nipponkoa Insurance, Swiss Re, Tokio Marine Holdings, XL Catlin, Zurich Insurance Group
Dezember 2016	Trusted IoT Alliance	36	Aero Token, BigchainDB, BitSE, BNY Mellon, BOSCH, Chronicled, Cisco Systems, Clause, Consensus Systems, FOAM, Gemalto, IOTA, Ledger, QTUM, Riddle&Code, skuchain, slock.it, T-Labs Blockchain Group, UBS, usbank
März 2017	Enterprise Ethereum Alliance	500+	Accenture, BNY Mellon, BBVA, BNP Paribas, BP, Cisco, CME Group, Credit Suisse, Deloitte, DTCC, IC3, ING, Intel, J. P. Morgan, Mastercard, Microsoft, Samsung SDS, Santander, Thomas Reuters, Toyota Research, UBS
Mai 2017	Energy Web Foundation	37	Centrica, Eandis, Elia, Eneco, Engie, Eon, Innogy, PG&E, Royal Dutch Shell, Sempra Energy, SP Group, Statoil ASA, Stedin, Swisspower, TWL, Tepco,
Mai 2017	Enerchain	40+	RWE, Eon, Uniper, Wien Energie, Eneco, Verbund, Vattenfall, EDF, Statkrat, Total, Capital Stage, OMV, Iberdrola, Axpo
September 2017	IBM Food Trust	10	Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever, Walmart
Mai 2018	MOBI (Mobility Open Blockchain Initiative)	40+	Accenture, BigchainDB, Blockchain at Berkeley, BMW, Bosch, ConsenSys Systems, Crypto Valley Association, Ford, General Motors, Hyperledger, IBM, IOTA Foundation, MotionWerk, Renault, Trusted IoT Alliance, VeChain, Xain, ZF Friedrichshafen AG

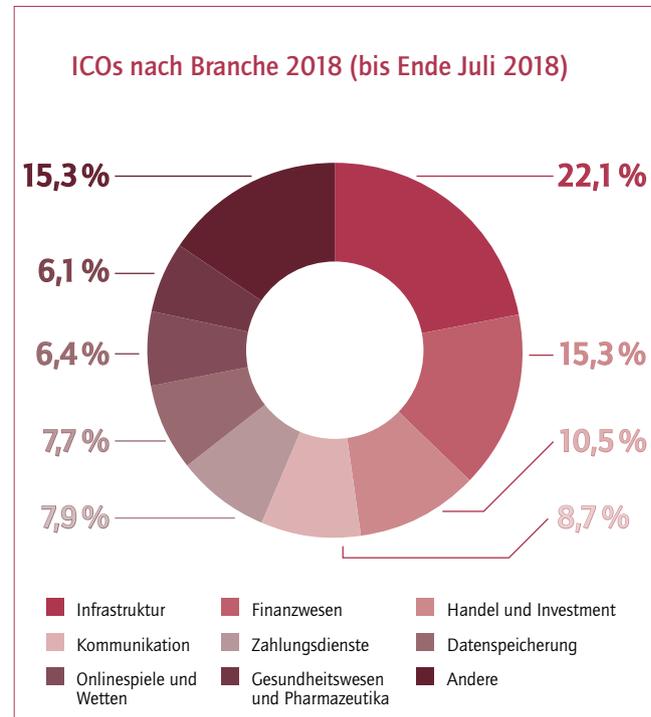
3.3 ICOs und Patente zeigen: Der Wettlauf um Blockchain hat begonnen

Regierungen vieler Staaten zeigen Interesse an der Blockchain-Technologie, vor allem asiatische Staaten und Russland. Innerhalb Europas positionieren sich die Schweiz, Estland, Gibraltar und Malta mit einem günstigen Rechtsraum für ICOs. Patentanmeldungen werden vor allem in den USA und in China getätigt. Deutschland ist in diesem weltweiten Patentranking eher im hinteren Feld positioniert.

Deutschland gerät in eine Schieflage. Viele Blockchain-Startups haben Teams, die in Berlin leben und arbeiten. Das dort geschaffene geistige Eigentum und die Unternehmen selbst werden dann aber nicht in Deutschland angemeldet. Andere Staaten bieten mittlerweile günstigere Rahmenbedingungen für ICOs und bemühen sich aktiv um die Ansiedlung von Blockchain-Startups. Deutschland droht damit im internationalen Wettbewerb zurückzufallen.

ICOs liefern schnelles Geld – kluge Köpfe folgen

Initial Coin Offerings haben sich als neues, allerdings regulierungsbedürftiges, Finanzinstrument etabliert, als zentrale Kapitalquelle für Blockchain-Startups in allen Bereichen. Ein innovationsfreundlicher regulatorischer Rahmen ist Voraussetzung, damit Kapital in deutsche Start-ups fließt.



Quelle: Eigene Darstellung auf Basis von CoinSchedule 2018²⁶

„Die Schweiz hat das Branding von Blockchains verstanden.“

ICO Gesamtvolumen im Verlauf seit 2016	
ICO Gesamtvolumen 2016:	USD 95.181.391
ICO Gesamtvolumen 2017:	USD 3.695.018.203
ICO Gesamtvolumen 2018 (bis Ende Juli 2018):	USD 16.921.733.861

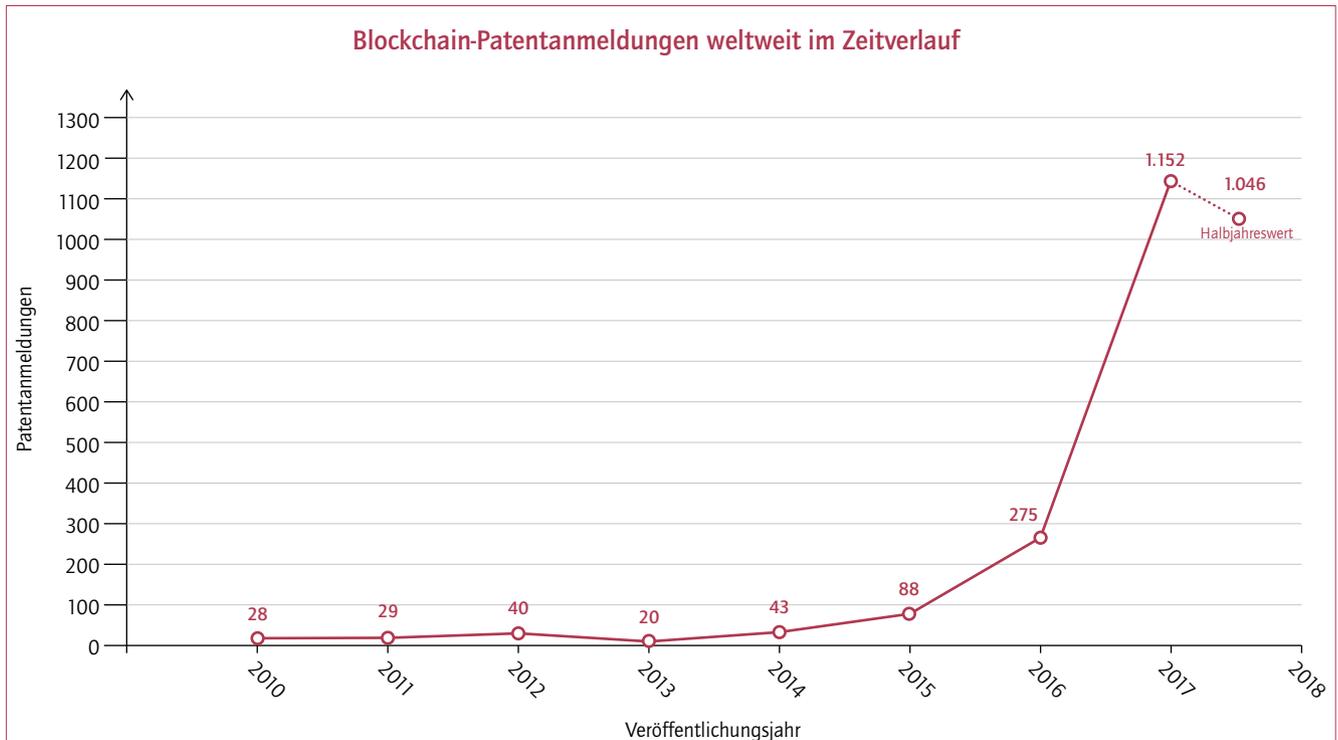
Quelle: Eigene Darstellung auf Basis von CoinSchedule 2018²⁶

Die weltweiten Patentanmeldungsaktivitäten zu Blockchain und anderen Distributed Ledger Technologien sind seit 2017 rasant gestiegen. Im ersten Halbjahr 2018 lagen bereits 1046 Patentveröffentlichungen vor – also bereits fast so viele wie im gesamten Jahr 2017.

Weitere Informationen und aktuelle Zahlen zu ICOs finden Sie hier:



<https://www.acatech.de/horizonte/blockchain/ico>

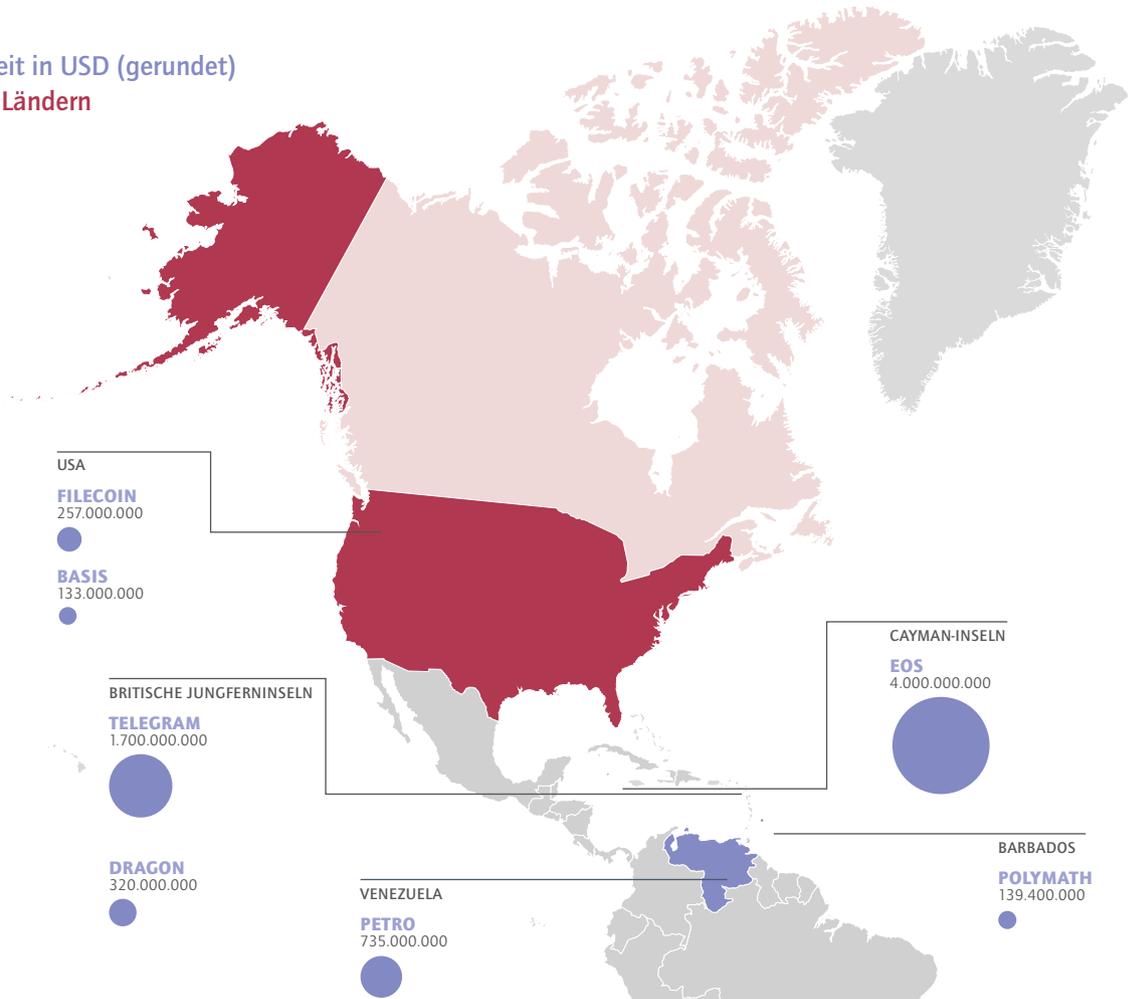
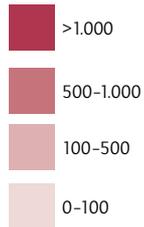


Eigene Darstellung auf Basis einer Patentrecherche von PROvendis, Analysezeitraum 01.01.2010 bis 30.07.18.

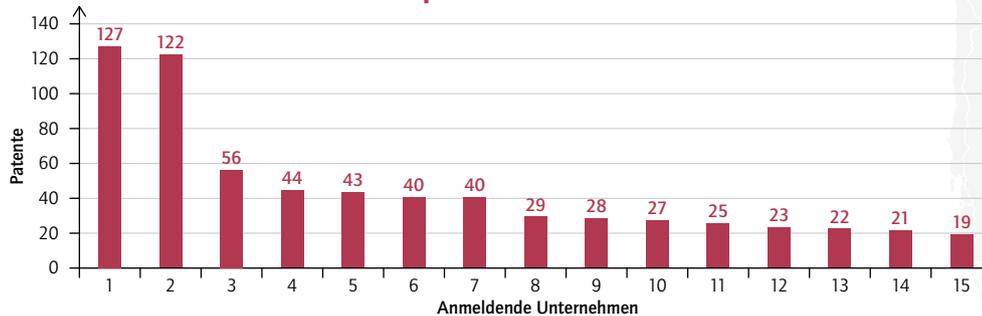


20 größte ICOs weltweit in USD (gerundet)

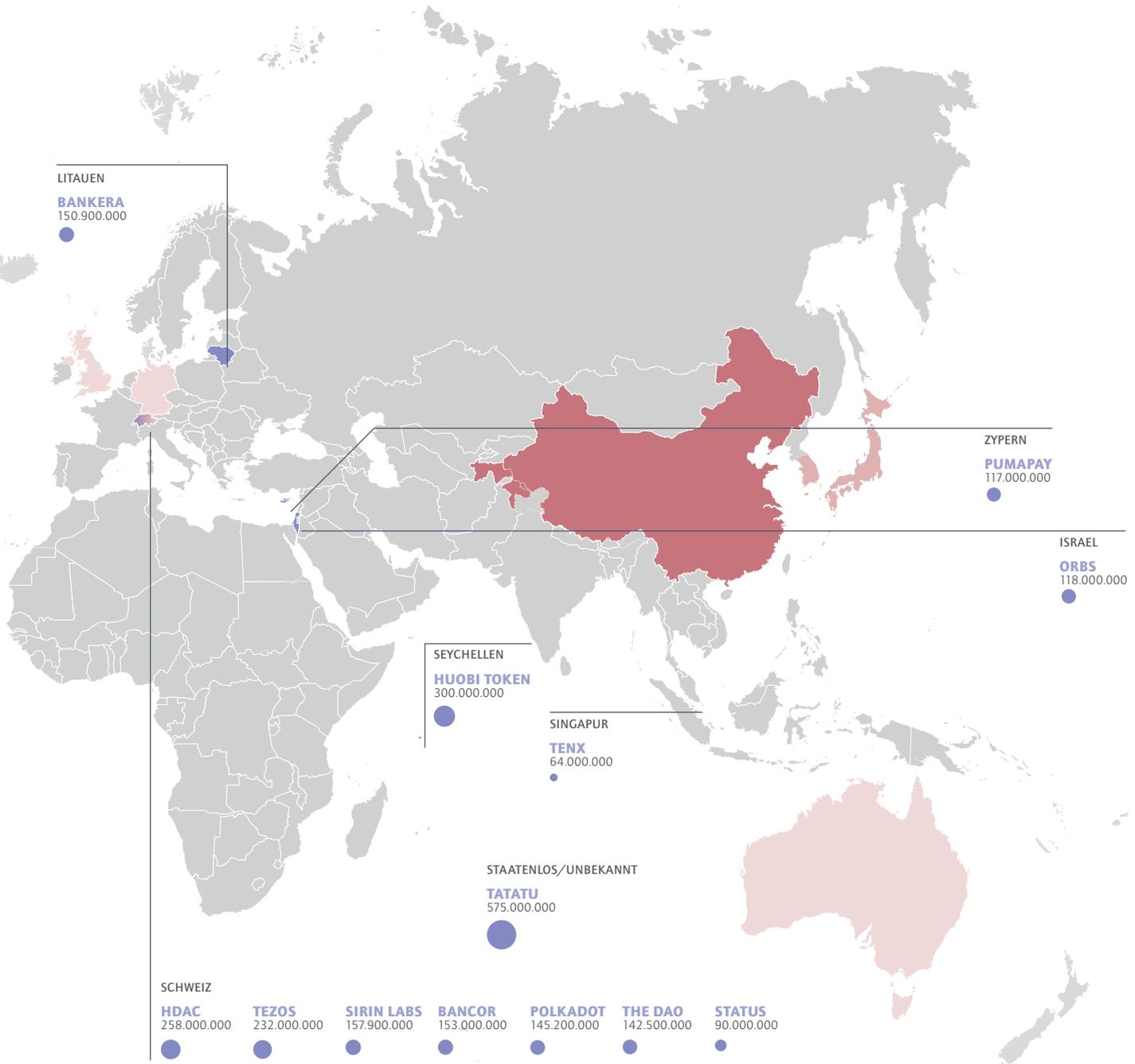
Patentintensität nach Ländern



Blockchain-Patente Top 15 nach Unternehmen weltweit



1. Coinplug Inc.
2. IBM
3. Bank of America
4. Qualcomm
5. Intel
6. Mastercard
7. LG Electronics
8. Apple
9. Beijing Rui Zhuo Xi Technology Development Co. Ltd
10. Alibaba Group
11. Amazon Technologies Inc.
12. Ericsson
13. Samsung Electronics
14. American Express
15. Jiangsu Payegis Technology Co. Ltd.



3.4 Akademische Blockchain-Aktivitäten

Weltweit wurden in den vergangenen Jahren erste akademisch ausgerichtete Blockchain-Zentren gegründet. Expertinnen und Experten bewerten die Aktivitäten in anderen Staaten, auch innerhalb Europas, als weiter vorangeschritten. Sie begrüßen daher erste Initiativen wie das Frankfurt School Blockchain Center, das Fraunhofer Blockchain-Labor und den geplanten Blockchain-Master der Hochschule Mittweida. Weiterhin fehlt in Deutschland ihrer Einschätzung nach aber ein „Hub“, ein

Zentrum mit kritischer Masse. Sie mahnen daher eine Bündelung der Kräfte an, die in ihren Augen nur mit Unterstützung durch die Politik verwirklicht werden kann.

Die Europäische Kommission hat im Februar 2018 das European Blockchain Observatory eingerichtet und angekündigt, bis 2020 bis zu 340 Millionen Euro in Blockchain-Projekte zu investieren.

Akademische Blockchain-Aktivitäten in Europa (Schlaglichter)



FINNLAND
HELSINKI
SOFIE Project



DÄNEMARK
KOPENHAGEN
European Blockchain Center



NIEDERLANDE
AMSTERDAM
Blockchain & Society Policy Research Lab



BELGIEN
BRÜSSEL
Blockchain: a new framework for swarm Robotic Systems



VEREINIGTES KÖNIGREICH
LONDON
Blockchain at LSE



DEUTSCHLAND
SANKT AUGUSTIN, BAYREUTH
Fraunhofer Blockchain-Labor

MITTWEIDA
Blockchain Competence Centre

FRANKFURT
Frankfurt School Blockchain Center

DARMSTADT
Center for Secure Distributed
Ledgers and Contracts

MÜNCHEN
TUM Blockchain Research Center



ÖSTERREICH
WIEN
Institut für Kryptoökonomie



SCHWEIZ
UNIVERSITÄT BASEL
Center for Innovative Finance

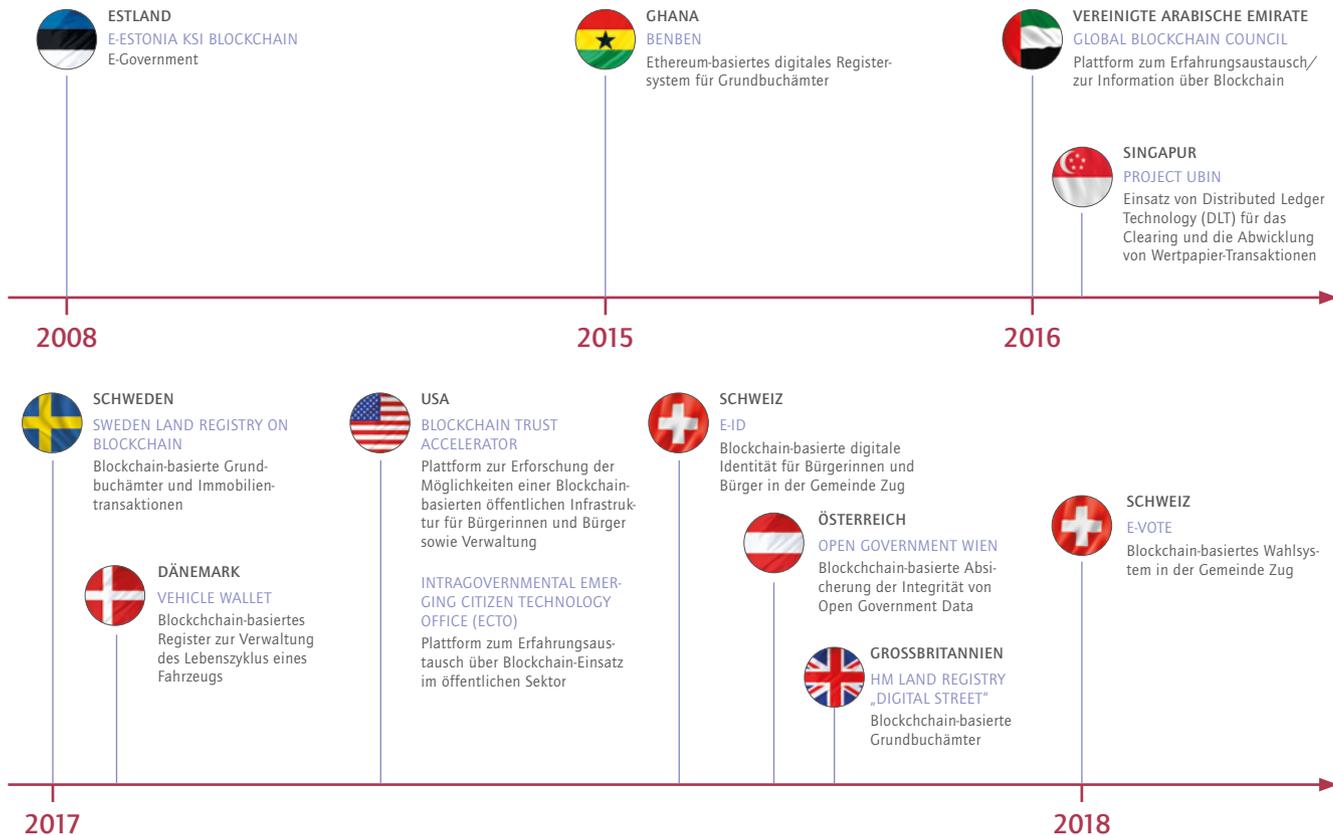


ITALIEN
TURIN
Titanium (Tools for the Investigation
of Transactions in Underground
Markets), Blockchain Initiative

3.5 Blockchain-Anwendungen im öffentlichen Sektor, privat-öffentliche Initiativen weltweit

Es sind weltweit Konsortien entstanden, die den Einsatz der Blockchain-Technologie im öffentlichen Sektor in unterschiedlichen Bereichen erforschen. Diese Konsortien schaffen meist eigene Plattformen, zugeschnitten auf die Bedürfnisse ihrer Mitglieder.

Blockchain-Anwendungen im öffentlichen Sektor





acatech HORIZONTE erklärt Blockchain

Blockchain zeichnet sich klar als bedeutendes Technikfeld der Zukunft ab - die gesellschaftliche und politische Debatte steht jedoch erst am Anfang. Was macht die Technologie aus? Welche Chancen bietet sie? Welche Hürden gilt es zu bewältigen?

Unser **Blockchain Erklärfilm** gibt in drei Minuten einen kurzen Einblick in die Blockchain-Technologie. Erfahren Sie, wo die Technologie bereits Anwendung findet und vor welchen Herausforderungen wir noch stehen.

Unseren **Blockchain Erklärfilm** finden Sie auf unserer **acatech HORIZONTE** Website unter:



[https://www.acatech.de/
horizonte/blockchain/
erklaerfilm](https://www.acatech.de/horizonte/blockchain/erklaerfilm)

3.6 Standardisierung stellt Weichen für die Marktentwicklung

Die Standardisierung von Begriffen und Prozessen ist eine wichtige Voraussetzung für die Entwicklung des Rechtsrahmens. Standards stellen Weichen für die weitere Entwicklung der Technologie und formalisieren Wertvorstellungen (z. B. europäische Anforderungen an Datenschutz versus niedrige Schutzniveaus in China). Die Beteiligung an Standardisierungsaktivitäten eröffnet zudem einen Zugang zu internationalen Netzwerken. Die ISO-Gruppe „Blockchain and distributed ledger technologies“ weist sehr viel Dynamik und ein großes staatliches Interesse vieler Länder auf, unter anderem von Russland (Vorsitz der Security-Gruppe) und China.

DIN bringt sich bei der ISO ein

Das DIN hat bei der ISO-Gruppe zu Smart Contracts den Vorsitz. Das deutsche Engagement in dieser Gruppe erfolgt in einem erheblichen Maße aus Wirtschaft und Wissenschaft. Den Expertinnen und Experten zufolge gibt es aber (zu) wenig Engagement und Aufmerksamkeit vonseiten der deutschen Politik, zudem ist die deutsche Delegation eher klein.

Beispiel Interoperabilität

Problemstellung: Bislang gibt es keine bis wenig Interoperabilität zwischen einzelnen Blockchain-Projekten. Folgen: wenig Flexibilität für wechselwillige Nutzerinnen und Nutzer; Entwicklerinnen und Entwickler müssen sich aufwendig in neue Blockchain-Strukturen einarbeiten.

Standards können dazu beitragen, diese Hürden abzubauen.

Initiativen haben sich gegründet, die explizit Interoperabilität zum Ziel haben, zum Beispiel BIA (Blockchain Interoperability Alliance).

Öffentlich geförderte BC-Projekte sollten sich an Standards und Normen orientieren. Dies steigert die wirtschaftliche Verwertbarkeit der entwickelten Blockchains (insbesondere auch durch KMU) und könnte indirekt die deutsche Normungsarbeit stärken.

„Normung und Standardisierung können helfen, Ängste und Vorbehalte zu adressieren.“

4

Handlungsfelder – Gestaltungsspielräume



Ob, wo und wie sich die Blockchain in Wirtschaft und Gesellschaft bewähren wird, können wir heute noch nicht mit Sicherheit vorhersehen. Fest steht aber, dass die Weichen jetzt gestellt werden müssen, wenn Deutschland vom möglichen weltweiten Durchbruch der Blockchain profitieren soll. So breit wie die vorgestellten Anwendungsmöglichkeiten der neuen Technologie sind, so umfassend muss auch eine deutsche Blockchain-Strategie aufgestellt sein. Im Folgenden werden sowohl politische Gestaltungschancen als auch offene Fragen vorgestellt. ►



4.1 Eine Gestaltungsaufgabe über alle Politikfelder hinweg

Die Blockchain ist ein Paradebeispiel für den Querschnittscharakter der Digitalisierung. Sie betrifft auch Politikfelder, die bislang selten mit digitalen Technologien in Berührung gekommen sind.

Ein sämtliche Politikfelder übergreifender Austausch über die Blockchain ist daher notwendig. Dieser vermeidet ineffiziente Parallelstrukturen und das Entstehen inkompatibler Inselösungen. Er ist auch die Voraussetzung für die Entwicklung klarer Impulse für eine deutsche Blockchain-Strategie.

Die Chance einer deutschen Blockchain-Strategie

Die Blockchain hat in den technologiepolitischen Strategiepapieren anderer Staaten bereits jetzt einen festen Platz gefunden, beispielsweise in China. Dort wird sie gleichrangig neben der Künstlichen Intelligenz und den Quantentechnologien genannt.

Mit der Formulierung einer Blockchain-Strategie wäre Deutschland daher keineswegs ein Vorreiter, könnte aber zumindest mit den internationalen Wettbewerbern gleichziehen. Die Chance für die Bundesrepublik liegt darin, als große Volkswirtschaft mit hoch angesehenen regulatorischen Standards eine jetzt noch existierende Leerstelle in Europa zu besetzen.

Politikerinnen und Politiker sollten hier bereit sein, Risiken einzugehen. Noch hat sich die Blockchain-Technologie nicht endgültig bewährt und sie könnte im breiten Einsatz scheitern. Wird sie aber zur erhofften wirtschaftlichen und gesellschaftlichen Revolution, werden nur diejenigen die Gewinne mit nach Hause nehmen, die sich früh engagiert und investiert haben.

Blockchain ist Team sport

Ganz oben auf der Wunschliste der deutschen Blockchain-Community stehen die politische Aufmerksamkeit für das Thema und konkrete Ansprechpartnerinnen und -partner bei Unsicherheiten und offenen Fragen. Nachrangig, aber für die Community gleichwohl von hoher Bedeutung, sind neue Förderprogramme oder konkrete Gesetzesänderungen.

Über ein klares politisches Bekenntnis zum Experimentieren mit der jungen Technologie und ihren Einsatzmöglichkeiten hinaus könnte die Politik mit zwei konkreten Aktivitäten auf diesen Wunsch antworten:

- Erstens mit einer Bündelung der deutschen Blockchain-Expertise in Wirtschaft, Wissenschaft und Zivilgesellschaft in einem kontinuierlichen Dialog mit der Politik. Dieser Austausch sollte die Ausarbeitung eines grundlegenden Regulierungsrahmens und seine Weiterentwicklung begleiten.
- Zweitens sollte der Staat eigene Blockchain-Pilotprojekte sichtbar vorantreiben. Dies hätte nicht nur eine internationale Leuchtturmwirkung zur Folge, die Köpfe, Unternehmen und Kapital an den Blockchain-Standort Deutschland locken würde. Pilotprojekte bieten zudem Politik und Behörden die Chance, selbst dringend benötigte Kompetenzen im Umgang mit einer potenziellen neuen digitalen Basistechnologie zu erwerben. Darüber hinaus sollte sich der Staat mit seinen Anforderungen frühzeitig in den Entwicklungsprozess vor allem jener privatwirtschaftlicher Blockchains einbringen, in denen er selbst ein wichtiger Teilnehmer sein wird.

4.2 Regulierung von Token und ICOs

In Bezug auf ICOs (► Kapitel 1.4) herrscht in Deutschland momentan noch hohe regulatorische Unsicherheit. Diese kann zur Abwanderung von Talenten und Unternehmen in Staaten mit einem weiter ausgearbeiteten Regulierungsrahmen führen. Zum anderen trägt die Nichtregulierung zum Vorhandensein von vielen zweifelhaften Akteuren auf dem Markt bei, die wenig ausgearbeitete Unternehmenskonzepte ohne Funktionsgarantie bei ICOs präsentieren, um schnell Kapital einzusammeln.

Status quo in Deutschland

Die BaFin hat sich mit Maßnahmen gegen Anbieter von Kryptowährungen/Token bisher weitgehend zurückgehalten. Gewarnt wurde jedoch vor ICOs, da diese unreguliert, oft intransparent und technologisch nicht ausreichend getestet seien.

Marktteilnehmer, die einen ICO veranstalten wollen, wird eine frühzeitige Kontaktaufnahme zu den Fachreferaten der BaFin empfohlen. Diese nehmen dann auf Basis der bestehenden Gesetze eine Einzelfallprüfung vor.

Dieses Verfahren wird von der BaFin durch die Komplexität und Verschiedenheit der Projekte und der entsprechenden Token-Launches begründet. Für klarere Strukturen, umfassendere Zuständigkeiten und für Grundsatzentscheidungen zu ICOs würde die BaFin ein konkretes politisches Mandat benötigen.

Internationaler Kontext der ICO-Regulierung

Es gibt eine sehr heterogene Regulierungslandschaft. Die Schweiz ist ICO-freundlich, China hingegen hat ICOs verboten, eine international anerkannte Token-Klassifizierung fehlt. Anlegerinnen und Anleger wissen oft nicht, worauf sie sich einlassen, da Informationsangebote (analog zur Prospektspflicht beim klassischen Börsengang) meist nicht zur Verfügung stehen.



Handlungsempfehlungen

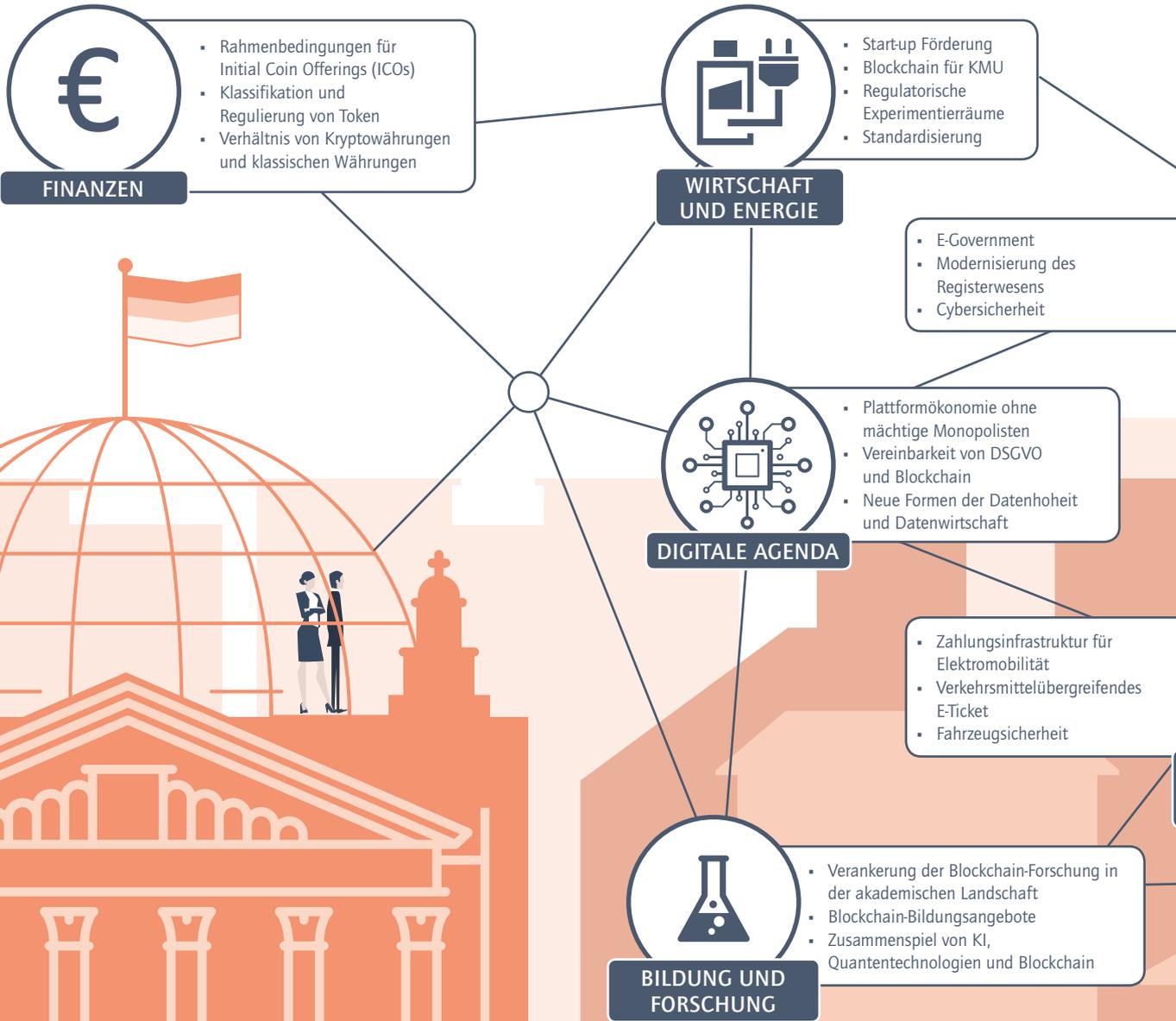
Klarer Rechtsrahmen für ICOs und alle Arten von Token. Expertinnen und Experten regen eine einheitliche, internationale Token-Klassifizierung an. Orientierung bietet in diesem Kontext beispielsweise die Klassifizierung der Schweizer FINMA. Auch die steuerliche Behandlung von Token ist in vielen Bereichen noch unklar. Nicht das wirtschaftliche Spekulationsrisiko im Zusammenhang mit ICOs soll verringert werden, sondern das Betrugsrisiko, wie zum Beispiel Möglichkeiten zur Steuerhinterziehung oder Geldwäsche. Eine Prospektpflicht sollte in diesem Kontext geprüft werden, darf aber nicht zur Hürde für Start-ups werden.

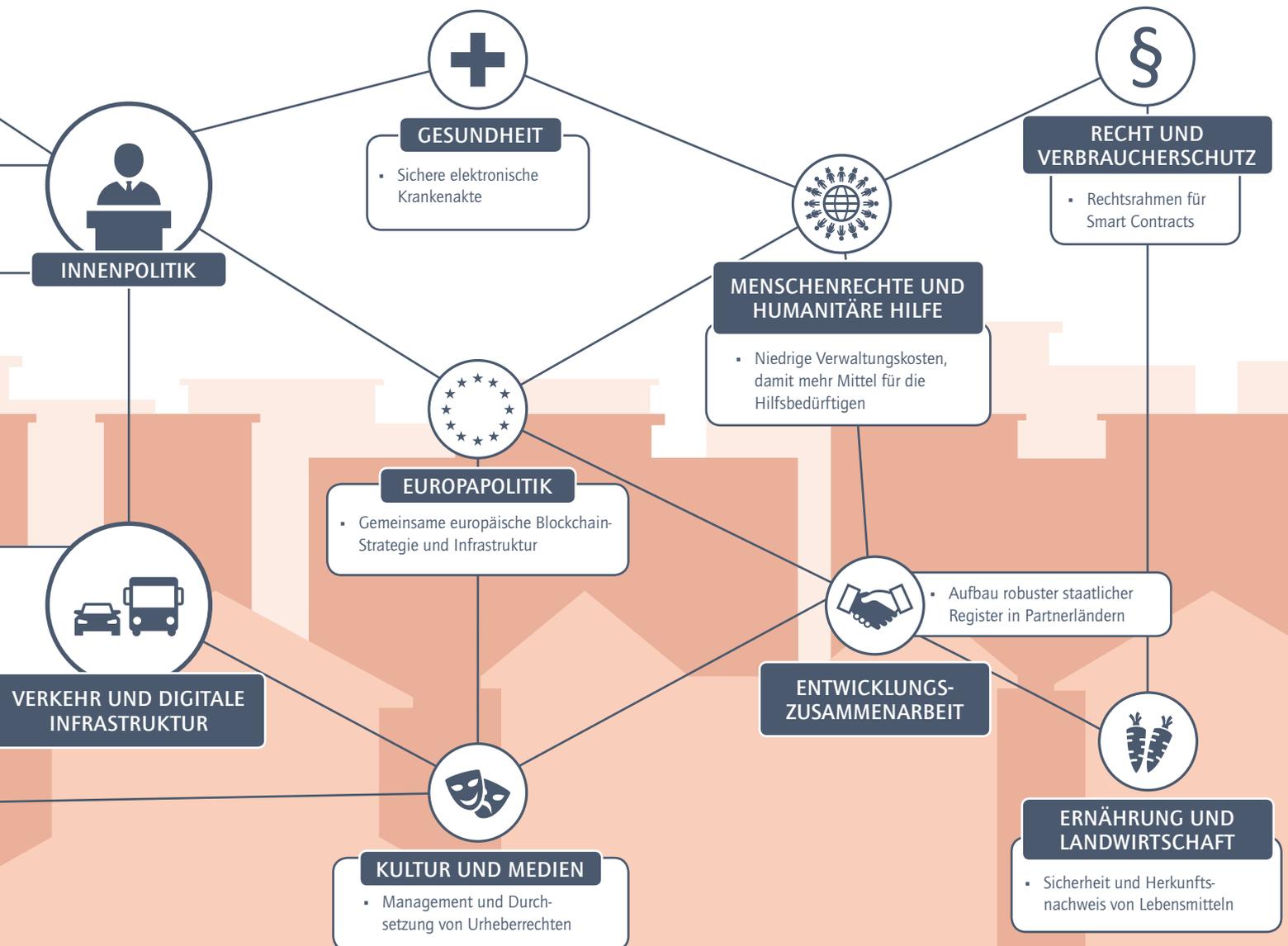
ICO können sich zu einer guten Ergänzung des klassischen Börsengangs entwickeln

ICOs werden zunehmend auch von etablierten, innovativen Unternehmen in Betracht gezogen. Mit einem innovationsfreundlichen, verlässlichen Regelwerk (keine Einzelfallentscheidung), kann auch unternehmerisches Potenzial nach Deutschland angezogen werden.

Chancen	Herausforderungen
Schnelle, investorenfreundliche Regulierung kann Kapital, Fachkräfte und Start-ups nach Deutschland locken und dort halten	ICOs bieten die Möglichkeit, in kurzer Zeit viel Geld zu beschaffen, sind aber höchst spekulativ und unsicher für Anlegerinnen und Anleger

Blockchain als politisches Querschnittsthema





4.3 Datenwirtschaft und Datenschutz

Die Blockchain verspricht Datenschutz, indem sie den Nutzerinnen und Nutzern, anstelle eines Plattform-Anbieters, die Datenhoheit gibt. Dies ist richtig, aber auch kein Automatismus. Man könnte mit der Blockchain ebenso gut Register gläserner Bürgerinnen und Bürger schaffen.

Hohe Schutzstandards müssen aktiv in Blockchain-Anwendungen einprogrammiert werden. Die deutsche Blockchain-Szene (► [Kapitel 3.1](#)) setzt sich in der großen Mehrheit aus innerer Überzeugung für eine maximale digitale Souveränität der privaten und geschäftlichen Nutzerinnen und Nutzer ihrer Blockchains ein.

Prinzipiell hat die Szene daher kein Problem mit anspruchsvollen rechtlichen Vorgaben. Entsprechende internationale Standards würde sie sogar begrüßen, denn Datenschutz und Datensouveränität besitzen nicht überall eine ähnlich hohe Priorität wie in Europa.

Datenschutzgrundverordnung (DSGVO) ist nicht technologieneutral

Es sind nicht die anspruchsvollen Ziele der DSGVO, welche die Blockchain-Entwicklung in Deutschland zu hemmen drohen. Es sind die darin festgelegten Wege, sie zu erreichen.

Die DSGVO ist auf die zentralisierte Struktur der gegenwärtigen Plattformökonomie ausgerichtet. Die Regulierung nimmt die Plattformbetreiber in die Pflicht, welche die Daten zentral speichern und verarbeiten. Auskunftsansprüche und auch solche, die das „Recht auf Vergessen“ beinhalten, können also an eine bestimmte Adresse gerichtet werden.

Dies passt nicht gut zur Blockchain-Technologie, die auf Dezentralisierung setzt. Es zeigt sich, dass die DSGVO nicht technologieneutral formuliert ist und viele ihrer Konzepte im Kontext von Blockchains an ihre Grenzen stoßen.

Private oder konsortiale, genehmigungsbasierte Blockchains haben identifizierbare Betreiber. Eine Umsetzung der DSGVO ist hier einfacher und vor allem eine technologische Herausforderung.

Auf erhebliche Rechtsunsicherheiten und damit Wettbewerbsnachteile trifft man hingegen bei öffentlichen Blockchains. Je nach Lesart gibt es beispielsweise keinen oder aber tausende, über die gesamte Welt verteilte anonyme Betreiber, an die man seine Ansprüche richten müsste.



Handlungsempfehlungen

Auslegung und Weiterentwicklung der DSGVO

Kurzfristig ist eine innovationsfreundliche Auslegung der DSGVO ratsam, die sich vor allem an den mit ihr verfolgten Zielen orientiert. Perspektivisch ist bei einer Überarbeitung der DSGVO auf eine technologieneutrale Ausformulierung zu achten, die auch dezentrale Systeme mitbedenkt.

DSGVO-konforme Lösungen aktiv fördern

Trotz aller Probleme sehen Expertinnen und Experten keine prinzipielle Unvereinbarkeit von Blockchain und DSGVO. Es fehlt hier aber an Forschung, Entwicklung und klaren Antworten des Regulators. Am Ende entsprechender Bemühungen könnten beispielsweise Referenzlösungen für konforme Blockchains und Smart Contracts oder auch Zertifizierungsmöglichkeiten stehen.

Chancen

Technische Garantie von Datenhoheit und Datensouveränität

Herausforderungen

Unklare oder rigide Auslegung der DSGVO lähmt Innovation

4.4 Forschung und Fachkräfte – Was braucht es, um Blockchain zu fördern?

Blockchain entstand in freien Entwicklercommunities, die Lösungen und Ansätze aus der Grundlagenforschung und angewandten Forschung auf unerwartete Weise kombinierten. Auch heute noch entstehen und agieren viele Blockchain-Startups im Umfeld von innovativen Universitäten und Forschungseinrichtungen, die ihnen als Akzeleratoren und Inkubatoren dienen.

Gleichzeitig erreichen aber klassische Förderinstrumente die Communities und Start-ups nur schwer. Manche der Expertinnen und Experten sprechen sich daher für niederschwellige, schnell bewilligte Förderangebote mit kleineren Fördersummen aus. Andere unterstreichen hingegen, dass die staatlichen Summen im

Gegensatz zu den hohen Fördersummen aus der Wirtschaft oft wenig attraktiv für Start-ups sind, betonen aber, dass die EU seit Kurzem interessante Fördersummen bereitstellt.

Chancen	Herausforderungen
Beste unternehmerische und akademische Köpfe in Deutschland versammeln und halten	Fachkräftemangel und schwache institutionelle Verankerung der Blockchain-Forschung

Handlungsempfehlungen

Akademische Forschung: Die Blockchain-Technologie speist sich aus vielen, akademisch gut etablierten Disziplinen. Dennoch ist Blockchain als eigenständiges Thema bislang nur schwach akademisch institutionalisiert und stark von den Initiativen der Aktivität einzelner Personen abhängig. Thematisch auf Blockchain ausgerichtete Lehrstühle, Studienangebote wie zum Beispiel der im Herbst 2018 startende „Blockchain & DLT“-Master der HS Mittweida oder auch Graduiertenschulen und Summer Schools können dazu beitragen, die Technologie in der Wissenschaft stärker zu verankern.

Themen für öffentlich geförderte FuE: Staatlicher Förderung bedürfen insbesondere Themen, die noch wenig Aufmerksamkeit in der Wirtschaft erhalten, wie zum Beispiel alternative Konsensmechanismen und deren Sicherheit. Forschungsbedarf weiterhin in den Bereichen Geschäftsmodelle, Herstellung und Überprüfung der Konformität (öffentlicher) Blockchains mit der DSGVO und

anderen IT-Gesetzen, staatliche Einsatzmöglichkeiten sowie zu Pilotprojekten in diesem Kontext.

Standardisierung von FuE: Eine vorgeschriebene Sichtung der bestehenden Normen und Standards kann dazu beitragen, dass öffentlich geförderte Projekte keine Insellösungen, sondern integrierte Lösungen (insbesondere auch für und mit KMU) hervorbringen. Allgemein sollten Forschungsprojekte interdisziplinär vernetzt stattfinden und insbesondere wissenschaftlich fundiert neue technische und organisatorische Normen und Standards entwickeln.

Entwicklercommunities stärken: Sowohl außerakademische Entwicklercommunities und die Startup-Szene als auch die akademische Forschung profitieren vom Zuzug intelligenter Köpfe nach Deutschland. Diesen gilt es möglichst einfach und unbürokratisch zu ermöglichen. Zudem bedarf es einer Intensivierung des Wissenstransfers zwischen Entwicklercommunities und akademischer Wissenschaft.



4.5 Verantwortung, Sicherheit und Kontrolle

Nicht nur der Datenschutz, sondern auch viele andere Gesetze setzen voraus, dass es zentrale Betreiber von Diensten gibt. Von diesen wird einerseits angenommen, dass sie eindeutig identifizierbar sind, selbst wenn sie in einem anderen Rechtsraum ansässig sein sollten. Andererseits geht man davon aus, dass sie einen Generalschlüssel für alle Daten auf ihren Plattformen besitzen.

Für Ansprüche von Bürgerinnen und Bürgern sowie staatliche Vorgaben gibt es in dieser Konzeption immer einen Adressaten, der sie umsetzen kann. Schwierig wird es immer dann, wenn diese Voraussetzungen entfallen.

An wen kann man sich wenden, wenn man seinen privaten kryptografischen Schlüssel verloren hat und sich so aus einer Blockchain ausgesperrt hat? Wer kann autonome Smart Contracts stilllegen, die durch eine Gesetzesänderung illegal geworden sind?

Auf Fragen wie diese müssen Antworten gefunden werden, wenn die Blockchain-Technologie eine breite Akzeptanz erfahren soll.

Schnittmenge der Debatten über KI und Blockchain

Die Suche nach Antworten muss dabei nicht bei null beginnen. Auch die bereits stattfindenden Diskussionen um Künstliche Intelligenz drehen sich um ähnliche Fragen. Der potenzielle Mehrwert beider Technologien liegt zu einem großen Teil in der Automatisierung von Tätigkeiten. Das bedeutet aber auch einen Verlust direkter Kontrolle über die dafür eingesetzten digitalen Helfer.

Zudem lässt sich nur schwer voraussehen, wie autonome und lernfähige Assistenten und Geräte miteinander interagieren werden. Wer ist verantwortlich, wenn ein Schaden nicht durch das Fehlverhalten eines einzelnen Systems entsteht, sondern durch das Zusammenspiel von für sich jeweils korrekt funktionierenden Systemen?

Die Sicherheit neuer Technologien stellt nicht nur eine technische Herausforderung dar. Sicherheit bedeutet auch, dass Menschen im Schadensfall wissen, an wen sie sich wenden können, welche Rechte ihnen zustehen und welches Restrisiko sie selbst tragen müssen. Die gesellschaftliche Akzeptanz von Blockchain hängt genauso wie die der KI davon ab, frühzeitig tragfähige Antworten auf diese Fragen zu finden.



Handlungsempfehlungen

Interdisziplinärer und öffentlicher Diskurs

Die großen Chancen der Blockchain-Technologie sind wirtschaftlicher und gesellschaftlicher Natur. Die Herausforderungen sind es auch. Es braucht daher eine interdisziplinäre wie auch eine öffentliche Debatte über ihre Ausgestaltung.

Weiterentwicklung des Rechtsrahmens

Ansätze müssen gefunden werden, Rechtsgüter auch dann effektiv zu schützen, wenn keine zentralen Betreiber als Adressaten für Ansprüche existieren.

Chancen

Klarer und damit Akzeptanz fördernder Rechtsrahmen auch für dezentrale Systeme

Herausforderungen

Aktueller Rechtsrahmen setzt Existenz klar identifizierbarer, verantwortlicher Betreiber voraus

Interviewpartnerinnen und Interviewpartner

In Ergänzung zur Arbeit der Projektgruppe und zur Auswertung von Fachliteratur und anderer Studien haben die Mitarbeiterinnen und Mitarbeiter der acatech Geschäftsstelle für diese Publikation Experteninterviews mit 25 Vertreterinnen und Vertretern aus Wissenschaft, Wirtschaft, und Gesellschaft durchgeführt. Die Gespräche wurden im Zeitraum von Anfang Januar bis Ende Juli 2018 telefonisch oder persönlich geführt. Die genannten Funktionen der Interviewpartner beziehen sich auf den Zeitpunkt des jeweiligen Gesprächs. Zur Illustration einiger ausgewählter Kerngedanken der Befragten wurden im Text hin und wieder den Interviews entnommene anonymisierte Zitate aufgeführt.

Das acatech Präsidium dankt allen Beteiligten sehr herzlich für ihre Teilnahme an den Interviews.

- Dian Balta, fortiss, e-Government Forschungsteam
- Prof. Rudolf Bayer PhD, TU München, Lehrstuhl für Datenbanksysteme
- Prof. Dr. Gilbert Fridgen, Fraunhofer FIT, Projektgruppe Wirtschaftsinformatik; Uni Bayreuth, Professur für Wirtschaftsinformatik und Nachhaltiges IT-Management
- Florian Glatz, Blockchain Bundesverband, Präsident
- Fabian Gompf, Parity Technologies, Product- and Project Manager
- Dr. Markus Hablitzel, Munich Re, Innovation Manager
- Prof. Dr. Michael Henke, Fraunhofer-Institut für Materialfluss und Logistik IML, Institutsleiter
- Margit Hoffmann, Munich Re, Senior Innovation Manager
- Volker Jacumeit, DIN Deutsches Institut für Normung, Gruppenleiter IT und IT-Sicherheit
- Prof. Dr. Ulrich Klüh, TU Darmstadt, Professor für Volkswirtschaftslehre, Makroökonomik und Wirtschaftspolitik
- Ilya Komarov, Bundesdruckerei, Senior Innovation Developer
- Christoph Kreiterling, BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht, Referat SR3 – Finanztechnologische Innovationen, Abteilung Strategie und Risiko, Senior Officer
- Marco Liesenjohann, Bitkom, Bereichsleiter Blockchain & Cloud
- Jonas von Malotki, Daimler, Senior Manager Finance & Controlling
- Dr. Manfred Paeschke, Bundesdruckerei, Chief Visionary Officer, Fellow
- Prof. Wolfgang Prinz PhD, Fraunhofer FIT, Stellv. Institutsleiter
- Prof. Dr. Philipp Sandner, Frankfurt School of Finance and Management, Leiter des Frankfurt School Blockchain Centers
- Prof. Dr. Joachim Schrey, Kanzlei Noerr, Fachanwalt für Informationstechnologierecht, Partner
- Dr. Nina-Luisa Siedler, DWF Germany Rechtsanwaltsgesellschaft mbH, Partner
- Michael Spitz, main incubator, CEO
- Dr. Stefan Teis, Deutsche Börse, Director – Head of Blockchain Group Business & Product Development
- Markus Tradt, B3i, Munich Re, System Engineer
- Prof. Dr. Andranik Tumasjan, Uni Mainz, Lehrstuhl für Management und Digitale Transformation
- Franz von Weizsäcker, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Head of Blockchain Lab
- Prof. Dr. Isabell Welpel, TU München, Lehrstuhl für Betriebswirtschaftslehre – Strategie und Organisation

Literaturverzeichnis

- ¹ Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. Online verfügbar unter <https://bitcoin.org/bitcoin.pdf>, zuletzt geprüft am 31.01.2018.
- ² Blockchain Bundesverband e.V. & BlockchainHub (Hrsg.) (2017): German Blockchain Ecosystem. Online verfügbar unter <https://www.bundesblock.de/2017/10/02/blockchain-landschaft-in-deutschland/>, zuletzt geprüft am 26.07.2018.
- ³ Boucher, P.; Nascimento, S.; Kritikos, M. (2017): How blockchain technology could change our lives, European Parliamentary Research Service. Online verfügbar unter [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017\)581948_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf), zuletzt geprüft am 26.10.2017.
- ⁴ Schütte, J.; Fridgen, G.; Prinz, W.; Rose, T.; Urbach, N.; Hoeren, T. et al. (2017): Blockchain und Smart Contracts. Technologien, Forschungsfragen und Anwendungen, Fraunhofer-Institut für Angewandte Informationstechnik FIT. o. O. Online verfügbar unter https://www.iuk.fraunhofer.de/content/dam/iuk/de/documents/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf, zuletzt geprüft am 12.12.2017.
- ⁵ Voshmgir, S. (2016): Blockchains, Smart Contracts und das Dezentrale Web. Hg. v. Ch. Hammel. Berlin. Online verfügbar unter https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf.
- ⁶ Popov, S. (2017): The Tangle. IOTA Whitepaper. Online verfügbar unter http://iotatoken.com/IOTA_Whitepaper.pdf, zuletzt geprüft am 27.08.2018.
- ⁷ Government Office for Science (2016): Distributed Ledger Technology: Beyond block chain. A report by the UK Government Chief Scientific Adviser. London. Online verfügbar unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, zuletzt geprüft am 11.12.2017.
- ⁸ Nikolic, I.; Kolluri, A.; Sergey, I.; Saxena, P. et al. (2018): Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. In: arXiv. Online verfügbar unter <https://arxiv.org/pdf/1802.06038.pdf>, zuletzt geprüft am 27.08.018.
- ⁹ Tanriverdi, H. (2016): 53-Millionen-Dollar-Raub spaltet Verfechter von Kryptowährung. In: Süddeutsche Zeitung Online. Online verfügbar unter <https://www.sueddeutsche.de/digital/the-dao-millionen-dollar-raub-spaltet-verfechter-von-kryptowahrung-1.3044097>, zuletzt geprüft am 02.08.2018.
- ¹⁰ Steiner, J.; Wood, G. (2018): Our commitment to Ethereum and a decentralised future. Parity Technologies. Online verfügbar unter <https://paritytech.io/our-commitment-to-ethereum-and-a-decentralised-future>, zuletzt geprüft am 02.08.2018.
- ¹¹ OkeyDokey (2018): Whitepaper. Online verfügbar unter <https://github.com/team-okeydokey/okeydokey/wiki/OKEYDOKEY-White-Paper>, zuletzt geprüft am 23.08.2018.
- ¹² FINMA (2018): Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs). Ausgabe vom 16. Februar 2018. Bern. Online verfügbar unter <https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de>, zuletzt geprüft am 02.08.2018.
- ¹³ Kops, M. (2018): 35 Millionen Dollar in 30 Sekunden: Brave ICO ausverkauft. In: BTC-Echo. Online verfügbar unter <https://www.btc-echo.de/brave-35-millionen-dollar-30-sekunden>, zuletzt geprüft am 02.08.2018.
- ¹⁴ Vries, A. de (2018): Bitcoin's Growing Energy Problem. In: Joule (Volume 2, Issue 5), S. 801-805. DOI: 10.1016/j.joule.2018.04.016.
- ¹⁵ Androulaki, E., Barger, A., Bortnikov, V., Cachin et al. (2018): Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, 23.-26. April 2018. Porto. Online verfügbar unter <https://arxiv.org/pdf/1801.10228.pdf>, zuletzt geprüft am 23.08.2018.
- ¹⁶ Poon, J.; Dryja, T. (2016): The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Draft Version 0.5.9.2. Online verfügbar unter <https://lightning.network/lightning-network-paper.pdf>, zuletzt geprüft am 27.08.2018.
- ¹⁷ Blockchain Luxembourg S.A. (2018): Blockchain Charts. Online verfügbar unter <https://www.blockchain.com/de/charts>, zuletzt geprüft am 27.08.2018.
- ¹⁸ Churchill, J. (2017): Maersk and IBM target one of trade's biggest barriers. Online verfügbar unter <https://www.maersk.com/stories/maersk-and-ibm-target-one-of-trades-biggest-barriers>, zuletzt geprüft am 02.08.2018.
- ¹⁹ IBM Food Trust (2018): Transforming Global Food Safety with IBM Food Trust. Online verfügbar unter <https://www.vmt.nl/~media/617AF0B-A785B44FCA60E74A92FEC0615.pdf?la=nL&hash=EDA855E129F1F-6492088FA77070663F7D1161A03>, zuletzt geprüft am 23.08.2018.
- ²⁰ IBM & Maersk (2018): Open global trade digitization platform. Online verfügbar unter <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=02016702USEN>, zuletzt geprüft am 23.08.2018.
- ²¹ Normenkontrollrat (2017): Mehr Leistung für Bürger und Unternehmen. Online verfügbar unter https://www.normenkontrollrat.bund.de/Web/NKR/Content/DE/Download/2017-10-06_download_NKR%20Gutachten%202017.pdf?__blob=publicationFile&v=5, zuletzt geprüft am 23.08.2018.

- ²² World Economic Forum (2018): Whitepaper: Blockchain Beyond the Hype. A Practical Framework for Business Leaders. Online verfügbar unter http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf, zuletzt geprüft am 23.08.2018.
- ²³ Blockchain Bundesverband e.V. & BlockchainHub (Hrsg.) (2017): German Blockchain Ecosystem. Online verfügbar unter <https://www.bundesblock.de/2017/10/02/blockchain-landschaft-in-deutschland/>, zuletzt geprüft am 26.07.2018.
- ²⁴ BlockchainHub (2018): Mapping the German Blockchain Ecosystem. Online verfügbar unter <https://blockchainhub.net/blog/blog/mapping-the-german-blockchain-ecosystem/>, zuletzt geprüft am 02.08.2018.
- ²⁵ Chain (2018): ICOs of German Startups. Online verfügbar unter <https://www.chain.de>, zuletzt geprüft am 02.08.2018.
- ²⁶ CoinSchedule (2018): Cryptocurrency ICO Stats 2016, 2017 & 2018. Online verfügbar unter <https://www.coinschedule.com/stats.html>, zuletzt geprüft am 25.07.2018.
- ²⁷ PwC (2018): Initial Coin Offerings. A strategic perspective. Online verfügbar unter https://www.pwc.ch/en/publications/2018/20180628_PwC%20S&%20CVA%20ICO%20Report_EN.pdf, zuletzt geprüft am 25.07.2018
- ²⁸ Berryhill, J.; Bourger, T.; Hanson, A. (2018): Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. OECD Working Papers on Public Governance. Nr. 28. OECD Publishing. Paris. Online verfügbar unter <https://oecd-opsi.org/wp-content/uploads/2018/06/Blockchains-Unchained-Guide.pdf>, zuletzt geprüft am 09.08.2018.
- ²⁹ European Commission EU Blockchain Observatory & Forum (2018): Workshop - Government services and digital identity. Brussels, July 5 2018.

Mitwirkende

Gesamtleitung acatech Technikfeldanalyse:

Prof. Dr.-Ing. Jürgen Gausemeier, acatech Vizepräsident,
Heinz Nixdorf Institut der Universität Paderborn

Projektgruppe Blockchain:

Prof. Dr. Roman Beck, IT University of Copenhagen,
BusinessIT Department, European Blockchain Center

Prof. Dr. Manfred Broy (Leiter), Zentrum Digitalisierung,
Bayern, Gründungspräsident

Prof. Dr. Helmut Krcmar, TU München,
Lehrstuhl für Wirtschaftsinformatik

Hauke Stars, Deutsche Börse AG, Mitglied des Vorstands

Dirk Wittkopp, IBM Deutschland Research & Development GmbH,
Geschäftsführer

Torsten Zube, SAP SE, Head of Blockchain,
SAP Innovation Center Network

Leitung acatech Horizonte:

Dr. Christoph Egle, acatech Geschäftsstelle,
Innovationsforum

Konzeption, Text und Experteninterviews:

Florian Süssenguth, acatech Geschäftsstelle, Innovationsforum
(federführender Autor)

Anna-Laura Liebenstund, acatech Geschäftsstelle,
Innovationsforum (Autorin)

Kerstin Podere, acatech Geschäftsstelle,
Innovationsforum (Koordination/Redaktion)

Mit Unterstützung durch:

Markus Glätzer, acatech Geschäftsstelle, Innovationsforum

Iris Michalik, acatech Geschäftsstelle, Innovationsforum

HERAUSGEBER:

acatech – Deutsche Akademie der Technikwissenschaften

ADRESSEN STANDORTE**Geschäftsstelle**

Karolinenplatz 4
80333 München

T +49(0)89/520309-0
F +49(0)89/520309-900

Hauptstadtbüro

Pariser Platz 4a
10117 Berlin

T +49(0)30/2063096-0
F +49(0)30/2063096-11

Brüssel-Büro

Rue d'Egmont/Egmontstraat 13
B-1000 Brüssel

T +32(0)2/2 13 81-80
F +32(0)2/2 13 81-89

horizonte@acatech.de
www.acatech.de
<https://www.acatech.de/horizonte>

Empfohlene Zitierweise:

acatech (Hrsg.), Blockchain (acatech HORIZONTE). München/Berlin,
2018

Layout und Satz:

Atelier Hauer+Dörfler GmbH, Berlin

Druck:

Komplan Biechteler GmbH & Co. KG, München

München 2018

acatech HORIZONTE ISSN 2625-9605



 **acatech**

DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

Über acatech

acatech berät Politik und Gesellschaft, unterstützt die innovationspolitische Willensbildung und vertritt die Technikwissenschaften international. Ihren von Bund und Ländern erteilten Beratungsauftrag erfüllt die Akademie unabhängig, wissenschaftsbasiert und gemeinwohlorientiert. acatech verdeutlicht Chancen und Risiken technologischer Entwicklungen und setzt sich dafür ein, dass aus Ideen Innovationen und aus Innovationen Wohlstand, Wohlfahrt und Lebensqualität erwachsen. acatech bringt

Wissenschaft und Wirtschaft zusammen. Die Mitglieder der Akademie sind herausragende Wissenschaftlerinnen und Wissenschaftler aus den Ingenieur- und den Naturwissenschaften, der Medizin sowie aus den Geistes- und Sozialwissenschaften. Die Senatorinnen und Senatoren sind Persönlichkeiten aus technologieorientierten Unternehmen und Vereinigungen sowie den großen Wissenschaftsorganisationen. Neben dem acatech FORUM in München als Hauptsitz unterhält acatech Büros in Berlin und Brüssel.