Online-Konsultation zur Erarbeitung der Blockchain-Strategie der Bundesregierung

Bitkom-Stellungnahme

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Patrick Hansen | Bitkom e.V.
T 030 27576-410 | p.hansen@bitkom.org

Verantwortliches Bitkom-Gremium

AK Blockchain

Satz & Layout

Kea Schwandt | Bitkom e.V.

Titelbild

© Markus Spiske – unsplash.com

Inhaltsverzeichnis

1 Relevanz der Blockchain-Technologie 5

2 Blockchain-Technologie – Funktionsweise, Anwendungen, Potenziale 9

2.1 Was ist eine »Blockchain«? 9

2.2 Anwendungsfelder 14
Anwendungsfeld a) Finanzsektor (1/2) 15
Anwendungsfeld a) Finanzsektor (2/2) 22
Anwendungsfeld b) Energie (1/2) 25
Anwendungsfeld b) Energie (2/2) 31
Anwendungsfeld c) Gesundheit/Pflege 35
Anwendungsfeld d) Mobilität 39
Anwendungsfeld e) Lieferketten/Logistik 44
Anwendungsfeld f) Internet der Dinge 50
Anwendungsfeld g) Identitäten-/Rechtemanagement (1/2) 53
Anwendungsfeld g) Identitäten-/Rechtemanagement (2/2) 57
Anwendungsfeld h) Verwaltung 59
Anwendungsfeld i) Plattformökonomie 64

3 Zentrale Fragestellungen der Blockchain-Technologie 68

3.1 Technologische Herausforderungen 68
Technologische Herausforderungen a) Skalierbarkeit 68
Technologische Herausforderungen b) Ineffizienz durch Redundanz 71
Technologische Herausforderungen c) Technische Anforderungen 74
Technologische Herausforderungen d) Interoperabilität 75
Technologische Herausforderungen e) Irreversibilität 77
Technologische Herausforderungen f) IT-Sicherheit 78

3.2 Ökonomische Fragestellungen 82
Ökonomische Fragestellungen a) Ökonomisches Potenzial 82
Ökonomische Fragestellungen b) KMU 86

3.3 Ökologische Fragestellungen 88

3.4 Rechtliche Fragestellungen 91
Rechtliche Fragestellungen a) Anwendbares Recht 93
Rechtliche Fragestellungen b) Rechtliche Verantwortlichkeit und Rechtsdurchsetzung 95
Rechtliche Fragestellungen c) Smart Contracts 96
Rechtliche Fragestellungen d) Ersetzbarkeit von Intermediären 100
Rechtliche Fragestellungen e) Datenschutz
(insbesondere Anforderungen nach der DSGVO) 101
Rechtliche Fragestellungen f) Formvorschriften 107
Rechtliche Fragestellungen g) Steuern 109

4 Praxisbeispiele 112

1 Relevanz der Blockchain-Technologie

1 Relevanz der Blockchain-Technologie

Die Blockchain-Technologie gilt als eine potenzielle neue Basistechnologie der Digitalisierung. Sie hat Eigenschaften, die ein breites, sektorübergreifendes Feld an Anwendungsmöglichkeiten eröffnen. Die Blockchain-Technologie könnte zu einer wichtigen Schlüsseltechnologie der Digitalisierung werden und disruptive Veränderungen des Wirtschafts- und Gesellschaftslebens mit sich bringen. Als mögliche Alternative zu heutigen digitalen Plattformen und etablierten Intermediären (zum Beispiel: Handelsplätze) kann sie in betroffenen Anwendungsgebieten zu einer Verschiebung ökonomischer Machtverhältnisse führen und auch dadurch volkswirtschaftliche Relevanz erlangen. Diese Entwicklung bedarf der vertieften Analyse und der politischen Begleitung.

Neuartige Vertrauenslösung: Blockchains sind dezentrale, digitale Register, die durch kryptografische Verfahren und dezentrale Speicherung ein hohes Maß an Datenintegrität und Vertrauenswürdigkeit bieten können. Ihr großes Potenzial beruht auf ihrer Funktionsweise, die manipulationssichere und nachprüfbare Transaktionen ermöglicht. Sie stellen damit eine technologische Lösung für Vertrauensprobleme dar, die sich an ganz unterschiedlichen Stellen des Wirtschaftslebens und der Verwaltung ergeben.

Alternative zu Intermediären: Zur Schaffung von Vertrauen, Sicherheit und Transparenz werden derzeit in der Regel Intermediäre gebraucht. Blockchain-Lösungen könnten den Grad der Notwendigkeit von Intermediären senken und sie unter Umständen sogar ersetzen. Das kann ökonomisch zu einer Senkung von Transaktionskosten und zum Abbau von Zutrittshürden zu Märkten führen.

Register und Dokumentation: Effizienzgewinne könnten insbesondere dort denkbar sein, wo Register, Dokumentationen und Verzeichnisse geführt werden müssen. Die Blockchain könnte daher Anwendung finden bei der Modernisierung von Registern und zur Digitalisierung von Dokumentationsprozessen beitragen.

Automatisierung: Mittelfristig wird der Blockchain-Technologie eine mögliche Funktion als Mechanismus zur Automatisierung in der Vertragserfüllung und als Steuerungstechnologie insbesondere im Internet der Dinge beigemessen.

Es handelt sich um eine vergleichsweise junge Technologie. Dementsprechend findet derzeit eine breite Erprobung statt, erste Anwendungen werden von der Wirtschaft umgesetzt. In Deutschland und insbesondere in Berlin hat sich ein Zentrum für die Blockchain-Technologie mit vielen Entwicklern und Vordenkern gebildet.

Eine Reihe von Unternehmen in Deutschland erprobt bereits die Blockchain-Technologie. Etliche Universitäten und Forschungsinstitute haben Kompetenzzentren gebildet und es gibt verschiedene Netzwerkzusammenschlüsse auf lokaler Ebene. Junge Blockchain-Projekte werden über Venture-Capital-Geber und auch über sogenannte Initial Coin Offerings finanziert, bei denen Investoren für ihren Finanzierungsbeitrag sogenannte Krypto-Token erhalten.

Für die Bundesregierung stellt sich in diesem Zusammenhang die Herausforderung, eine technologische Entwicklung zu begleiten, deren Potenziale oder Risiken derzeit nicht vollständig einschätzbar sind. Gleichzeitig ist eine strategische Begleitung dieser Entwicklung bereits zu diesem frühen Stadium der Technologie erforderlich, um die Wettbewerbs- und Innovationsfähigkeit der deutschen Wirtschaft zu stärken, technologische Souveränität zu sichern und gesellschaftliche, ökonomische und ökologische Herausforderungen zu adressieren. Dies ist auch von besonderer Bedeutung vor dem Hintergrund der potenziellen Innovationsdynamik der Technologie sowie der Tatsache, dass ein wesentlicher Teil der bisherigen Entwicklung aus Berlin heraus betrieben wird.

Die Blockchain-Technologie unterscheidet sich dabei von anderen Digitaltechnologien dadurch, dass die technologische Weiterentwicklung im Ausgangspunkt weniger stark wissenschafts- oder unternehmensgetrieben ist, sondern im Wesentlichen aus der Entwickler- und Gründerszene stammt. Damit kommt hier der Förderung von Startup- und Gründernetzwerken durch attraktive Rahmenbedingungen und deren Vernetzung mit etablierten Akteuren ein großer Stellenwert zu. Spezifische innovationspolitische Instrumente für diese Zielgruppe sind deswegen von besonderer Relevanz.

Ein weiterer wesentlicher Aspekt für die Blockchain-Strategie der Bundesregierung ist die Schaffung guter Rahmenbedingungen. Diese müssen zum einen die Rechtssicherheit für die Entwicklung und Anwendung von Blockchain-Lösungen bieten und zum anderen die nötige Innovationsoffenheit des Ordnungsrahmens sicherstellen. Flankierend gehört dazu auch die Klärung offener Forschungsfragen bei der Implementierung der Blockchain-Technologie in konkreten Anwendungsfällen, etwa in den Bereichen Sicherheit, Beachtung rechtlicher Vorgaben insbesondere zum Daten- und Privatsphärenschutz, Governance-Strukturen, Energie- und Ressourcenverbrauch, sowie des Transfers im Rahmen der anwendungsnahen Forschungsförderung. Bei der Erarbeitung der Blockchain-Strategie ist im Übrigen zu beachten, dass für deren Umsetzung die haushaltspolitischen Festlegungen des Koalitionsvertrages gelten. Eine evtl. konkrete Bereitstellung von Mitteln kann erst im Rahmen der kommenden Haushaltsaufstellungsverfahren bzw. der Erstellung der kommenden Finanzpläne erfolgen.

Bitte geben Sie Ihre Stellungnahme zu den Anwendungsfeldern ein:

Bitkom Stellungnahme:

Die Blockchain-Technologie bietet neben dem Finanzsektor vor allem auch in der Logistik, insbesondere entlang ganzer Supply Chains großes Potenzial zur Optimierung einer Vielzahl an Prozessen. Überall dort, wo Nachweise über geleistete Transaktionen erbracht werden müssen oder der ordnungsgemäße Transfer von Gütern zu belegen ist, besteht ein Anwendungsfeld für die Blockchain-Technologie. Im Supply Chain Management können neben der manipulationssicheren Speicherung von Daten und Transaktionen in der Blockchain beispielsweise Zahlungsprozesse mittels Smart Contracts automatisiert und in Kombination mit den cyberphysischen Systemen im Internet der Dinge zunehmend auch autonomisiert

werden. Durch das Entfallen manueller Tätigkeiten werden die involvierten Prozesse hierbei erheblich beschleunigt.

Jeweils unterschiedliche Eigenschaften der Blockchain sind für die Anwendungsfelder und Branchen relevant. So sind beispielsweise für das Internet der Dinge vor allem die Smart Contracts mit die damit verbundenen Automatisierungs- und Autonomisierungspotenziale von zentraler Bedeutung. In Ergänzung dazu sind es bei Anwendungsfeldern aus den Bereichen Logistik und Supply Chain Management, digitale Medien oder für Herkunftsnachweise die irreversible Speicherung der Daten und Transaktionen.

Grundsätzlich stimmt der Bitkom den obenstehenden Aussagen zu, allerdings kommt die Bedeutung von ergänzenden dezentralen Technologien zu kurz. Die Blockchain Technologie allein kann die oben angeführten Veränderungen nicht allein herbeiführen, dazu bedarf es weiterer, ergänzender Technologien, wie z. B. dezentrale Storage Lösungen (z. B. IPFS). Ergänzend suggeriert die explizite Namensgebung »Blockchain«, dass nun nur eine Strategie für Blockchain erarbeitet werden soll, welches, wenn man es ganz genau nimmt, Lösungen wie Directed Acyclic Graph DAG (Tangle) und weiteren Basistechnologien ausschließen würde. Viele der genannten Innovationen werden auch oder insbesondere durch die Smart Contract Technologie ermöglicht, welche ein Bestandteil von einer Blockchain sein kann (siehe Ethereum), aber nicht muss (siehe Bitcoin), aber gerade dieser technologische Teil wirft viele regulatorische, juristische und organisatorische Fragestellungen auf.

Hier sollte außerdem der Hinweis erfolgen, dass nicht nur Startups und Gründer die Blockchain-Technologie vorantreiben, sondern auch etablierte (große) Unternehmen maßgeblich in Forschung und Entwicklung investieren und betriebsbereite Lösungen mit einem hohen Reifegrad für die Industrie entwickeln. Diese Lösungen werden in der Regel im kollaborativen Ansatz (Startup, Mittelstand, große Unternehmen) erstellt und durch Open Source bereitgestellt. Auch Forschungseinrichtungen wie das Fraunhofer IML in Dortmund oder die HAW in Hamburg treiben Blockchain-Anwendungsfälle voran. So gibt es beispielsweise konkrete Überlegungen für ein Blockchain Institut (für Logistik und Supply Chain Management) sowie ein Blockchain-Reallabor (für Energie und Daseinsvorsorge) in NRW.

2 Blockchain-Technologie – Funktionsweise, Anwendungen, Potenziale

2 Blockchain-Technologie – Funktionsweise, Anwendungen, Potenziale

2.1 Was ist eine »Blockchain«?

Die Blockchain ist ein sicheres Logbuch für Transaktionen. Sie ist eine Unterkategorie eines dezentral verteilten Registers, in dem alle Transaktionen eines Netzwerkes gespeichert werden (englisch: Distributed Ledger Technology, DLT). Dabei werden mehrere Transaktionen zu einem Block zusammengefasst und Blöcke in chronologischer Reihenfolge miteinander verkettet (deswegen der Name »block chain«). Entscheidend dabei ist, dass die Richtigkeit einer Information nicht mehr durch eine zentrale Instanz verifiziert werden muss, sondern mittels eines unter den Teilnehmern transparenten Konsensmechanismus bestätigt wird.

Die Blockchain-Technologie entstand 2008, als ein bis heute unbekannt gebliebener Autor bzw. eine Autorengruppe unter dem Pseudonym Satoshi Nakamoto ein Forschungspapier mit der technologischen Grundidee veröffentlichte. 2009 ging die Kryptowährung Bitcoin als erster Anwendungsfall online und so wurde die erste öffentliche Blockchain gestartet.

Heute gibt es nicht nur »die eine«, sondern eine Vielzahl unterschiedlicher Ausprägungen von Blockchains, deren Elemente bausteinartig zusammengesetzt werden können (siehe unten). Dennoch lassen sich einige Grundprinzipien der Blockchain-Technologie beschreiben.

Dezentralität: Aufgrund der verteilten Konsensbildung kann die Blockchain-Technologie ohne eine zentrale Instanz funktionieren. Die daraus resultierende Verschlankung der Prozessstruktur durch den Wegfall von Zwischenschritten über die zentrale Instanz kann in geeigneten Anwendungsfällen erhebliche Effizienzgewinne ermöglichen. Ein weiterer Aspekt der Dezentralität ist, dass alle Daten bei mehreren, oft auch allen Teilnehmern eines Netzwerks gespeichert werden. Aufgrund der Redundanz der Daten ist es im Gegensatz zu einer klassischen Datenbank- oder Cloud-Lösung unproblematisch, wenn ein Server ausfällt. Durch die Dezentralität sind Blockchain-Anwendungen außerdem eine Alternative zu Plattformen, deren Aufgabe als zentraler Intermediär durch die Technologie hinfällig werden kann. Darin liegt ein erhebliches Potenzial der Verschiebung von Marktmacht, die derzeit in einigen Branchen stark konzentriert bei Plattformen liegt.

Manipulationssicherheit: Blockchain-Lösungen gelten wegen der Verknüpfung der einzelnen Blöcke durch Hash-Funktionen (Streuwertfunktionen) und der vielen redundanten Kopien der Datenbank im gesamten Netzwerk als relativ manipulationssicher. Insbesondere für große, öffentliche Blockchains gilt, dass Daten irreversibel abgespeichert sind und im Prinzip nachträglich nicht mehr verändert werden können.

Werttransfer: Die in einer Blockchain abgespeicherten Werte können eindeutig einem Inhaber zugewiesen und deren Transfer zweifelsfrei nachverfolgt werden. Aus diesem Grund wird die Blockchain-Technologie als Grundlage für ein »Internet der Werte« gesehen. Anders als in dem heutigen »Internet der Informationen« werden dabei Informationen nicht mehr einfach nur

kopiert und geteilt, sondern Herkunft und Inhaberschaft der Wertrechte bleiben protokolliert und transparent nachvollziehbar.

Verschlüsselung: Die Nutzung von Kryptografie für die Transaktionsdaten in einer Blockchain ermöglicht eine Transparenz der Transaktionen, ohne dass die Transaktionsbeteiligten unmittelbar erkennbar sind. Obwohl alle Transaktionen in einer öffentlichen Blockchain transparent und nachvollziehbar sind, bleiben die Akteure bei entsprechender Ausgestaltung der Blockchain unbekannt, solange die Daten nicht entschlüsselt werden. Nur der sogenannte öffentliche Schlüssel des Akteurs, eine Art Kontonummer, wird angegeben.

Automatisierungspotenzial: Auf Basis der Blockchain-Technologie können bestimmte Vertragsbedingungen digital abgebildet sowie automatisch und permanent kontrolliert werden. Diese automatisierten Verträge, sogenannte Smart Contracts, ermöglichen ein enormes Automatisierungspotenzial.

Die Blockchain-Technologie ermöglicht **Dezentrale Apps** (DApps), d.h. dezentrale Internet-Anwendungen, bei denen anders als bei herkömmlichen Internet-Anwendungen die Daten und Teile des Programmcodes nicht auf einem zentralen Server gespeichert werden, sondern dezentral in der Blockchain. Durch diese Funktionalität ermöglicht die Blockchain-Technologie grundsätzlich eine stärkere Dezentralisierung von Internetanwendungen und könnte zur Verschiebung von Marktmacht führen. Anwendungen können eine Social-Media-Plattform sein, aber auch im weiteren Sinne eine Kryptowährung wie Ethereum-Token ermöglichen dabei in öffentlichen Blockchains den Zugang zur DApp und bieten zudem Anreize für die Teilnehmer, die notwendige Infrastruktur (Programmentwicklung, Rechnerinfrastruktur) zur Verfügung zu stellen. DApps interagieren häufig mit Smart Contracts.

Smart Contracts sind ein wesentliches Merkmal der meisten Blockchain-Technologien, bei dem Transaktionen mit Programmcode zu sogenannten Smart Contracts verknüpft werden. Mit diesen lassen sich unter anderem Vertragsbeziehungen ganz oder teilweise abbilden und auch ganz oder zum Teil vollautomatisch erfüllen. Dadurch könnten die Geschwindigkeit der Erfüllung von Verträgen deutlich erhöht und die Kosten verringert werden. Mit Smart Contracts wird eine Vielzahl von Anwendungen optimiert, wie unter anderem Mikrozahlungen, Logistikabwicklungen und Vernetzungen im Internet der Dinge. Je nach Komplexität dieser automatisierten Vertragsbeziehungen lassen sich sogar neue Organisationsformen abbilden wie zum Beispiel eine **Dezentrale Autonome Organisation (DAO)**, bei der ab Inbetriebnahme die Handlungen der Organisation im Wesentlichen auf Geschäftsregeln und Prozessen beruhen, die über mehrere Smart Contracts abgebildet werden, und nicht auf Handlungen eines zentralen Managements.

Die erläuterten Potenziale und Eigenschaften der Blockchain-Technologie beziehen sich auf die grundsätzliche Idee von Blockchains. Es gibt aber nicht »die eine« Blockchain, sondern eine Vielzahl an »Bausteinen« für die Ausgestaltung von Blockchains. Deren Kombination bietet individualisierte Lösungen für viele Anwendungsfälle. Folgende **Typisierungen von Blockchains** sind möglich:

Teilnahme: In öffentlichen Blockchains (zum Beispiel Bitcoin) steht die Teilnahme am Netzwerk jedem offen. Bei privaten Blockchains ist der Teilnehmerkreis hingegen begrenzt (zum Beispiel bei einer unternehmensinternen Nutzung). Bei öffentlichen Blockchains existiert kein zentraler Ansprechpartner, während bei einer privaten Blockchain der Betreiber als Moderator verstanden werden kann.

Lese- und Schreibrechte: Während genehmigungsfreie Blockchains jedem Teilnehmer sowohl Lese- als auch Schreibrechte zugestehen, werden diese in genehmigungspflichtigen Blockchains eingeschränkt.

Aus der Unterscheidung zwischen privaten und öffentlichen beziehungsweise genehmigungsfreien und genehmigungspflichtigen Blockchains ergibt sich folgendes Schema, nach dem relevante Blockchain-Typen systematisiert werden können.

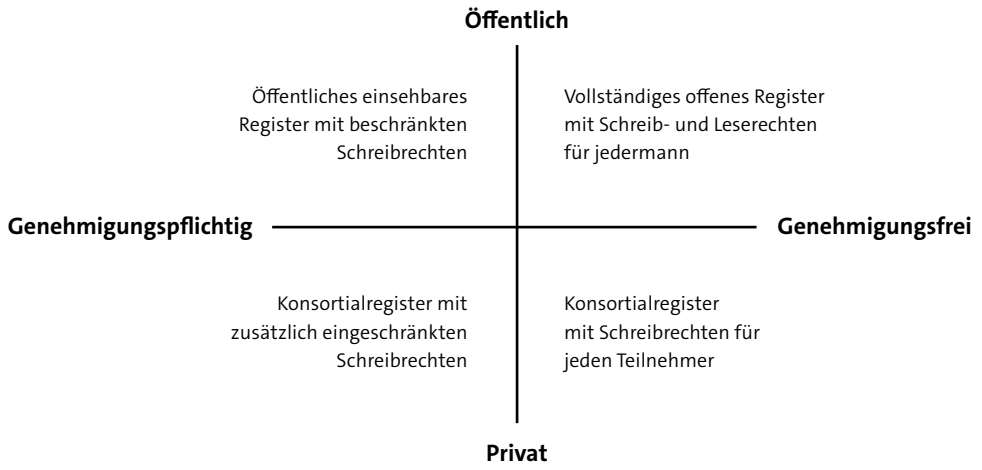

Abbildung 1: Kompetenzzentrum öffentliche Informationstechnologie: »Mythos Blockchain: Herausforderung für den öffentlichen Sektor«, März 2017

Konsensfindung: Das bisher gängigste Verfahren der Ausgestaltung des dezentralen Konsensmechanismus für die Verifizierung von Blöcken heißt »Proof of Work«. Die Netzwerkteilnehmer, die einen neuen Block vom Netzwerk bestätigen lassen wollen, müssen einen Arbeitsnachweis erbringen. Auf Basis der im Block zusammengefassten Transaktionen, eines Zeitstempels, dem »Hashwert« (eine Art Fingerabdruck) des Vorgängerblocks und einer Zufallszahl wird ein gültiger Hashwert des aktuellen Blocks errechnet. An die Berechnung eines gültigen Hashwerts werden Bedingungen geknüpft, sodass unterschiedliche Zufallszahlen ausprobiert werden müssen, bis ein gültiger Hashwert gefunden wird. Der Netzwerkteilnehmer, der als Erster einen gültigen Hashwert gefunden hat, bekommt den von ihm vorgeschlagenen Block mit Transaktionen bestätigt und erhält zudem eine Belohnung. Alle anderen Teilnehmer erhalten nichts. Wenn zwei Blöcke nahezu gleichzeitig bestätigt werden – also eine Gabelung der Blockchain droht – entscheidet die Mehrheit des Netzwerks darüber, wie die Kette fortgesetzt wird. Die längere Kette wird als »richtige Kette« verstanden. Die Blöcke, die an der kürzeren Gabelung angehängt waren, werden

wieder aufgelöst und die Transaktionen müssen erneut bestätigt werden. Ein weiteres Verfahren zur Konsensfindung heißt »Proof of Stake«. Dabei werden Netzwerkteilnehmer entsprechend ihren Anteilen an der zugrundeliegenden Kryptowährung oder auf Basis eines Zufallsmechanismus ausgewählt, um Blöcke zu validieren. Das ressourcenintensive Mining entfällt hierbei.

Anreizsystem: Zur Pflege einer jeden Blockchain braucht es ein entsprechendes Anreizsystem. In öffentlichen Blockchains können hoher Energie- und Ressourcenverbrauch und hohe Kosten für die notwendigen Rechenkapazitäten, um einen gültigen neuen Block zu berechnen, entstehen. Netzwerkteilnehmer, die Blöcke berechnen, heißen Miner, und sie werden durch die zugrundeliegende Kryptowährung der Blockchain entlohnt. In privaten (konsortialen) Blockchains können Anreize auch außerhalb der Blockchain gesetzt werden, zum Beispiel über Verträge unter den Konsortialpartnern.

Andere Bausteine sind beispielsweise die **Skalierbarkeit** der Blockchain, also die Anzahl von Transaktionen, die in einen Block aufgenommen werden können. Auch der **Grad an Transparenz** der in einer Blockchain gespeicherten Informationen, der **Grad an Anonymität** der Teilnehmer oder das **Ausmaß an Dezentralität** sind je nach Blockchain gestaltbar.

Möglichkeit zur Stellungnahme bezüglich der Funktionsweise der Blockchain-Technologie

Bitkom Stellungnahme:

Die Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) verdeutlicht, wie sehr das Begriffsverständnis von Blockchain und DLT in Deutschland variiert. Während in Unternehmen die für »digitale Technologien« verantwortlichen Mitarbeiter fast alle (95%) den Begriff »Blockchain« erklären können, fällt die Abgrenzung zu DLT und anderen DLT-Verfahren noch schwer (nur 26%). Trotz der Schwierigkeit, Blockchain in einem kurzen Abschnitt zu definieren, möchten wir nochmal auf einige im Abschnitt genannte Punkt eingehen:

- Der Begriff »Verschlüsselung« wird oft im Bereich der Blockchain-Technologie verwendet und kann zu Verwirrung führen. Da es in der Blockchain-Technologie hauptsächlich um Hashwerte und digitale Signaturen geht, empfehlen wir an der Stelle des Begriffes »Verschlüsselung« – den Begriff »Kryptographie« zu nutzen. Bei der Verschlüsselung geht es um spätere Entschlüsselung. Bei den Hashwerten geht es um eine Einwegfunktion. Die Transaktionsdaten in einer Blockchain sind nicht verschlüsselt, da Teilnehmer ihre Korrektheit ansonsten nicht verifizieren können. Die verwendeten kryptographischen Mechanismen sind in der Regel nur dafür gedacht, Transaktionen transparent und nachvollziehbar zu machen, jedoch nicht dafür die Identität der Akteure zu verbergen. Die Verwendung eines öffentlichen Schlüssels ist, genau wie die Verwendung einer Kontonummer, kein geeigneter Mechanismus zum Schutz von Identitäten.

- Im Abschnitt »Automatisierungpotenzial« sollte der Fokus nicht nur auf Verträgen liegen, sondern das Automatisierungspotenzial von Regeln und Abläufen allgemein hervorgehoben werden. Smart Contracts sind keine Verträge im juristischen Sinne, auch wenn Smart Contracts als Instrument zur effizienten Vertragsdurchführung genutzt werden können. Ein Vertrag im juristischen Sinne setzt ein willentliches Handeln von natürlichen Personen (Menschen) voraus, da ja natürliche Personen von einem Vertrag verpflichtet werden. An diesem Prinzip sollte auch in der Blockchain-Welt festgehalten werden.

- Im Abschnitt »Dezentrale Apps« sollte beachtet werden, dass auch DApps von einem Anbieter (Marktteilnehmer) herausgegeben werden können und nicht zwangsweise Marktmacht verschieben.

- Private Blockchains werden selten unternehmensintern genutzt (außer z.B. zu Compliance Zwecken) und sind eher im Konsortium relevant.

- Man sollte sich bei der Beschreibung nicht ausschließlich auf die Blockchain-Technologie oder Ethereum als öffentliche Blockchain fokussieren, sondern den Betrachtungsrahmen auch für Technologien wie IOTA oder Hashgraph offen halten.

- Skalierbarkeit kann auch die verarbeiteten Transaktionen in einem bestimmten Zeitraum beschreiben, nicht nur die Anzahl der Transaktionen pro Block.

- Viele der Grundideen der Blockchain-Technologie wurden bereits deutlich vor 2008 veröffentlicht. Die meisten technologischen Grundlagen, wie Hashfunktionen und Signaturen sind sogar noch älter. Der wesentliche Beitrag von Satoshi Nakamoto ist die Integration der unterschiedlichen Technologien im Rahmen der Anwendung Bitcoin.

- Bei »Proof-of-Stake« werden immer Nutzer ausgewählt, die einen Anteil an der zugrundeliegenden Kryptowährung haben. Eine rein zufällige Auswahl unter allen Teilnehmern des Netzwerks würde die Sicherheit der Blockchain gefährden. Richtig wäre daher, dass Teilnehmer auf Basis ihres Anteils und nach einem Zufallsprinzip ausgewählt werden. Zudem sollten auch weitere Konsensmechanismen wie »Proof of Activity«, »Proof of Authority« etc. nicht vernachlässigt werden, da es sich bei DLT um eine noch sehr junge Technologie handelt, deren Ausgestaltung und Entwicklung in Zukunft nicht absehbar ist.

- Im Abschnitt »Anreizsystem« sollte beachtet werden, dass der häufig als negativ angeführte, hohe Energieverbrauch bei privaten Blockchains nicht gegeben ist, da das sogenannte Mining-Verfahren entfällt. Zudem kann in privaten Blockchain-Netzwerken durch vereinbarte Lese-, Schreib- und Administrationsrechte der Grad an Transparenz zwischen den Partnern von Wertschöpfungsnetzwerken individuell festgelegt werden. Private Blockchains werden daher im B2B-Bereich in den nächsten Jahren zunehmende Akzeptanz erfahren.

- Weitere Grundprinzipien, die explizit genannt werden sollten, sind die Transparenz und die Verteilung von Daten, sowie die lückenlose Nachvollziehbarkeit von aufgezeichneten Transaktionen.

2.2 Anwendungsfelder

Die Blockchain-Technologie ist eine vielversprechende Schlüsseltechnologie für viele Anwendungsfelder, wenn auch nicht überall einsetzbar. Eine Blockchain-Lösung bietet immer dann einen Mehrwert, wenn vertrauensvolle Informationen zwischen vielen Teilnehmern ausgetauscht werden sollen, aber keine gemeinsame vertrauenswürdige Grundlage besteht.

Dabei bietet sich die Nutzung der Blockchain-Technologie insbesondere dann an, wenn der Austausch bislang über eine zentrale Stelle lief und das dafür bisher genutzte System im Vergleich dazu langsam, ineffizient oder teuer ist bzw. wenig Vertrauen in diese Stelle besteht. Im Umkehrschluss lohnt sich der Einsatz der Blockchain-Technologie möglicherweise nicht, wenn es nur eine kleine Anzahl von Teilnehmern gibt, die bereits ein Vertrauensverhältnis aufgebaut haben, bzw. ein effizientes zentralisiertes System besteht.

Daher ist der Einsatz einer Blockchain im Einzelfall sehr genau abzuwägen, da die Nutzung der Technologie erhebliche Kosten und Aufwand sowie Herausforderungen mit sich bringen kann. Hinzu kommt, dass in vielen Bereichen bisher nur Modellversuche durchgeführt werden bzw. laufende Prozesse nur in geringem Umfang in einer Arbeitsumgebung auf Blockchain-Basis abgebildet sind.

In den nachfolgenden Anwendungsbereichen erscheint der Einsatz der Blockchain-Technologie volkswirtschaftlich von besonderem Interesse, allerdings ist die Zusammenstellung nicht abschließend:

Bitte geben Sie Ihre Stellungnahme zu den Anwendungsfeldern ein:

Bitkom Stellungnahme:

Jeweils unterschiedliche Eigenschaften der Blockchain sind für die Anwendungsfelder und Branchen relevant. So sind beispielsweise für das Internet der Dinge vor allem die Smart Contracts mit den damit verbundenen Automatisierungs- und Autonomisierungspotenzialen von zentraler Bedeutung. In Ergänzung dazu sind es bei Anwendungsfeldern aus den Bereichen Logistik und Supply Chain Management, digitale Medien oder für Herkunftsnachweise die irreversible Speicherung der Daten und Transaktionen. Der Einsatz von Blockchain sollte in diesem Sinne im Einzelfall abgewogen und niemals vorwegentschieden werden. Valide geschäftliche und technische Gründe müssen den Ausschlag geben.

Das Anwendungspotenzial von Blockchain wird laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) je nach Unternehmensgröße sehr unterschiedlich betrachtet. Während Unternehmen ab 500 Mitarbeitern der Blockchain-Technologie generell positiver gegenüberstehen und in sich in den meisten Fällen mit Anwendungsmöglichkeiten befassen, ist der Einsatz von Blockchain für die meisten kleinen Unternehmen noch kein Thema. In den Unternehmen findet der Blockchaineinsatz vor allem in der Unternehmensverwaltung (Buchhaltung, Finanzen, Controlling; 56%), in Logistik- und Lagerprozessen (34%), oder im Marketing/Vertrieb (26%) statt. Ziele des Blockchain-Einsatzes sind dabei insbesondere die Effizienzsteigerung (87%), die Sicherheit der Prozesse (80%), die Informationssicherheit (68%), die Senkung der Transaktionskosten (65%), die Vertrauensbildung bei der Zusammenarbeit mit anderen Organisationen (41%).

Fehlen aus Ihrer Sicht Anwendungsfelder? Bitte benennen und begründen Sie dieses:

Bitkom Stellungnahme:

Grundsätzlich ist zuzustimmen, dass in den aufgeführten Anwendungsfeldern/Sektoren die größten Potenziale für Blockchainanwendungen liegen. Ergänzend könnte der Hinweis auf den Anwendungsfalls der übergreifenden »Vernetzung« von Sektoren noch angebracht werden. DLT hat da Potenzial, Industriesektoren zu verschmelzen, z.B. indem aus einem rein technischen und einem reinen Finanzprozess ein gemeinsamer Blockchain-basierter Prozess geschaffen wird.

Darüber hinaus wäre es natürlich möglich, in den einzelnen genannten »Makro-« Anwendungsfeldern noch detailliertere Anwendungsmöglichkeiten zu nennen bzw. diese aufzugliedern. »Verwaltung« beispielsweise ist als Betrachtungsebene sehr weit gefasst. Hier könnte eine weitere Differenzierungsebene wie »Innere und Äußere Sicherheit« eingebaut werden, da hier ggf. andere Anforderungen im Kontext Daten-/Geheimschutz gelten. Auch der Bereich der industriellen Fertigung, des Maschinen- und Anlagebaus könnte noch expliziter, neben dem »Internet der Dinge«, genannt werden.

Anwendungsfeld a) Finanzsektor (1/2)

Kryptowährungen und Token: Der Finanzsektor ist bereits sehr frühzeitig mit der Blockchain-Technologie in Berührung gekommen. Ursächlich dafür ist die Kryptowährung Bitcoin, der erste praktische Anwendungsfall der Blockchain. Kryptowährungen wie Bitcoin wurden ursprünglich entwickelt, um Online-Bezahlungen zu erleichtern, ohne dass ein vertrauenswürdiger Dritter – in der Regel ein Dienstleister des Finanzsektors – benötigt wird. Bei Kryptowährungen handelt es sich nicht um staatliche Währungen. Kryptowährungen werden von keiner Zentralbank oder öffentlichen Stelle emittiert und sind regelmäßig nicht an eine gesetzlich festgelegte Währung

gebunden. Gleichwohl werden sie von einigen natürlichen oder juristischen Personen als Tauschmittel akzeptiert. Inzwischen gibt es über 2.000 Kryptowährungen und Token mit einer Marktkapitalisierung von rund 100 Mrd. Euro. Auswirkungen auf die Finanzstabilität bestehen aufgrund des geringen Marktvolumens und der geringen Verbundenheit zum Finanzsektor bislang nicht.

Kryptowährungen sind ein Spezialfall digitaler (Wert-)Einheiten (Token), die auf einer Blockchain auf elektronischem Wege übertragen, gespeichert und gehandelt werden können. Mit diesen Token können verschiedenste Rechte verbunden sein. So gewähren sogenannte Utility-Token Zugang zu digitalen Nutzungsrechten oder Dienstleistungen. Andere Token, sogenannte Security Token, sollen mitgliedschaftliche Rechte oder vergleichbare vermögenswerte Rechte, ähnlich wie Aktien oder Anleihen, gewähren. Denkbar ist, dass Token zukünftig auch Rechte an Sachen repräsentieren können. Diese Entwicklung wird Tokenisierung genannt.

Um Kryptowährungen und andere Token hat sich zudem ein Ökosystem entwickelt, das neben Tauschplattformen u.a. sogenannte Wallet-Provider umfasst, die die jeweiligen kryptografischen Schlüssel der Inhaber von Kryptowährungen und Token verwalten.

Initial Coin Offerings: Zunächst zur Finanzierung von Blockchain-basierten Startups hat sich seit ca. 2015 mit sogenannten Initial Coin Offerings (ICOs) eine neue Blockchain-basierte Finanzierungsform entwickelt. ICOs stellen einen Prozess dar, in dem Unternehmen oder andere Projektträger Kapital für ihre Projekte im Austausch für Token beschaffen. Für den internationalen Markt kommt eine im Herbst 2019 veröffentlichte Studie (Ernst & Young, Initial Coin Offering, The Class of 2017 one year later vom 19. Oktober 2018) zu dem Ergebnis, dass im Jahr 2017 über ICOs 4,1 Mrd. US-Dollar Anlegergelder eingesammelt wurden und im ersten Halbjahr 2018 15,5 Mrd. US-Dollar. Von den 2017 emittierten Token notieren 86 Prozent unter ihrer ersten Kursfeststellung; 30 Prozent haben nahezu ihren vollständigen Wert verloren. Im Durchschnitt weisen ICOs aus dem Jahr 2017 einen Verlust gegenüber den erreichten Höchstkursen von 66 Prozent aus. Die erzielten Volumina deuten darauf hin, dass ICOs grundsätzlich eine attraktive Finanzierungsform für junge Startups sein können. Inwieweit sie als nachhaltige Anlageform geeignet sind, muss sich angesichts der dargestellten Verluste jedoch noch zeigen.

ICOs unterscheiden sich dabei erheblich von bisher etablierten Formen der Unternehmens- und Projektfinanzierung: Der Begriff ICO lehnt sich zwar an den Begriff Initial Public Offering (IPO) an. ICOs sind im Gegensatz zu IPOs jedoch nicht zwingend unternehmensbezogen, sondern können projektbezogen sein, das heißt die im Rahmen des ICOs angebotenen Token können der Beteiligung am Erfolg eines Open-Source-Projektes ohne zentrale Instanz dienen, wie zum Beispiel der Ethereum-Blockchain. IPOs werden von Unternehmen durchgeführt, die in der Regel über eine erfolgreiche Geschäftshistorie verfügen. ICOs dienen hingegen der Frühphasenfinanzierung von Unternehmen oder Projekten, bei denen oft nur ein Projektkonzept vorliegt, ähnlich einem Fundraising. Von einer klassischen Frühphasenfinanzierung durch eine Venture-Capital (VC)-Gesellschaft unterscheiden sich ICOs dadurch, dass sich an diesen auch Kleinanleger unmittelbar beteiligen können. Ein weiterer entscheidender Unterschied ist die durch die weltweite Handel-

barkeit über Tauschplattformen grundsätzlich mögliche Handelsliquidität der emittierten Token. Eine klassische VC-Beteiligung ist hingegen bis zu einem IPO illiquide.

Im Gegensatz zu einem IPO werden bei einem ICO regelmäßig keine Beteiligungsrechte in Form von Aktien emittiert. Auch erhält der Anleger bei einem ICO in der Regel keine Beteiligung am Cash Flow des Emittenten in Form von Zinsen oder Dividenden. Vielmehr erhält der Anleger in der Mehrzahl der ICOs Utility-Token bzw. Kryptowährungen. Diese gewähren als Utility-Token Zugang zu den vom Projektträger zu entwickelnden digitalen Plattformen, respektive den dort angebotenen Rechten und Dienstleistungen. Dabei steht für viele Anleger nicht der Erwerb der späteren Nutzungsmöglichkeit im Vordergrund, sondern eine erwartete Wertsteigerung des Tokens bei Erfolg des finanzierten Unternehmens/Projektes. Da derzeit regelmäßig keine Beteiligungsrechte, Zinsen oder Dividendenansprüche gewährt werden, resultiert diese mögliche Wertsteigerung bei ICOs allein aus einem möglichen Nachfrageanstieg nach den Token im Falle des Erfolges des Projektes/Unternehmens. Gleichzeitig sind die Tokeninhaber bei dezentralen Open-Source-Projekten durch die Möglichkeit des Wertanstieges der Token incentiviert, zum Erfolg des Projektes beizutragen, zum Beispiel durch Beiträge zur Entwicklung der Open-Source-Software. Dadurch können sich positive Netzwerkeffekte ergeben.

Bisher gibt es noch keine allgemein anerkannten Bewertungsmodelle für ICOs, da die zugrundeliegenden ökonomischen Mechanismen noch nicht abschließend erforscht sind.

In der Gesamtschau eignen sich ICOs mit Utility-Token und Kryptowährungen primär zur Finanzierung dezentralisierter Blockchainprojekte. Bei diesen ist regelmäßig eine Beteiligung über klassische Eigen- und Fremdkapitalinstrumente nicht möglich, da es an der zentralen Beteiligungsinstanz fehlt. Darüber hinaus erfüllen Utility-Token oder Kryptowährungen im Rahmen von Blockchain-Anwendungen spezifische Funktionen. Utility-Token und Kryptowährungen erscheinen jedoch nach derzeitigem Kenntnisstand weniger geeignet für die Finanzierung von KMUs, die keine Blockchain-bezogenen Produkte und Dienstleistungen anbieten. Aus Anlegersicht stehen den Chancen einer Beteiligung an einer ggf. liquiden Frühphasenfinanzierung die in dieser Phase besonders hohen Risiken und Informationsasymmetrien sowie die nur indirekte Beteiligung am Projekt/Unternehmenserfolg gegenüber.

ICOs könnten jedoch nicht auf Utility-Token und Kryptowährungen beschränkt bleiben. Perspektivisch denkbar wäre auch der Einsatz von Security-Token, die Beteiligungs-, Zins- und/oder Dividendenrechte abbilden. Damit könnte sich möglicherweise auch ein Markt für ICOs vor allem von KMU ohne Blockchain-bezogene Dienstleistungen und Produkte entwickeln.

Kapitalmarktrecht: Kryptowährungen, Token und ICOs stellen auch neue Herausforderungen an das Kapitalmarktrecht. Je nach Ausgestaltung sind diese bereits heute von finanzmarktrechtlichen Vorschriften erfasst. So müssen beispielsweise in Deutschland ansässige Kryptohandelsplätze dieselben geldwäscherechtlichen Vorschriften befolgen wie andere Finanzdienstleister – vor allem, was die Identifizierung von Kunden angeht. Auf europäischer Ebene sieht die Änderungsrichtlinie zur 4. Geldwäscherichtlinie EU/2015/849 vor, dass Dienstleister, die »Virtuelle Währungen« in staatliche Währungen (zum Beispiel Euro) und umgekehrt tauschen, sowie

Anbieter von elektronischen Geldbörsen in den Kreis der geldwäscherechtlich Verpflichteten aufgenommen werden müssen. Das hat unter anderem zur Folge, dass die Umtauschplattformen und Anbieter elektronischer Geldbörsen gegenüber ihren Kunden geldwäscherechtliche Sorgfaltspflichten anzuwenden haben, d.h. vor allem die Identifizierung der Kunden etwa beim Umtausch von staatlichen in virtuelle Währungen und umgekehrt bzw. beim Anlegen einer elektronischen Geldbörse. Die Bundesregierung bereitet gerade die notwendigen Anpassungsmaßnahmen der deutschen rechtlichen Bestimmungen vor.

Zudem ergeben sich bei der Rechtsanwendung häufig Auslegungsfragen, die zu Rechtsunsicherheit bei den Marktteilnehmern führen können. Um Rechtssicherheit zu schaffen, hat die BaFin im Februar 2018 ein Hinweisschreiben zur aufsichtsrechtlichen Einordnung von sogenannten Initial Coin Offerings (ICOs) zugrundeliegenden Token bzw. Kryptowährungen herausgegeben.

Daneben gibt es allerdings auch Bereiche, die bislang regulatorisch nicht erfasst sind (wie etwa die Emission von Utility-Token und Kryptowährungen), bzw. die bestehende Regulierung, die technische Spezifika der Blockchain nicht berücksichtigt.

Aufgrund des grenzüberschreitenden Charakters von öffentlichen Blockchains, auf denen Kryptowährungen und Token gespeichert und transferiert werden, sowie der weltweiten Handelbarkeit ist vor allem eine internationale und europäisch abgestimmte Herangehensweise sinnvoll. Die Bundesregierung setzt sich daher auf internationaler und europäischer Ebene mit Nachdruck für einen abgestimmten Umgang mit Krypto-Token ein. Auf deutsch-französische Initiative hin befassen sich seit März 2018 die G20 zusammen mit den internationalen Standardsetzern (insb. FSB, FATF, IOSCO) intensiv mit dem Thema Krypto-Assets. Im Vordergrund stehen hier vor allem Fragen der Geldwäscheprävention, der Finanzstabilität, des Anlegerschutzes und der Marktintegrität. Innerhalb der G7 hat Deutschland zusammen mit Japan die Leitung einer G7-Koordinierungsgruppe zu Krypto-Assets übernommen. Zudem befasst sich auf europäischer Ebene die Europäische Kommission im Zusammenhang mit dem FinTech-Aktionsplan mit Krypto-Assets und mit sogenannten Initial Coin Offerings. In die dazu von der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) durchgeführten Arbeiten bringt sich die deutsche Finanzaufsicht aktiv ein.

Derzeit prüft die Bundesregierung, ob bereits vor Abschluss der internationalen und europäischen Arbeiten auf nationaler Ebene weiterer Handlungsbedarf besteht. Dies umfasst insbesondere die elektronische Begebung von Wertpapieren.

Bitte geben Sie Ihre Stellungnahme zu dem Themengebiet Kryptowährungen, Token und ICOs ein:

Bitkom Stellungnahme:

Kryptowährungen erwecken die Hoffnung auf neue, alternative Zahlungsmittel. Der Wert der meisten Kryptowährungen ist heute lediglich durch Angebot und Nachfrage am Markt zu

ermitteln. Aufgrund ungleicher Verteilung der Coins/Tokens in oftmals nicht liquiden Märkten können Preise sehr stark manipuliert werden. Insbesondere bei Kryptowährungen mit niedrigen Marktkapitailisierungen und geringen Handelsvolumina ist das der Fall. Der Wert der »Utility« von Utility Tokens zeigt sich auch erst nach dem Netzwerklaunch und wird hauptsächlich durch typische, ökonomische Parameter wie dem intrinsischen Wert (Anzahl Nutzer, Anzahl der Transaktionen, etc.) und dem Spekulationswert bestimmt. Der Gegenwert der Tokens die in einem ICO ausgegeben werden, entspricht also diesen beiden Dimensionen. Da oft noch keinerlei Nutzerbasis besteht, die Incentives der einzelnen Teilnehmer (Token Economics) nicht zureichend ausgetestet sind, sowie der Grundnutzen der Utility unklar ist, sind viele ICOs extrem spekulative Investments. Ob ICOs, ohne weitere Regularien und ohne Showcases, in denen Businessmodelle erfolgreich in eine Token Economy überführt wurden, eine zweite Renaissance erleben, ist sehr fraglich. Das Risiko eines Investments war in der Vergangenheit bei vielen Projekten als äußerst hoch einzuschätzen und somit für Privatanleger als höchst fraglich zu bewerten.

So sehen Unternehmen im Einsammeln von Finanzmitteln im Rahmen von ICOs laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) das geringste Potenzial der Blockchain (nur 36% stimmen dem zu).

Durch eine entsprechende Schaffung von Rechtssicherheit und bindender Regelungen können ICOs zur Finanzierung von Unternehmen und Geschäftsprozessen jedoch durchaus Sinn machen. Die Ausgabe von Token, z. B. bei Immobilieninvestments, könnte Kleinstinvestitionen erst ermöglichen. Privatanleger erhalten so erstmals die Möglichkeit, in Asset-Klassen zu investieren, die ihnen aufgrund hoher Mindestinvestitionssummen zuvor nicht zugänglich waren. Dies stellt unter Einhaltung aller verbraucherschutzrechtlichen Voraussetzungen eine Demokratisierung alternativer Investments dar.

Wir empfehlen Stablecoins in der Aufzählung hinzuzufügen. Stable coins sind spezielle Token, die bewusst an eine Fiat-Währung gekoppelt sind und dadurch das Währungsrisiko gegenüber FIAT-Währungen reduzieren. Am Fraunhofer IML bzw. durch das von dort ausgegründete Startup Ledger Engineers wird z.B. mit LogCoin ein bilanzierungsfähiger und an die FIAT-Währungen gekoppelter Krypto-Token für die Logistik entwickelt. Dies ist ein möglicher Schritt um Manipulationen und Wertschwankungen vorzubeugen, ohne die Vorteile der Tokenisierung aufzugeben.

Gibt es – außerhalb der Spekulation – nachhaltige Anwendungsmöglichkeiten für Kryptowährungen?

Bitkom Stellungnahme:

Kryptowährungen bilden eine Grundvoraussetzung für den Betrieb von öffentlichen Blockchains oder ähnlichen Netzwerken, da diese als Anreiz für die Bereitstellung von Ressourcen wie Rechenleistung, Speicherplatz, etc. und zur Absicherung des Netzwerkes gegen Angriffe

benötigt werden. Ob der Wert einer Kryptowährung dabei losgelöst von einer zugrundeliegenden FIAT-Währung sein muss, ist fraglich. Allerdings können Kryptowährungen ihren Sinn nur dann optimal erfüllen, wenn ihr Wert an den Wert des Netzwerkes und der dort gespeicherten/verwalteten Werte gekoppelt ist. Die Notwendigkeit von dedizierten Kryptowährungen für eine DApp sollte jedoch grundsätzlich diskutiert werden.

Stablecoins, aber auch andere Kryptowährungen ohne entsprechende Volatilität bieten die hinreichend bekannten Vorteile bei der Zahlungsabwicklung, sodass Kryptowährungen auch abseits der Spekulation Sinn machen. Ein Beispiel dafür ist das Building Blocks-Programm des World Food Programs (WFP), bei dem Flüchtlinge in Krisenregionen mit Hilfe einer Kryptowährung in einem »permissioned network« Waren kaufen können. Hierbei werden nicht nur Kosten für Intermediäre bei der Zahlungsabwicklung gespart, sondern auch die Geschwindigkeit und Kontrolle, mit denen das WFP die Gelder verwalten und verteilen kann, haben sich verbessert. Durch das Hinzufügen weiterer Autoritäten in dem Blockchainnetzwerk ergibt sich die Möglichkeit, dass verschiedene Sektionen der UN transparent Spendengelder verwalten können.

Insgesamt können Kryptowährungen die weitergehende Digitalisierung von Finanzprodukten vorantreiben.

Ist die Token-Emission eine zukunftsfähige Form der Unternehmens- und Projektfinanzierung bzw. unter welchen Rahmenbedingungen könnte sie sich dazu entwickeln?

Bitkom Stellungnahme:

Grundsätzlich ja, da der Token eine digitalere Form eines Anspruchs darstellen kann (Anteile an Unternehmen, Anleihen, Währung, Wertgegenstände, etc.). Die grundsätzlichen Vorteile der Zahlungsabwicklungen (Geschwindigkeit, Transparenz, geringere Transaktionskosten) werden auch in Zukunft eine große Rolle spielen.

Welche Tokenarten werden den Markt der ICOs in den nächsten 5 Jahren dominieren?

Bitkom Stellungnahme:

Security Tokens, die neue Anlegerkreise und Sekundärmärkte erschließen können, werden in unseren Augen eine große Rolle spielen. Zusätzlich gehen wir davon aus, dass auch Utility Token und Kryptowährungen weiter Bestand haben werden.

Welche Missbrauchsrisiken bestehen? Welche Risiken bestehen für Kleinanleger?

Bitkom Stellungnahme:

Anleger, die in Kryptowährungen investieren, kaufen ein Versprechen in die Zukunft, das meist keinen gesicherten physischen Gegenwert hat. Es handelt sich daher um reine Spekulationsobjekte, die, im Gegensatz zu Aktien, nicht an den Erfolg des emittierenden Unternehmens gekoppelt sind. Wie auch bei Gutscheinen ist eine Wertsteigerung rein spekulativ. Ein Problem ist auch die asymmetrische Informationsverteilung bei ICOs. Kleinanleger können die Risiken, Produkte, und die token-emittierenden Unternehmen nur schlecht einschätzen.

Sollte die Emission von Utility-Token und Kryptowährungen reguliert werden? Sollte diese Regulierung auf europäischer oder auf nationaler Ebene erfolgen?

Bitkom Stellungnahme:

Ja, die Regulierung sollte auf europäischer Ebene erfolgen. Mit nationalen Alleingängen kann das Problem nicht gelöst werden. Insbesondere ICO Investoren müssen auch die rechtlichen Vorgaben ihres Heimatlandes erfüllen, selbst bei fortschrittlicher Regulierung in kleinen Staaten. Kleinanlegerschutz und kapitalmarktrechtliche Anforderungen sollten möglichst europäisch reguliert werde.

Welche inhaltlichen Aspekte (zum Beispiel Anlegerschutz, Marktintegrität (insbesondere bezüglich Insiderhandel und Kursmanipulation), Handelstransparenz, Erlaubnispflichten für bestimmte Dienstleistungen) sollte eine etwaige Regulierung adressieren?

Bitkom Stellungnahme:

Eine Regulierung sollte Anlegerschutz und Informationspflichten adressieren, und dabei Transparenz über die Tokenverteilung, Lock Up Periods, und Investmentpreise der einzelnen Marktteilnehmer (insbesondere bei mehrstufigen ICO-Modellen) schaffen. Zudem sollten auch Bewegungen von großen Tokenmengen im Handelsverlauf transparenter und sichtbarer werden, ggf. müssen auch OTC Deals mit adressiert werden. Zusätzlich müssten wohl auch Gefahren der Geldwäsche und betrügerischem Missbrauch der Blockchain-Technologie und ihrer Möglichkeiten adressiert werde.

Wie werden Potenziale von Kryptowährungen, die an Realwährungen gekoppelt sind, also sogenannte stable coins, bewertet?

Bitkom Stellungnahme:

Die Potenziale von Stable Coins sind langfristig sehr hoch einzuschätzen, da die Fungibilität der Token im digitalen Finanzsystem der Zukunft sehr wichtig sein wird. Zudem haben die Zentralbanken derzeit mehrheitlich nicht vor, FIAT-Währungen auf Blockchain-Basis anzubieten. Auch bei Stable Coins ist Transparenz der entscheidende Punkt. Es muss sichergestellt werden, dass die Realwerte der Währungen auch im Token hinterlegt wurden.

Anwendungsfeld a) Finanzsektor (2/2)

Anwendung in der Finanzwirtschaft: Das von vielen in der Blockchain-Technologie gesehene Innovationspotenzial für die Finanzwirtschaft über Kryptowährungen und ICOs hinaus beruht auf der Möglichkeit, komplexe Transaktionsprozesse ggf. einfacher, transparenter und stärker automatisiert abzubilden und damit Transaktionskosten zu senken. Dementsprechend finden sich Erprobungs- und Anwendungsfälle in der Finanzwirtschaft unter anderem in den Bereichen Zahlungsverkehr, Wertpapierabwicklung und Handelsfinanzierungen. Beispielsweise haben die Deutsche Bundesbank und die Deutsche Börse zwei Prototypen zur Wertpapierabwicklung auf Basis der Blockchain-Technologie erfolgreich entwickelt und getestet. Im internationalen Zahlungsverkehr haben sich über 70 Banken zu einem »Interbank Information Network« zusammengeschlossen, um Blockchain-basiert internationalen Zahlungsverkehr durchzuführen. Die Daimler AG und die Landesbank Baden-Württemberg (LBBW) haben pilotweise gemeinsam die Blockchain-Technologie eingesetzt, um eine Finanztransaktion mit einem Schuldscheindarlehen im Volumen von 100 Mio. Euro darzustellen. Unter anderem aufgrund der notwendigen Vertraulichkeit von Geschäftsprozessen kommen bei (Pilot-)Anwendungen in der Finanzwirtschaft private Blockchainlösungen zum Einsatz. Ein Beispiel hierfür ist Hyperledger, eine Open-Source-Kollaboration der Linux Foundation und zahlreicher Industriepartner, die entwickelt wurde, um branchenübergreifende Blockchain-Technologien zu entwickeln.

Die deutsche Finanzwirtschaft steht nach einer Umfrage von PWC (Blockchain in Financial Services – Mehr als nur ein Hype?, Juli 2018) der Blockchain-Technologie jedoch noch abwartend gegenüber. So ist für knapp zwei Drittel der befragten Finanzdienstleister die Etablierung von Blockchain-Lösungen kein Teil der strategischen Planung.

Bitte geben Sie Ihre Stellungnahme zu dem Themengebiet Anwendung in der Finanzwirtschaft ein:

Bitkom Stellungnahme:

Das Innovationspotenzial der Blockchain im Finanz- und Versicherungswesen wird gemeinhin darin gesehen, aktuell langwierige und komplexe Transaktionen zwischen Partnern, wie zum Beispiel zwei Finanzinstituten, durch Automatisierung zu beschleunigen und die Transaktionen zugleich manipulationssicher und transparent abzubilden und damit letztendlich Transaktionskosten zu reduzieren.

Laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) sehen drei Viertel der Banken und Versicherungen sehr großes bis eher großes Potenzial im Einsatz der Blockchain in ihrem Unternehmen. Vor allem als dezentrales Transaktionssystem und Handelsplattform (77%), zur sicheren und transparenten Übertragung von Eigentumsnachweisen (76%), und zur Verbriefung von realen Gütern und Finanztiteln (61%) wird Blockchain hohes Potenzial eingeräumt. Jedoch haben erst 6% der Banken und Versicherungen DLT im Einsatz.

Neben NASDAQ und ASX setzen auch zahlreiche Finanzunternehmen auf die Technologie. Es sind mehrere Blockchain-Konsortien entstanden, deren Teilnehmer Finanzunternehmen sind, zum Beispiel BCCC, R3, u.a..

Eine Vielzahl von Banken (z.B. Deutsche Bank, Santander, UBS, Barclays Bank, usw.) experimentiert mit der Technologie. Das Hyperledger-Projekt Iroha stellt beispielsweise für mehrere Unternehmen die Möglichkeit des gemeinsamen Managements der KYC-Daten (Know Your Customer) zur Verfügung.

Aus Verbrauchersicht können durch den lückenlosen Nachweis von Transkationen bei DLT einfacher Regressansprüche belegt werden. Zudem können Transaktionskosten für Marktteilnehmer, darunter auch Endverbraucher, durch die Ausschaltung von Mittelsmännern sinken. Blockchain-Lösungen können für erhöhte Transparenz sorgen.

Für Supply Chain Finance bietet die Blockchain-Technologie in Verbindung mit Smart Contracts ein vielversprechendes Anwendungsfeld. Durch die Harmonisierung und zeitliche Annäherung von Finanz- und Materialströmen (bis hin zur Echtzeit-Transaktion) profitieren Lieferanten von einer schnelleren Bezahlung. Vor allem bei Waren mit einer hohen Umschlaghäufigkeit bewegen sich die Materialströme so schnell, dass die Finanzströme i.d.R. erst mit einer größeren zeitlichen Verzögerung erfolgen. Der Einsatz innovativer Supply-Chain-Finance-Lösungen kann durch die Blockchain-Technologie befördert werden.

Mithilfe der Blockchain-Technologie und Smart Contracts können rechnungslose Transaktionen ermöglicht werden und die mehrheitlichen Papierrechnungen, welche langwierige, manuelle Prozesse erfordern, ersetzen. Dabei sichert die Blockchain die Vertragsinhalte und die Smart Contracts überprüfen die Vertragsausführung und lösen die Transaktionen automatisch aus. Die Transaktionsbestätigung wird ebenso in der Blockchain gespeichert.

In welchen Anwendungsbereichen im Finanzsektor sind Blockchain-Anwendungen bereits im produktiven Einsatz bzw. wo werden sie in absehbarer Zeit zum Einsatz kommen?

Bitkom Stellungnahme:

Es gibt zahlreiche Anwendungsbeispiele für den Blockchain Einsatz im Finanzwesen:

- Blockchain World Wire (IBM, Stellar)
- Blockchain bei Schuldschein-Transaktion (Daimler und LBBW)
- Automatisierter Buchungsabgleich (webjet limited, Reychain)
- Energiehandelsplattform (BP, Royal Dutch Shell, Statoil, Innogy)
- Anleiheemission, bei der der Token die Aufgabe zur Hinterlegung einer Globalurkunder übernimmt (Bitbond)
- Akkreditivkreditenplattform we.trade (IBM)
- Anreizsystem für Plastikmüllsammlung (Plastic Bank)
- Kredit Derivate (DTCC)

Zu welchen Erkenntnissen hat die Erprobung geführt mit Blick auf den zukünftigen Einsatz der Blockchain als Alternative zu bestehenden Systemen?

Bitkom Stellungnahme:

Allein die Effizienzsteigerung klassischer Finanzgeschäfte wird zukünftig für Banken nicht ausreichen, um am Markt zu bestehen. Es bedarf zusätzlich der Entwicklung neuer Produkte und disruptiver Geschäftsmodelle für Finanzdienstleister. Die Kombination von Material-, Informations- und Finanzflüssen mit Hilfe von auf vertrauenswürdigen Technologien beruhenden Transaktionssystemen wie Blockchain bewirkt die Vereinfachung des Zahlungsverkehrs und der Handelsfinanzierung und schafft gleichzeitig die Grundlage für ein durchgängiges Management von Supply Chains (end-to-end). Über eine Blockchain-basierte Plattform können Banken z.B. mit den Akteuren entlang der Wertschöpfungskette verbunden werden, um Handelsgeschäfte zukünftig schneller, effizienter und effektiver abwickeln zu können.

Wie ist die deutsche Finanzwirtschaft im Vergleich zur Finanzwirtschaft in Europa, USA und Asien im Bereich Blockchain-Technologie positioniert?

Bitkom Stellungnahme:

Im Bereich Blockchain-Technologie ist die Finanzwirtschaft einer der führenden Treiber und Stakeholder. Es existieren verschiedene, große Bankeninitiativen (z.B. we.trade) oder auch das R3-Konsortium um die Technologie »Corda«, an welchen Finanzinstitute aus aller Welt beteiligt sind.

Ein Großteil der Entwicklungen findet in Europa, insbesondere in London, statt. Diese Initiativen verfolgen das Ziel, »klassisches« Finanzgeschäft wie z.B. Transaction Banking, Finanzierung und/oder Wertpapierhandel auf der Blockchain abzuwickeln.

Asien ist der Hotspot für den Handel verschiedener Kryptowährungen. Hier ist insbesondere Südkorea mit diversen Handelsplätzen zu nennen.

Insgesamt hat die deutsche Finanzwirtschaft im Bereich Blockchain sicherlich noch Nachholbedarf was Blockchain Testphasen, Einsatz, und eingebrachte finanzielle und personelle Ressourcen angeht. Laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) sehen die meisten Unternehmen Deutschland bei der Einführung von Blockchain maximal im Mittelfeld. 8% beschreiben Deutschland sogar schon als abgeschlagen. Als Vorreiter werden insbesondere die Schweiz, Malta, Singapur oder Liechtenstein genannt.

Anwendungsfeld b) Energie (1/2)

Stromhandel: Die Blockchain-Technologie könnte zu einem Baustein der Energiewende werden: In Zeiten kleinteiliger Stromerzeugung und -speicherung birgt der direkte Handel zwischen zwei Parteien, dem Erzeuger und dem Verbraucher, große Potenziale – gerade für die Marktintegration von kleinen und flexiblen Energieerzeugungsanlagen. So ist es möglich, soweit die Netz-Infrastruktur darauf ausgelegt ist, den Strom direkt zu liefern und die Zahlungen digital abzuwickeln. Für das Gesamtsystem können sich daraus allerdings auch neue Herausforderungen, wie zum Beispiel die Finanzierung und Regulierung der Netze, Versorgungssicherheit und die Integration von erneuerbaren Energien, ergeben.

Die bisherige Regulierung im Energiesektor ist nicht auf dezentrale Peer-to-Peer-Beziehungen ausgerichtet. Sie zeichnet sich durch die Trennung von Netzbetreiberaufgaben und der Versorgung von Kunden aus. Kunden können ihren Stromlieferanten selbst auswählen. Jeder Kunde ist hierfür einem Bilanzkreis und einem Bilanzkreisverantwortlichen zugeordnet. Außerdem ist erforderlich, dass ein Abgleich zwischen geplantem und tatsächlichem Verbrauch stattfindet (»Clearing«). Für eine Stromlieferung ist somit eine komplexe Struktur an Beteiligten erforderlich.

Innerhalb der bisherigen Regulierung würden sich u.a. die Fragen stellen, wer Messstellenbetreiber ist, wer die Prognose an den Übertragungsnetzbetreiber meldet, wer eine Zulassung als Stromlieferant besitzt und wer Bilanzkreisverantwortlicher ist. Nach dem bisherigen Verständnis würde jeder Energieverbraucher beispielsweise zum Bilanzkreisverantwortlichen werden und hätte die damit einhergehenden Anforderungen zu erfüllen (insbesondere die Meldung von Lastprognosen an den Netzbetreiber). Aus diesem Grund erscheint die Koordination von Netzwerk-Teilnehmern in einer konsortialen Blockchain – wie bereits in der Praxis geschehen – in diesen Fällen eine durchaus denkbare Variante zu sein.

Das Potenzial der Blockchain liegt darin, eine direkte Vertragsbeziehung zwischen Energieverbraucher und -erzeuger zu ermöglichen. Durch die Technologie kann eine klare Zuordnung des eingespeisten und verbrauchten Stroms zu variablen Preisen erfolgen. Gewisse Funktionen zwischengeschalteter Akteure sind bei einer Blockchain-Struktur entbehrlich. Auch könnten Vorgaben zu Preisanpassung, zu Kündigungsterminen, zum Rücktrittsrecht, zum Lieferantenwechsel und zu geltenden Tarifen in einem System »gematchter Stromlieferungen« im Gegensatz zu langfristigen Lieferbeziehungen obsolet werden. Es sollte daher erwogen werden, inwiefern bei dem Einsatz der Blockchain-Technologie von den regulatorischen Anforderungen, unter Wahrung der rechtlichen Vorgaben zum Schutz personenbezogener Daten und des Privatsphärenschutzes, abgesehen werden kann, gegebenenfalls auch in Experimentierräumen.

Bitte geben Sie Ihre Stellungnahme zu dem Themengebiet Energie, insbesondere Stromhandel, ein:

Bitkom Stellungnahme:

Die Energiewende ist ohne Dezentralisierung und Digitalisierung nicht denkbar. Aufgrund der Zunahme an dezentralen Erzeugungs- und Verbrauchseinheiten, der steigenden Anzahl an Marktakteuren (Prosumer, Internet der Dinge, Elektrofahrzeuge) ist der Einsatz neuer Informations- und Kommunikations-Technologien nicht mehr wegzudenken. Blockchain kann hier ein zuverlässiges Register für Handelsbeziehungen darstellen.

Man stelle sich zudem ein Zukunftsszenario vor, in dem lokale Stromverbraucher sowie Erzeuger über die dynamische Anpassung der Netzentgelte zu einem netzdienlichen Verhalten angereizt werden. Die Netzentgelte als Steuerungsmechanismus – dieser Methode würde mannigfaltige Änderungen bei der Regulierung mit sich bringen.

In Zeiten kleinteiliger Stromerzeugung und -speicherung birgt der direkte Handel zwischen zwei Parteien, dem Erzeuger und dem Verbraucher, große Potenziale – gerade für die Marktintegration von kleinen und flexiblen Energieerzeugungsanlagen. Gerade ab dem Jahr 2024, wenn viele kleine PV-Anlagen aus der EEG-Förderungen herauszufallen, ist der lokale P2P Handel eine attraktive Alternative. So ist es möglich, soweit die Netz-Infrastruktur darauf ausgelegt ist, den Strom direkt zu liefern und die Zahlungen digital abzuwickeln. Der Nachweis

bezüglich des Doppelvermarkungsverbots über eine Blockchain sowie das sichere und schnelle Teilen von Informationen stellen einen technischen Mehrwert für den P2P Stromhandel dar.

Durch DLT kann eine klare Zuordnung des eingespeisten und verbrauchten Stroms zu variablen Preisen erfolgen. Hier sind digitale Stromzähler und die damit einhergehenden Datenbestände eine wesentliche Voraussetzung für die Umsetzung. Der in Deutschland verzögerte Smart-Meter-Rollout kann sich somit auch als Hemmnis für die kurzfristige Ausbreitung der Technologie und der entsprechenden Use Cases darstellen.

Das Anwendungsfeld Energie wird sehr häufig als perfektes Anwendungsbeispiel aufgeführt, ist in Bezug auf die Herausforderungen jedoch eine Stufe komplexer als klassische Anwendungsfelder wie Kryptowährungen und Finanzdienstleistungen. Ursache ist dafür ist u.a., dass zum einen die physikalischen Gesetzmäßigkeiten und marktechnischen Notwendigkeiten beim Transport von Strom beachtet werden müssen, und zum anderen die Intermediäre nur schwer zu ersetzen sind. Die aktuellen Transaktionszeiten der public Blockchains lassen zudem im Energiehandel noch keinen aktiven Handel im Großhandelsmarkt zu, so dass es eine Limitierung der möglichen Einsatzgebiete nicht nur durch regulatorische Anforderungen gibt. Ein Handel im Intraday-Markt wäre zum Beispiel durch ein Algotrading-Tool aktuell noch nicht abbildbar.

Welche besonders relevanten/geeigneten Anwendungsfälle werden im Energiebereich gesehen?

Bitkom Stellungnahme:

Der zentrale Anwendungsfall im Energiesektor ist der dezentrale Stromhandel. Die Anzahl der Energieerzeuger steigt kontinuierlich. Immer mehr Verbraucher betreiben eigene Solar-, Wind- oder Biogasanlagen, deren überproduzierte Energie sie ins Stromnetz einspeisen bzw. direkt an den Nachbarn oder ein nahegelegenes Unternehmen verkaufen könnten. Über die Blockchain könnten diese Transaktionen in Echtzeit nachgehalten und zugleich abgerechnet werden – kryptographisch verschlüsselt und dennoch nachvollziehbar für alle Beteiligten. Dabei handelt es sich um einen weiteren Anwendungsfall, der sich besonders für den Blockchain-Einsatz eignet, da entsprechende Micro Payments bisher an Aufwand und Kosten scheitern. Weitere Anwendungsfälle, die sich sowohl technisch als auch regulatorisch abbilden lassen, sind der Lieferantenwechsel und Mieterstrom. Bei diesen Beispielen fungiert die Blockchain als Protokoll, um den sicheren Austausch von Information fälschungssicher zu gewährleisten. Die Bruttowertschöpfung von Strom zu steigern, Prozesskosten zu reduzieren und die Abrechnung zwischen den Beteiligten zu vereinfachen.

Weitere mögliche Anwendungsfälle im Energiebereich sind z.B.:

- Engpassmanagement in Elektrizitätsverteilernetzen

- Energiedienstleistungen für Gebäude & Industrieprozesse
- Anmeldung von Anlagen im Marktstammdatenregister (MaStR)
- Zertifizierung von Herkunftsnachweisen
- Abrechnung von Entgelten und Umlagen (Strom)
- Kündigung und Lieferantenwechsel (Strom)
- Außerbörslicher Großhandel (Strom)
- Handel und Allokation von Netzkapazitäten (Strom)
- Dezentrales Roaming für EV inkl. Abrechnung beim Sharing (privater) Wallboxen
- Finanzierung und Sharing Investments von Anlagen gemäß Erneuerbare-Energien-Gesetz (Security Token)
- Transaktionslösungen für Quartiere, Ermöglichen autarker Quartierversorgung

Welche Erfahrungen konnten mit Blockchain-basierten Anwendungen im Handel von Strom und Gas gewonnen werden?

Bitkom Stellungnahme:

Ein Beispiel ist das Projekt Share & Charge, einem Spin-Off des Innogy Innovation Hubs. Das Aufladen von Elektroautos wird durch die Blockchain modernisiert. Dadurch werden die Besitzer der Elektroautos einfach per App für das Aufladen bezahlen können. Share & Charge setzt auf das Tobalaba Protocol der Energy Web Foundation, und hat die IP in eine eigene Foundation überführt.

Im Energiegroßhandel wird außerdem z.B. das Projekt Enerchain im Konsortium von 40 europäischen Energieversorgungsunternehmen vorangetrieben, durch das der Handel mit Strom und Gas über die Blockchain einfacher und günstiger werden soll.

Insgesamt konnten P2P-Handelsszenarien bislang meist nur simuliert werden, da die Regulierung keine Anwendung im Markt zulässt. Dabei könnten Tokens und Schlüssel Herkunft und Qualität nachweisen, was die Grundlage für kleinteilige Marktmechanismen darstellt.

Hürden bestehen insofern im Bereich des Regulierungsrahmens, z.B. dem Energierecht, Wettbewerbsrecht/Kartellrecht, oder Datenschutz. Die Bundesregierung sollte einen Rahmen

schaffen, durch welchen diese Hürden bewältigt werden und Prosumer in die Lage versetzt werden können, zukünftig am Markt teilzunehmen, und dabei gleichzeitig Systemstabilität gewährleistet ist.

Welche regulatorischen Anpassungen sind notwendig, um solche Pilotprojekte in die Praxis umzusetzen? Stehen diese in einem vertretbaren Verhältnis zu dem erwarteten Nutzen wie evtl. höherer Systemstabilität und –effizienz?

Bitkom Stellungnahme:

Für den Peer-to-Peer Handel müssten die Rollen und Pflichten der Marktteilnehmer durchlässiger werden, sodass z.B. ein Privatkunde Strom direkt kaufen/verkaufen kann und die Pflichten aus dem Bilanzkreis etc. gegebenenfalls an einen Service-Provider auslagern kann. Dies würde zu einer zukünftigen, stärker verteilten Energieproduktion aus erneuerbaren Anlagen führen und zum Ausgleich und der Stabilität der Netze auf lokaler Ebene beitragen.

Außerdem wären Klarheit im Kontext Datenschutz erstrebenswert (Recht auf Vergessen, Anonymität etc.), sowie für Fragen des MsbGs: Welche Zählwerte dürfen genutzt werden? Wie kommen die Daten aus dem Smart Meter/SMGW in die Blockchain? Wie kann ich Zählwerte erfassen, so lange noch kein SM/SMGW installiert ist (Rollout steht noch aus und wird lange dauern)?

Kleine Marktteilnehmer müssen befähigt werden, direkt am Markt teilzunehmen. Dafür müssen einige Fragen beantwortet werden: Wer managed den Bilanzkreis? Wer gleicht Differenzmengen aus? Wie erfolgt die Kommunikation gegenüber Verteil- und Transportnetz?

Zudem sind alle Regeln der Marktkommunikation auf die Anwendung der Blockchain zu untersuchen.

Eine befürwortete regulatorische Anpassung könnte die Möglichkeit zum Aufsetzen eines Test-Micro-Grids sein, um Auswirkungen direkt zu erforschen und den Wandel zu beobachten. Dafür wäre es nötig, einige regulatorische Beschränkungen für ein solches Testfeld aufzuheben und gleichzeitig Untersuchungen mit öffentlichen Forschungsmitteln zu fördern.

Welche Regulierungsanforderungen bestehen an die Ausgestaltung der Blockchain-Technologie für einen Einsatz im Strommarkt?

Bitkom Stellungnahme:

Verschiedene, mitunter technische Fragen müssen geklärt werden: Wie kommen »reale Werte« in die Blockchain? Wie werden die Informationen von Zentralregistern (Marktstamm-

datenregister, Regionalregister, etc.) für die Blockchain nutzbar gemacht. Können Zentralregister sogar überführt werden? Daraufhin können Regulierungsanforderungen an die Ausgestaltung der Blockchain-Technologie für einen Einsatz im Strommarkt untersucht werden.

Mit welchen Maßnahmen könnte und sollte der Energiesektor auf die Dezentralisierung von Wirtschaftsbeziehungen ausgerichtet werden?

Bitkom Stellungnahme:

Der Smart Meter/Gateway Rollout ein Hebel für die Digitalisierung der Energiewende. Neben dem Smart Meter sollten auch der Transport, die Erzeugung, und die Speicherung »smart« und dezentral gestaltbar sein. Zudem sollten alle Marktakteure im Rahmen des Internets der Dinge (Assets, die Flexibilität handeln können) einem dezentralen Register zugeordnet werden, damit die Identifikation, die Interaktion und die Transaktion in Bezug auf Demand/Response automatisch und interaktiv geregelt werden kann.

Bisher sind das Stromnetz sowie auch die Stromerzeugung zentral organisiert. Auch fehlt es auf der Niederspannungsebene (an den »Endpunkten« des Netzes) an Zustandsdaten und Live-Informationen. Durch die Einbringung intelligenter Messsysteme in Gebäuden werden diese verteilten Endpunkte zunehmend in das Gesamtsystem eingebunden. Durch die Nutzung des Smart Meter Gateways werden dezentrale Akteure Teil von bestehenden Marktplätzen und können gleichzeitig neue dezentralisierte Marktplattformen auf Basis der Blockchain-Technologie etablieren. Selbst nach dem Rollout der SMGW könnten diese aber u.a. aufgrund der technischen Richtlinie nicht für den Einsatz in dezentralen Marktplätzen genutzt werden. Es ist demnach durch die Blockchain-Strategie ein Weg aufzuzeigen, wie Smart Meter/Smart Meter Gateways für dezentralisierte Marktplattformen auf Basis von Blockchain-Technologie genutzt werden sollen/können. Da der Rollout nicht für alle Marktteilnehmer vorgesehen ist, müssen dezentralisierte Marktplattformen auch ohne diese Infrastuktur möglich sein.

Die Etablierung eines Test-Migrogrids mit regulatorischer Sonderrolle und die Bereitstellung von öffentlichen Forschungsgeldern könnten dabei helfen, am realen Beispiel die Auswirkungen zu untersuchen und Dezentralisierung zu testen.

Zudem wären folgende, zusätzliche Maßnahmen denkbar:

- Schaffung eines Ordnungsrahmens der beschreibt, wie »Prosumer« direkt am Markt teilnehmen können.
- Es müssen Authorities (Marktrollen) in Blockchains abgebildet werden. Das erfordert eine Marketauthority, die zur Anlage anderer Authorities authorisiert ist. Diese ist idealerweise staatlich einzurichten.
- Öffentliche Ausschreibungen in Bezug auf Blockchain prüfen und ggf. anpassen.

- Forschungsanstrengungen zu Data Aging in Blockchain zum Lösen des Speicherbedarfs intensivieren.

Ist der Anbieterwechsel ein geeigneter Anwendungsfall für Blockchain? Gibt es Hindernisse? Gibt es weitere Anwendungsfälle?

Bitkom Stellungnahme:

Für den Anbieterwechsel bedarf es der Angabe personenbezogener Daten. Da in einer Blockchain die Rechte des Betroffenen gem. DSGVO derzeit rechtlich nicht sicher geregelt sind, scheint dieser Anwendungsfall bisher schwierig. Dies trifft natürlich nur dann zu, wenn die personenbezogenen Daten »onchain« geführt werden. Ein weiteres Hindernis ist das Wettbewerbsrecht. Die dena-Studie »Blockchain in der integrierten Energiewende« (2019) hat diesen Anwendungsfall differenziert betrachtet und bewertet.

Welche Schätzungen gibt es zur Energie- und Klimabilanz des Einsatzes von Blockchain-Technologie im Energiesektor (auch im Vergleich mit alternativen Maßnahmen)?

Bitkom Stellungnahme:

Wenn hier auf den Energiebedarf bei Proof of Work Blockchains angespielt wird, dann ist bereits heute klar, dass PoW basierte Netzwerke eine zu vernachlässigende Rolle in industriellen Kontext spielen werden. Schon heute werden entsprechende Use Cases primär auf Konsortial-Chains aufgebaut. Diese nutzen in der Regel andere Konsens-Mechanismen wie z.B. PoA (Proof of Authority), PoS (Proof of Stake) u.a.. Jedoch haben all diese Verfahren eins gemein, sie sind sehr energieeffizient und schnell. In diesem Setup existiert kein Unterschied in Sachen Energie- und Klimabilanz im Vergleich zu zentral organisierten Systemen/Netzwerken. Des Weiteren ist einer der Schwerpunkte in Sachen Technologieentwicklung die Skalierbarkeit von Blockchains, was im Umkehrschluss bedeutet, dass die Effizienz dieser Technologie mit der Weiterentwicklung steigen wird. Auch Off-Chain Lösungen, wie z.B. L2 Netzwerke (Raidon Netzwerk) und weitere flankierende Technologien werden hier einen positiven Beitrag leisten.

Anwendungsfeld b) Energie (2/2)

Stromnetze: Auch bei der Stabilisierung des Stromnetzes kann die Blockchain-Technologie grundsätzlich zum Einsatz kommen. Derzeit erprobt der Übertragungsnetzbetreiber TenneT zusammen mit der Firma sonnen GmbH die Verwendung von dezentralen Batteriespeichern für die kurzfristige Änderung des Kraftwerkeinsatzes zur Vermeidung von Netzengpässen (Redi-

spatch). Die Heimspeicher sollen mittels Blockchain in das Stromnetz eingebunden werden, um automatisiert netzentlastend ein- und ausspeichern zu können.

Mittels Blockchain und Smart Contracts können kleine Stromerzeuger ihren Strom zeitgenau und in exakt der benötigten Menge einspeisen, wie ein regionaler Verbraucher diesen benötigt. Das kann Netzbetreiber bei der Stabilisierung des Stromnetzes entlasten.

Bitte geben Sie Ihre Stellungnahme zu dem Themengebiet Stromnetze ein:

Bitkom Stellungnahme:

Der Verweis auf Verteilnetzbetreiber fehlt in der Stellungnahme (z.B. bei der Integration EEG zu nennen). Die Möglichkeit lokaler Märkte (quasi Verbindung Abschnitt a. Stromhandel und b. Stromnetze) durch die Blockchain-Technologie wird nicht betont.

Die Blockchain-Technologie ist geeignet um kleinere Märket autark steuern zu können und mit der Hilfe von Smart-Contracts die Netzsteuerung autark zu übernehmen und auch kleinste Mengen genau abzurechnen. Das würde auch die Einbindung von E-Mobility in die Netze erleichtern, da die Lade-/Entladezeit genau nachvollzogen bzw. gesteuert werden könnte. Auch eine Prognose wäre zu einem gewissen Grad obsolet, da das Netz innerhalb kürzester Zyklen ausgeglichen werden kann.

Die Einspeisung erfolgt dann wenn Wind weht oder Sonne scheint. Eine Verschiebung der Einspeisung wäre nur dann möglich wenn jede EEG Anlage direkt mit einem dezentralen Speicher verbunden wäre, der die Energie bis zur Einspeisung puffern kann.

Für steuerbare Erzeugungsanlagen und Verbraucher ist es möglich über Preissignale o.ä. Lastverschiebungen zu incentivieren. Idealerweise sollte die Optimierung, d.h. Vermeidung von Peak Lasten im Netz in den Ortsnetzen beginnen und von dort aus über alle Netzebenen hinweg betrieben werden.

Ergeben sich Risiken für kritische Netzinfrastrukturen durch dezentralen Stromhandel?

Bitkom Stellungnahme:

»Richtig« gesteuert und verwaltet, wird das Risiko für kritische Netzinfrastrukturen minimiert werden. In Sachen »richtig« Steuern, Verwalten und Tracken wird DLT/Blockchains einen großen Beitrag leisten können. Zudem können Netzstabilitätsparameter direkt und in Echtzeit in den Stromhandel einbezogen werden und damit sichergestellt werden, dass der Handel/Markt nicht versucht physikalische Grenzen zu überwinden.

Generell wird durch einen dezentralen Stromhandel die Resilienz des Gesamtsystems gestärkt, da zentrale, kritische Knotenpunkte an Bedeutung verlieren. Dies steht und fällt aber mit dem Sicherheitslevel der eingebrachten dezentral verteilten Teilnehmer. Smart Meter Gateways bieten an dieser Stelle einen BSI-zertifizierten Standard an IT-Sicherheit und Daten-Integrität, den Steuerungslösungen, die über den Internetzugang des Endkunden kommunizieren, nicht gewährleisten können.

Die Infrastruktur muss redundant und hoch verfügbar sein. Wenn die Infrastruktur ausreichend geschützt ist, trägt die Dezentralität eher zur Sicherheit bei, da es keinen »Single-Point of Failure« für eine Attacke/Ausfall gibt.

Dezentraler Stromhandel kann praktisch nicht ohne Nutzung des (lokalen) Micro Grids erfolgen. Ein Risiko ist insbesondere, dass das Anreizsystem nicht passend genug definiert ist und damit der Handel gegenteilig zum netzdienlichen Verhalten erfolgt.

Weitere Risiken:

1. **Ungewollte Transparenz:**

- Wettbewerbsrechtliche Implikationen durch volle Transparenz der Markteilnehmer untereinander.
- Denanonymisierung der Marktteilnehmer.
- Ungewollte Transparenz bei den Verbrauchern (DSVGO), abhängig davon, ob personenbezogene Daten unverschlüsselt »onchain« geführt werden.

2. **Ungewollte Zentralisierung durch Token Economy auf einzelne private Blockchains und damit einhergehende Zentralisierung der Entwicklungstätigkeit.**

3. **Unbeherrschbares Datenspeicherwachstum durch fehlendes Löschen.**

Welche Auswirkungen werden durch den Einsatz von Blockchain auf die Bepreisung von Strom sowie die Finanzierung und die Regulierung der Netze gesehen?

Bitkom Stellungnahme:

Grundsätzlich muss geklärt werden, ob man mehr oder anders gelagerte Anreizmechanismen bieten möchte, um z.B. netzdienliches Verhalten zu fördern oder nicht, ganz abgesehen von der Blockchain. Tendenziell kann mit einer Senkung der Gebühren durch eine schlankere Infrastruktur und durch eine höhere Automatisierung gerechnet werden.

Welche Auswirkungen werden durch den Einsatz von Blockchain auf die Versorgungssicherheit und die Integration von erneuerbaren Energien gesehen?

Bitkom Stellungnahme:

Grundsätzlich ist ein möglicher Ansatz um den notwendigen Netzausbau zu minimieren bei gleichzeitigem Ausbau von erneuerbaren Energien, Angebot und Nachfrage möglichst lokal und zeitgleich auszugleichen. Um solche Zellen effizient und über verschiedene Parteien hinweg verwalten zu können, kann der Einsatz von DLT/Blockchain-basierten Lösungen das Mittel der Wahl sein.

Durch die bessere Integration der Anlagen (auch Kleinstanlagen) ist ein flexiblerer und kleinteiligerer Ausgleich der Netzte möglich.

Welcher zusätzliche nationale Stromverbrauch ergäbe sich durch eine ausgeweitete Nutzung der Blockchain-Technologie? Wären Netzkapazitäten hierfür ausreichend ausgelegt?

Bitkom Stellungnahme:

Die Blockchain-Technologie an sich ist keine besonders energiehungrige Technologie. Die Anreizsysteme führen zu der stetig wachsenden Installation von Rechenleistung in PoW basierten Netzwerken. Zudem werden keine PoW basierten Chains in Szenarien, wie hier beschrieben, verwendet werden. Die Effizienz von dezentralen Netzwerken wird immer weiter steigen, da die Skalierbarkeit immer weiter verbessert werden wird. Schon heute ist der Stromverbrauch von Blockchains (wie z.B. der Energy Web Chain) auf dem Niveau von zentral organisierten Systemen.

Können dezentrale Kleinspeicher mittels Blockchain zu einem virtuellen Großspeicher zusammengeschaltet werden?

Bitkom Stellungnahme:

Ja. Es könnte bei Aufruf eines bestimmten Smart Contracts immer eine klar definierte Gruppe von dezentralen Kleinspeichern gemeinsam angesprochen werden. In Summe agieren diese dann wie ein virtueller Großspeicher. Technisch ist das demnach machbar, aufgrund der doppelten Netzentgelte (laden des Speichers/abrufen vom Speicher) ist das allerdings heute nicht wirtschaftlich.

Generell sollte das Energiesystem als Ganzes betrachtet werden. Dies impliziert eine virtuelle Zusammenschaltung von Einzelanlagen. In Bezug auf lokale Netzengpässe sind dabei jedoch

die physikalischen Grenzen zu berücksichtigen. Wenn in Stadt A ein großer Speicher zur Beseitigung von Netzengpässen benötigt wird, hilft hier kein virtueller Zusammenschluss der Speicher des ganzen Landes. Einfacher ist es, wenn diese sich in einem Bilanzkreis befinden.

Kann eine lokale just-in-time Vermarktung von Strom zur Stabilität des Stromnetzes beitragen?

Bitkom Stellungnahme:

Dies ist möglich, aber davon abhängig unter welcher Zielsetzung diese Vermarktung erfolgt. Im Sinne der Netz-Stabilität ist ein kostenoptimierender Handel nicht immer zielführend.

Wichtig ist die Einbeziehung der Akteure, die auch heute für die Stabilität des Stromnetzes verantwortlich sind, d.h. Übertragungsnetzbetreiber, Verteilnetzbetreiber und Bilanzkreisverantwortliche. Wenn diese die Rahmenbedingungen bzw. ihre Anforderungen aus Netzsicht in einen just-in-time Handel von Strom einbringen, kann das Ergebnis durchaus zur Stabilität des Stromnetzes beitragen.

Eine Incentivierung im Sinne der Netzdienlichkeit gekoppelt mit dezentralen Handelsmechanismen kann dazu führen, dass Netzlasten optimiert werden.

Anwendungsfeld c) Gesundheit/Pflege

Im Gesundheitswesen sind sehr oft besonders sensible persönliche Daten tangiert. Transparente Blockchain-Technologie und entsprechende Anwendungen im Gesundheitswesen müssen daher besonders hohen Anforderungen im Hinblick auf die Gewährleistung der im Gesundheitsbereich bestehenden Standards bei Datenschutz und Datensicherheit gerecht werden, die denen anderer Anwendungen im Gesundheitsbereich entsprechen müssen. Sollte die Technologie dazu beitragen können, die Datensouveränität von Patienten zu erhöhen, wäre dies eine positive Errungenschaft. Sollte sich die Blockchain-Technologie in Bereichen des Gesundheitswesens durchsetzen, könnte diese Technologie einen maßgeblichen Einfluss auf den digitalen Wandel im Gesundheitswesen haben. Das Bundesministerium für Gesundheit (BMG) hat einen Ideenwettbewerb für Anwendungskonzepte der Blockchain-Technologie im deutschen Gesundheitswesen initiiert. In diesem Wettbewerb soll sondiert werden, ob es Anwendungen im Gesundheitssystem gibt, für die die Blockchain-Technologie nutzbringend sein kann. In dieser frühen Stufe sollen eingereichte Konzepte insbesondere anhand der Kriterien Relevanz und Mehrwert sowie Zukunftsfähigkeit, Interoperabilität und (Daten-)Sicherheit bewertet werden. Neben der Patientensouveränität stehen dabei auch andere schutzwürdigen Interessen der Patientinnen und Patienten im Vordergrund.

Bitte geben Sie Ihre Stellungnahme zu dem Anwendungsfeld Gesundheit/Pflege ein:

Bitkom Stellungnahme:

Das Gesundheitswesen steht vor vielen Herausforderungen, die den Einsatz von Blockchain-Technologien rechtfertigen könnten. Die darin involvierten zahlreichen Parteien (Patient, Arzt, Krankenkasse, Pflegedienst, Apotheker, Arzneimittelhersteller usw.) benötigen bei der Interaktion miteinander zahlreiche Nachweise und Bestätigungen, Rechte und Zugriffsmöglichkeiten müssen geregelt und sicher nachverfolgt werden, etc. Eine sichere Kommunikation zwischen den Parteien kann durch die Blockchain-Technologie sichergestellt werden.

Tatsächlich wird es in diesem Umfeld maßgeblich relevant sein, wie Daten in einem zentralen Ledger gespeichert, geregelt zugegriffen und gelöscht werden können. Die Technologie hätte grundsätzlich wegen der Ausfallsicherheit ein großes Potential (z.B. könnten Krankenhäuser für Notfälle die relevanten Blockchain-Daten aller Patienten in ihrem PLZ Bereich vorhalten, Ärzte und Krankenkassen jeweils für Ihre Patienten, der Patient auf seinem mobile Device, etc.). Derzeit ist die Speicherung von Gesundheitsdaten auf der Blockchain jedoch noch problematisch. Perspektivisch kann dies bedeuten, dass Blockchain-Lösungen im Gesundheitswesen sich eher als Referenzarchitektur z.B. für die Steuerung von Zugriffen auf Gesundheitsdaten der Patienten dienen könnten, während die (personenbezogenen) Daten selbst in einer klassischen Datenbank liegen.

Welche Anwendungsfälle gibt es im Bereich Gesundheit/Pflege?

Bitkom Stellungnahme:

Anwendungsfälle und Beispiele sind unter anderem in der Agenda der »Zukunftswerkstatt Blockchain im Gesundheitswesen« des BMG zu finden. Beispiele für Blockchain-Anwendungen im Gesundheitswesen sind z.B.:

- Diverse medizinische Register (Organspende, Transplantaten, Nachweise, Verschreibungen usw.).
- Identitätsmanagement (einschließlich Pflegeberechtigungen).
- Pharmaunternehmen übergreifendes Adhärenz-Management zur Inklusion von Wechselwirkungen sowie Smart Contract basiertem Nebenwirkungsmeldungs-Management (Arzneimitteltherapiesicherheit).
- Patienten-Überleitungsmanagement: Daten-Übertragung zwischen Krankenhaus, niedergelassenem Arzt und Spezialist. Inklusive der Erfassung der korrekten Handhabung des Krankenhaus-Entlassbriefes.

- Nutzung von Smart Contracts für »Outcome-based«: Abrechnungsmodelle zwischen Pharmaunternehmen, Kostenträgern und Digital Health-Lösungsanbietern auf Basis des Therapieerfolges statt der reinen Leistungserbringung.

- Elektronische Patientenakte in Bezug auf Datenzugriffsrechte und Dokumentation (weniger der Datenspeicherung).

- Protokollierung und Nachverfolgung der Lieferkette für verschreibungspflichtige Medikamenten (Vom Hersteller bis zum Patient).

Zeigt die Blockchain-Technologie für diese Anwendungsfälle einen Mehrwert gegenüber herkömmlichen Technologien?

Bitkom Stellungnahme:

Die Frage lässt sich pauschal nicht beantworten. Der Mehrwert der Dezentralität, der revisionssicheren Dokumentation sowie die Ausfallsicherheit können Vorteile darstellen – insbesondere in stark fragmentieren Bereichen, die viele Akteure involvieren, wie es oft der Fall im Gesundheitswesen ist. Die Frage nach der Wirtschaftlichkeit einer Blockchain-basierten Lösung und eine konsequente Kosten-Nutzen-Betrachtung sind komplizierter und stark vom Anwendungsfall abhängig.

Im Rahmen der Ideenwerkstatt des Bundesministeriums für Gesundheit hat ein Anwendungsfall gewonnen, der für diesen spezifischen Fall einen großen Mehrwert abbildet. Die Gewinnerlösung ist eine Anwendung, die alle Betäubungsmitteltransaktionen sicher, unveränderbar und nachvollziehbar in einem verteilten Register speichert und überträgt. Es handelt sich dabei um eine private Blockchain, an der Ärzte, Apotheken und Aufsichtsbehörden beteiligt sind. Diese Akteure dokumentieren gemeinsam die anfallenden Betäubungsmitteltransaktionen, ohne dass nachträgliche Änderungen möglich wären, was die Transparenz erhöht und das Missbrauchsrisiko senkt. Das Projekt wird nun zur Erprobung umgesetzt. Auch in diesem Projekt stellt sich noch die Frage nach der Wirtschaftlichkeit, weil die Etablierung der Lösung mit hohen Kosten verbunden ist. Kosten und Nutzen können aber nur dann objektiv bewertet werden, wenn für geeignet befundene Lösungen ausprobiert und evaluiert werden. Daher sind solche Ansätze zu begrüßen.

Welche rechtlichen und organisatorischen Herausforderungen gibt es beim Einsatz in diesen Bereichen?

Bitkom Stellungnahme:

Beim Verhältnis zwischen den datenschutzrechtlichen Vorgaben und der Nutzung von Blockchain-Technologien stellen sich heute noch unterschiedliche Fragen. Dazu gehören

beispielsweise die Frage des Blockchain-Ownerships und die daraus resultierenden Verantwortlichkeiten oder Lösch- und Korrekturanforderungen. Eine weitere Hürde kann der hohe Bedarf an Rechenleistung in einigen Anwendungsfällen darstellen.

Wie könnten datenschutzrechtskonforme Lösungen zur Anwendung von Blockchain aussehen, vor dem Hintergrund der besonderen Anforderungen im Umgang mit Gesundheitsdaten?

Bitkom Stellungnahme:

Auch hierbei ist die datenschutzrechtskonforme Umsetzung stark abhängig vom Anwendungsfall. Eine sinnvolle Orientierung kann hierbei die die Stellungnahme »Blockchain and the GDPR« des European Union Blockchain Observatory & Forum darstellen. Allgemein ist die Speicherung der Daten außerhalb der Blockchain zu empfehlen, »on-chain« sollten nur Hash-Werte gespeichert werden. Private Blockchain-Lösungen sind datenschutzrechtlich klar im Vorteil, da hier die Beteiligten bekannt sind, Datenschutzrechte adressiert werden können (da hier u.a. klar ist, wem gegenüber ein Auskunftsanspruch ausgeübt werden kann) und eingegrenzt werden kann, wo die Verarbeitung stattfindet (innerhalb/außerhalb der EU). Zudem kann hier durch Vereinbarung zwischen den Beteiligten besser festgelegt werden, wer Controller- bzw. Prozessorpflichten übernimmt, so dass Unklarheiten vermieden werden. Anwendungen zur Anonymisierung und Verschlüsselung werden zudem mit Hochdruck weiterentwickelt, so dass auch auf technischer Ebene Lösungen vorangetrieben werden.

Die Datenhoheit des Patienten sollte im Vordergrund stehen (bei Patienten-bedingten Anwendungen), sowie klare Regelungen der Verwendung des Privat-Keys bestehen (Vormundschaften, Einsicht für Angehörige, usw.). Wie bereits angebracht, wäre es denkbar, für einige Anwendungen die Speicherung der Daten (konventionell, zentral verschlüsselt), und den Zugriff der Daten über die Blockchain zu trennen.

Gibt es ethische Bedenken, die sich aus einer Ansammlung von Gesundheitsdaten in einer Blockchain ergeben?

Bitkom Stellungnahme:

Diese Frage lässt sich nicht grundsätzlich beantworten. Ethische Bedenken würde sich aus dem Zweck der Ansammlung der Art der Daten sowie der Art der Akteure, die Zugriff auf diese Daten haben etc. ergeben. Dadurch sind mögliche ethische Bedenken immer anwendungsspezifisch.

Blockchain und Smart Contracts sind als Technologie zunächst neutrale Werkzeuge. Der Anwendungsfall sollte daher auf ethische Fragen überprüft werden. Beispiel: Ist es ethisch vertretbar einen Algorithmus zu entwickeln, welcher einen Patienten darauf hinweist, dass

er im Zeitraum X beim Beibehalten seines Verhaltensmusters Krankheitsverlauf/Ergebnis Y erleiden wird?

Es bleibt festzuhalten, dass die Gesundheitsdaten selbst vermutlich nicht auf der Blockchain gespeichert werden sollten, sondern z.B. nur der Zugriff über eine Blockchain-Lösung geregelt wird.

Anwendungsfeld d) Mobilität

Die Zeichen im Mobilitätssektor stehen auf Digitalisierung und Automatisierung. Dabei spielt der datenschutzkonforme sichere und automatisierte Austausch von Mess-, Sensor-, Nutzungs- und Abrechnungsdaten sowie Fahrzeugdaten im Allgemeinen eine zentrale Rolle. Für Fahrzeuge, die autonom fahren, untereinander oder mit Verkehrsinfrastrukturen und Ladesäulen kommunizieren, bedarf es neuer Technologien. Ebenso wird sich die Welt der branchenspezifischen Dienstleistungen, wie z.B. Vermietung, Leasing, Versicherungen etc., an diesen Wandel anpassen. Dabei sind die Kriterien, insbesondere der Zweck, der Umfang und die Zugriffsrechte, bei der Generation und dem Austausch von Daten bei Teilnahme am Verkehr zu definieren – unabhängig davon, ob diese Daten von Personen selbst, Dritten oder technischen Einrichtungen erzeugt werden.

Bitte geben Sie Ihre Stellungnahme zu dem Anwendungsfeld Mobilität ein:

Bitkom Stellungnahme:

Laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) ist die Automobilindustrie im Branchenvergleich die einzige Industrie, in der sich die Mehrheit der Unternehmen inhaltlich mit der Blockchain-Technologie auseinandergesetzt hat. Jedes dritte Automobilunternehmen sieht in der Blockchain die Möglichkeit, bestehende Produkte bzw. Dienstleistungen anzupassen. Jedes vierte (27%) sieht das Potenzial, neue Produkte bzw. Dienstleistungen Blockchain-basiert anzubieten. Für 31% der Unternehmen ist sogar die Entwicklung gänzlich neuer Geschäftsmodelle denkbar.

In der Mobilität kommt auch der Gedanke einer Machine Economy (M2M Interaktion/Angebot und Nutzung und Bezahlung von Services) sehr schnell zum Tragen, Welche eine neue Infrastruktur benötigt, hier reicht ein Internet der Information nicht mehr aus.

Dabei sind die Anwendungsmöglichkeiten im Bereich Mobilität eng verbunden mit der Logistik (der Mobilität von Gütern).

Der Dreh- und Angelpunkt ist dabei das Eigentum. Konkret geht es um das Eigentum am Fahrzeug sowie die Möglichkeit, anderen Personen oder Maschinen Rechte einzuräumen.

Über das Eigentum am Fahrzeug werden z.B.

- weitere Rechte vergeben/verwaltet wie z.B. Nutzungsrechte, Veräußerungsrechte, Verfügungsrechte,
- Freigaben zur Erhebung und Verarbeitung von Fahrzeugdaten (z.B. Telematik) vergeben,
- Dienstleistungen (Versicherung, HU/AU, Reparaturen, ...) in Anspruch genommen.

Somit basieren heutige wie auch zukünftige Dienstleistungen wie Carsharing, sich selbst ladende Fahrzeuge, autonom fahrende Fahrzeuge, Telematikdienste, Fahrzeugleasing, Fahrzeugvermietung, etc. selbst im Bereich »Machine to Machine« zunächst einmal darauf, dass das Eigentum oder die notwendigen Rechte am Fahrzeug geklärt und von einer Person oder Maschine nachgewiesen wurden. Im Anschluss daran kann dann die Dienstleistung in Anspruch genommen werden.

Welche Anwendungsfälle im Bereich der Mobilität zeichnen sich ab (z.B. im Bereich des automatisierten und vernetzten Fahrens, der Erhebung von Straßenbenutzungsgebühren, der intermodalen Transporte (Personen und Güter))?

Bitkom Stellungnahme:

Anwendungsfälle sind nicht nur im Bereich des automatisierten und vernetzten Fahrens denkbar, sondern auch bei der Integration von Verkehrslösungen (z.B. regionaler Verkehrsverbünde). Beispielsweise reist eine Person von Rostock nach Heidelberg und nutzt hierfür verschiedene Mobilitätsangebote (Bus, Bahn, Flugzeug, e-Bike etc.). Diese sind untereinander momentan nicht vernetzt, nicht kompatibel und die jeweiligen Kundendaten werden nicht verknüpft. Es geht aber nicht darum, alles auf eine gemeinsame Plattform zu laden. Die jeweiligen Mobilitätsanbieter behalten die Hoheit über ihre Daten, insbesondere die Kundendaten, und tauschen nur die jeweils unbedingt notwendigen Information für die Abwicklung der Mobilitätsanforderung aus, und auch die Verrechnung der jeweiligen Erlöse und Aufwände erfolgt direkt über technische Integration. BC ist eine per se geeignete Technologie, um das notwendige Vertrauen zwischen hierbei aktiven und passiven Geschäftspartnern und den jeweiligen Kunden herzustellen. Ebenso sollten KI-basierte Lösungen mit BC kombiniert werden, um eine solche Integration zu erreichen.

Weitere Anwendungsbeispiele sind z.B.

- Maut-, Parkgebühren usw.
- Zahlen für Benzin/Strom von autonomen Fahrzeugen
- Paketdienstleistungen
- Vehicle2Grid
- Autonome Beförderungsdienste
- Intermodaler Transport von Containern und Prozessieren der Frachtpapiere über Blockchain
- Digitale Authentifizierung
- Digitaler Identitätscheck
- Führerscheindatenbank (Regierung von Bahrein)
- Automatische Rückerstattung von Kosten per smart contracts bei Verspätungen oder Ausfall
- Zulassung von Beförderungsmaschinen (e-Scooter etc.)

Wird gesetzlicher Handlungsbedarf im Bereich der Mobilität gesehen, um Blockchain-basierte Mobilitätslösungen massenmarktfähig einzusetzen?

Bitkom Stellungnahme:

Grundsätzlich sind manche Formulierungen/Vorgaben in der DSVGO mit DLT schwer umzusetzen, hier wäre eine Anpassung wie z.B. in Frankreich bezüglich der Löschung und Vernichtung von gespeicherten Datensätzen hilfreich. Außerdem wäre die Datenprotokollierung von Fahrzeugen in ein »offenes, verteiltes System« für die Implementierung von Blockchain-Lösungen ein großer Schritt.

Bisher ausschließlich über analoge Dokumente nachweisbare Rechte (z.B. Verfügungsrecht) sollten auch ohne die Ausstellung oder Bezug auf analoge Dokumente digital erfolgen dürfen. Dafür fehlt derzeit die rechtliche Grundlage.

Inwiefern sollten Blockchain-basierte Mobilitätslösungen auf staatlichen Infrastrukturen aufsetzen? Welche Rolle könnte der geplanten europäischen Blockchain-Services-Infrastruktur dabei zukommen?

Bitkom Stellungnahme:

Kommt auf den Use Case an, eine generelle Aussage fällt dazu schwer. Generell muss sichergestellt werden, dass entsprechende Anbieter/Entwickler von Lösungen den notwendigen Freiraum für Innovation behalten. Des Weiteren ist die Wahrscheinlichkeit hoch, dass es noch zu früh ist eine bestimmte Blockchain/DLT-Technologiewahl für ein solches Vorhaben zu treffen, es hat sich noch kein übergreifender Standard etabliert und rasante Entwicklungszyklen sind an der Tagesordnung.

Behörden spielen in diesen Ökosystemen zum Teil eine wichtige Rolle und sollten an einer Blockchain-Lösung anschließbar sein; ob dies private oder staatliche Infrastrukturen sein sollten, hängt am ehesten vom Anwendungsfall ab. Es wird in diesem Zusammenhang auch an Interoperabilitätslösungen zwischen den Blockchain-Implementierungen gearbeitet, so dass verschiedene Blockchains miteinander kommunizieren und Daten austauschen können werden (siehe z.B. Hyperledger Burrow, um Ethereum dApps auf Hyperledger Fabric oder Sawtooth Lake auszuführen).

Eine staatliche Rolle sollte außerdem eine reine Governancefunktion einnehmen (z.B. welches System wird verwendet, welche Updates werden ausgespielt), das System sollte aber dezentral funktionieren. Eine Archivierung (z.B. Bundesarchiv) könnte aber eine sinnvolle hoheitliche Funktion darstellen.

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

Bitkom Stellungnahme:

Es gibt Ansätze, diesen Anforderungen gerecht zu werden, z.B. durch die Off-Chain Speicherung entsprechender Datensätze, allerdings können gezielte Anpassungen an DSVGO (wie z.B. in Frankreich bereits geschehen) helfen solche Themen effizienter zu implementieren. Ergänzend können regional-, regulatorisch-, oder gesetzlichspezifische Subchains aufgesetzt werden, welche, sofern benötigt, aggregierte Informationen zu einer Haupt-Chain melden, um dort z.B. Auditoren für bestimmte Prozesse einzubinden. Das Plasma-Konzept bei Ethereum, das Polkadot Projekt oder die Energy-Web-Chain-spezifische Integration von Polkadot verdeutlichen hier die Idee/den Ansatz.

Prinzipiell kommt es hier auf die Ausgestaltung der Blockchain-Lösung im konkreten Einzelfall an. Insofern sollte auf die Stellungnahme »Blockchain and the GDPR« des European union

blockchain observatory & forum Bezug genommen werden. Allgemein ist die Speicherung der Daten außerhalb der BC zu empfehlen, »on-chain« sollten nur Hash-Werte gespeichert werden. Private Blockchain-Lösungen sind datenschutzrechtlich klar im Vorteil, da hier die Beteiligten bekannt sind, Datenschutzrechte adressiert werden können (da hier u.a. klar ist, wem gegenüber ein Auskunftsanspruch ausgeübt werden kann) und eingegrenzt werden kann, wo die Verarbeitung stattfindet (innerhalb/außerhalb der EU). Zudem kann hier durch Vereinbarung zwischen den Beteiligten besser festgelegt werden, wer Controller- bzw. Prozessorpflichten übernimmt, so dass Unklarheiten vermieden werden. Anwendungen zur Anonymisierung und Verschlüsselung werden zudem mit Hochdruck weiterentwickelt, so dass auch auf technischer Ebene Lösungen vorangetrieben werden.

Mess- und Sensordaten werden vermutlich ohne Eichung oder Kalibrierung der Messgeräte oder Sensoren genutzt. Ist dieser Aspekt zukünftig in der Mess- und Eichverordnung zu berücksichtigen?

Bitkom Stellungnahme:

Das Eichrecht ist eine grundsätzliche Herausforderung, auch ohne Blockchain. Die Frage ist, ob eine »Aufweichung« der Anforderungen ein anzustrebendes Ziel ist, denn auch bei Blockchain/DLT basierten Systemen gilt: »Shit in, Shit out«. Digitale Prozesse bedürfen grundsätzlich verlässlichen Daten und Datenquellen. Blockchains/DLTs können dies sicherstellen, sie können jedoch nicht sicherstellen, dass die Digitalisierung der in der Realwelt aufgenommenen Informationen korrekt und vertrauenswürdig von Statten geht. Allerdings wäre eventuell die Zulassung von neuen Verfahren zur Ermittlung von Richtigkeit/Vertrauenswürdigkeit von Daten hilfreich. Hier können, auch dank der Blockchain, entsprechende Anreiz- und Bestraf-Mechanismen eingeführt werden. Denn je mehr Datenquellen in der Welt vorhanden sind, desto komplexer und aufwändiger wird die Überprüfung der Einhaltung von Normen, Eichung und Kalibrierung werden. Und was nutzen die besten Normen, wenn deren Einhaltung nicht wirksam »erzwungen« werden kann?

Der Zuverlässigkeit von Sensordaten wird eine besondere Bedeutung zukommen. Denkbar ist, dass spezielle geeichte Sensoren im Rahmen der Eichung ein »digitales Zertifikat« z.B. der PtB erhalten, mit dem nachgewiesen werden kann, dass die Daten von einem geeichten Gerät stammen. Dies wäre gesetzlich zu verankern.

Sensordaten werden außerdem zunehmend mit Hilfe entsprechender Algorithmen kalibriert, die von den Sensorbetreibern auf ihren jeweiligen Plattformen bereitgestellt werden. Diese Algorithmen sollen in der Mess- und Eichverordnung berücksichtigt und in Zusammenarbeit mit entsprechenden Agenturen (TÜV, DEKRA, BSI etc.) überprüfbar gemacht werden. Dabei ist die Kritikalität der Daten (siehe kritische Infrastruktur) ein wesentliches Kriterium des Prüfaufwandes.

Anwendungsfeld e) Lieferketten/Logistik

Lieferketten: Für Produzenten und Konsumenten kann die Blockchain-Technologie für eine verlässliche Zusammenarbeit und Transparenz in komplexen Lieferkettensystemen mit vielen Wertschöpfungsschritten sorgen. So sind die Rückverfolgung und Dokumentation von Transport- und Produktionsabläufen zur Qualitätssicherung von Produkten sowie die Evaluierung und Optimierung möglich auch mit Blick auf soziale und ökologische Standards. Analog wäre eine engmaschige Kontrolle und transparente Nachverfolgung von Bauteilen und Rohstoffen einfach in einer Blockchain umzusetzen. Dadurch können neben der Qualitätssicherung von Produkten insbesondere die Arbeitsbedingungen von Menschen am Anfang des Produktzyklus verbessert werden. Diese Transparenz verspricht globale Lieferketten nachhaltiger und gerechter zu gestalten.

Logistik: Um eine Ware beispielsweise von Deutschland in die USA zu verschicken, sei es auf dem Luft- oder Wasserweg, ist auf jeder Seite des Atlantiks eine Vielzahl von Dienstleistern involviert. Dabei werden Vorgänge teilweise noch auf dem Papier abgewickelt und müssen daher beim Transport mitgeführt werden. Die Umstellung auf digitale, Blockchain-basierte Frachtbriefe und Frachtbeförderungsinformationen könnten die zeitaufwändigen Abläufe bei einem Zugewinn an Sicherheit vereinfachen, Vertrauen schaffen und Effizienzpotenziale heben. Bei einer eventuell möglichen Anwendung von Blockchain im internationalen Warenverkehr ist zu beachten, dass Abstimmungsbedarf innerhalb der EU bzw. auf internationaler Ebene entstehen dürfte (Bsp. Zoll).

Blockchain-Lösungen haben das Potenzial, gerade bei kleinteiligen Vertragsbeziehungen zwischen vielen Parteien und bei abzurechnenden Kleinstbeträgen (Micro Payments), die Transaktionskosten zu senken und damit solche Geschäftsmodelle erst möglich zu machen. Micro Payments in geschlossenen Flotten bzw. zwischen Teilnehmern in LKW-Platoons sind ein früher Anwendungsfall für Blockchain in der Logistik. Insbesondere zu diesem Anwendungsfall lässt das Bundesministerium für Verkehr und digitale Infrastruktur derzeit ein Grundgutachten zu den Chancen und Herausforderungen der Blockchain-/Distributed-Ledger-Technologie in der Mobilität erstellen.

Bitte geben Sie Ihre Stellungnahme zu dem Anwendungsfeld Lieferketten/Logistik ein:

Bitkom Stellungnahme:

Ebenso wie im Medizin-Bereich, sind in der Logistik-Branche zahlreiche voneinander unabhängige Parteien involviert, die Mengen an Nachweisen und Bestätigungen in Bezug auf einen bestimmten Wert (Produkt) zwischen einander austauschen. Wenn wir über solche physischen Werte, wie Bauteile, Medikamente, Rohstoffe usw. reden, dürfen wir nicht vergessen, dass die Blockchain-Technologie nur die digitale Seite abdecken kann. Z.B. jedem Wert wird eine digitale ID zugeordnet (ein digitaler Token) und entsprechend protokolliert (wann, wo, unter welchen Bedingungen ist dieser Wert angetroffen worden). Was die Blockchain-Techno-

logie nicht abdecken kann, ist eine manipulationssichere Zuordnung der digitalen ID's zu den physischen Objekten. Diverse Kennzeichnungsmethoden können hier eingesetzt werden (RFID-Chips, QR-Codes, IoT-Geräte, usw.). Diese sind aber auf physischer Seite manipulierbar.

Der Blockchain-Einsatz in der Logistik ist neben der Verwaltung von Unternehmensprozessen der häufigste Anwendungsfall in deutschen Unternehmen (siehe Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019)). Im Bereich der Lieferketten führt die neue Transparenz sicherlich zu vermehrten Kooperationsmodellen. Demnach plant jedes zehnte Unternehmen in Deutschland eine Kooperation mit Zulieferern (siehe Bitkom-Studie). Auch für Verbraucher kann die durch DLT entstandene Transparenz in der Lieferkette (z. B. bei Biozertifikaten, Medikamenten etc.) sehr positive Folgen haben.

Der Einsatz der Blockchain-Technologie in Logistik und Supply Chain Management dient neben einer Kosteneinsparung der Optimierung der weltweiten Ressourcennutzung (Effizienz- und Effektivitätssteigerung), indem Transportwege optimiert und Unternehmensrisiken durch die Erhöhung von Transparenz, Vertrauen und Planungsgenauigkeit gesenkt werden können. Auto-ID-Technik in Kombination mit der Blockchain-Technologie ermöglicht eine Nachverfolgbarkeit über den gesamten Produktlebenszyklus. Zudem können Logistik- und Zahlungsprozesse verbessert und Verluste verhindert bzw. Supply Chain Unterbrechungen reduziert werden. In einem Blockchain-basierten Supply-Chain-Netzwerk fungiert die Blockchain als verteilter Datenspeicher und sichert alle relevanten Informationen für den Smart Contract. Dieser überprüft basierend auf den vorhandenen Informationen die Einhaltung der Vertragsinhalte und legitimiert selbstständig Finanztransaktionen, sofern die Vertragsbedingungen erfüllt wurden. Dabei wird in die Manipulations- und Revisionssicherheit der Blockchain-Technologie vertraut.

Welche Anwendungsfälle bzw. auch Projekte im Regeleinsatz gibt es für die Logistik?

Bitkom Stellungnahme:

Zu den Branchen, die von einer verlässlichen Rückverfolgbarkeit der Produkte vom Ursprungsort bis hin zum Konsumenten profitieren können, zählen u.a. die Pharma- und Lebensmittelindustrie sowie die Edelsteinbranche. Weiteres großes Potenzial für die Blockchain bietet der Güterumschlag, wo der administrative Aufwand beim Warentransport durch die Automatisierung mit Hilfe von Smart Contracts besonders stark reduziert werden kann.

Anwendungsfelder im Einkauf: Viele Beschaffungsprozesse werden heute noch papierbasiert abgewickelt, während die Unternehmen durch den Trend der Individualisierung einer immer größer werdenden Variantenvielfalt ausgesetzt sind. Dies erhöht insgesamt den administrativen Aufwand für den Beschaffungsprozess. Oft ist eine digitale Anbindung von Lieferanten und Partnerunternehmen mit großem finanziellen und personellen Einsatz verbunden. Durch die Vielzahl unterschiedlicher Schnittstellen bedeutet dies einen großen Anpassungsaufwand,

sobald Änderungen im Datenaustauschprozess vorgenommen werden. Einen Lösungsansatz zur Harmonisierung der Schnittstellen bietet die Blockchain-Technologie, welche als Kommunikationsmedium eingesetzt werden kann. Somit können alle Partner, je nach Lese-, Schreib- und Zugriffrechten auf dieselben Informationen zugreifen. Auch Nachbestellungen können mittels Smart Contracts automatisiert ausgeführt werden. Durch die schnelle Datenübermittlung kann die Bedarfs- und Distributionsplanung optimiert werden, die papierlose Abwicklung reduziert den administrativen Aufwand.

Weitere Blockchain-Anwendungsfälle in der Logistik sind z.B.:

- Fälschungssichere Zertifikate bei Luxusartikeln: Um Fälschungen vorzubeugen kann eine Blockchain hilfreich sein. Sie erlaubt eine sichere Rückverfolgung, sodass es schwieriger wird Fälschungen zu verkaufen, als auch teilweise ein Schwarzmarkt unterbunden werden kann.

- Intermodaler Transport von Containern und Prozessieren der Frachtpapiere über Blockchain (TradeLens,Maersk und IBM).

- Auftragsabwicklung (Abwicklung von Bestellungen ohne Plattformen (wie SupplyOn), welche teilweise hohe Gebühren verlangen).

- Rückverfolgung von Rohstoffen aus nachhaltigem/verantwortungsbewussten Quellen (Beispiel Cobalt). Unternehmen haben aktuell kaum Transparenz darüber, woher Grundrohstoffe in ihre Produkten kommen (Beispiel Cobalt in der E-Auto Batterie). Diese Grundstoffe werden oftmals unter nach westlichen Standards nicht zu vertretenden Bedingungen gewonnen (Beispiel Cobalt: Kinderarbeit im Kongo). Aktuell wird mit Zertifizierungsstellen zusammengearbeitet, welche jedoch als nicht 100% zuverlässig gelten. Durch Nutzung einer Blockchain könnte hier Transparenz geschaffen werden.

- In Verbindung mit Sensortechnik und darauf aufbauenden »smarten Ladungsträgern« (Verbindung »Internet of Things«) ist eine Verfolgung des Zustandes von Waren in der Lieferkette möglich. Bei dieser könnten auf Basis von smart contracts bei Veränderungen des Zustandes entsprechende Maßnahmen getroffen werden (Bsp.: Entschädigungszahlungen bei Beschädigung der Ware). Dies würde Vertuschung erschweren.

Welche Anreize und Hindernisse bestehen bei der Etablierung einer Blockchain im Lieferketten-Bereich sowohl national als auch international?

Bitkom Stellungnahme:

Anreize:

- Manipulationssicherheit, revisionssichere Buchungen und Verhandlungen
- unwiderrufliche Transaktionshistorie
- Automatisierung/Autonomisierung der Vertragsausführung, inkl. automatisierte Transaktionen und Payment-Prozesse entlang der Lieferkette
- Umgehung oder Reduzierung von Intermediären empfiehlt sich, wenn flüchtig bekannte Kooperationspartner involviert sind, wo eine Vertrauensbasis fehlt
- Transaktionsgeschwindigkeit
- Transparenz

Hindernisse:

- Exit Strategie: Wie können Teilnehmer, die das Netzwerk verlassen wollen, ihre Daten in der Blockchain »löschen«?
- mangelnde Standardisierung (verschiedene Entitäten aus verschiedenen Ländern mit verschiedenen Gesetzen und verschiedenen Eigeninteressen machen die Standardisierung der Formate und Informationen zu einem schwierigen Unterfangen)
- Interoperabilität unterschiedlicher Blockchain-Lösungen
- Klärung der Rollen- und Aufgabenverteilung innerhalb des Netzwerkes
- Geringer Digitalisierungsfortschritt/-Fachkompetenz im Bereich Logistik bremst Innovation

Gibt es – wenn ja, welche – insbesondere rechtliche und organisatorische Herausforderungen beim Einsatz in diesem Bereich?

Bitkom Stellungnahme:

(Siehe Punkt »Hindernisse« hiervor).

Organisatorische Herausforderungen:

- Vergabe von Lese- und Schreibrechten an einzelne Supply Chain Partner (Wer entscheidet, was die anderen sehen?)
- Wer gehören die Daten bzw. wer kann darauf zugreifen?

- Wie werden Entscheidungen im Konsortium getroffen?
- Wie ist die Governancestruktur? Falls die Governance nicht alle Teilnehmer einbezieht, fair, neutral etc. stattfindet, sind Abspaltungen (Forks) zu erwarten.
- Übertragung von Verifikationen von staatlichen Institutionen (wie dem Zoll) in die Blockchainnetzwerke
- Wie lässt sich die reale Existenz über die Blockchain übertragener Werte verifizieren?

Das Governance Problem ist wohl eine der größten organisatorischen Herausforderungen. Ist diese nämlich nicht entsprechend demokratisch aufgesetzt, so entsteht hinter der Blockchain erneut ein »Mittelsmann«, der die Prozesse in der Lieferkette kontrolliert und von dem folglich alle Teilnehmer abhängig sind. Ein demokratisches System andererseits verlangt von den Teilnehmern eine aktive Teilnahme an Entscheidungsprozessen. Eine Bereitschaft zur Partizipation muss also gegeben sein. Weitere Fragen, die sich stellen, sind: Wie genau ist die Governance strukturiert? Wer haftet? Werden Entscheidungen on-chain oder off-chain getroffen.

Rechtliche Herausforderungen:

- Wie lässt sich die Verbreitung rechtswidriger Inhalte in der Blockchain stoppen?
- Wie kann eine IT-Sicherheit in der Blockchain gewährleistet werden?
- Welche Rechtskraft besitzen die in einer Blockchain gespeicherten Daten und Transaktionen (Nachweiswert von Blockchain-Inhalten)?
- Besteht das Blockchain-Netzwerk aus Teilnehmern in unterschiedlichen Ländern, stellt sich die Frage, welche Rechtsordnung anwendbar ist.
- Zwar lassen sich durch die Blockchain Transaktionen rechtssicher durchführen, aber es lassen sich keine rechtlichen Ansprüche in der Blockchain begründen.
- Wie lässt sich die Identität der Blockchain-Teilnehmer verifizieren, z.B. wenn die Identität für die Durchsetzung eines Anspruchs oder für eine Klageerhebung erforderlich ist?

Ist die Abwicklung von Liefer- und Bezahlvorgängen über öffentliche und offene Blockchains (public permissionless) denkbar oder ist eine Moderation und Supervision innerhalb der Blockchain (private permissioned) auf Basis der bisherigen Praxiserfahrungen erforderlich?

Bitkom Stellungnahme:

Die bisherigen Umsetzungen zeigen, dass für die Abwicklung von Liefervorgängen eine permissionbased Blockchain erforderlich ist. Gegen den Einsatz einer permissionless Blockchain (mit PoW-Konsensmechanismus) wie z.B. Ethereum sprechen:

- Bis eine Transaktion in einen Block geschrieben wurde, dauert es ca. 20 Sekunden, wobei maximal 25 Transaktionen pro Sekunde möglich sind. Dies würde nicht einmal für einen einzigen Anwendungsfall auch nur annähernd ausreichen (permissionbased Blockchains > 1.500 Transaktionen/Sekunde).

- Abhängigkeit von den Minern (unbekannte Dritte), die die Sicherheit des Netzwerkes garantieren müssen. Wenn die eingesetzte Blockchain-Lösung an Beliebtheit verliert bzw. Sicherheitslücken bekannt werden (DAO-Hack), dann würde der Prozess ausfallen und müsste neu entwickelt werden. Dies kann zu existenzgefährdenden Ausfällen führen.

- Energieverbrauch, der durch das Mining entsteht.

- Die Daten werden transparent für alle gespeichert, wodurch auch sensible Informationen preisgegeben werden könnten. Durch Datenauswertungen können Rückschlüsse auf die Prozessabläufe gezogen werden.

Unternehmen sind nicht bereit, diese Risiken einzugehen und greifen auf permissionbased Blockchains zurück. Ebenso werden Bezahlvorgänge nicht mit permissionless Blockchains durchgeführt, da die aktuellen Kryptowährungen zu großen Schwankungen unterworfen sind. Auch Stable Coins sind von einer Währung (meist Dollar) abhängig, wobei das Fremdwährungsrisiko getragen werden muss. Auch hier gilt die Abhängigkeit von unbekannten Dritten (Minern), die den reibungslosen und sicheren Ablauf gewährleisten sollen.

Neben den sogenannten »Enterprise Blockchains« mit im Kern zentralen Governance-Strukturen sind »public permissioned« Blockchains eine richtungsweise Basis um echte dezentrale Netzwerke aufzubauen. Hier werden die Vorteile von öffentlichen Blockchains hinsichtlich Sicherheit und Möglichkeiten der dezentralen Governance basierend auf den Anforderungen der Enterprise-Welt verfügbar gemacht. Die Unternehmen XAIN, evan.network und CHAINSTEP entwickeln z.B. gemeinsam mit Marktpartnern seit Ende 2018 Applikationen für ein dezentrales Netzwerk für die Transportlogistik, basierend auf offenen Standards und dezentraler Governance.

Welche Schnittstellen oder sonstigen technischen und rechtlichen Voraussetzungen werden benötigt, um anbieterübergreifende Bezahlvorgänge zu ermöglichen?

Bitkom Stellungnahme:

Für anbieterübergreifende Bezahlvorgänge muss eine Interoperabilität zwischen den verschiedenen Blockchain-Lösungen geschaffen werden. Hierbei sind nicht die Schnittstellen das Problem, sondern die Nachvollziehbarkeit und Manipulationssicherheit von Transaktionen. Somit müsste ein Netzwerkteilnehmer gleichzeitig als Full Node für eine Blockchain-Lösung und als Light Node für alle kompatiblen Lösungen fungieren. Als Alternative kann eine Kontrollschicht auf Blockchain Basis geschaffen werden, welche die Interaktion zwischen den einzelnen Lösungen koordiniert. Hierdurch könnte eine Nachvollziehbarkeit aller Transaktionen gewährleistet werden. Wie dies im Detail aussehen könnte, bedarf allerdings noch weiterer Forschung.

Generell sollte auch Rechtssicherheit in Bezug auf Token als Zahlmittel geschaffen werden (u.a. Rechtssicherheit bzgl. Vertragstypus – Kaufvertrag/Tauschvertrag).

Anwendungsfeld f) Internet der Dinge

Internet der Dinge (Internet of Things/IoT): Die Verknüpfung von Blockchain mit dem Internet der Dinge birgt großes Innovationspotenzial. Beim Internet der Dinge steht die digitale Vernetzung physischer Objekte im Mittelpunkt, die dann die Grundlage für datenbasierte Dienstleistungen (Smart Services) bildet. Blockchain kann hier die authentische Kommunikation zwischen IoT-Geräten und die nachweisbare Übermittlung von Informationen ermöglichen. So kann man sich zum Beispiel im Bereich von Smart Homes Blockchain-basierte Kommunikation zwischen »smarten« Küchengeräten, Steckdosen und Schlössern in Türen oder Autos vorstellen. Weiterhin könnten industrielle Anlagen über Unternehmen und Wertschöpfungsprozesse Blockchain-basiert vernetzt werden. In Verbindung mit sogenannten Smart Contracts (digitale automatisierte »Verträge«) ist es denkbar, dass diese Anlagen selbstständig entgeltliche Leistungen erbringen, Wartungsbedarf melden und Rechnungen stellen.

Bitte geben Sie Ihre Stellungnahme zu dem Anwendungsfeld Internet der Dinge ein:

Bitkom Stellungnahme:

Laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) bewerten acht von zehn Unternehmen das Potenzial der Blockchain für ein Transaktionssystem für das Internet der Dinge als groß. Insbesondere drei Anwendungsszenarien scheinen hier besonders interessant: Digital Twin, Track & Trace Lösungen sowie Pay per Use Geschäftsmodelle. Dabei sind insbesondere die Themen Skalierbarkeit, Rechenkapazität, und Speicherkapazität beim Thema IoT entscheidend, um erfolgreiche Anwendungsfälle zu ermöglichen.

Die Blockchain bietet eine ideale Lösung, um IoT-Geräte zuverlässig zu verbinden und zu verwalten, insbesondere im B2B-Bereich. Dabei ist die Logistik eine der Hauptanwendungsdomäne für die Verknüpfung von Blockchain mit dem Internet der Dinge. Durch die unternehmensinterne oder unternehmensübergreifende Vernetzung von Ressourcen und Gütern, die ihre Zustände austauschen oder Interaktionen aushandeln, sind sichere Speicherorte notwendig, die die wertschöpfenden Tätigkeiten nachhalten. So können sich beispielsweise fahrerlose Transportsysteme mit anderen Produktionsanlagen zur Versorgung mit Bauteilen und Zwischenprodukten abstimmen.

Ein anderer Anwendungsfall zeigt sich in der automatischen Nachbestellung von Ersatzteilen.

Durch die Kombination von Blockchain und Smart Contracts mit dem Internet der Dinge lassen sich im Supply Chain Management Material-, Informations- und Finanzflüsse synchronisieren und automatisieren sowie zukünftig autonomisieren. DLTs werden aus M2M-Beziehungen nicht wegzudenken sein und stellen einen Integralen Bestandteil der dafür benötigten IT Infrastruktur dar.

In der kombinierten Verwendung von IoT-Infrastrukturen und Blockchains bestehen zwei Herausforderungen. Wenn man Daten manipulieren will, wäre es viel einfacher, die IoT Devices direkt anzugreifen, was gerade heute verhältnismäßig einfach ist. In diesem Fall hätte man in der Blockchain unveränderliche, aber an der Quelle manipulierte Daten. Zweitens stellt sich gerade in diesem Fall die Frage der Skalierbarkeit: IoT-Devices erzeugen massive Datenvolumina, welche noch exponentiell wachsen werden. Diese und weitere Fragestellungen sollten adressiert werden.

Welche Technologien haben ähnliche Funktionalitäten wie die Blockchain, um im Bereich IoT eingesetzt zu werden?

Bitkom Stellungnahme:

Schwierig, da jede Technologie eigene Vorteile/Nachteile mit sich bringt. Breit gefasst könnte man hier DAGs, Proprietäre Plattformen, Cloud-Dienste nennen.

Welche rechtlichen und technologischen Hindernisse gibt es beim Einsatz von Blockchains im Bereich IoT?

Bitkom Stellungnahme:

Rechtliche Hindernisse:

- Grundsätzlich vom Use Case abhängig, jedoch kann die Auslegung der DSVGO ein Hindernis sein.

Technologische Hindernisse:

- Skalierbarkeit.
- Benötigter Ressourcenbedarf von Blockchain/DAG Clients auf Embedded Devices.
- Wie werden die Daten vertrauensvoll in der realen Welt aufgenommen/gemessen, digitalisiert und dann den Prozessen auf der Blockchain zugeführt.
- Nachweis der sicheren Identität von Sensoren.
- Schaffung von Anreizen, um Gerätehersteller zum Offenlegen der Gerätedaten zu incentivieren.

Welche Herausforderungen bestehen hinsichtlich der Interoperabilität?

Bitkom Stellungnahme:

Der Abgleich der Inhalte unterschiedlicher Blockchain-Instanzen und die Verteilung der Inhalte zwischen diesen ist eine zentrale Herausforderung. Außerdem gibt es viele unterschiedliche Lösungen mit eigenen API's, die allerdings auf die gleichen Technologien zurückgreifen (Ethereum oder Bitcoin als Kerntechnologie). Diese API's müssten angeglichen und eine Menge an Funktionen sichergestellt werden, um eine Interoperabilität der einzelnen Technologien zu gewährleisten. Es müssen also passende Konzepte zur Cross-Chain Kommunikation entwickelt und umgesetzt werden. Diese Konzepte müssen Lösungen mit Intermediären und ohne Mittelmänner bieten, abhängig davon, ob ein Use Case eine starke Dezentralität benötigt oder nicht.

Sind Blockchains auf die großen Datenmengen im IoT-Bereich skalierbar? Falls ja, welche Varianten sind hierfür besonders geeignet?

Bitkom Stellungnahme:

Nach dem heutigen Stand der Technik bei Blockchains können große Datenmengen nur von permissionbased Blockchains verarbeitet werden, da die aufwändigen Mining-Mechanismen (Erlangen des Schreibrechtes) nicht durchgeführt werden müssen. Bisher gibt es noch keine Blockchains, die eine beliebige Skalierbarkeit zulassen. Die Transaktionen pro Sekunde konnten durch neue Konsensmechanismen wie dem Byzantine Fault Tolerance Consensus immens gesteigert werden, von <10 Transaktionen/Sekunde bei der ersten Bitcoin-Variante auf mittlerweile >3500 Transaktionen/Sekunde, dies reicht aber bei weitem nicht für ein vollumfängliches IoT aus. Denkbar wären hier kleinere Subnetze, die für bestimmte Bereiche eingerichtet werden und möglicherweise über Projekte wie den IDS (International Data Spaces) adressierbar sind.

Wie kann sichergestellt werden, dass der Übertrag von nicht automatisch digitalisierten IoT-Daten auf die Blockchain und in Smart Contracts fehlerfrei erfolgt?

Bitkom Stellungnahme:

Generell können in solchen Szenarien keine Garantien auf Fehlerfreiheit usw. gegeben werden. Anreizsysteme können hier unterstützen. Es können auch reputationsbasierte Konzepte genutzt werden um das Risiko zu minimieren. Generell bergen Medienbrüche in jeglicher Art von digitalen Prozessen ein Risiko.

Über Light Nodes können manuelle Eingaben, die zur Entscheidungsfindung von Smart Contracts herangezogen werden einem bestimmten Gerät/Unternehmen/Person zugeordnet werden. Bei Falschinformationen kann eineindeutig nachgewiesen werden, woher diese kommen und der verantwortliche Netzwerkpartner hierfür haftbar gemacht werden. Wichtig sind hierbei Mechanismen, die kausale und logische Zusammenhänge von Events überprüfen, dies könnte über die Einbindung von Artificial Intelligence (AI) erfolgen. Über selbstlernende Algorithmen könnten Abweichungen vom normalen Prozessablauf aufgezeigt werden.

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

Bitkom Stellungnahme:

Prinzipiell kommt es hier auf die Ausgestaltung der Blockchain-Lösung im konkreten Einzelfall an. Insofern sollte auf die Stellungnahme »Blockchain and the GDPR« des European union blockchain observatory & forum Bezug genommen werden. Allgemein ist die Speicherung der Daten außerhalb der BC zu empfehlen, »on-chain« sollten nur Hash-Werte gespeichert werden. Private Blockchain-Lösungen sind datenschutzrechtlich klar im Vorteil, da hier die Beteiligten bekannt sind, Datenschutzrechte adressiert werden können (da hier u.a. klar ist, wem gegenüber ein Auskunftsanspruch ausgeübt werden kann) und eingegrenzt werden kann, wo die Verarbeitung stattfindet (innerhalb/außerhalb der EU). Zudem kann hier durch Vereinbarung zwischen den Beteiligten besser festgelegt werden, wer Controller- bzw. Prozessorpflichten übernimmt, so dass Unklarheiten vermieden werden. Anwendungen zur Anonymisierung und Verschlüsselung werden zudem mit Hochdruck weiterentwickelt, so dass auch auf technischer Ebene Lösungen vorangetrieben werden.

Anwendungsfeld g) Identitäten-/Rechtemanagement (1/2)

Digitale Identitäten: Digitale Identitäten sind eine wichtige Grundlage für die digitale Vernetzung, denn sie ermöglichen Kommunikation, Datenaustausch und Transaktionen. Jeder Mensch

besitzt eine Vielzahl digitaler Identitäten, oftmals sind diese anwendungsabhängig, sodass für jede digitale Dienstleistung eine neue digitale Identität geschaffen werden muss. Die Blockchain-Technologie könnte hier eine Lösung ermöglichen. Digitale Identitäten auf Blockchain-Basis müssten datenschutzkonform ausgestaltet sein, sodass die Betroffenen in dem rechtlich vorgegebenen erforderlichen Umfang die Steuerung von Zugriffen vorbehalten und auch gewährleisten kann. Die jeweiligen Betroffenen müssen darüber hinaus einfach und transparent nachvollziehen können, wer wann auf diese Daten Zugriff hatte. Diese Ausgestaltung könnte dazu führen, dass Bürgerinnen und Bürger einen größeren Grad an informationeller Selbstbestimmung erhalten. Eine datenschutzrechtliche Herausforderung ist dabei jedoch insbesondere, dass aufgrund der kryptografischen Verkettung einmal in die Blockchain eingetragene Daten nicht mehr gelöscht werden können. Verschiedene Unternehmen und Verbünde arbeiten an einer solchen digitalen Identität, die vollständig unter der Kontrolle des Nutzers liegt und anwendungsunabhängig für alle Dienstleistungen genutzt werden kann. So soll eine sichere Kommunikation auf Basis von Blockchain-Technologie gewährleistet werden.

Bitte geben Sie Ihre Stellungnahme zu dem Themengebiet Digitale Identitäten ein:

Bitkom Stellungnahme:

Neben dem oben beschriebenen isolierten Identitätsmodel (jeder Service hat einen eigenen Identity Provider) gibt es weitere Identitätsmodelle, wie zentrales (mehrere Services haben einen Identitätsprovider) und nutzerzentriertes Identitätsmodell (Nutzer ist zugleich Provider seiner eigener Identität und ist für seine Identitätsdaten verantwortlich, er/sie entscheidet selbst, wer und für wie lange einen Zugriff zu seinen/ihren Daten haben darf). Die Blockchain-Technologie ermöglicht ein solches nutzerzentriertes Identitätsmodell. Dieses wird auch selbstverwaltete-Identität (Self-Sovereign-Identity) genannt.

So können die durch eine rechtsverbindliche Identifizierung erzeugten digitalen Identitäten in einer Blockchain (Private Permissioned aus Gründen des Datenschutzes sowie Nachweisbarkeit und Informationssicherheit) abgelegt werden. Der Nutzer kann diese dann basierend auf Smart Contracts regelbasiert freigeben, gleichzeitig wird die Integrität und, in Verbindung mit den TrustServices der eIDAS-Verordnung (Qualif. eSignatur, eSiegel) die Authentizität der Identitätsdaten gewährleistet. Die Herausforderung besteht dabei jedoch in der Gewährleistung der Vorgaben der DSGVO so insbesondere die Rechte des Betroffenen.

- Recht auf Auskunft (Art. 15) = Abruf der Daten,
- Recht auf Berichtigung (Art 16) = Veränderung der Daten,
- Recht auf Datenübertragbarkeit in einem strukturierten, gängigen, maschinenlesbaren Format (Art. 20) = Abruf der Daten aus der Blockchain,

- Recht auf Löschung bzw. Recht auf »Vergessenwerden« (Art. 17) = rückstandsloses, physisches Löschen.

Das Aufkommen Blockchain-basierter digitaler Identitäten könnte ein Anlass sein, in Deutschland Fortschritte hinsichtlich der Verbreitung und Nutzbarkeit solcher digitalen Identitäten zu erzielen, welche nicht unter der Kontrolle großer Plattformkonzerne stehen und welche die faktische Nutzung digitaler Identitäten in Lebensrealität der Bevölkerung derzeit dominieren. Es sind jedoch noch zahlreiche Fragen offen, etwa hinsichtlich der tatsächlichen Realisierbarkeit skalierbarer DSGVO- und eIDAS-konformer Blockchain-Identitätslösungen, dem praktikablen Schlüsselmanagement (Recovery, Revocation) bei gleichzeitiger Nichtverletzung von Blockchain-Grundprinzipien etc.

Die Blockchain Technologie und die damit verbundenen Möglichkeiten kann folglich als starker Aufhänger genutzt werden, um endlich eine Public-Key Infrastruktur aufzubauen, die für digitale Identitäten notwendig ist. Bisherige Lösungen (X.509, PGP, GPG) führen weiterhin nur ein Nischendasein, die Signaturfunktion des neuen Personalausweises wird (auch wegen der Kosten) kaum genutzt.

Welche Aufgaben kann bzw. sollte der Staat bei der Bereitstellung rechtssicherer digitaler Identitäten übernehmen?

Bitkom Stellungnahme:

Da eine digitale Identität aus mehreren Attributen besteht (Name, Adresse, Führerschein, Bildungszeugnisse, usw.) sollten diese ggf. von einer anerkannten Institution bestätigt werden. Die Änderungen an digitalen Identitäten, für die besondere Rechtssicherheit erforderlich ist (z.B. Wohnadresse), sollten zumindest anfangs vom Staat bestätigt werden – wie dies derzeit beim Meldeamt der Fall ist (analog dazu Digitale Identitäten an juristischen Personen). Mit fortschreitender Digitalisierung kann dies reduziert werden (digitale Mietverträge können z.B. dazu führen, dass Ummeldungen einfacher möglich werden).

Der Staat sollte weiterhin, wie auch in der eIDAS-Verordnung vorgesehen, die regulatorischen Rahmenbedingungen setzen, die Überwachung/Zertifizierung der Identitätsprovider und TrustServices und sonstiger Anbieter von Verfahren in denen eine sichere Identifizierung notwendig ist sowie die Notifizierung von eID-Mitteln übernehmen. Ebenso sollten Personalausweise, elektronische Aufenthaltstitel, Pässe etc. und hierauf basierende digitale Identitäten weiterhin staatlicherseits erzeugt werden. Ergo: Staatlicherseits sind Sicherheit und Rechtsverbindlichkeit digitaler Identitäten durch entsprechende Rahmenbedingungen und Überwachungsaufgaben zu gewährleisten.

Neben der Überwachung der Ausstellung und Verwaltung öffentlich überprüfbarer Identitäten kann der Staat ggf. Zertifikate bzw. Verifizierungen von öffentlichen Schlüsseln zur Verbin-

dung mit der natürlichen oder juristischen Person ausstellen. Auf internationaler Ebene kann er helfen internationale, rechtliche Rahmenbedingungen voranzubringen.

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

Bitkom Stellungnahme:

Auf dem Markt sind aktuell zahlreiche Self-Sovereign-Identity-Lösungen zu finden. Wichtig zu beachten ist, ob die zugrundeliegende Blockchain private oder public ist. Wenn private, dann sind die Rechtsbestimmungen des jeweiligen Landes, aus welchem die Lösung kommt, zu beachten. Zumeist werden nur Hashwerte der Identitätsattribute in der Blockchain protokolliert. Die Klartextdaten sind dann entweder beim Identitätsbesitzer und der jeweiligen Behörde gespeichert oder bei dem Identitätsbesitzer und aus Sicherheitsgründen verschlüsselt und verteilt auf mehrere Cloudspeicher (z.B. CloudRAID).

Derzeit können die Vorgaben der DSGVO bspw. durch die externe Speicherung der eigentlichen personenbezogenen Daten und reine Ablage von Hashwerten bzw. Verweisen in der Blockchain erreicht werden. Darüber hinaus wäre eine alternative Hashverkettung der Blöcke auf Basis von Merkle-Hashbäumen denkbar, bei denen äquivalent dem Verfahren nach RFC 4998/6283 (Vgl. auch DIN 31647, BSI TR-03125 TR-ESOR) der Hashbaum zwar die verhashten Datenobjekte absichert, jedoch ein Löschen der Objekte unabhängig von der Hashabsicherung möglich ist und der Hashbaum selbst weiterhin konsistent bleibt.

Prinzipiell kommt es auch hier auf die Ausgestaltung der Blockchain-Lösung im konkreten Einzelfall an. Insofern sollte auf die Stellungnahme »Blockchain and the GDPR« des European union blockchain observatory & forum Bezug genommen werden. Allgemein ist die Speicherung der Daten außerhalb der BC zu empfehlen, »on-chain« sollten nur Hash-Werte gespeichert werden. Private Blockchain-Lösungen sind datenschutzrechtlich klar im Vorteil, da hier die Beteiligten bekannt sind, Datenschutzrechte adressiert werden können (da hier u.a. klar ist, wem gegenüber ein Auskunftsanspruch ausgeübt werden kann) und eingegrenzt werden kann, wo die Verarbeitung stattfindet (innerhalb/außerhalb der EU).

Welche Akzeptanzkriterien sind bei dezentralem Identitätsmanagement durch Bürgerinnen, Bürger und Unternehmen zu berücksichtigen?

Bitkom Stellungnahme:

Neben den fundamentalen Datenschutzanforderungen (DSGVO etc.) ist insbesondere auch die einfache praktische Nutzbarkeit der digitalen Identitäten zu beachten. Hierbei ist der zweiseitige Markt zu berücksichtigen: Sie müssen sowohl für Bürgerinnen und Bürger einfach

nutzbar, als auch für Unternehmen (sowie öffentliche Verwaltungen) einfach in ihre Services einzubinden sein. Nur so lässt sich eine kritische Masse für beide Seiten erreichen. Zudem ist für beide Seiten ein klarer Mehrwert durch die Nutzung dezentraler Identitäten gegenüber des Status Quo herauszustellen. Sonst wird der Aufwand, welcher sich aus dem Wechsel ergibt (veränderte mentale Modelle, neues Interaktionsparadigma, ggf. Investitionen in neue Software/Hardware) diesen verhindern. Als Negativbeispiel muss hier leider der neue Personalausweis genannt werden.

Die grundsätzliche Usability von Blockchain-(Identitäts-)Lösungen gilt zu untersuchen und erfordert noch signifikanten Forschungs- und Entwicklungsaufwand: Inwiefern entsprechen Blockchain-Lösungen den mentalen Modellen von Endnutzern für die Bedienung von Softwaresystemen? In welchen Bereichen benötigen Nutzer gegebenenfalls Hilfestellungen? Existierende Anwendungsbeispiele für asymmetrische Verschlüsselungsverfahren, beispielsweise E-Mail Verschlüsselung, zeigen, dass diese Nutzer vor bedeutende Hürden stellen.

Als wesentliches Hindernis insbesondere in Unternehmen ist zudem die Rechts- und Informationssicherheit eines dezentralen Identitätsmanagements speziell im Kontext geltender europäischer Rechtsvorgaben wie der eIDAS zu nennen. Ebenso stellt sich die Frage der Standardisierung und der internationalen Übertragbarkeit. Wesentlich ist aus Privacy- und Nachweisgründen vor allem der Speicherort der Daten (Europa oder weltweit). Seitens des Bürgers sind Rechts- und Informationssicherheit ebenso zu nennen.

Wie kann ein eindeutiger, rechtssicherer Identitätsnachweis erfolgen und Missbrauch verhindert werden?

Bitkom Stellungnahme:

Insgesamt müssen die Vorgaben der DSGVO, der eIDAS-Verordnung, deren Implementing Acts sowie die nationalen Vorgaben und Standards zur sicheren Identifizierung (OZG, Meldegesetz, Verfügung des BMWi zu VideoIdent, Geldwäschegesetz etc.) sowie der rechtssichere Identitätsnachweis technologieunabhängig beachtet und umgesetzt werden.

Anwendungsfeld g) Identitäten-/Rechtemanagement (2/2)

Urheberrechte: Im »Internet der Informationen« ist es schwierig, das Urheberrecht wirksam durchzusetzen. Durch die Blockchain-Technologie könnte dies deutlich vereinfacht werden, da die Rückverfolgung von Transaktionen lückenlos möglich ist. Bei digitalen Gütern (Texte, Musik, Film, Software) geht es darum, Nutzungen in komplexen Verwertungsketten zu monetarisieren und Vergütungen fair und transparent zwischen allen Beteiligten (z.B. Komponisten, Musiker, Labels, Remixer) zu verteilen. Erste Ansätze gibt es beispielsweise bei frei zugänglichen, globalen Datenbanken für Musikrechte. Künstlerinnen und Künstler könnten damit u.U. auch ihre verwertungs-

und lizenzierungsrelevanten Informationen selbst verwalten und auf Intermediäre bei der Vermarktung ihrer Leistungen verzichten. Aber auch für klassische Intermediäre (Verlage, Labels, Verwertungsgesellschaften) weist die Blockchain-Technologie interessante Potenziale auf.

Bitte geben Sie Ihre Stellungnahme zu dem Themengebiet Urheberrechte ein:

Bitkom Stellungnahme:

Im Bereich Film/Software liegen alle erforderlichen Rechte zumeist in einer Hand, weshalb die Lizenzierung relativ unkompliziert ist. Hier wäre Blockchain wohl bahnbrechend für Nachvergütungsansprüche, weil der Nutzungsumfang transparent wird.

Im Bereich Musik sind die Rechte meist verstreut, weshalb die Lizenzierung aufwendig und langwierig ist. Hier wäre die Blockchain gepaart mit »smart contracts« schon bahnbrechend für die Lizenzierung, daneben für Nachvergütungsansprüche, weil der Nutzungsumfang transparent wird.

Gibt es konkrete Blockchain-basierte Lösungen im Bereich Urheberrecht?

Bitkom Stellungnahme:

Das Blockchain-basierte Register von Artory protokolliert beispielsweise die Herkunft von Kunst und Sammlerstücken. Weitere Beispiele sind:

- Peertracks (Musikstreamingdienst),
- Bittunes (Musikdownloads zum Kaufen),
- Dot blockchain music (Datenbank zu Urheber- und Leistungsschutzrechten an musikalischen Werken),
- Mediaocean (Blockchain für die digitale Lieferkette für Anzeigen),
- True Tickets (Konzertkarten).

Sind diese Lösungen den herkömmlichen Lösungen überlegen?

Bitkom Stellungnahme:

Für den Musikbereich ist die Unterscheidung zwischen Lizenzierung/Rechteverwaltung elementar:

Lizenzierung: Ja. Der Rechtehandel per Blockchain ist schneller und transparenter als herkömmliche Methoden.

Rechteverwaltung: Weniger. Von der Schöpfung eines Werks bis zum Auslaufen der Schutzfrist geschehen die meisten Änderungen »offline«, Blockchain ist also nicht wie bei Kryptowährung konstitutiv für die Rechteänderung, sondern kann nur aufzeichnen. Vorteile einer Blockchain kommen nicht zum Tragen, und für reine Aufzeichnung sind herkömmliche Datenbanken effizienter. Zudem bestehen hohe Hürden, bereits bestehende Werke in eine Blockchain-Datenbank zu übertragen.

Welche Geschäftsmodelle stehen hinter den Lösungen?

Bitkom Stellungnahme:

Ein Treiber ist beispielsweise die Vermeidung von Betrug mit Ersatzteilen.

Könnte die Blockchain-Technologie zu einer Neudefinition der Rolle der Urheberrechtsintermediäre führen?

Bitkom Stellungnahme:

Im Musikbereich zum Beispiel ist das denkbar. Theoretisch könnte ein Künstler die Verwertung selbst übernehmen, da durch die Blockchain die Lizenzierung schnell und einfach erfolgt (bislang sind Lizenzierung und Abrechnung aufwendig, weshalb praktisch nie einzelne Werke sondern immer ganze Repertoires lizenziert werden). Die Rechte müssten nicht mehr an Intermediäre abgegeben werden, sondern könnten vermehrt beim Künstler verbleiben und diesem eine größere Souveränität ermöglichen.

Anwendungsfeld h) Verwaltung

Die Blockchain-Technologie ist besonders dazu geeignet, Informationen zum Nachweis von Herkunft, Echtheit oder Rechten von und an Dokumenten oder Gütern zu verwalten. Außerdem können die Informationen effizient einem berechtigten Netzwerk zur Verfügung gestellt werden. Der Blockchain-Technologie kann damit eine Rolle zur Verschlankung und Digitalisierung von Verwaltungsprozessen zukommen. Soweit Informationen in staatlichen Registern gesammelt und vorgehalten werden, könnte die Technologie Potenziale für eine effiziente öffentliche Registerführung bieten. Dabei muss aber berücksichtigt werden, dass Register wie das Grundbuch

und das Handelsregister – anders als viele entsprechende ausländische Register – nicht nur der Sammlung von Informationen dienen, sondern vor allem einer inhaltlichen rechtlichen Prüfung durch eine staatliche Stelle, die über die Prüfung der Dokumentenechtheit weit hinausgeht (zum Beispiel Grundbuchamt und Registergericht). Diese rechtliche Prüfung kann durch Einsatz der Blockchain-Technologie nicht ersetzt werden. Weiter ist dabei zu berücksichtigen, dass Pflichten zur Entfernung von Eintragungen (zum Beispiel beim Bundeszentralregister) in einer irreversiblen Blockchain nicht ohne Weiteres umgesetzt werden können. Die Blockchain-Technologie könnte auch Potenziale für eine bürokratieärmere Verwaltung von Dokumenten (zum Beispiel Zeugnisse) und den Informationsaustausch von Behörden mit Privatpersonen und Unternehmen bieten. Beim Einsatz der Blockchain in Verwaltungsprozessen ist zudem zu beachten, dass die Ausübung von Ermessen letztlich durch einen menschlichen Entscheider erfolgen muss. Das Bundesamt für Migration und Flüchtlinge arbeitet im Asylprozess mit Blockchain mit einer Technologie, die behördenübergreifende Abläufe datensicher, transparent und effektiv strukturieren kann. Die Bundesdruckerei hat das Konzept einer Blockchain-ähnlichen Struktur entwickelt (sog. ID-Chain), mit der Verwaltungsprozesse modernisiert werden könnten. Pilotprojekte dieser Technologie sind angelaufen.

Auf europäischer Ebene ist die Bundesregierung in der Europäischen Blockchain-Partnerschaft vertreten. Diese strebt an, eine europäische öffentliche Blockchain-Services-Infrastruktur zu errichten, die länderübergreifend zur Bereitstellung bestimmter öffentlicher Dienstleistungen genutzt werden kann.

Bitte geben Sie Ihre Stellungnahme zu dem Anwendungsfeld Verwaltung ein:

Bitkom Stellungnahme:

Die Blockchain-Technologie als dezentrales System ist sehr gut geeignet, um Daten, die aufgrund der Funktionstrennung bei einzelnen Behörden und nicht in großen zentralen Töpfen gespeichert werden sollen, nachprüfbar auf Anforderung anderen Behörden zur Verfügung zu stellen. Die Daten werden dabei nicht in der Blockchain gespeichert, aber über selbige abgesichert und der Ursprungszustand nachweisbar gemacht.

Insgesamt sollte hier seitens der Bundesregierung auch ausgeführt werden, wie Deutschland sich im Rahmen der Europäischen Blockchain-Partnerschaft zu positionieren gedenkt. Insgesamt sollte die die öffentliche Hand als ein Hauptabnehmer von IT und vor dem Hintergrund der Digitalisierungspläne der Verwaltung proaktiv für Blockchain-Projekte in der Verwaltung einsetzen, um Potentiale zu testen, und als »Leuchtturm-Sektor« Blockchain-Lösungen in Deutschland zu fördern (bspw. im Registerwesen).

Gewisse Prüfungsaufgaben können nicht über eine Blockchain abgebildet werden (z.B. die Verpflichtung des Notars zur unabhängigen Beratung). Allerdings können Teilprozesse (z.B. Umschreibung nach digitaler Ausstellung der Unbedenklichkeitsbescheinigung durch das

Finanzamt) automatisiert werden. Durch eine Abwicklung über eine Blockchain wird das Verfahren transparenter (z.B. auch der Verfahrenstand). Dies führt zu weniger Rückfragen. Hoheitliche Aufgaben würden einer stärkeren Transparenz und öffentlichen Kontrolle unterliegen.

Die bestehende Trennung zwischen statischen Registerdaten und parallelen Transaktionen bspw. Grundstücksverkäufe, Änderung von Firmenstandorten, Gewerbe/Kfzan-/ab-/ummeldungen, Kfz-Verkäufe, Testamentsabwicklungen etc. könnte aufgehoben und die Transaktionen inkl. Änderung der Registerdaten durch SmartContracts auf Blockchainbasis vollständig im bestehenden Register abgebildet werden. Ähnliches gilt für Transaktionen, die mehrere Registerverfahren betreffen (z.B. Gewerbean-/ab-/ummeldungen oder Überwachung von Umweltzonen, Abbildung von Lebenslagen wie Umzügen, Geburten etc., die mehrere Verwaltungsprozesse implizieren wie Geburtsurkunde, Kita-Platz, Kindergeld etc). In allen Fällen ergibt die Kombination aus Blockchain mit den eID-Mitteln und TrustServices der eIDAS-Verordnung (sichere Authentifizierung, Rechtsverbindlichkeit des Vertrags/Bescheids inkl. Echtheit und Nachweisfähigkeit, sichere wie nachweisfähige Archivierung) umfassendes wie dispruptives Potenzial zur Vereinfachung und vollständigen wie vertrauenswürdigen Digitalisierung von Verwaltungsprozessen – insbesondere in Verbindung mit den Ausführungen zu SelfSovereignIdentity (vgl. Anwendungsfeld g).

In Europa gehört Estland (»e-Estonia«) zu den Vorreitern. Bereits seit 1999 arbeitet das estnische Kabinett papierlos. Seit Entstehung der Technologie im Jahr 2008 experimentiert die estnische Regierung mit der Blockchain. Seit 2012 ist die Blockchain bereits in vielen Registern Estlands, so im Gesundheitswesen, im parlamentarischen Raum, in der Justiz und im Bereich der Sicherheitsbehörden, eingeführt.

Welchen Mehrwert und welche Nachteile bietet eine verteilte Datenbank bei öffentlichen Registern?

Bitkom Stellungnahme:

Vorteile:

Ein Mehrwert besteht gerade bei Registern, bei denen es um die Gesamtheit der Einträge geht und ein Löschungsanspruch nicht besteht (z.B. Grundbuch). Blockchain bietet wie beschrieben vier herausragende Eigenschaften: die Unveränderlichkeit, der Konsensus (alle spielen aufgrund der einprogrammierten Abläufe nach denselben Regeln, deren Einhaltung von den Teilnehmern verifiziert wird), die chronologische Historiendokumentation durch das ausschließliche Anhängen von Blöcken sowie die Finalität einer Transaktion, welches auch bedeutet, dass die Teilnehmer implizit vereinbaren, die Ergebnisse der Blockchaintransaktion anzuerkennen. Diese Eigenschaften sind alle bei öffentlichen Registern wichtig, um als vertrauenswürdig anerkannt zu werden. Zudem sind die Transparenz des Verfahrensstandes, sowie die Vermeidung von Redundanz in der Datenhaltung Vorteile.

Nachteile:

Die Automation und die gemeinsamen Regeln bei einer Blockchain-Anwendung benötigen harmonisierte Standards, welche ggf. erarbeitet werden müssen und ggf. dem Föderalismus entgegenlaufen.

Welchen Grad an Zentralisierung braucht eine von der öffentlichen Verwaltung eingesetzte Datenbank?

Bitkom Stellungnahme:

Aufgrund der erforderlichen Governance und spezifischer rechtlicher Rahmenbedingungen für Verwaltungsakte je Land scheint eine Bundes- oder besser EU-betriebene Blockchain am geeignetsten. Es benötigt eine zentrale Governance und Transparenz über die Regeln und deren Einhaltung.

Allein zur Gewährleistung des Datenschutzes gem. GDPR sind Datenowner und (Auftrags-) Datenverarbeiter eindeutig bestimmbar zu halten. Insofern erscheint der Betrieb eines blockchainbasierten IT-Dienstes nur durch ein entsprechendes öffentliches/privates Rechenzentrum denkbar, in dem Betreiber und Datenowner klar identifizierbar sind. Gleiches ist notwendig, um etwaige Haftungsansprüche etc. geltend zu machen, bis hin zu Fragen nach Finanzierung/Kosten/Weiterentwicklung etc. der eingesetzten Lösung auf Basis von Blockchaintechnologie.

Welchen Grad an Zentralisierung braucht eine von der öffentlichen Verwaltung eingesetzte Datenbank?

Bitkom Stellungnahme:

Verwaltungsvorgänge, die heute mittels Dokumentenvorlage (papier-basiert) erfolgen, und mehrere beteiligte Behörden (z.B. beim Zusammenwirken im Rahmen eines Verwaltungsaktes) umfassen, können Blockchain-basiert effizienter und fälschungssicher abgewickelt werden. Weitere Beispiele:

- Prozesse die in einem Register enden (z.B. Grundbuch, Unternehmensregister, Vereinsregister) und bei denen der Prozessablauf für die Beteiligten interessant ist.
- Alle Prozesse (Anträge, etc.) bei denen der Bürger ein Interesse am Ergebnis hat (z.B. KFZ-Zulassung, Führerschein, Baugenehmigungen, etc.).
- Interne Behördenprozesse die ausschließlich der Transparenz über die Arbeit der Verwaltung dienen.

- Anwendungen in Verbindung mit den eIDAS-Werkzeugen (digitale Identitäten, eID-Mittel, Trustservices).

Welche Restriktionen ergeben sich bei der Anwendung von Smart Contracts im Hinblick auf die automatisierte Entscheidung rechtsverbindlicher Verwaltungsakte?

Bitkom Stellungnahme:

SmartContracts prüfen im Grunde genommen automatisiert zuvor definierte Eigenschaften ab und lösen auf dieser Basis Transaktionen aus. Der Bescheid wiederum kann als gesiegeltes Dokument (Auslösung des Siegels durch SmartContracts) weiterhin per eDelivery-Services gem. eIDAS zugestellt werden. Die Blockchain-Technologie fungiert hier aus Basisinfrastruktur. Die Rechtsverbindlichkeit wird durch die TrustServices der eIDAS gewährleistet. Die Restriktion besteht in der Frage, inwieweit eine menschliche Prüfung bestimmter Sachverhalte vor Bescheiderstellung und -versendung gesetzlich determiniert ist. Die Korrektur von fehlerhaften Smart Contracts mit Schwachstellen sind eine Hürde, für die entsprechende Lösungen gefunden werden müssen.

Schließt der Rechtsrahmen einen Einsatz in bestimmten Anwendungsbereichen derzeit aus?

Bitkom Stellungnahme:

Die Erfordernisse DSVGO und ggf. andere Aspekte im Datenschutz/Geheimschutz sind hinsichtlich einer Anwendung für Blockchain zu prüfen und mit entsprechenden Empfehlungen/Richtlinien zur Umsetzung zu versehen.

Ergeben sich neue strategische Überlegungen bei der IT-Konsolidierung öffentlicher Netze?

Bitkom Stellungnahme:

Ja, mittelfristig ergibt sich der Austausch von Informationen der einzelnen Behörden über Systemgrenzen hinweg. Langfristig ergeben sich einheitlichere Systeme.

Welche Governance-Aspekte sind bei internationalen Blockchain-Anwendungen mit öffentlicher Beteiligung zu beachten?

Bitkom Stellungnahme:

Hier sind neben Fragen der Interoperabilität auch verschiedene Rechtssysteme zu beachten und Regelungen zu treffen, nach welchen Regeln im grenzüberschreitenden Verwaltungsverfahren vorgegangen wird. ISO/TC 307 arbeitet gerade an einem Vorstandard für »legally binding smart contracts«, welche Datenmodelle und Sorgfaltspflichten von Programmierern als Checkliste an die Hand geben möchte, um auch bei internationalen (privatrechtlichen) Abläufen in verschiedenen Rechtssystemen die erforderlichen Aspekte abprüfbar zu machen.

Wesentlich ist vor allem der Speicherort der Daten. Hier ist zu prüfen, dass sich die Daten mindestens in Europa befinden (DSGVO). Ebenso ist zu prüfen, inwieweit eine Speicherung hoheitlicher Daten außerhalb Deutschlands rechtlich möglich ist. Diese Fragen sind jedoch grundsätzlich unabhängig von der Blockchain-Technologie.

Anwendungsfeld i) Plattformökonomie

Auf Basis Blockchain-basierter Systeme des Identitätsmanagements könnte möglicherweise ein Informations- und Wertetransfer beispielsweise zwischen Konsumenten oder zwischen Konsumenten und Unternehmen effizient ausgestaltet werden, ohne dass ein Intermediär eingeschaltet wird. Das wäre insbesondere im Bereich der Sharing Economy relevant, bei der gegenwärtig digitale Plattformen als Intermediäre eine zentrale Rolle spielen und eine erhebliche Marktmacht aufbauen können. Diese Marktmacht entsteht letztlich aufgrund von Netzwerkeffekten, die zu einer Konzentration von Nutzerdaten beim Plattformanbieter führen. Blockchain-basierte Alternativen können möglicherweise auch ein Beitrag sein, um der marktbeherrschenden Stellung einzelner Anbieter entgegenzuwirken. Ökonomisch kann dies aber nur funktionieren, wenn der Nutzer in dem Blockchain-basierten Gegenstück zur klassischen Plattform tatsächlich die Souveränität über seine Daten behält. Hier besteht daher ein enger Zusammenhang zu der Frage digitaler Identitäten (self-sovereign identities, SSID).

Bitte geben Sie Ihre Stellungnahme zu dem Anwendungsfeld Plattformökonomie ein:

Bitkom Stellungnahme:

Das ist in Teilen so richtig, viele heutige zentrale und datensammelnde Plattformen bieten aber auch zusätzlich noch Mehrwerte für den Endkunden und sind ggf. nicht einfach durch Code ersetzbar. Es möchte auch nicht jeder Verbraucher eine große Fertigungstiefe selber ausführen – da wird es sicherlich Verschiebungen geben; ob es auch Verhaltensänderungen geben wird, wird von den Mehrwerten für die an der Plattform beteiligten Parteien abhängen.

Aus Verbrauchersicht kann durch DLT mehr Kontrolle über die digitale Identität und die Möglichkeit granularer Zugriffsregelungen für personenbezogene Daten (Personal Information Management System auf Blockchain Basis) gewährt werden. In Verbindung mit dezentralen Infrastrukturen für den vertrauenswürdigen unternehmensübergreifenden Datenaustausch (wie dem Industrial Data Space) ein vielversprechendes Anwendungsfeld für Blockchain. Blockchain kann, sofern richtig und sinnvoll eingesetzt, rein »Gatekeeper-Funktionen« zurückdrängen und den Nutzern die Hoheit über ihre Daten geben. Im B2B-Umfeld können hierdurch Kollaborations-Modelle aufgesetzt werden, ohne dass man sich in Abhängigkeit begibt und ohne dass man anderen vertrauen muss.

Welche Anreizstrukturen bestehen, um eine Blockchain-basierte Plattformlösung aufzubauen? Kommt mit Blick auf die erforderliche Dezentralität und Datensouveränität letztlich nur eine öffentliche Blockchain in Frage oder sind auch private Blockchains denkbar?

Bitkom Stellungnahme:

Damit peer-to-peer wirklich funktionieren kann und auch das Vertrauen begründet, welches heute oft über Intermediäre zustandekommt, sind Identitäten sowie eine funktionierende Governance-Struktur Dreh- und Angelpunkt. Im Zweifelsfall muss die Gegenpartei ermittelbar sein und zur Verantwortung gezogen werden können. Derzeit arbeiten öffentliche Blockchains oft noch mit nicht identifizierbaren Nutzern und/oder unklaren Governance-Strukturen, sodass private/permissioned Blockchain-Implementierungen nach derzeitigem Stand geeigneter sind.

Die privaten Blockchains erleichtern vielen Unternehmen auch den Zugang zur Blockchain-Technologie. Nach einem damit (hoffentlich) einhergehenden Paradigmenwechsel zu mehr Vertrauen und Transparenz entlang von Supply Chains kommen dann zukünftig auch mehr und mehr öffentliche Blockchains in Frage (evolutionäre Entwicklung von privaten zu öffentlichen Blockchains).

Trotzdem muss hier sichergestellt werden, dass private (permissioned) Blockchains im Endeffekt nicht einen ähnlichen Lock-In Effekt wie aktuelle proprietäre Plattformen haben. Die Technologie, trotz zahlreicher Anreize wie Transparenz, Automatisierung, Cybersicherheit, Dezentralität muss sich noch stärker von bisherigen dezentralen Lösungen abgrenzen.

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

Bitkom Stellungnahme:

Prinzipiell kommt es hier auf die Ausgestaltung der Blockchain-Lösung im konkreten Einzelfall an. Insofern sollte auf die Stellungnahme »Blockchain and the GDPR« des European union blockchain observatory & forum Bezug genommen werden. Allgemein ist die Speicherung der Daten außerhalb der BC zu empfehlen, »on-chain« sollten nur Hash-Werte gespeichert werden. Private und public permissioned Blockchain-Lösungen sind datenschutzrechtlich klar im Vorteil, da hier die Beteiligten bekannt sind, Datenschutzrechte adressiert werden können (da hier u.a. klar ist, wem gegenüber ein Auskunftsanspruch ausgeübt werden kann) und eingegrenzt werden kann, wo die Verarbeitung stattfindet (innerhalb/außerhalb der EU). Zudem kann hier durch Vereinbarung zwischen den Beteiligten besser festgelegt werden, wer Controller- bzw. Prozessorpflichten übernimmt, so dass Unklarheiten vermieden werden. Anwendungen zur Anonymisierung und Verschlüsselung werden zudem mit Hochdruck weiterentwickelt, so dass auch auf technischer Ebene Lösungen vorangetrieben werden.

Welches Geschäfts- bzw. Betreibermodell sollte hinter einer Blockchain-basierten Plattformlösung stehen?

Bitkom Stellungnahme:

Es gibt keine One-Size-Fits-All Lösung, es kommt auf den Anwendungsfall an. Ein transparentes und klar beschriebenes Modell mit klarer Governancestruktur ist in jedem Fall wesentlich. Geschäfts- bzw. Betreibermodelle sollten auf jeden Fall der Coopetition-Logik folgen.

Welche Rolle spielt Blockchain für den Aufbau von digitalen Genossenschaften (»platform cooperatives«)?

Bitkom Stellungnahme:

In immer mehr Branchen wird an verschiedenen Möglichkeiten von »platform cooperatives« gearbeitet. Wir gehen davon aus, dass immer mehr eher Teile von »Branchen-Infrastrukturen« durch derartige Konzepte zur Verfügung gestellt werden. Hierbei wird die dezentrale Governance (s.o.) eine entscheidende Rolle spielen.

3 Zentrale Fragestellungen der Blockchain-Technologie

3 Zentrale Fragestellungen der Blockchain-Technologie

3.1 Technologische Herausforderungen

Die bislang junge Blockchain-Technologie steht weiterhin vor grundlegenden technologischen Herausforderungen. Denn wie jede Technologie haben auch Blockchain-Lösungen einige Nachteile. Viele dieser Herausforderungen können adressiert werden. Über die Grundlagenforschung und anwendungsbezogene Pilotprojekte sollte untersucht werden, welche Vor- und Nachteile eine Blockchain-Lösung gegenüber anderen Technologien und Datenbanksystemen bieten kann. Dies betrifft nicht nur die Blockchain an sich, sondern auch die unterschiedlichen Komponenten und Konzepte, aus denen eine konkrete Blockchain wie in einem Baukasten zusammengesetzt werden kann.

Bitte geben Sie Ihre Stellungnahme zur Technologischen Herausforderung der Blockchain-Technologie ein:

Bitkom Stellungnahme:

An den Blockchain-Implementierungen und ihren Funktionalitäten wird derzeit immer noch sehr dynamisch gearbeitet. Eine Lösung, welche auf Blockchain-Technologie implementiert wird, diese Funktionalität aber nicht wirklich benötigt, wird am Markt nicht lange bestehen, da der dezentrale Charakter mit den Abstimmungsprozessen aufwändiger ist als bei einer zentralen Lösung.

In der geplanten Blockchain-Strategie sollte der Einsatz von Reallaboren, Testfeldern und Modellversuchen unterstützt und ausgeweitet werden, um die Erprobung neuer Technologien, die öffentliche Vergabe und neue Geschäftsmodelle in der Praxis mit geringerem Risiko zu ermöglichen und dadurch den praxistauglichen Anpassungsbedarf im Ordnungsrahmen abzuleiten.

Die technologischen Herausforderungen sind im Vergleich zu den prozessualen Herausforderungen dabei meist leichter zu lösen. Die Implementierung scheitert in der Regel nicht an den technologischen Problemen, sondern daran, dass kein Ansatzpunkt für ein Implementierungsprojekt gefunden wird (bspw. wer übernimmt die Führung in einem multilateralen Projekt).

Technologische Herausforderungen a) Skalierbarkeit

Öffentliche Blockchains: Transaktionen müssen von Minern sequentiell verarbeitet werden. Damit ist die maximale Anzahl der Transaktionen pro Minute endlich. Zusätzlich wird aus Gründen der Sicherheit die maximale Anzahl neuer Blöcke pro Zeiteinheit meist limitiert,

wodurch ein »Datenstau« entstehen kann, wenn viele Transaktionen gleichzeitig abgewickelt werden müssen. Es existiert eine Vielzahl an Vorschlägen, um das Problem der Skalierbarkeit in Blockchain-Systemen beispielsweise durch andere Blockgrößen oder andere Governance-Strukturen zu lösen. Diese sind aber immer auch mit einem Trade-off verbunden.

Private Blockchains: Sie sind in deutlich geringerem Umfang mit dem Problem der Skalierbarkeit konfrontiert, da ein Mining nicht erforderlich ist, sondern neue Einträge durch zentralisiertere Instanzen in die Datenbank erfolgen können. Dies geht jedoch zu Lasten der Dezentralität – einer wesentlichen Funktionalität der Blockchain-Technologie

Bitte geben Sie Ihre Stellungnahme zu der Herausforderung der Skalierbarkeit ein:

Bitkom Stellungnahme:

Laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) sehen 50 % der Unternehmen, die Blockchain im Einsatz haben, die fehlende Performance und Skalierbarkeit als Problem.

Private Blockchain:

Private bzw. permissioned Blockchains haben keine Datenbank, sie haben ebenfalls verkettete Blöcke, die auch nicht »zentralisierter« gebildet werden. Da mit Identitäten gearbeitet wird, ist der Schutz der Teilnehmer vor sich unbemerkt bildenden und potentiell inhaltsverändernden Mehrheiten bei den Minern (sog. 51% Attacke) schlichtweg nicht nötig. Die Teilnehmer selber haben nachvollziehbare Regeln und Abstimmungsprozesse und legen fest, wie viele Teilnehmer eine Transaktion bestätigen müssen, damit sie als gültig validiert anerkannt wird. Bei ggf. maliziös arbeitenden Teilnehmern kann dies aufgrund der Identität nachgewiesen werden und durch die anderen Teilnehmer zur Rechenschaft herangezogen werden. Die Dezentralität, sprich Ausfallsicherheit durch Redundanz der verteilten Daten und Kommunikationsstrukturen unter den Teilnehmern ist ebenfalls gegeben.

Öffentliche Blockchain:

Durch die Datenstruktur der Blockchain-Technologie und der damit verbundenen Speicherung der Transaktionen in einer gemeinsamen Kette an Blöcken, ist der schreibende Zugriff auf die Blockchain exklusiv. Auch wenn es bisher schon unterschiedliche Verbesserungen der Schreibmechanismen gab, so kann damit nur die Geschwindigkeit erhöht, aber bisher keine echte Skalierbarkeit hergestellt werden.

Wichtig ist zu beachten, dass die Dezentralität der Blockchain-Technologie direkt mit der Sicherheit der darauf basierenden Lösung verbunden ist. Ebenso wie eine festgelegte Größe

der Blöcke und die Block-Erstellungszeit. Diese Parameter dienen der Sicherheit des Blockchain-basierten Systems. Mehrere Lösungen des Skalierbarkeitsproblems der Blockchain-Technologie werden aktuell erprobt (Sharding, plasma, casper, SegWit, usw.).

Abgesehen vom Konsensmechanismus Proof of Work gibt es den Proof of Stake und es wird noch an weiteren Verfahren geforscht, die deutlich besser zu skalieren sind – und muss weiterhin geforscht werden, z.B. Proof of time. Kombinierte Modelle (auch zwischen privaten und öffentlichen Blockchains) sind dabei erfolgsversprechend.

Welche Lösungsansätze für das Skalierbarkeitsproblem von (öffentlichen) Blockchains sind erfolgversprechend?

Bitkom Stellungnahme:

Eine Lösung könnte die Aufteilung der Blockchain in mehrere Bereiche sein, die jeweils nur mit einer Untermenge des Blockchain-Netzwerkes geteilt werden, sodass paralleles Schreiben in diese verschiedenen Bereiche möglich wird. Zu beachten ist hierbei allerdings, dass die Datensicherheit weiterhin gewahrt bleiben muss. Aktuell werden diese einzelnen Bereiche über zusätzliche Mechanismen abgesichert (Hashchain, die Datenchains absichert), was eine echte Skalierbarkeit allerdings wieder verhindert und nur den Durchsatz erhöht. Es gibt durchaus Distributed Ledger Technologien (z.B. Corda) die sich mit diesem Thema beschäftigen und gute Ansätze haben, allerdings ist dies bei der Blockchain-Technologie ungleich schwerer durch die Verkettung.

Die Parallelisierung von Transaktionen oder ganzen Anwendungen (mit Hinblick auf Interoperabilität) ist aber ein erfolgsversprechender Ansatz. Außerdem sind auch höhere Protokoll-Ebenen (Layer 2, etc.) neben den Netzwerk-Segmentierungen erfolgsversprechend.

Inwiefern kann den Herausforderungen der Skalierbarkeit durch Interoperabilität von Blockchains begegnet werden?

Bitkom Stellungnahme:

Durch eine Interoperabilität der Blockchains könnten wiederum verschiedene Bereiche geschaffen werden, die gleichzeitige Schreibzugriffe ermöglichen. Dadurch ließe sich die Skalierbarkeit der Blockchain schaffen, ob dies allerdings durch die Interoperabilität von unterschiedlichen Blockchain-Lösungen geschieht oder das Mehrfachinstanziieren der gleichen, spielt für die Skalierbarkeit keine Rolle. Die Interoperabilität ist wichtig im Hinblick auf die vielen unterschiedlichen Lösungen, um deren Vor- und Nachteile optimal nutzen zu können.

Es können wie gesagt Themen-spezifische Chains aufgesetzt werden und der dadurch entstehende Fokus auf die Abarbeitung spezifischer Tasks trägt zu einer parallelen Abarbeitung bei.

Diese müssen dann natürlich durch eine übergeordnete Instanz »überwacht« werden. Polkadot ist eine der möglichen Antworten auf diese Frage.

Die Parallelisierung von anwendungsspezifischen Blockchains, die entsprechend ihrer Spezialisierung Transaktionen/Daten verarbeiten, ist somit entscheidend. Vorangehende und anschließende Verarbeitungsprozesse, die andere technologische Anforderungen haben, können auf weitere, dafür spezialisierte Blockchains ausgelagert werden.

Welche Hindernisse (technisch und verfahrensrechtlich) müssen zur Skalierung von bestehenden bzw. potenziellen Pilotprojekten überwunden werden?

Bitkom Stellungnahme:

Die Herausforderung der Lastskalierbarkeit der Blockchain Technologie, in Bezug auf die Menge an Transaktionen, die pro Sekunde verarbeitet werden können, kann auch Auswirkungen auf die Skalierbarkeit von Projekten haben. Dies hängt in erster Linie vom Anwendungsfall ab. Für die meisten Projekte sind die aktuell möglichen rund 1.500 Transaktionen pro Sekunde ausreichend. Aktuell forscht das Fraunhofer-Institut an der Lösung dieser Herausforderung, insbesondere über die Parallelisierung von Blockchain-Instanzen und die Interoperabilität unterschiedlicher Blockchain-Lösungen. Als weitere Herausforderung ist noch die fehlende Auswertungsmöglichkeit der gespeicherten Daten zu nennen. Bei aktuellen Blockchain-Lösungen werden bereits Möglichkeiten zur Strukturierung und Suche von Daten angeboten und weiter verbessert. Eine Lösung dieser Herausforderung ist also zeitnah zu erwarten.

Technologische Herausforderungen b) Ineffizienz durch Redundanz

In einem Blockchain-Netzwerk werden die Daten auf allen Rechnern der Teilnehmer gespeichert. Diese Redundanz ist notwendige Voraussetzung für die Idee der Blockchain, verbraucht aber ein Vielfaches an Speicherkapazitäten und Energie im Vergleich zu zentralisierten Datenbanken. Die Ineffizienz kann durch die Einschränkung der Redundanz und Vollständigkeit adressiert werden. So gibt es verschiedene Ansätze, nicht die vollständige Kette bei allen Teilnehmern abzuspeichern, sondern nur notwendige Ausschnitte. Auch hier muss Erfahrung gesammelt werden, welche Auswirkungen dies auf Konsistenz und Sicherheit hat.

Bitte geben Sie Ihre Stellungnahme zu der Herausforderung der Ineffizienz durch Redundanz ein:

Bitkom Stellungnahme:

Dezentral bedeutet verteilte, mehrfach vorhandene Datenbestände. Dies ist gegenüber der zentralen Datenhaltung nicht ineffizient, da zentrale Datenbanken einen zentralen Administrator haben, dem alle Teilnehmer vertrauen müssen. Dezentrale Datenbestände sind unabhängiger und somit widerstandsfähiger gegenüber Ausfällen von Komponenten im Netzwerk. Diese Resilienz ist ebenfalls eine Idee, welche die Blockchain-Implementierungen verfolgen.

Die Redundanz kann demnach auch positiv bewertet werden. Ähnlich wie bei Cloud-Speichern kann durch die Redundanz die Datensicherung verbessert werden. Somit werden für die einzelnen Unternehmen die Backup-Prozesse einfacher. Ein großer Vorteil ist hierbei, dass das Auseinanderlaufen von Datenständen, das noch ein großes Problem bei Datenbanken ist, verhindert wird und jeder Teilnehmer die gleichen und aktuellen Daten vorliegen hat. Außerdem ist Speicherplatz heutzutage sehr günstig.

Der Segmentierung von Daten wird nichtsdestotrotz eine entscheidende Rolle zukommen, es wird dauerhaft schwierig sein, jegliche Blockchain bei allen Teilnehmern 100% präsent zu halten. Allerdings erfordert dies eine Koordination, sodass zumindest immer eine mindestens erforderliche Redundanz gegeben ist (Monetäre Incentivierung oder gesetzliche Auflage.

In welchem Maße konkurriert die Blockchain mit anderen Datenbanklösungen?

Bitkom Stellungnahme:

Datenbanken erfüllen einen anderen Zweck als Blockchains. Blockchains verteilen Daten und speichern diese manipulationssicher ab, insbesondere werden Server miteinander vernetzt. Datenbanken dagegen dienen in erster Linie zur Verknüpfung und Auswertung von Daten (Big Data, relationale Datenhaltung). Somit ist die Blockchain-Technologie komplementär oder adressiert Anwendungsfälle, die mit klassischen Datenbanken nicht abbildbar sind. Blockchain findet nachhaltig nur dann ein Einsatzgebiet über die PoC-Phase hinaus, wenn Mehrwerte gegenüber der Datenbank nachweislich sind.

Der Anwendungsfall für Blockchain ist ausschließlich in Szenarien, in denen eine architektonische Dezentralisierung bei gleichzeitiger organisatorischer Dezentralisierung gegeben ist. Dies sind Rahmenbedingungen, die klassische Datenbanktechnologien nicht abdecken können. Für die Fälle 1) architektonisch zentral, organisatorisch zentral; und 2) architektonisch dezentral, organisatorisch zentral sind Datenbanken die bessere Lösung.

In welchen Szenarien überwiegen die Vorteile der redundanten Datenspeicherung die Nachteile?

Bitkom Stellungnahme:

Die redundante Datenspeicherung dient dem Informationsaustausch, wenn mehrere Parteien eine Geschäftsbeziehung unterhalten. Insbesondere wenn der Informationsaustausch über Unternehmensgrenzen hinaus erfolgen soll, kann die Blockchain das hierfür nötige Vertrauen schaffen. Im Gegensatz zu traditionellen Datenbanksystemen kann über die Redundanz der Blockchain ein auseinanderlaufen der Datenbasis verhindert werden.

Die redundante Datenspeicherung ist eine Kerneigenschaft der Blockchain. Dies trägt zur Resilienz und Fälschungssicherheit des Gesamtsystems bei. Der damit einhergehende erhöhte Ressourcenverbrauch ist daher unter Umständen gerechtfertigt. Insbesondere für Anwendungen aus dem Bereich der kritischen Infrastruktur (Energie- und Wasserversorgung, medizinischer Bereich) überwiegen die Vorteile deutlich, weil zentrale Angriffspunkte wegfallen.

Kryptowährungen profitieren außerdem durch die geringen Speicheranforderungen einzelner Transaktionen von der erhöhten Sicherheit bei redundanter Datenspeicherung.

Welche Lösungsansätze für das Redundanzproblem von Blockchains sind erfolgversprechend?

Bitkom Stellungnahme:

Viele permissioned-Blockchain-Lösungen gehen bereits dazu über, die Redundanz der Datenspeicherung zu verringern. Dabei werden innerhalb von Blockchain-Netzwerken unterschiedliche Bereiche geschaffen, die über eigene Berechtigungskonzepte verfügen. So müssen diese Bereiche nur noch mit Servern redundant persistiert werden, die auch auf diese Daten zugreifen sollen.

Light Clients bieten außerdem die Möglichkeit, sicher und dezentralisiert mit der Blockchain zu kommunizieren, ohne dabei auf den als Intermediären eingesetzten Full Nodes vertrauen zu müssen. Dies kann zum Beispiel durch die Verwendung der normalerweise im Header vorhandenen Merkle Tree Root erreicht werden.

Lösungsansätze wie der Betrieb weniger Full-Nodes und vieler Light-Nodes ist eine Option zur Reduktion des Ressourcenaufwands. Hier ist jedoch darauf zu achten, dass ein solcher Ansatz das Gesamtsystem ein Stück weit zentralisiert und somit die eigentlichen Stärken der Blockchain relativiert werden. Kompensiert werden könnte diese Relativierung durch Nutzung sicherer Systeme, wie z.B. die im Aufbau befindliche Smart Metering Infrastruktur. Auf den vielen Tausend Smart Meter Gateways im Feld könnte jeweils ein Light Node betrieben werden, während die Full Nodes beispielsweise in den zertifizierten Rechenzentren der Smart Meter Gateway Administratoren und der sog. aktiven Externen Marktteilnehmern gehostet werden könnten.

Insgesamt ist das »Redundanzproblem« jedoch zu hinterfragen, da es sich in den meisten Fällen um eine bewusste Designentscheidung handelt.

Technologische Herausforderungen c) Technische Anforderungen

Oftmals ist es schwierig, Blockchains in bestehende IT-Infrastrukturen einzubinden. Erfolgsbeispiele basieren vielfach auf Greenfield-Ansätzen. Um externe Daten in eine Blockchain zu integrieren, ist die Entwicklung sicherer und vertrauenswürdiger smarterer Orakel von zentraler Bedeutung. Was die Einbindung in bestehende Systeme angeht, muss bei den smarten Orakeln über Prüfbarkeit und Auditierbarkeit nachgedacht werden, auch bedarf es einer Vielzahl an Beispielen erfolgreicher Transitionen. Das vom Bundesministerium für Bildung und Forschung geförderte Vorhaben iBlockchain untersucht unter anderem diese Fragestellung aktuell. Im Unternehmensumfeld lassen sich Aspekte wie Compliance oder zeitnahe Fehlerbereinigungen bisher nur schwer in die hochverteilte Struktur der derzeitigen Blockchain-Systeme integrieren. Eine Aufgabe für die Zukunft wird sein, diese Systeme so anzupassen, dass auch die Anforderungen des Unternehmenseinsatzes erfüllt werden können. Für eine breitere Nutzung insbesondere in der mittelständischen Wirtschaft wären leicht zugängliche Entwickler-Tools, Anwendungsprogrammierschnittstellen (APIs) und Baukästen wichtig. Hierfür könnten in Technologieprogrammen Open-Source-Komponenten entwickelt werden, um den Unternehmen die Möglichkeit zu geben, sich zukünftig Blockchains für einzelne Anwendungsfälle einfach zusammenbauen zu können. Weitere notwendige Voraussetzungen sind ein schneller Netzzugang und ein hohes fachliches Know-how.

Bitte geben Sie Ihre Stellungnahme zu der Herausforderung der technischen Anforderungen ein:

Bitkom Stellungnahme:

Die Aussage, dass bestehende Systeme in Blockchain-Anwendungen nur schwer integriert werden können und oft auf Greenfield-Approach basieren, ist nicht gänzlich nachzuvollziehen. In den inzwischen produktiven Blockchain-Lösungen wie der IBM FoodTrust für die sichere Lebensmittelkette sowie TradeLens für die Verfolgung von Containern und ihrer Frachtpapiere wurden z.B. API-Schnittstellen eingebaut, damit von den existierenden Systemen die Daten übertragen werden sowie die Daten aus der Blockchain-Anwendung in die vorhandenen Systeme transferiert werden können.

Die Definition von Standards für offen zugängliche APIs ist hier entscheidend. Selbstverständlich ist das Öffnen von privaten Blockchains deutlich einfacher zu gestalten, da hier die Teilnehmer meist bekannt sind und das Risiko geringer ist, durch die Öffnung an Vertrauen und Sicherheit einzubüßen.

Welche Anforderungen bestehen, um die Integration von Blockchain-Lösungen in die Unternehmenstätigkeit, v.a. vor dem Hintergrund bestehender zentralisierter Systeme, zu ermöglichen?

Bitkom Stellungnahme:

Die Blockchain-Lösungen für Unternehmenstätigkeiten müssen administrierbar (permission-based) sein. Dies impliziert vor allem Schreib- und Leserechte auf die gespeicherten Daten. Blockchains ergänzen aktuelle zentralisierte Systeme durch die Aufnahme von vertrauenswürdigen Daten durch authentifizierte Oracles. Dadurch können z.B. in ERP-Systemen automatisch Prozesse angestoßen werden.

Die zentralisierten Systeme werden durch die aktuellen Blockchain-Lösungen nicht abgelöst. Zudem müssen die Technologie einerseits sowie rechtliche Klarstellungen (rund um DSGVO etc.) andererseits weiter vorangetrieben werden.

Sollte es ein Zertifizierungsverfahren für Blockchain-Technologien im Hinblick auf die versprochenen Funktionalitäten geben?

Bitkom Stellungnahme:

Es existieren bereits Verfahren, z.B. IDW PS 890 (Institut der Wirtschaftsprüfer), allerdings ist es durchaus sinnvoll für spezifische Anwendungen einen eigenen Kriterienkatalog (Analog des BSI C5 für Cloud) aufzulegen. Auch in Open Source Gremien findet dies bereits statt – fehlende Funktionalitäten werden als defekt gemeldet und behandelt (z.B. Hyperledger). Generell sollte auf Freiwilligkeit und bestehende Vorgaben (bspw. solcher der DSGVO) gesetzt werden.

Technologische Herausforderungen d) Interoperabilität

Blockchains sind heute in der Regel für bestimmte Anwendungen optimiert und funktionieren in ihren fachlichen Silos gut. Es gibt jedoch keinen Transfer von Daten und Werten zwischen den Silos oder den Blockchains. Für eine breite Anwendbarkeit von Blockchain-Lösungen müsste ein Transfer von Daten und Vermögenswerten zwischen Blockchains möglich sein. Zur Lösung des Problems gibt es bereits unterschiedliche Ansätze. Ein Konzept für eine Übersetzungsarchitektur ist Polkadot, was die Verbindung von individuell angepassten Sidechains mit öffentlichen Blockchains ermöglicht. Durch Polkadot können verschiedene Blockchains Nachrichten auf sichere und vertrauenswürdige Weise untereinander austauschen. Auch die Normung und Standardisierung hat großes Potenzial, Blockchains und konventionelle Systeme interoperabler zu gestalten, indem Standards erarbeitet werden, die gemeinsame Schnittstellen und Protokolle definieren. Daneben gibt es noch andere Lösungsansätze, und auch hier muss noch Erfahrung gesammelt werden, welches Konzept in welcher Anwendung am tragfähigsten ist.

Bitte geben Sie Ihre Stellungnahme zu der Herausforderung der Interoperabilität ein:

Bitkom Stellungnahme:

Wie gesagt existieren bereits Verfahren (siehe hiervor), die die Interoperabilität fördern. Allerdings könnte es durchaus sinnvoll für spezifische Anwendungen sein, einen eigenen Kriterienkatalog (Analog des BSI C5 für Cloud) aufzulegen.

Herausforderungen, die mit Interoperabilität einhergehen sind z.B.:

- Daten verlieren das Vertrauen bzw. Ihre Authentizität sobald sie externalisiert werden.
- Ein Integrationsmechanismus oder Layer braucht ebenfalls Vertrauen in die Technologie und den Anbieter.
- Es besteht die Tendenz, einen weiteren Mittelsmann einzuführen.
- Interoperabilität erzeugt neue Schwierigkeiten die Durchgängigkeit des Vertrauens über Technologien und beteiligte Parteien sicherzustellen.

Welche Lösungen bzw. Lösungsansätze gibt es, um die Interoperabilität von Blockchains herzustellen? Wie »marktfähig« sind derartige Lösungsansätze?

Bitkom Stellungnahme:

Ein Lösungsbeispiel ist beispielsweise Hyperledger Burrow, eine permissioned Ethereum smart-contract Blockchain. Ein Ziel von Burrow ist es, eine Blockchain-Grundlage für EVM-Extensions zu bilden.

Bringen bestimmte Mindeststandards einen »Mehrwert« für alle Teilnehmer? Welche »Standards« könnten das sein?

Bitkom Stellungnahme:

Damit Kreativität und Wettbewerb innerhalb der verschiedenen Gremien, welche Blockchains entwickeln, sich weiter frei entfalten können, sollten Standards, welche allen Teilnehmern einen Mehrwert bringen, vor allem auf Schnittstellen zielen.

Weitere Themen in der Planung von Blockchain-Anwendungen sind z.B. standardisiert gemessene Durchsätze der jeweiligen Implementierung (siehe z.B. Hyperledger Caliper), um derzeitige Limits in der Skalierung darzustellen, die Projekte als Kriterium für ihren Anwendungsfall heranziehen können.

Allgemein können Zugriffe über standardisierte Schnittstellen (APIs) über Technologien hinweg helfen, um eine Integration auf der Applikationsebene übergreifend und unabhängig umsetzen zu können. Der Mehrwert für den Anwender besteht in der Übertragbarkeit oder der Nachprüfbarkeit für Dritte (bei entsprechenden gesetzlichen Vorgaben.)

Technologische Herausforderungen e) Irreversibilität

Geht ein privater Schlüssel verloren oder wird dieser gestohlen, gehen damit korrespondierende Inhalte unwiederbringlich verloren. Darüber hinaus kann es notwendig sein, Inhalte aus einer Blockchain zu löschen, beispielsweise wenn illegale Inhalte in einer Blockchain gespeichert, Verträge für nichtig erklärt wurden oder datenschutzrechtliche Löschansprüche oder -pflichten bestehen. Auch besteht die Möglichkeit, Diskriminierungen ausgesetzt zu sein, da einmal eingetragene persönliche Informationen (zum Beispiel aufgrund Geschlecht, Alter, sexueller Orientierung bzw. Identität, Herkunft etc.) nicht ohne Weiteres gelöscht werden können. Für die Durchbrechung der Irreversibilität lassen sich Lösungsansätze denken, jedoch würde hier an einem der wesentlichen Grundprinzipen und Leistungsmerkmalen der Blockchains gerüttelt. Viele dieser neuen Ansätze verändern die Sicherheit und Zuverlässigkeit und bedürfen daher der weiteren Analyse und Erprobung.

Bitte geben Sie Ihre Stellungnahme zu der Herausforderung der Irreversibilität ein:

Bitkom Stellungnahme:

Das zentrale Wertversprechen der Blockchain ist es, unveränderlich zu sein. Hierauf müssen Geschäfts- und Datenmodelle abgestimmt sein, um die bestehenden Regelungen einzuhalten (z.B. durch Nutzung einer privaten Blockchain und der Speicherung von personenbezogenen Daten außerhalb der Blockchain.

In der Irreversibilität besteht ein grundsätzlicher Vorteil von Blockchains, welcher jedoch auch zahlreiche Nachteile mit sich bringt, etwa wenn im Falle von Bugs/Fehlern oder geänderten Rahmenbedingungen Smart Contracts angepasst werden müssen, kryptografische Schlüssel verloren gehen/gestohlen werden sowie hinsichtlich der bereits zahlreich in anderen Punkten angesprochenen Anforderungen der DSGVO. Im Kontext Datenschutz ist unbedingt im Sinne von »Handlungsempfehlungen/Richtlinien« zu prüfen, welche Arten der Datenspeicherung in einer Blockchain überhaupt zulässig ist, um die übergeordneten Ansprüche und Erfordernisse zu gewährleisten.

Reicht es zur Erfüllung von Löschansprüchen oder -pflichten aus, Daten, z.B. illegale Inhalte, im übertragenen Sinne »zu schwärzen« – sie also für die Nutzer und Teilnehmer unkenntlich zu machen? Wie könnte das technisch umgesetzt werden?

Ist es möglich, Daten spurenlos physisch zu löschen? Wenn ja, wie? In welchen Fällen könnte dies erforderlich sein?

Bitkom Stellungnahme:

Wenn Daten gelöscht werden können, spricht man nicht mehr von Blockchain-Technologie. Eine fundamentale Eigenschaft dieser Technologie ist die Unveränderbarkeit von Daten. Ist dies nicht mehr gegeben, entfällt ein wesentliches Charakteristikum. In Öffentlichen Blockchains wird dies, schon alleine da eine unbekannte Anzahl an Repliken bestehen kann, technisch nicht machbar sein. Ohne die entsprechenden Schlüssel zur Entschlüsselung kritischer Daten ist die Information aber nicht mehr nutzbar.

Technologische Herausforderungen f) IT-Sicherheit

In einem Blockchain-System basieren Sicherheit und Vertrauen zum großen Teil auf kryptografischen Mechanismen wie Hashfunktionen oder digitalen Signaturen. Diese bilden eine solide Grundlage für die systemischen Sicherheitseigenschaften, sind aber alleine noch nicht ausreichend für ein valides Sicherheitskonzept. Abhängig von der Wahl des Blockchain-Typs und den angestrebten Sicherheitszielen müssen neben den klassischen Blockchain-Zielen wie Manipulationssicherheit, Verfügbarkeit und Pseudonymität auch Aspekte wie Vertraulichkeit, Authentizität, Anonymität und Identitätsmanagement passend modelliert und sicher umgesetzt werden. Außerdem muss das Sicherheitskonzept auch die Sicherheit des zugrundeliegenden Netzwerks, der verwendeten Hardwarekomponenten und der externen Schnittstellen der Blockchain entsprechend miteinbeziehen. Bereits beim Aufsetzen einer Blockchain müssen Verfahren etabliert werden, um bei Sicherheitsvorfällen angemessen reagieren und zum Beispiel Sicherheitsmechanismen austauschen zu können.

Das BSI als die nationale Cybersicherheitsbehörde beschäftigt sich mit allen Fragen der IT-Sicherheit im Blockchain-Umfeld und hat dazu bereits ein Eckpunktepapier mit grundlegenden Sicherheitsaussagen herausgegeben. Aktuell wird außerdem an der Erstellung eines Leitfadens zum Thema »Blockchain und IT-Sicherheit« gearbeitet, der potenziellen Nutzern der Blockchain-Technologie eine Hilfestellung zum sicheren Einsatz von Blockchains geben soll. Auch in der Welt der Normung und Standardisierung hat die IT-Sicherheit mit Bezug auf Blockchains an Bedeutung gewonnen, sodass sich zwei Arbeitsgruppen des ISO/TC 307 mit der Thematik »security, identity, privacy« beschäftigen.

Bitte geben Sie Ihre Stellungnahme zu der Herausforderung der IT-Sicherheit ein:

Bitkom Stellungnahme:

Wie bei der Einführung jeder neuen Technologie, sollten für eine sichere Entwicklung und einen vertrauensvollen Betrieb allgemeingültige als auch Blockchain-spezifische Cybersicherheitsrisiken frühzeitig betrachtet werden. Die Mehrheit der Unternehmen bzw. der Blockchain-Vorreiterunternehmen (64 bzw. 61%) sieht die Anforderungen der Blockchain an die IT-Sicherheit als problematisch (Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019)).

Dazu ist ein Cyber-Risikomanagement zu etablieren, das Risiken aus Bereichen wie Governance, Architektur, Dienstleistersteuerung, Compliance, Skalierung oder Cyber-Angriffe identifiziert und aus Business- wie IT-Sicht bewertet, um effektive Mitigationsmaßnahmen zu definieren.

Ein effektiver Schutz jeder Blockchain-Anwendung basiert auf einer daten-zentrischen Sicherheitsstrategie. Hierzu ist es essentiell, dass alle verarbeiteten Daten identifiziert und klassifiziert werden, um dedizierte Sicherheitskonzepte – abhängig vom Schutzbedarf der Daten – zu entwickeln.

Neben einem vertrauensvollen Schlüssel- und Berechtigungsmanagement sowie einer Sicherheits-Sensibilisierung aller Blockchain-Akteure, ist eine sichere Software-Entwicklung zwingend erforderlich.

Fehler im Code der Blockchain-Applikationen oder Smart Contracts sind eines der größten Risiken, da ihre Ausnutzung die gesamte Sicherheit und damit das Vertrauen in die Blockchain maßgeblich beeinträchtigen kann. Daher sind Maßnahmen wie »Sichere Coding-Standards« und Training der internen und externen Entwickler erforderlich.

Bei öffentlichen Blockchains besteht die Gefahr, dass sich koordinierte »Mining-/Staking-Pools« bilden, welche die Dezentralität und das wesentliche Sicherheitsfeature von Blockchains unterlaufen. Hier wäre zu klären, wie dem entgegengewirkt werden könnte und welchen Einfluss dies auf die grundsätzliche Nutzbarkeit der Technologie hätte.

Allgemeine Anmerkung: Anstelle von »IT-Sicherheit« ist der Begriff »Cyber-Sicherheit« ggf. passender. »IT-Sicherheit« adressiert eher technische Aspekte der Sicherheit, während z.B. organisatorische und prozessuale Aspekte oder der Faktor Mensch nicht im Scope liegen und damit Themen wie Informationsklassifizierung oder Sensibilisierung vernachlässigt werden. Der Begriff »Cyber-Sicherheit« hat einen größeren Umfang und umfasst alle relevanten Aspekte.

Welche Anforderungen an die IT-Sicherheit eines Blockchain-Systems stellen technologiebedingt eine besondere Herausforderung dar?

Bitkom Stellungnahme:

Der korrekte Einsatz von kryptographischen Mechanismen ist eine besondere Anforderung. Die Blockchain vereint eine Vielzahl solcher Mechanismen. Bereits kleine Fehler in der Anwendung eines einzelnen Mechanismus können jedoch zu dem vollständigen Verlust der Sicherheit des Gesamtsystems führen. Im Fall der Blockchain ist das besonders kritisch, da jeder Teilnehmer die gleiche Client-Software verwenden muss und die Sicherheit des Netzwerks daher davon abhängt, dass diese keine Fehler enthält. Ähnlich verhält es sich auch mit Smart Contracts, die automatisch bei allen Teilnehmern ausgeführt werden. Hier sind Sicherheitslücken besonders fatal.

Das ist insbesondere vor dem Hintergrund, dass die Blockchain noch in ihren Kinderschuhen steckt und dementsprechend hochvolatil ist, besorgniserregend. Sicherheitskritische Kernkomponenten erfahren regelmäßig tiefgreifende Änderungen und besitzen nicht den gleichen Reifegrad im Hinblick auf Code-Qualität und durchgeführter Security-Audits, wie sicherheitsrelevante Komponenten anderer Technologien (wie beispielsweise OpenSSL), die flächendeckend im Einsatz sind. Zur Sicherheit eines Produktes gehören weiterhin auch immer operative Aspekte, wie strukturierte Entwicklungs- und Review-Prozesse, Produktpflege, sowie ein definierter Prozess zum Umgang mit Sicherheitslücken. Insbesondere junge Unternehmen, die im Kontext von Blockchain-Technologie tätig sind, besitzen oft keine gleichermaßen ausgereiften Prozesse des IT-Sicherheitsmanagements, wie auf dem Markt etablierte Unternehmen.

Eine besondere Herausforderung stellt sich außerdem hinsichtlich des Sicherheitsziels der Unveränderlichkeit. Unveränderlichkeit ist nur erreichbar, wenn eine kritische Menge ehrlicher Teilnehmer des Netzwerks aktiv Transaktionen verifizieren. Populäre Anwendungen, wie beispielsweise Ethereum, erreichen diese kritische Menge zurzeit, jedoch ist es nicht vorherzusagen, ob das in Zukunft auch weiterhin der Fall sein wird. Beispielsweise liegt die Hoheit der Rechenkapazität von Bitcoin bereits jetzt schon zu einem großen Teil in China. Daten, die heute in einem Blockchain-basierten, unveränderlichen Datenspeicher abgelegt werden, können daher in Zukunft möglicherweise doch verändert werden. Diese Herausforderung muss beim Einsatz dieser Technologie stets berücksichtigt werden.

Zudem sind Verschlüsselungsverfahren, welche auch im Quantum-Zeitalter noch Bestand haben werden, natürlich auch in einem Blockchain-System eine schwierige Anforderung.

Wo und wie könnten »klassische« Sicherheitsansätze (wie z.B. eine Public Key Infrastructure) die Blockchain-Technologie ergänzen?

Bitkom Stellungnahme:

Die Blockchain-Technologie bietet die Möglichkeit, Vertrauen zwischen einander unbekannten Parteien zu schaffen. In bestimmten Fällen ist es aber essenziell, Kenntnis über die genaue Identität eines Akteurs/einer Anlage zu haben. Z.B. für Herkunftsnachweise von Grünstrom muss die Identität der Erzeugereinheit zweifelsfrei geklärt sein. Hier bieten PKIs (z.B. die Smart Meter PKI, deren Root CA vom BSI gehalten wird) eine sichere Methode des Identitätsnachweises und können so die Blockchain-Technologie ergänzen.

Weitere klassische Sicherheitsansätze wie der Betrieb einer entsprechenden Firewall oder einer (TSL) verschlüsselten Datenübertragung können die Blockchain-Technologie ebenfalls gut ergänzen.

Klassische Sicherheitsansätze sind integraler Bestandteil einer guten Lösung und sollten durch hoheitliche Organisationen (Bundesbehörde, UNO, ...) unterstützt werden, indem z.B. Zertifikate ausgestellt bzw. Schlüssel »beglaubigt« werden.

Die in eIDAS verbindlich definierten TrustServices, insbesondere qualifizierte eSignaturen und Siegel können eine eindeutige wie rechtsverbindliche Authentizität von Daten und Transaktionen gewährleisten. Qualifizierte Zeitstempel können außerdem den zur Nachweisführung und IT-Sicherheit notwendigen Proof of Existence gewährleisten. Eine Verbindung von Blockchain mit den TrustServices erscheint als elementarer Erfolgsfaktor der Blockchain-Technologie zur Anwendung in regulierten Industrien.

Sollte es eine Sicherheitszertifizierung für Blockchain-Produkte geben?

Bitkom Stellungnahme:

Grundsätzlich kann über eine freiwillige Zertifizierung nachgedacht werden. Hier sind aber unbedingt die mögliche Qualität einer Zertifizierung und deren Konsequenzen abzuwägen. Zertifizierungen sind sehr zeitaufwendig und könnten wirkungsvolle Lösungen zeitlich beeinträchtigen. Deshalb sollte in jedem Falle auf freiwillige Sicherheitszertifizierungen gesetzt werden, welche die Nachprüfbarkeit der vorgeblichen Eigenschaften für Dritte transparent wie nachweisbar dokumentieren und somit für mehr Vertrauen und breitere Anwendung der Technologie sorgen.

In Einzelfällen findet dies bereits statt. Hyperledger-Produkte z.B. werden zu bestimmten Zeitpunkten extern auf Sicherheitsrisiken auditiert.

Können potenzielle technische IKT-Probleme, ungezielte oder gar gezielte Angriffe bei Einsatz von Blockchain-Lösungen in besonderer Weise Auswirkungen auf zentrale Komponenten, Kommunikationswege oder Clientsysteme haben und die notwendige Verfügbarkeit und Reaktionszeit gefährden?

Bitkom Stellungnahme:

In der Vergangenheit hat sich gezeigt, dass öffentliche Blockchains tatsächlich für SPAM/DDoS Attacken verletzlich waren. Dies würde sich entsprechend auch auf die Kommunikationswege/Clientsysteme und Anwendungen generell ausüben. Das Risiko wird allerdings nicht höher eingeschätzt als bei klassischen, Nicht-Blockchainsystemen.

Ein Beispiel für einen Angriff mit Auswirkungen ist der DAO-Angriff, der eine Schwachstelle im smart contract nutzte, vgl.: ↗https://hackernoon.com/smart-contract-attacks-part-1-3-attacks-we-should-all-learn-from-the-dao-909ae4483f0a

Wie könnte sich der Einsatz von Blockchains bei der Bekämpfung von Cybersicherheitsrisiken, insbesondere in Bereichen der kritischen Versorgung, zukünftig auswirken?

Bitkom Stellungnahme:

Die Blockchain-Technologie bietet eine Vielzahl von Mechanismen, die das Sicherheitsniveau der gesamten Anwendung erhöhen kann und klassische Cybersicherheitsrisiken minimiert. Insbesondere trägt die Blockchain dazu bei, dass die Authentizität und Integrität der Daten wesentlich verbessert wird, was in konventionellen Umgebungen häufig ein Cybersicherheitsrisiko darstellt. Durch Hashing-Funktionen, digitale Signaturen, Konsensmechanismen oder der Unveränderlichkeit der Daten setzt die Blockchain-Technologie einheitliche Standards, die effizient von allen Akteuren »out-of-the-box« genutzt werden können.

Durch die Redundanz von Blockchain-Knoten müsste ein Hacker in den meisten Blockchain-Implementierungen Manipulationen gleichzeitig und gleichartig an vielen Knoten durchführen können, um das Konsensusverfahren von seiner Version der Wahrheit zu überzeugen. Dies ist zumindest mal sehr aufwändig.

Eine Frühdetektion von Cyber-Angriffen durch Mustererkennung z.B. auf Basis von selbstlernenden KI-Algorithmen könnte mittels Blockchain effizient und schnell an eine große Gruppe von Nutzern weitergegeben werden. Diese könnte dann Gegenmaßnahmen ergreifen.

3.2 Ökonomische Fragestellungen

Ökonomische Fragestellungen a) Ökonomisches Potenzial

Das ökonomische Potenzial der Blockchain-Technologie ist nur sehr schwer einzuschätzen – valide Schätzungen existieren bisher noch nicht. Das hat vielfältige Gründe: Wie oben beschrieben gibt es nicht »die eine« Blockchain, sondern vielzählige Ausgestaltungen, die anwendungsbezo-

gen individuelle Lösungen ermöglichen. Die Blockchain-Technologie kann in vielfältigen Anwendungsfeldern eingesetzt werden, wobei der Umfang konkreter Anwendungen und Geschäftsmodelle noch nicht absehbar ist. Zudem besteht noch viel Unsicherheit darüber, wie sich die Technologie weiterentwickeln wird.

Gleichwohl bezeichnen viele die Blockchain-Technologie schon jetzt als einen »Megatrend« (u.a. World Economic Forum), die als neue digitale Schüsseltechnologie das »Internet der Werte« etablieren könnte. International haben bereits viele Akteure aus Wirtschaft und Politik das Potenzial der Blockchain-Technologie erkannt.

Bei aller Unsicherheit einer Quantifizierung von (volks-)wirtschaftlichen Potenzialen geben verschiedene Studien einige Hinweise auf die hohe Relevanz und insbesondere die mögliche Dynamik der Technologie.

Marktpotenzial: Die Analysten von MarketsandMarkets gehen aktuell davon aus, dass der weltweite Blockchain-Markt zwischen 2018 und 2023 von etwa 1 Milliarde US-Dollar auf etwa 23 Milliarden US-Dollar wachsen dürfte – ein durchschnittlicher Anstieg von mehr als 80 Prozent pro Jahr (2018) [1]. Es wird erwartet, dass das prognostizierte Marktwachstum auf verschiedene Faktoren, wie beispielsweise den Anstieg an Wagniskapitalinvestitionen in Blockchain-Start-Ups, und den steigenden Bedarf an schnelleren und transparenteren Transaktionen in allen Branchen zurückzuführen ist. Etwa die Hälfte der vom World Economic Forum befragten Experten hält es für wahrscheinlich, dass im Jahr 2027 etwa 10 Prozent des Bruttoweltprodukts auf Blockchains gespeichert sein werden. Experten von McKinsey & Company wiesen darauf hin, dass die Transformationskraft der Blockchain-Technologie bisher gering ist und dass der kurzfristige Wert der Blockchain vor allem darin besteht, Kosten zu reduzieren. Größere, disruptivere Geschäftsmodelle erwarte man erst in den nächsten drei bis fünf Jahren.

Gründungen: Eine aktuelle Studie der TUM School of Management auf Basis von Daten aus dem Jahr 2016 identifiziert weltweit 1.140 Startups im Bereich der Blockchain-Technologie – 80 Prozent in den Wirtschaftsbereichen Finanz- sowie Informations- und Kommunikationstechnologien (IKT).Die meisten Blockchain-Startups sind im Finanz- und Versicherungssektor zu finden. Neben diesen FinTech-Startups ist der nächstgrößte Anteil der Blockchain-Startups im Informations- und Kommunikationssektor tätig. In Deutschland gibt es insgesamt rund 170 Blockchain-Startups, die meisten davon sind in Berlin ansässig (Stand: Februar 2019). [2]

Wagniskapital: In die in obiger Studie genannten 1.140 Startups wurde Wagniskapital in Höhe von etwa 1,5 Mrd. US-Dollar investiert. Zahlen der Wirtschaftsprüfungsgesellschaft KPMG zeigen, dass Wagniskapitalinvestitionen in Blockchain-basierte Unternehmen weltweit von 13 Mio. US-Dollar in 2013 auf fast 400 Mio. US-Dollar im Jahr 2016 gestiegen sind. Im Jahr 2018 wurden weltweit mindestens 1,3 Mrd. US-Dollar an Wagniskapital in die Blockchain-Technologie investiert. [3] Gemäß einer Studie von EY belief sich das Gesamtvolumen der Kapitalauf-

nahme im Rahmen von Initial Coin Offerings weltweit auf knapp 4 Mrd. US-Dollar (Dezember 2017), jedoch geht der Trend seit Ende 2017 langsam zurück.

Patente: Weltweit wurden im Zeitraum von 1999-2018 über 3.000 Patente eingereicht. China reichte die meisten Anträge ein (1.500), danach folgen die USA (950), Südkorea (220) und Europa (131).

Bitte geben Sie Ihre Stellungnahme zum ökonomischen Potenzial ein:

Bitkom Stellungnahme:

Eine quantitative Bewertung ist sicherlich sehr schwierig. Ein erstes Fazit bzgl. des Erfolgs von Prototypen und Use Case erlaubt die Schlussfolgerung, dass das Automatisierungspotential enorm ist. Dies lässt sicherlich die Schlussfolgerung zu, dass die Blockchain-Technologie auch ökonomisch einen wertvollen Beitrag im Rahmen verschiedenster Digitalisierungsprojekte leisten wird.

Laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019), geht immerhin jedes siebte Unternehmen davon aus, dass Blockchain die Gesellschaft und Wirtschaft so stark verändern wird, wie es das Internet getan hat.

Potenzielle Mehrwerte lassen sich vergleichsweise einfach einschätzen, deutlich schwieriger ist es, einzuschätzen, ob angedachte Lösungen überhaupt umsetzbar sind und wenn ja, zu welchen Kosten. Die Machbarkeit kann an einer »nicht-Implementierbarkeit« scheitern, die dann meistens eher prozessual als technisch ist. Probleme liegen insbesondere darin.

- Die für einen generischen Use-Case erforderlichen Unternehmensprozesse sind operativ nicht umsetzbar (bspw. bei der Rückverfolgbarkeit von seltenen Erden: diese werden kontinuierlichen gefördert (kein diskretes Produkt) und sind nicht markier- und unterscheidbar).

- Notwendige Teilnehmer sind nicht identifizierbar, wechseln schnell oder haben kein Interesse an einer Teilnahme (bspw. Bergwerke, Logistikdienstleister bzw. Zwischenhändler).

Ein vielversprechender Ansatz zur Ermittlung ökonomischer Potenziale ist der Weg über Demonstratoren und kleine Use-Cases die Herausforderungen in der Implementierung zu entdecken und zu lösen. Zu beachten ist dabei, dass diese Use-Cases für sich in der Regel kein tragfähiges Geschäftsmodell haben bzw. keinen Mehrwert generieren.

Wie schätzen Sie das ökonomische Potenzial der Blockchain-Technologie in den nächsten fünf Jahren ein?

Bitkom Stellungnahme:

In fünf Jahren werden die ersten Produkte auf Basis der Blockchain laufen. Mit dem zunehmenden Einsatz von cyberphysischen Systemen im Internet der Dinge – in Kombination mit AI-Anwendungen – kann von einem exponentiellen Anstieg des Einsatzes solcher Produkte und von einer drastischen Erhöhung des ökonomischen Potenzials der Blockchain-Technologie ausgegangen werden.

Es werden klarere Governance-Strukturen vorherrschen und somit mehr Vertrauen seitens der Unternehmen bestehen, sich am Netzwerk anzuschließen.

Wie schätzen Sie das ökonomische Potenzial von privaten Blockchains im Vergleich zu öffentlichen Blockchains ein?

Bitkom Stellungnahme:

Der Einsatz öffentlicher Blockchains in B2B-Anwendungsfällen ist gemäß heutigem Stand sicherlich eher klein. Dies liegt auch an dem vorher erwähnten Evolutionsprozess, der mit dem zum Paradigmenwechsel notwendigen Einsatz von privaten Blockchains startet.

Welches sind die zentralen ökonomischen Herausforderungen für private Blockchain-Anwendungen bzw. Anwendungen auf öffentlichen Blockchains?

Bitkom Stellungnahme:

Bei beiden Blockchain-Anwendungen müssen Unternehmen bereit sein, entlang von Supply Chains (ein gewisses Maß an) Transparenz zuzulassen, was ihrem bisherigen Geschäftsgebaren allerdings widerspricht. Dieses Maß an Transparenz liegt bei privaten Blockchains deutlich niedriger im Vergleich zu öffentlichen Blockchains, weil sie von den beteiligten Partnern selbst festgelegt und administriert werden kann.

Es besteht kein Zwang, sich an einer Blockchain-Lösung zu beteiligen. Also muss es für die beteiligten Unternehmen vorteilhaft sein, im Netzwerk mitzumachen. Je mehr Teilnehmer einem Netzwerk beitreten, umso mehr können sich Vorteile für den einzelnen bisherigen Teilnehmer verschieben. Ein Netzwerk mit einer guten Governance achtet daher immer darauf, dass es keine Teilnehmer gibt, die besonders profitieren, sondern ermöglicht eine Anpassung der Konditionen, wenn sich die Mehrwerte gravierend verschieben. Dazu benötigt man eine klare Governance-Struktur und Gremien wie Kundenboards, die Rückmeldung geben.

Weitere ökonomische Herausforderungen sind die IT-Sicherheit, fehlende Rechtssicherheit für öffentliche Blockchains, sowie Vertrauen seitens der Unternehmen, Bürger, und Verwaltung.

Ökonomische Fragestellungen b) KMU

In einer Onlineumfrage des Statistischen Bundesamts (2017) gaben 43 Prozent der befragten Entscheider aus deutschen mittelständischen Unternehmen an, keine Einsatzmöglichkeiten der Blockchain zu kennen. Nur 18 Prozent der Befragten gaben an, dass ihnen bekannt sei, dass man mit einer Blockchain Echtheitszertifikate verwalten kann. Trotz möglicher Anwendungsbereiche der Technologie in vielen Unternehmen besteht ein Unterschied zwischen dem Blockchain-Wissen innerhalb der Blockchain Community einerseits und in mittelständischen Unternehmensführungen, aber auch in der allgemeinen Bevölkerung andererseits. Eine stärkere Vernetzung und Austausch im Blockchain-Bereich könnten diese Unterschiede überwinden, aber Hürden hierfür sowie konkrete Projekte müssen weiter diskutiert werden.

Bitte geben Sie Ihre Stellungnahme zu KMU ein:

Bitkom Stellungnahme:

Die Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) illustriert sehr deutlich, dass der Einsatz der Blockchain-Technologie in Deutschland sehr von der Unternehmensgröße abhängt. Bei über 90% der Unternehmen unter 200 Mitarbeitern ist der Blockchain Einsatz gar kein Thema, bei unter 1% ist die Technologie bereits im Einsatz. Ein weiteres wichtiges Thema ist die Zusammenarbeit zwischen Großunternehmen und Startups. Laut der Studie arbeiten nur 5% der Blockchain-Anwenderunternehmen mit Startups zusammen. Diese beiden Fakten verdeutlichen das enorme Wachstums- und Verbesserungspotenzial bzgl. des Einsatzes von Blockchain in KMUs.

KMUs benötigen meist noch grundlegende Digitalisierung: Automatisierte Datenaufnahme, digitalisierte Bestellungen über APIs zur direkten Weiterverarbeitung etc. Dies wird häufig als Voraussetzung betrachtet, um die Blockchain-Technologie einzusetzen, was aktuell einer ernsthaften Beschäftigung damit noch entgegensteht. Es muss Verständnis geschaffen werden, dass Blockchain bereits helfen kann, diese grundlegende Digitalisierung zu schaffen. Wenn dieses Verständnis einmal geschaffen worden ist, dann sind es aber gerade KMUs, die in verteilten Wertschöpfungsprozessen von den Vorteilen der Blockchain-Technologie profitieren können.

KMUs haben jedoch zum einen höchst selten entsprechende interne Kompetenzen, nur sehr überschaubare interne Ressourcen und zum anderen wesentlich weniger Optionen auf externen Sachverstand (Beratungsunternehmen, etc.) zuzugreifen (Ausnahmen: Fraunhofer-Gesellschaft; Universitäre Partner) bzw. diesen intern aufzubauen.

Gerade in Deutschland als Export-Weltmeister mit vielen sehr international tätigen mittelständischen Unternehmen können transparente Abläufe und Qualität, die oft mit »made in Germany« als Markenversprechen verbunden sind, auch über Blockchain-Lösungen als Technologie weiter unterstützt werden. Echtheitsüberprüfung von Ersatzteilen, Teilnahme an

Projekten zur Lieferketten-Überwachung für bessere Planung bei weniger Kosten als die heutige oft noch papierbasierte Variante – es gibt einige Beispiele. Es hapert aber in Deutschland allgemein am Trend zur Digitalisierung, dies wird zum Teil ausgesessen und gefährdet die Wettbewerbsfähigkeit des Standorts.

Wie kann das Potenzial der Blockchain-Technologie nicht nur in der Startup-Szene, sondern auch bei mittelständischen Unternehmen, insbesondere kleinen und mittleren Unternehmen, gehoben werden?

Bitkom Stellungnahme:

Einerseits kann dies durch Pilotprojekte erfolgen, in deren Rahmen erfolgreiche Proof of Concepts durchgeführt werden. Öffentlich (co-)finanzierte Forschungsprojekte senken hierbei deutlich die Einstiegshürde für KMU's. Darüber hinaus kann die Verbreitung von Wissen im Rahmen von Seminaren oder Workshops helfen. Das Fraunhofer IML z.B. bietet KMU im Rahmen des Kompetenzzentrums Digital in NRW ein Blockchain-Seminar an.

Viele KMUs haben keine eigene IT-Abteilung, manche auch keinen einzigen IT-Mitarbeiter. Daher ist es wichtig Open-Source-Blockchain-Lösungen und -Konsortien zu fördern, und gleichzeitig die KMUs für neue (Open-Source-)Lösungen zu sensibilisieren und bei der Implementierung zu unterstützen.

Für KMUs machen isolierte Blockchain-Anwendungen aufgrund der Größe zumeist keinen Sinn. Interoperabilität könnte hier den Weg öffnen, um in kleineren Konsortium-Netzwerken bestimmte Prozesse beispielsweise in der Lieferkette abzubilden. Die nötige Relevanz dieser Prozesse nach außen hin und in Bezug auf Dritte wird durch die Anbindung dieser individuellen »Intranets« an die Blockchain-Netzwerke weiterer Parteien realisiert.

Viele KMU warten zudem bei vermeintlichen Hypes bis eine gewisse »Bestätigung« der Technologie durch entweder große Unternehmen oder gesetzliche Regulierung erfolgt. Daher müssen Use-Cases der großen Unternehmen publik (z.B. IHKs, Presse, ...) gemacht werden und vom Gesetzgeber Regulierungen erlassen werden.

Die KMUs könnten außerdem in strukturierter Weise Geschäftsprozesse benennen, welche häufig Friktionen im Multiparteiensystem beinhalten und somit Kosten und Aufwand bedeuten. Wenn mehrere Unternehmen ein ähnlich gelagertes Problem benennen, könnte z.B. mit Hilfe von Branchenverbänden/Kompetenzzentren etc. eruiert werden, ob eine Lösung auf Basis von Blockchain-Technologie hier die nötige Transparenz und Automatisierung schaffen kann, um Abhilfe zu schaffen.

Welche Einsatzmöglichkeiten und Potenziale sehen Sie insbesondere bei kleinen und mittleren Unternehmen?

Bitkom Stellungnahme:

Mögliche Einsatzmöglichkeiten und Potenziale sind z.B.:

- Reputation und Ausweitung des Geschäftes als transparenter Geschäftspartner, der seine Lieferkette im Griff hat und daher zuverlässig ist – B2B wie B2C.
- Blockchain reduziert und automatisiert administrative Prozesse. Die könnte die zumeist knappen personellen Ressourcen entlasten.
- Die Vernetzung von Unternehmen, wobei vor allem sichere Datenkanäle durch die Technologie ermöglicht werden.

3.3 Ökologische Fragestellungen

Die Blockchain-Technologie wirft hinsichtlich ihrer ökologischen Wirkungen neue Fragen auf. Einerseits bergen ihre Eigenschaften grundsätzlich neues Potenzial für einen umwelt-, klima- und ressourcenschonenden Wandel in Wirtschaft, Gesellschaft und Konsum. Blockchain-Nutzungsszenarien für die Umwelt entstehen unter anderem durch effizientere und dezentrale Systeme, den Peer-to-Peer-Handel mit Ressourcen, die Transparenz von Lieferketten sowie nachhaltige Finanzierungsmodelle und erstrecken sich auf zentrale ökologische Handlungsfelder wie den Klimawandel, den Schutz der Ozeane, den Verlust der Artenvielfalt oder Luftverschmutzung. Ob Blockchain-Anwendungen auch im großen Maßstab zu einer nachhaltigen Entwicklung beitragen können, hängt dabei neben ihrer technischen Leistungsfähigkeit auch vom Grad ihrer Skalierbarkeit und verantwortungsvoller Entwicklung ab. Dies erfordert zweckmäßige und unterstützende Regelungen.

Andererseits stehen Einsparungen und Chancen erhebliche Energie- und Rohstoffbedarfe gegenüber. Um die Blockchain-Technologie zum Modernisierungs- und Innovationstreiber zu machen, muss sie auch vor dem Hintergrund ökologischer Herausforderungen und der weltweiten Klimaziele betrachtet werden.

Öffentliche Blockchains: Der am weitesten verbreitete Blockchain-Konsensmechanismus ist der sogenannte Proof-of-Work (PoW). Er wird bei der Kryptowährung Bitcoin genutzt und dient als Blaupause für eine Vielzahl von nachfolgenden Blockchain-Anwendungen. Beim PoW wird der Schwierigkeitsgrad für das mathematische Problem, das die Miner für die Verknüpfung neuer Blöcke lösen müssen, mit ihrem technischen Fortschritt erhöht, sodass die Anzahl der Blöcke, die in einer bestimmten Zeit berechnet werden können, konstant bleibt. Dadurch steigen die Anforderungen an Rechnerleistung im Laufe der Zeit und es kommt zu einer

Spirale aus technischer Nachrüstung und steigendem Schwierigkeitsgrad. Der dadurch ausgelöste Rent-Seeking-Wettbewerb führt zu einem zunehmenden Energieverbrauch. Es wird prognostiziert, dass das Bitcoin-Netzwerk rund 47 TWh pro Jahr verbraucht, was dem Stromverbrauch von Singapur entspricht (Stichtag: 6. Februar 2019).[1] Da Mining nicht an den Ort der Transaktion gebunden ist, bestehen große Anreize zur weltweiten Verlagerung an Orte mit geringen oder gar keinen Strompreisen, in denen Strom in der Regel auch nicht nachhaltig erzeugt wird. Aus klimapolitischen, ökologischen und ökonomischen Gründen erscheint PoW daher derzeit nicht sinnvoll und sollte kritisch hinterfragt werden.

Das Ressourcen-Problem lässt sich je nach Anwendungsfall ggf. durch andere Konsensmechanismen lösen. Viele Blockchain-Projekte arbeiten daran, Proof-of-Work durch andere Konsensmechanismen zu ersetzen und stattdessen identitäts- oder zeitbasierte Konsensschemata zu nutzen. Ein identitätsbasiertes Verfahren ist das Proof-of-Stake-Verfahren, bei dem die Miner, die einen neuen Block berechnen können, nach ihren Anteilen an der Kryptowährung oder über ein Zufallsverfahren ausgewählt werden. Über eine Vielzahl von Projekten sollte Erfahrung gesammelt werden, welche Konsensverfahren abhängig vom Einsatzgebiet die beste Lösung bzgl. Sicherheit, Liability, Kosten, Skalierung und Leistungsfähigkeit biete.

Private Blockchains können durch den Verzicht auf rechenintensive Konsensmechanismen energieeffizient betrieben werden.

Bitte geben Sie Ihre Stellungnahme zu ökologischen Fragestellungen ein:

Bitkom Stellungnahme:

Die Blockchain verbraucht nicht per se enorm viel Energie. Der hohe Energieverbrauch ist insbesondere auf den aufwendigen Mining-Prozess im Rahmen von einzelnen Kryptowährungen zurückzuführen.

Private Blockchains können durch die Arbeit mit Identitäten der Teilnehmer auf rechenintensive Konsensmechanismen verzichten und daher energieeffizient betrieben werden. Proof of Work ist ein Protokoll, welches anonyme oder pseudonyme Teilnehmer vor unbemerkten Mehrheitsbildungen durch weitere anonyme oder pseudonyme Teilnehmer zum Zwecke der Transaktionsmanipulation schützen soll. In den sogenannten privaten bzw. Konsortialblockchains ist das Stimmverhalten nachvollziehbar und manipulative Eingriffsversuche können geahndet werden.

In welchen Anwendungsfeldern werden zentrale ökologische Chancen bzw. Risiken durch die Nutzung der Blockchain-Technologie gesehen (Use Cases)?

Bitkom Stellungnahme:

Öffentliche Blockchains scheiden aufgrund des exorbitanten Energieverbrauchs im Kontext Klimaschutz, Energiewende sowie eines wirtschaftlichen IT-Einsatzes faktisch aus. Aus Umweltschutzgründen lässt sich faktisch nur der Einsatz privater Blockchains empfehlen.

Welche Lösungsansätze für das Ressourcenproblem von (öffentlichen) Blockchains sind erfolgversprechend? Wann ist die Umsetzung solcher Lösungsansätze zu erwarten?

Bitkom Stellungnahme:

Es gibt die Möglichkeit, den Konsensmechanismus vom aufwendigen Proof of Work hin zu Proof of Stake zu ändern. Abgesehen davon gibt es auch Forschungsansätze, verschiedene Unter-Blockchains mit Proof of Work Mechanismus zu kreieren.

Durch welche Regelungs-, Regulierungs- und Anreizsysteme könnte eine nachhaltige Nutzung der Blockchain-Technologie unterstützt werden? Welche europäischen oder internationalen Governance-Strukturen sind denkbar?

Bitkom Stellungnahme:

Gerade wenn eine öffentliche Organisation eine Governance Rolle übernimmt, kann in einem verteilten System (vgl. z.B. das DNS System durch die ICANN) auf »Zero-Trust« Konsensmechanismen verzichtet werden. Für eine Standardisierung wäre eine solche Governancefunktion sinnvoll, um eine Zersplitterung durch unzählige Forks zu verhindern.

Wie hoch wird der Stromverbrauch für Blockchain-Anwendungen heute und im erwarteten Trend eingeschätzt? Und wie verhalten sich demgegenüber mögliche Einsparungen?

Bitkom Stellungnahme:

Bei Verwendung von Blockchains mit Identitäten und entsprechenden Konsensusverfahren wie z.B. die Hyperledger-Familie entspricht der Stromverbrauch vergleichbaren messaging-basierten Anwendungen. Die Kosteneinsparungen für die Effizienzen in den Prozessen sind deutlich höher, schwanken natürlich je nach Anwendungsfall.

Welche Änderungen in der Konstruktion der Blockchain, z.B. zugunsten der Transaktionsgeschwindigkeit und des Energieverbrauchs, unterwandern wiederum die Kerneigenschaften der Technologie wie z.B. Transparenz und Manipulationssicherheit?

Bitkom Stellungnahme:

Solche Überlegungen sind ziemlich theoretisch, jedenfalls in Open Source Gremien mit Governancestruktur wird das Ziel des Projektes selten untergraben, solche Vorschläge würden nicht akzeptiert bzw. unterstützt und es würde zu Abspaltungen führen.

Sollte es ein Zertifizierungsverfahren für Blockchain-Technologien im Hinblick auf Energie-/Ressourcenverbrauch geben?

Bitkom Stellungnahme:

Das könnte Sinn machen. Smart Contracts sind de facto Programmcode und somit nicht für jeden Nutzer unmittelbar nachvollziehbar. Es ist von Vorteil, wenn eine vorgelagerte Instanz (z.B. eine Zertifizierungsstelle) den hinterlegten Smart Contract prüft und dies entsprechend bestätigt. Insgesamt hängt der Einsatz von ressourcenaufwendigen Blockchain-Technologien aber vom Markt ab. Wenn der Business Case den Energieverbrauch tragen kann und von den Teilnehmern als wichtiger eingeordnet wird, werden solche Anwendungsfälle auch umgesetzt werden. Effizientere Alternativen setzen sich nach der Marktlogik eigenständig durch.

3.4 Rechtliche Fragestellungen

Der überwiegende Teil der Rechtsordnung ist technologieneutral ausgestaltet. Die Blockchain-Technologie als solche löst keinen unmittelbaren Regulierungsbedarf aus. Für die Frage der Regulierung ist nicht die Technologie entscheidend, sondern ihre Anwendung. Eine Vielzahl rechtlicher Fragestellungen ist demnach anhand des konkreten, unter Verwendung der Blockchain-Technologie verfolgten Geschäftsmodells zu beurteilen.

Jedoch ergibt sich aus zentralen Architekturkomponenten der Blockchain unter anderem in Form der Unveränderlichkeit der Einträge und der dezentralen Organisation und Anonymität von öffentlichen Blockchains eine Reihe grundsätzlicher, rechtlicher Fragestellungen. Dabei liegt der Schwerpunkt dieser Fragestellungen im Bereich der öffentlichen Blockchains und weniger im Bereich der privaten Blockchains, da dort im Rahmen der Vertragsgestaltung der beteiligten Personen viele Fragestellungen einer Klärung zugeführt werden können. In der folgenden Darstellung wird – soweit relevant – zwischen öffentlichen und privaten Blockchains unterschieden.

Bitte geben Sie Ihre Stellungnahme zu rechtlichen Fragestellungen ein:

Bitkom Stellungnahme:

Die prinzipielle Differenzierung zwischen public und private Blockchain ist richtig. Insgesamt muss an dieser Stelle nochmals betont werden, dass rechtliche Unklarheiten zu den größten Hürden beim Einsatz der Blockchain zählen. So geben laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) zwei Drittel der Unternehmen an, dass rechtliche Unsicherheiten ein Hemmnis beim Einsatz der Blockchain sind. Allerdings muss die Technologieneutralität des geltenden Rechts beibehalten werden. Die Blockchain-Technologie ist für viele Zwecke und Geschäftsmodelle gut geeignet, für andere Vorgänge (z.B. solche, die personenbezogene Daten umfassen, oder solche, die eine Möglichkeit zur Rückabwicklung erfordern) weniger gut. Das sollte aber nicht zu dem Schluss verleiten, dass das geltende Recht spezifisch auf die Blockchain-Technologie zugeschnitten werden muss. Dennoch sind Anpassungen des geltenden Rechts an den Stellen angezeigt, in denen die Blockchain-Technologie ohne sachlichen Grund benachteiligt wird (z.B. bei Formvorschriften).

Welchen Unterschied sehen Sie mit Blick auf die rechtlichen Herausforderungen zwischen öffentlichen und privaten Blockchains?

Bitkom Stellungnahme:

Öffentliche Blockchains beruhen im Kern auf einem Modell des Vertrauens in die Community der Blockchain. Es ist faktisch nicht möglich, mehr als 51% der Knoten zu übernehmen. Ein Vertrauen in eine Community oder Organisation besteht nach deutschem und europäischem Recht nicht. Vielmehr basiert das Vertrauen auf Vertrauensketten und vertrauenswürdigen Dritten, was sich insbesondere in der rechtsverbindlichen eIDAS-Verordnung, der GDPR sowie der geltenden Vorgaben für Dokumentations-/Nachweispflichten zeigt. Eine grundlegende Änderung des europäischen wie deutschen Rechtsrahmens ist absehbar nicht zu erwarten. Die Integration der eID-Mittel und Vertrauensdienste nach eIDAS und ähnlicher Werkzeuge könnte die öffentliche Blockchain für weitere Anwendungsbereiche zugänglich machen. Ein wesentlicher Unterschied zwischen öffentlicher und privater Blockchain besteht regelmäßig darin, dass die Identität der Teilnehmer in öffentlichen Blockchains den anderen Teilnehmern weitgehend unbekannt ist.

Private Blockchains dagegen integrieren sich direkt in das bestehende Vertrauensmodell, indem sie von vertrauenswürdigen Dritten betrieben werden. Direkte rechtliche Herausforderungen stellen sich für private Blockchains derzeit nicht. Es besteht Identifizierbarkeit der Beteiligten und damit auch der rechtlich Handelnden. Dies führt dazu, dass Rechte und Pflichten eindeutig zugeordnet, geltend gemacht und durchgesetzt werden könne. Zudem ist auch der Ort der Datenverarbeitung eingrenzbar, was z.B. im Rahmen des Datenschutzrechts relevant ist. Im Vertragsrecht können etwaige Vertragsstörungen oder Anpassungen direkt zwischen den Beteiligten vorgenommen werden, auch technische Lösungen kommen hier in

Betracht, um einen rechtlichen Disput zu lösen. Während eine Private Blockchain regelmäßig auf einer vertragsrechtlichen Grundlage des geltenden Rechts beruht (z.B. GbR, Konsortialvertrag), existiert für das Netzwerk einer Public Blockchain kein unmittelbar anwendbares Rechtsinstitut des geltenden Rechts (die Rechtsbeziehungen einzelner Blockchain-Teilnehmeruntereinander lassen sich dagegen wieder durch Vertragstypen des geltenden Rechts erfassen).

Rechtliche Fragestellungen a) Anwendbares Recht

Öffentliche Blockchains: Öffentliche Blockchains haben als dezentrales Netzwerk keinen Standort (etwa einen Server), der für die Zuordnung zu einem Rechtsraum ausschlaggebend sein könnte. Transaktionsbeteiligte können sich in unterschiedlichen Jurisdiktionen mit sich widersprechenden Regelwerken befinden. Dies kann neue Herausforderungen an das internationale Privatrecht stellen, wenn bisher auf den Ort eines Registers oder den Sitz eines Intermediärs abgestellt wurde.

Im Privatrecht wäre grundsätzlich eine Rechtswahl durch die Parteien denkbar. Einschränkungen aufgrund international zwingender Vorschriften (z.B. regulatorische Vorgaben, Verbraucherschutz, Grundstücksrecht) müssen jedoch beachtet werden.

Private Blockchains: In privaten Blockchains wird regelmäßig vertraglich das anwendbare Recht festgelegt. Im Übrigen kann die Existenz eines zentralen Betreibers die Bestimmung des anwendbaren Rechts erleichtern.

Bitte geben Sie Ihre Stellungnahme zum anwendbaren Recht ein:

Bitkom Stellungnahme:

Zur Bestimmung des jeweils anwendbaren Rechts für eine Transaktion über die Blockchain ist zu unterscheiden, ob es sich um rein vertragsrechtliche Vorgänge oder um die Zuordnung eines Gegenstands zu einem Berechtigten und deren Änderung handelt. Für vertragsrechtliche Beziehungen kennt das Recht einschlägige Regelungen (Internationales Privatrecht, Verordnung (EG) Nr. 593/2008 – Rom I), die jedoch durch Vereinbarung zwischen den Vertragsparteien abgeändert werden können (eine solche Vereinbarung wäre grundsätzlich auch in Public Blockchains denkbar). Für (Eigentums-)Rechte an Gegenständen und geistigem Eigentum sowie deren Einräumung und Übertragung sind zwingende rechtliche Vorgaben zu beachten. Danach gilt jeweils die nationale Rechtsordnung an dem Ort, an dem sich das Rechtsobjekt aktuell befindet.

Private Blockchains sind klar im Vorteil, da es in privaten (permissioned) Blockchains einen zentralen Betreiber gibt, meist eine extra für diesen Zweck gegründete legale Entität, die aus

einem Konsortium hervorgegangen ist und zur Klärung und Vereinfachung des Rechtsrahmens von den Konsortiumsmitgliedern gegründet wurde.

Private Blockchains unterliegen den jeweiligen vertraglichen Regelungen. Bei der öffentlichen Blockchain könnte man über eine Art Bestellerprinzip bzw. Empfängerprinzip nachdenken. Allerdings müsste diese Regelung, dass das Bestellerprinzip Anwendung findet ebenfalls rechtsraumübergreifend geregelt werden.

Welches Recht soll etwa in den Fällen anwendbar sein, in denen herkömmlich an den Standort eines nun in der Blockchain verbrieften Rechts oder den Sitz eines durch die Blockchain entbehrlich gewordenen Intermediärs angeknüpft wird?

Bitkom Stellungnahme:

Die Verwendung privater Blockchains und damit eines eindeutig bestimmbaren vertrauenswürdigen Dritten und dessen Sitz ist für die Umsetzbarkeit der Technologie ein entscheidender Vorteil. In privaten Blockchains können die bestehenden Vorgehensweisen zur Identifikation des anwendbaren Rechts einfach übertragen werden. Bei öffentlichen Blockchains ist es schwieriger, es könnte ggf. bei Leistungen auf den Erfüllungsort abgestellt werden. Für (Eigentums-)Rechte an Gegenständen und geistigem Eigentum sowie deren Einräumung und Übertragung sind zwingende rechtliche Vorgaben zu beachten (vgl. Bitkom-Stellungnahme zur vorhergehenden Frage).

Können Transaktionen, die verschiedenen Rechtsordnungen unterliegen, in einer Blockchain abgebildet werden und welche Herausforderungen stellt dies an die Blockchain?

Bitkom Stellungnahme:

Ja, denn dies ist heute bereits auf Papier auch möglich, sonst würde kein Welthandel funktionieren. Im Zuge der Technologieneutralität der Gesetzgebung geht das dann auch mit Blockchain-Technologie, wenn im Anwendungsfall (der Geschäftslogik) dafür Vorsorge getroffen wurde, was man mit Papier auch machen würde.

In ISO/TC 307 arbeitet man gerade an einer technischen Spezifizierung für »legally binding smart contracts«, welche den Entwicklern einer Blockchain-Anwendung, die in verschiedenen Jurisdiktionen eingesetzt werden soll, einen Sorgfalts-Checkliste zur Hand geben wird.

Die Möglichkeit einer internationalen Schlichtungsstelle sollte geprüft werden. Verpflichtungen sollten entsprechend in den Nutzungsbedingungen der jeweiligen Blockchain festgeschrieben werden.

Wie können in Blockchains wesentliche Verbraucherschutzrechte und rechtsstaatliche Grundsätze (Rule of Law) sichergestellt werden?

Bitkom Stellungnahme:

Das hängt von der Ausgestaltung ab. Blockchain-Technologie hat hier dem Recht zu folgen (und steht nicht über dem Recht), entsprechend ist schon auf Design-Ebene darauf zu achten, dass entsprechende Rechte wahrgenommen werden können. Dies ist bei privaten Blockchains naturgemäß wieder einfacher zu gestalten. Gerade für Verbraucher können Blockchains aber auch erhebliche Erleichterungen bei der Rechtsdurchsetzung bieten, wenn die rechtlichen Vorgaben in Smart Contracts abgebildet und automatisch exekutiert werden (z.B. bei Entschädigungen für Flug- oder Zugverspätungen).

Rechtliche Fragestellungen b) Rechtliche Verantwortlichkeit und Rechtsdurchsetzung

Öffentliche Blockchains: Rechtliche Normen haben immer einen Regelungsadressaten. In einer öffentlichen Blockchain existiert allerdings kein zentraler Ansprechpartner. Betroffene wären vielmehr alle am Netzwerk Teilnehmenden, welche aber anonym agieren können.

Bei einigen Blockchain-Anwendungen wird es daher strukturell notwendig sein, die Identifikation der Akteure zu ermöglichen. Dies gilt aus regulatorischen Gründen (zum Beispiel. Wertpapierhandel, Geldwäschegesetz) oder auch bei Anwendungen, bei welchen die Identifikation der Transaktionsbeteiligten wesensimmanent ist (zum Beispiel gewerbliche Schutzrechte, Kraftfahrzeugregister). [1]

Aber auch bei Identifikation der Akteure muss ein Regelungsadressat grundsätzlich Einfluss auf das von ihm geforderte Normverhalten haben. Von ihm können unmögliche Handlungen nicht verlangt werden.

Ein weiteres zentrales Problem im Zusammenhang mit rechtlicher Verantwortlichkeit ist die technische Unveränderlichkeit öffentlicher Blockchains. Eine Partei kann die von ihr ausgelösten Einträge und Transaktionen in die Blockchain nachträglich nicht mehr abändern. Jedoch bleibt den Parteien unbenommen, abändernde Abreden zu treffen. Letztlich wären diese Abreden außerhalb der Blockchain dann wieder mit den typischen Nachweis- und Durchsetzungsrisiken verbunden. Gelingt der Nachweis, könnte die Rückabwicklung in einem neuen Block festgeschrieben werden, sofern die Blockchain die dafür notwendigen technischen Funktionalitäten hat. Allerdings werden die getätigten Einträge und Transaktionen immer in der Blockchain stehen bleiben, demnach ist ein »Löschen« nicht möglich.

Unabhängig von den einzelnen Transaktionen stellt sich auch die Frage, wer in einem völlig dezentralen System, in dem weder eine Behörde noch ein Unternehmen die Blockchain-Anwendung zur Verfügung stellt, für die Sicherheit des Systems verantwortlich sein soll.

Private Blockchains: In privaten Blockchains fungiert die Stelle, welche über die Zuteilung von Lese- und Schreibrechten entscheidet, als »Gatekeeper« mit Einflussmöglichkeiten auf das Netzwerk. In dieser Funktion kann sie auch tauglicher Regelungsadressat sein. Darüber hinaus sind die Teilnehmer in der Regel identifizierbar und weitere rechtliche Verantwortlichkeiten werden regelmäßig vertraglich bestimmt. Dies kann auch regelmäßig die Korrektur erfolgter Einträge und Transaktionen umfassen, wobei auch bei privaten Blockchains eine rechtliche Problematik daraus entstehen kann, dass eine nachträgliche Korrektur ggf. technisch nicht zur Löschung des ursprünglichen Eintrages bzw. der ursprünglichen Transaktion führt, sondern lediglich zusätzlich ein/e Korrektureintrag/-transaktion erfolgt.

Bitte geben Sie Ihre Stellungnahme zur rechtlichen Verantwortlichkeit und Rechtsdurchsetzung ein:

Bitkom Stellungnahme:

Die Rechtsdurchsetzung sowie rechtliche Verantwortung sollte bei privaten Blockchains kein Problem sein, da die Beteiligten bekannt und in der Regel vertraglich verbunden sind. In datenschutzrechtlicher Hinsicht werden dort Daten außerhalb der Chain gespeichert werden. Inhalte können entsprechend korrigiert/gelöscht werden. Die rechtliche Verantwortlichkeit muss je nach Blockchain-Anwendungsfall geklärt werden- und ggf. müssen Einverständniserklärungen und Mandate vor Teilnahme von Endnutzern eingeholt werden.

Die Blockchain-Technologie ist für viele Zwecke und Geschäftsmodelle sehr gut geeignet, für andere Anwendungsbereiche weniger gut. Es sollte daher für jeden Anwendungsfall abgewogen werden, ob es sinnvoll und verhältnismäßig ist, die technologie-bedingten Schwierigkeiten bei der Nutzung einer öffentlichen Blockchain für bestimmte Anwendungsbereiche durch Anpassung des Rechts oder durch Modifizierung der Technologie zu überwinden.

Ggf.: Wie könnte ein solches technisches und regulatives Regime aussehen?

Bitkom Stellungnahme:

Siehe hiervor. Ein Regime müsste vorgeben, dass jede Transaktion mit einer dazu inversen Transaktion überarbeitet werden kann.

Rechtliche Fragestellungen c) Smart Contracts

Smart Contracts ermöglichen die selbständige Prüfung vordefinierter Ereignisse und die Ausführung von Transaktionen. Damit kann ein Smart Contract rechtlich relevante Handlungen abhän-

gig von digital prüfbaren Ereignissen steuern, kontrollieren und dokumentieren. Darüber hinaus könnten Smart Contracts theoretisch zu einer höheren Vertragssicherheit gegenüber der herkömmlichen Vertragserfüllung und zu einer Reduktion der Transaktions- und Rechtsdurchsetzungskosten führen, sodass die Erfüllung automatisch bei Eintritt der dafür vereinbarten Bedingungen erfolgt.

Die Anwendbarkeit von Smart Contracts ist aber in mehrfacher Hinsicht beschränkt:

(1) Die durchzuführende Leistung muss digital abbildbar sein. Ein »analoges« Ereignis kann durch die Blockchain nicht ausgeführt werden (bspw. Hardware-Reparatur Kfz).

(2) Es muss sich um ein digital erfassbares Ergebnis handeln. So kann überprüft werden, ob eine Zahlung eingegangen ist (true/false), und dann die rechtlich daran anknüpfende Handlung veranlasst werden (bspw. Betriebsbereitschaft eines Kfz herstellen). An ihre Grenzen geraten Smart Contracts, wenn das zu prüfende Ereignis mit unbestimmten Rechtsbegriffen verknüpft ist (bspw. Ablauf einer angemessenen Frist).

(3) Es können nur die Rechte vollzogen werden, die im Voraus im Smart Contract angelegt worden sind. Vergleichbar mit Standardverträgen können auch standardisierte »Wenn-dann-Bedingungen« in der Blockchain immer nur einen Ausschnitt denkbarer Lebenssachverhalte abbilden.

Smart Contracts können daher dort zum Einsatz kommen, wo ein geringes Risiko von »Vertragsabweichungen« besteht oder wo der Smart Contract selbst über Möglichkeiten verfügt, Schlechtleistungen auf Programmcodeebene abzuwickeln.

Aufgrund der Limitationen der Blockchain braucht es eine Art Schnittstelle (»Orakel«), die Begebenheiten aus der nicht-digitalen Welt recherchiert und verifiziert und diese Informationen der Blockchain, zum Beispiel für die Nutzung in Smart Contracts, zur Verfügung stellt und damit eine Sachverständigen- oder Notariatsfunktion hat. Diese Schnittstelle kann gegebenenfalls eine Rechtsdurchsetzung innerhalb der Blockchain erleichtern. [1]

Komplexe Smart Contracts sind – vor allem für Laien – bisher kaum nachvollziehbar. Dies gilt insbesondere für Blockchains mit mächtigen Smart-Contract-Sprachen wie Hyperledger und Ethereum (bis hin zu einer DAO). Um die Nutzbarkeit zu verbessern, sollten Möglichkeiten einer einfachen Nachvollziehbarkeit und einer automatisierten Prüfung beziehungsweise formalen Verifikation von Smart Contracts entwickelt und erforscht werden. Schließlich sollte jeder Vertragspartner qualifiziert beurteilen können, worauf er sich einlässt. Generell besteht ein hoher Bedarf an Forschung und Entwicklung im Bereich sicherer Smart Contracts – sowohl beim Einsatz formal verifizierbarer Sprachen als auch in der Unterstützung von Entwicklern und der Validierung von Code vor der Aufnahme in die Blockchain. Zudem müssen Smart Contracts sicher gegen Angriffe wie Reentrancy sein. In der Praxis ist dies nur »mit Aufwand« sicherzustellen.

Um im Bereich der Normung bei Smart Contracts eine gemeinsame Sprache zu schaffen und diese sicherer zu gestalten, hat sich im letzten Jahr die Working Group 3 »Smart contracts and

their applications« unter dem ISO/TC 307 gebildet. Dort wird derzeit aktiv an dem Projekt ISO/TS 23259 »Legally binding smart contracts« gearbeitet, das Modelle, Komponenten, Strukturen und Arbeitsabläufe für die Erstellung von Smart Contracts festlegt.

Bitte geben Sie Ihre Stellungnahme zu Smart Contracts ein:

Bitkom Stellungnahme:

Smart Contracts sind ein essentieller Bestandteil der Blockchains, um einen Mehrwert aus der manipulationssicheren Datenspeicherung zu ziehen. Durch Smart Contracts können Prozesse durch vordefinierte, automatisierte Abläufe effizienter gestaltet werden. Im ersten Schritt ist jedoch die Vorgabe von Parametern für Smart Contracts durch die beteiligten Personen unumgänglich. Sobald Abweichungen vom vorgegebenen Prozessablauf auftreten, sollte durch die beteiligten Personen entschieden werden, wie diese Abweichungen zu bewerten sind.

Mit der Einführung von Smart Contracts auf Blockchain-Basis wird in einer Kombination mit dem Internet der Dinge zumindest für die Anwendungsdomäne Logistik und Supply Chain Management die Vision einer Industrie 4.0 Wirklichkeit: die Dinge bewegen sich nicht nur autonom entlang von Supply Chains, sondern interagieren autonom miteinander im Rahmen der von den handelnden Akteuren definierten Parametern/Smart Contracts.

Da »Smart Contracts« frei definierbaren Code enthalten, wird sich die Lesbarkeit des einzelnen Ablaufs für Nicht-Programmierer in Grenzen halten. In einigen Implementierungen wird der Code aus Sicherheitserwägungen Nutzern gegenüber nicht zugänglich gemacht, sondern obliegt den Tests im Rahmen der vereinbarten Governance-Struktur. Es wird derzeit aber auch rege an Hilfestellungen für die Definition von Vertragskonstrukten für Nicht-Programmierer gearbeitet, Beispiel: Projekt ACCORD ↗https://www.accordproject.org

Sollte es Regelungen für Smart Contracts in unserer Rechtsordnung geben bzw. wie kann man sicherstellen, dass sich Smart Contracts einer Rechtsordnung und wesentlichen rechtsstaatlichen Grundgedanken unterordnen?

Bitkom Stellungnahme:

Insgesamt sind keine Sonderregeln erforderlich. Es sollte weiterhin ein einheitliches, technologieneutrales Recht geben, dem sich selbstverständlich auch die Blockchain-Technologie unterordnet. Für eine bessere Akzeptanz könnten zumindest Erklärungen dazu abgegeben werden, inwiefern smart contracts rechtlich einzuordnen sind. Außerdem wäre insgesamt die Entwicklung von Sprachen, die smart contracts ohne Programmierkenntnisse nachvoll-

ziehbar machen und nur die Vertragslogik formalisiert abbilden, für die breite Akzeptanz sehr hilfreich. Dies muss jedoch die Wirtschaft richten.

Wie kann eine transparente Vertragsgestaltung und -abwicklung (insbesondere für Verbraucher) gewährleistet werden?

Bitkom Stellungnahme:

Ein Smart Contract ist wie ein Automat, in der Regel wird es einen vorgeschalteten Vertrag (»Nutzungsbedingungen« etc.) geben, der Leistung und Gegenleistung festlegt. Für Verbraucher haben auch in diesem Kontext die entsprechenden rechtlichen Sonderbestimmungen zu gelten. Benutzeroberflächen müssen Inhalt und Ablauf des jeweiligen Smart Contract einfach und transparent erklären können.

Über die Autorisierung von Verbrauchern über Light Nodes, könnten diese auf bestimmte Bereiche der Blockchain lesend zugreifen. Damit wird eine Transparenz auch bei privaten Blockchains gewährleistet. Jegliche Entscheidung kann somit transparent und nachvollziehbar aufgezeigt werden.

Wie ist die grenzüberschreitende Wirksamkeit von Smart Contracts zu bewerten (z.B. bei internationalen Lieferketten)? Ist eine Vereinheitlichung internationalen Rechts erforderlich?

Bitkom Stellungnahme:

Ein einheitlicher Rechtsrahmen, auf den bei Bedarf zurückgegriffen werden kann, kann hilfreich sein. Ein gutes Beispiel ist insofern das UN-Kaufrecht (CSIG), das für den internationalen Handel von erheblicher Bedeutung ist. Allgemein sind auch natürlich auch so schon Rechtsgeschäfte zwischen Landesgrenzen möglich. Ähnliche Rechtsansichten vereinfachen dies jedoch.

Sollte es ein Zertifizierungsverfahren für Smart Contracts im Hinblick auf die versprochenen Funktionalitäten und die Cybersicherheit geben?

Bitkom Stellungnahme:

Sobald sich diese Technologie in einem breiteren Sinne durchsetzt, wird das sicherlich Sinn machen.

Rechtliche Fragestellungen d) Ersetzbarkeit von Intermediären

In einer Reihe von rechtlichen Konstruktionen spielt ein unabhängiger Intermediär eine entscheidende Rolle. Beschränkt sich die Funktion des Intermediärs auf die bloße Vermittlung, könnte diese Funktion durch die Blockchain ersetzbar sein. Anderes gilt, wenn die Intermediäre wie ein Notar neben der Vollzugs- auch eine Beratungsfunktion haben oder sie zusätzlich bestimmte Risiken absichern. So wird zum Beispiel im Kapitalmarktbereich durch die Beaufsichtigung von Intermediären unter anderem Marktintegrität und Anlegerschutz sichergestellt.

Bitte geben Sie Ihre Stellungnahme zur Ersetzbarkeit von Intermediären ein:

Bitkom Stellungnahme:

Ein Intermediär wird in Geschäftsbeziehungen häufig dazu eingesetzt, um die Interaktion zwischen den Geschäftspartnern zu verifizieren. Dies soll nachträgliche Manipulationen ausschließen und die Integrität der Daten sicherstellen. Durch die Manipulationssicherheit und Redundanz der in der Blockchain gespeicherten Daten, kann diese Integrität durch die Technologie sichergestellt und von jedem Teilnehmer direkt nachvollzogen werden. Somit wird die Blockchain zur vertrauenswürdigen Technologie, mit der Transaktionen ohne klassische Intermediäre ausgeführt werden können. Darin ist ein großes disruptives Potential z.B. für das traditionelle Bankengeschäft zu sehen.

Ggf. werden jedoch auch neue Intermediäre im Zuge der Blockchain-Technologie entstehen, mit neuen Funktionen und Strukturen.

Gibt es bereits Konzepte, wie dezentrale Handelsplattformen beaufsichtigt werden können?

Bitkom Stellungnahme:

Beispielsweise, indem ein »Live Monitoring« von Transaktionen auf der Blockchain erfolgt. Dieses Live Monitoring kann regulatorische Überwachung umfassen, aus der dann entsprechende Maßnahmen abgeleitet werden.

Welche Möglichkeiten gibt es, die Funktion von Intermediären anderweitig sicherzustellen?

Bitkom Stellungnahme:

Hinsichtlich der Vertrauenswürdigkeit von Verfahren oder Transaktionen und Daten faktisch nicht, da spätestens beim Authentizitätsnachweis von Transaktionen und Beteiligten der Rückgriff auf Werkzeuge vertrauenswürdiger Dritter (Identifizierung, digitale Identitäten, Vertrauensdienste) notwendig ist. Allerdings sind Mischformen denkbar wie bspw. eine öffentliche Blockchain, ergänzt um Mittel zur sicheren Identifizierung sowie Authentisierung, Authentizitäts-/Integritätsnachweis und Vertrauenswürdigkeit der Transaktionen (TrustServices gem. eIDAS).

In welchen Bereichen sollte auf einen Intermediär nicht verzichtet werden und warum?

Bitkom Stellungnahme:

Intermediäre haben besonders im B2B auch mit Blockchains eine nicht zu vernachlässigende Rolle. Immer dann, wenn Fragen zur Identität in Blockchain-Netzwerken beantwortet werden müssen, also z.B. für den klassischen Know-Your-Customer-Prozess (KYC) sind Intermediäre (heute) notwendig.

In allen Fällen, in denen die Transaktionen Dokumentations- und Nachweispflichten gegenüber Prüfinstanzen, Gerichten, Dritten unterliegen und damit Authentizität, Integrität und Nachvollziehbarkeit der Prozesse anhand der geschäftsrelevanten Aufzeichnungen inkl. Transaktionsdaten notwendig ist. Hierfür liegen rechtsverbindliche wie technisch hochstandardisierte und etablierte Mechanismen (Identifizierung, Authentisierung, digitale Identitäten, TrustServices/TSP, Bewahrung/Langzeitarchivierung, Beweiswerterhaltung, Dateninteroperabilität) und Verfahren (Notifizierung/Zertifizierungsverfahren in eIDAS, GoBD, Fachgesetzen etc.; Prüfung durch unabhängige Personen wie Notare, Prüfstellen) sowie entsprechende Infrastrukturen (Certification Authorities) vor. Blockchain kann dies als sicheres wie dynamisches Register ergänzen – eine reine Technologie erzeugt, ohne konkrete Kriterien und rechtlich wie technisch geprüfte und durch Dritte nachprüfbare und damit zertifizierte Standards keine Vertrauenswürdigkeit, die den Ersatz von Intermediären rechtfertigen würde. Vielmehr könnten nachprüfbare Kriterien entwickelt werden unter deren Voraussetzung eine Blockchain vertrauenswürdig sein kann. Ebenso sind Mischformen denkbar wie bspw. eine öffentliche Blockchain ergänzt um Mittel zur sicheren Identifizierung sowie Authentisierung, Authentizitäts-/Integritätsnachweis und Vertrauenswürdigkeit der Transaktionen (TrustServices gem. eIDAS).

Rechtliche Fragestellungen e) Datenschutz (insbesondere Anforderungen nach der DSGVO)

Öffentliche Blockchains: Öffentliche Blockchains werfen eine Reihe von datenschutzrechtlichen Fragestellungen auf, insbesondere im Hinblick auf ihre Transparenz, das heißt jeder Teilnehmer kann diese vollständig einsehen, und im Hinblick auf die Unveränderlichkeit der gespeicherten Daten.

So sind in einer öffentlichen Blockchain die Transaktionen identifizierbar und verfolgbar, auch wenn durch die Verwendung von kryptografischen Verfahren eine Pseudonymisierung erfolgt. Nutzt der Teilnehmer Dienste wie Bitcoin-Marktplätze, gibt er durch seine Anmeldung seine Identität preis. Darüber hinaus ist es möglich, mit Hilfe von Big-Data-Analysen auch über frei verfügbare Analysetools Blockchain-Teilnehmer mit immer geringerem Aufwand zu identifizieren.

Soweit die Datenverarbeitung mittels einer Blockchain die Verarbeitung personenbezogener Daten umfasst, stellt sich zunächst die Frage, wer Adressat der datenschutzrechtlichen Verpflichtungen ist. Konzeptionell geht die DSGVO in erster Linie von einer zentralen Stelle mit Einflussmöglichkeit auf die Datenverarbeitung aus. Jedoch kennt das EU-Datenschutzrecht auch Situationen einer gemeinsamen Datenverarbeitungsverantwortlichkeit mehrerer Beteiligter. Demnach könnte jeder, der eine Kopie der Blockchain besitzt, als »Verantwortlicher« der Datenverarbeitung in Betracht kommen. Unklar ist, inwieweit dem einzelnen Blockchain-Teilnehmer der rechtliche und tatsächliche Einfluss auf das »Ob« und »Wie« der Datenverarbeitung möglich ist.

Rechtsfragen ergeben sich darüber hinaus auch im Zusammenhang mit den Informations- und Löschungsrechten/-pflichten aus der DSGVO. Ein Wesensmerkmal der Blockchain ist aber gerade ihre Unveränderlichkeit, demnach die Unmöglichkeit des nachträglichen Löschens eines Eintrages. Bei entsprechender Blockchain-Architektur könnte es möglich sein, obsolete Transaktionen aus älteren Blöcken zu entfernen, denn sie sind nicht mehr notwendig, um die aktuelle Berechtigung nachzuweisen und die Kette fortzuschreiben (sog. Pruning). Demnach wäre beispielsweise bekannt, dass in der Vergangenheit bestimmte Gesundheitsdaten erhoben wurden, die personenbezogenen Daten wären hingegen gelöscht. Hier sind Lösungsansätze denkbar, entweder nicht die Daten selbst in der Blockchain zu speichern, sondern nur eine Referenz mit Prüfsumme, oder eine verschlüsselte Speicherung der personenbezogenen Daten, bei der über die Blockchain dann jeweils die Zugriffsrechte verwaltet und dokumentiert werden. Derartige Lösungskonzepte werden zum Beispiel im Projekt ISÆN untersucht.

Private Blockchains: In privaten Blockchains kann möglicherweise – vorbehaltlich weiterer Analyse und Prüfung – ein Teil der datenschutzrechtlichen Fragestellungen durch geeignete vertragliche Ausgestaltungen und durch das Vorhandensein eines »Gatekeepers« zufriedenstellend beantwortet werden. Beim Kriterium der »Unveränderbarkeit« unterliegen jedoch private Blockchains ähnlichen datenschutzrechtlichen Herausforderungen wie öffentliche Blockchains.

Bitte geben Sie Ihre Stellungnahme zum Datenschutz ein:

Bitkom Stellungnahme:

Das Thema Datenschutz ist für einen breiteren Einsatz der Blockchain-Technologie eine entscheidende Hürde. Zwei Drittel der Unternehmen bewerten laut der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) die Anforderungen des Datenschutzes als Hemmnis für den Einsatz der Blockchain in ihrem Unternehmen.

Die elementare Weichenstellung ist folgende: Stellen Public Keys personenbezogene Daten i.S.v. Art. 4 Nr. 1 DSGVO dar?

- Sofern ein Public Key nur aus einer Zahlen- und/oder Buchstabenfolge besteht und die dahinterstehenden Nutzer aus sich heraus nicht erkennen lässt, ergibt sich eine Parallele zu IP-Adressen;

- IP-Adressen sind laut EuGH nur dann personenbezogen, wenn dem jeweils Verantwortlichen Mittel zur Verfügung stehen, die es unter Anwendung verhältnismäßigen Aufwands ermöglichen, einen Personenbezug herzustellen;

- Daraus folgt, dass eine bloße Individualisierbarkeit eines Betroffenen (ohne ihn zu identifizieren) nicht genügt, um einen Personenbezug zu bejahen;

- Diese Gedanken lassen sich auf Public Keys auf Blockchains übertragen; demnach ist zu fragen, ob solche Mittel zur Verfügung stehen;

Public Blockchains:

- Am Beispiel der Bitcoin-Blockchain ist dies etwa sehr kritisch zu hinterfragen;

- Insbesondere wäre dies für jeden Verantwortlichen gesondert zu bewerten;

- Falls dies im Einzelfall zu verneinen wäre (und auf der jeweiligen Blockchain keine anderweitigen, eindeutig personenbezogenen Daten gespeichert wären), wäre der Anwendungsbereich des Datenschutzrechts mangels Personenbezug nicht eröffnet.

- Nutzt der Teilnehmer Dienste wie Bitcoin-Marktplätze, kann es sein, dass er durch den Know-Your-Customer (KYC) Prozess seine Identität an die Börse o.ä. preisgeben muss (z.B. Coinbase oder Bison Börse) und die Börse diese Daten auch schützen muss. Es gibt jedoch auch Bitcoin-Marktplätze, wie Binance oder dezentralisierte Börsen (z.B. etherdelta.com) die keinen KYC durchführen. Hier könnten Teilnehmer jedoch mit Hilfe von IP-Adressen, Cookies, etc. identifiziert und getrackt werden. Wurden Bitcoins jedoch über Peer-to-Peer (z.B. localbitcoins.com) im Austausch von Bargeld erworben, so wird die nachfolgende digitale Verfolgung erschwert, da keine Identität offengelegt werden musste.

Public Blockchains: Im Falle von private Blockchains wird in der Regel entsprechendes Zusatzwissen über die Nutzer vorliegen, das deren Identifizierung zulässt.

Prinzipiell kommt es hier auf die Ausgestaltung der Blockchain-Lösung im konkreten Einzelfall an. Insofern sollte auf die Stellungnahme »Blockchain and the GDPR« des European union blockchain observatory & forum Bezug genommen werden. Private Blockchain-Lösungen sind

datenschutzrechtlich klar im Vorteil, da hier die Beteiligten bekannt sind, Datenschutzrechte adressiert werden können (da hier u.a. klar ist, wem gegenüber ein Auskunftsanspruch ausgeübt werden kann) und eingegrenzt werden kann, wo die Verarbeitung stattfindet (innerhalb/außerhalb der EU). Zudem kann hier durch Vereinbarung zwischen den Beteiligten besser festgelegt werden, wer Controller- bzw. Prozessorpflichten übernimmt, so dass Unklarheiten vermieden werden. Anwendungen zur Anonymisierung und Verschlüsselung werden zudem mit Hochdruck weiterentwickelt, so dass auch auf technischer Ebene Lösungen vorangetrieben werden.

Ist ein Personenbezug gegeben (Grundsatzfrage, elementare Weichenstellung), ergeben sich weitere wichtige Fragen bzgl. der Anwendbarkeit des Datenschutzes in der Blockchain-Technologie sind: Fragen der Verantwortlichkeit, der Zulässigkeit der Datenverarbeitung, der Einwilligung, der berechtigten Interessen, der Informationspflichten, oder der Betroffenenrechte. Für eine ausführlichere Betrachtung dieser Fragen verweisen wir hier gerne auf das Bitkom Faktenpapier »Blockchain und Datenschutz«, das über folgenden Link einsehbar ist: ↗https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html

Wie kann der Einsatz der Blockchain-Technologie kompatibel mit datenschutzrechtlichen Anforderungen (informationelle Selbstbestimmung) gestaltet werden?

Bitkom Stellungnahme:

Bei der Bejahung der Anwendbarkeit von datenschutzrechtlichen Vorschriften (vgl. oben) ist bei der Frage nach einem datenschutzkonformen Einsatz der Blockchain-Technologie wesentlich zu prüfen, welche Akteure überhaupt, und wenn ja wie weit Adressaten datenschutzrechtlicher Pflichten sind:

- Aus datenschutzrechtlicher Sicht ist dabei maßgeblich, ob ein Akteur als Verantwortlicher oder lediglich Auftragsverarbeiter zu klassifizieren ist;
- Dies ist zu bewerten für Programmierer, Nutzer, Miner, Nodes-Betreiber, Handelsplätze, Wallet-Anbieter;
- Dies lässt sich zunächst auf Mikro- und Makroebene betrachten und bewerten;
  - Auf **Mikroebene** ließe sich eine Transaktion zum einen etwa in einzelne, bilaterale Beziehungen zwischen sämtlichen an der Transaktion beteiligten Akteuren zerlegen. Die so entstehenden Einzelverbindungen bzw. Datenströme könnten sodann dahingehend bewertet werden, ob die jeweils beteiligten Akteure als Verantwortlicher oder Auftragsverarbeiter zu klassifizieren sind (eine Betrachtung auf Mikroebene wird jedoch in der Regel zu kleinteilig ausfallen und nicht die wahren Machtverhältnisse im Rahmen einer

Datenverarbeitungsreihe repräsentativ widerspiegeln; vgl. Art.29-Datenschutzgruppe, WP 169, S. 20 und 27);

- Auf **Makroebene** wäre eine Transaktion demgegenüber als »Vorgangsreihe« einheitlich zu betrachten und daher die Stellung der Akteure als Verantwortliche bzw. Auftragsverarbeiter innerhalb dieser Vorgangsreihe insgesamt zu bewerten:

Public Blockchains:

- Aus tradierter datenschutzrechtlicher Sicht sprechen gute Argumente dafür, Nutzer als Verantwortliche und Nodes als Auftragsverarbeiter zu bewerten. Dies führt jedoch zu erheblichen praktischen Problemen, da zwischen Nutzern und Nodes-Betreibern stets Auftragsverarbeitungsverträge nach Art. 28 DSGVO abgeschlossen werden müssten;

- Vor diesem Hintergrund erscheint zielführender, jeden Akteur als Verantwortlichen einzustufen. Dies entspricht auch eher den tatsächlichen Verhältnissen zwischen den einzelnen Akteuren: Die Miner werden weder bewusst von den Nutzern ausgewählt, noch erfolgt eine Überwachung der Miner seitens der Nutzer. Miner sind insofern mit Bankinstituten vergleichbar, die den Geldtransfer übernehmen. Miner und Nodes sind nicht an einen Nutzer gebunden; vielmehr suchen sich die Miner autark aus, welche Transaktion sie validieren. Insofern könnte sogar argumentiert werden, dass Miner noch weisungsfreier agieren können, als herkömmliche Kreditinstitute bei der Ausführung von Überweisungsaufträgen, wobei allgemein anerkannt ist, dass Kreditinstitute dabei als eigene Verantwortliche tätig werden (vgl. etwa BayLDA, ↗https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf). Ferner ist fraglich, ob eine Einstufung als Auftragsverarbeiter dem eigenen Verständnis bzw. der eigenen Wahrnehmung der Miner im Hinblick auf ihre Funktion entspricht. So wirkt eher fernliegend, dass dort die Vorstellung herrscht, im Auftrag und streng nach Weisung der Nutzer tätig zu werden.

Hierauf aufbauend stellt sich sodann zunächst die Frage der datenschutzrechtlichen Zulässigkeit der Verarbeitung von auf der Blockchain gespeicherten personenbezogenen Daten durch die jeweiligen Akteure:

- Sofern es sich um die Daten von Transaktionsauslösern und -empfängern handelt, wird in der Regel Art. 6 Abs. 1 lit. b DSGVO angeführt werden können, da die Verarbeitung erforderlich ist, um die Transaktion durchzuführen;

- Dies sollte für alle an der jeweiligen Transaktion beteiligten Akteure gelten, da die dezentrale Aufstellung der Blockchain elementarer Bestandteil einer solchen Transaktion ist und daher auch vom Verarbeitungszweck gedeckt und insbesondere vom Vorstellungsbild der Betroffenen (Auslöser und Empfänger) umfasst sein sollte;

- Aus gleichen Gründen sollte dies auch für die fortgesetzte Speicherung der Transkation gelten, da auch diese elementarer Bestandteil der Nutzung von Blockchain-Technologie ist;

- Soweit Daten Dritter (d.h. an der Transaktion Nichtbeteiligter) in der Blockchain gespeichert werden sollen, ist im Einzelfall zu prüfen.

Auch die Betroffenenrechte können in diesem Lichte betrachtet und ausgelegt werden; so kann etwa argumentiert werden, dass ein Löschanspruch nach Art. 17 DSGVO nicht durchgreift, da die Daten i.S.v. Art. 17 Abs. 2 lit. a DSGVO eben noch für den Verarbeitungszweck (Nachweisbarkeit der Transaktion) erforderlich sind;

Für Standardanwendungsfälle könnten die Informationspflichten nach Art. 13, 14 DSGVO etwa durch die Community selbst oder einen Verband (etwa in Form eines Code of Conducts nach Art. 40 DSGVO) formuliert und allen Nutzern zur Verfügung gestellt werden.

Private Blockchains: Im Falle von private Blockchains wird es in der Regel eine zentral administrierende Stelle geben, welche jedenfalls den Großteil der datenschutzrechtlichen Verantwortung tragen wird.

Durch welche Methoden können personenbezogene Daten hinreichend anonymisiert werden (Verschlüsselung, Verschleierung, Aggregieren etc.)?

Bitkom Stellungnahme:

Wie zuvor erörtert ist entscheidend, ob ein Personenbezug mit verhältnismäßigem Aufwand hergestellt werden kann. Demnach sind Hürden aufzustellen, die eine solche Identifizierung erschweren und letztlich unverhältnismäßig erscheinen lassen:

- Technische Hürden (Verhashung, physische Segregation usw.);

- Organisatorische Hürden (gesellschaftsrechtliche Trennung, Dienstweisungen, Audits usw.);

- Vertragliche Hürden (Zusammenführungsgebote, Vertragsstrafen usw.).

Anhand dieses Maßstabs sind die jeweils eingesetzten Anonymisierungsmethoden zu evaluieren; im Falle einer Verhashung ist daher maßgeblich, ob eine Rückrechnung des Hashwerts möglich ist, etwa sofern ein Akteur im Besitz des eingesetzten Hash-Algorithmus ist oder die Verhashung mit verhältnismäßigem Aufwand zurückgerechnet werden kann (Brute-Force-Angriff).

Daten können insgesamt auch »off-chain« gehalten werden, und somit lediglich über eine Verlinkung/einen Referenzwert »on-chain« referenziert werden.

Gibt es eventuell auf indirektem Wege Berührungspunkte mit der DSGVO, selbst wenn alle personenbezogenen Daten »off-chain« gespeichert werden?

Bitkom Stellungnahme:

Sofern eine Zuordnung der »on-chain« gespeicherten Informationen zu den »off-chain« gespeicherten personenbezogenen Daten möglich ist (etwa durch die Vergabe einer individuellen ID), sind ebenfalls die »on-chain« Daten als personenbezogenen anzusehen. Dies ist für jede datenverarbeitende Stelle gesondert zu prüfen, etwa sofern eine sichere Identifizierung/Authentisierung der Nutzer einer Blockchain gewährleistet werden soll, und die Identitätsdaten zwar »off-chain«, jedoch zuordenbar abgelegt werden.

Rechtliche Fragestellungen f) Formvorschriften

Durch die Blockchain können Transaktionen verifiziert sowie digitale Werte und Rechte übertragen werden. Um die Nutzung der Technologie zu diesem Zweck zu ermöglichen, wäre eine Anpassung der Formvorschriften notwendig. Hier ist das Recht gerade nicht technologieneutral ausgestaltet. Formvorschriften haben die Funktion, Beweisbarkeit und damit Rechtssicherheit zu schaffen. Inwieweit die neue Technologie die klassische Funktion der Schriftform als Beweiskriterium ersetzen kann, ist auch eine Frage der Sicherheit der neuen Technologie. Nach derzeitigem Stand gilt die Technologie aufgrund ihrer laufenden und transparenten Aktualisierung als sicher, sodass eine neben der Schriftform gleichwertige Anerkennung möglich erscheint.

Darüber hinaus ermöglicht die Blockchain die Tokenisierung verschiedenster rechtlicher Beziehungen, das heißt deren Abbildung und Repräsentation durch einen in der Blockchain gespeicherten Token. Ein naheliegendes Beispiel dafür ist die Tokenisierung von Wertpapieren. Dem stehen jedoch die bestehenden Formvorschriften entgegen, die bei Wertpapieren eine Verkörperung in einer physischen Urkunde verlangen. Die Bundesregierung prüft derzeit, ob auf diese Unterlagen verzichtet und eine elektronische Begebung von Wertpapieren zugelassen werden kann.

Bitte geben Sie Ihre Stellungnahme zu Formvorschriften ein:

Bitkom Stellungnahme:

Die entscheidende Frage ist die Prüfung bestehender Formvorschriften nach dem Erfordernis der Schriftform. In einem zweiten Schritt muss geklärt werden, inwiefern über die Blockchain der Normzweck einer Vorschrift mit einem Schriftformerfordernis erreicht werden und die Blockchain damit mit der Schriftform gleichgesetzt werden kann. In einem weiteren Schritt sollten entsprechende Rechtsnormen technologieneutral umgestaltet werden.

Wie jede andere Technologie, die zur Abwicklung vertrauenswürdiger digitaler Transaktionen eingesetzt wird, muss auch die Blockchain allgemein die Erfüllung geltender Formvorschriften und Nutzung geltender Beweiserleichterungen für die darin entstandenen und/oder verarbeiteten und gespeicherten geschäftsrelevanten Aufzeichnungen ermöglichen. Rechtlich und technisch sind in eIDAS die entspr. Möglichkeiten geschaffen worden und leichter umsetzbar. Wesentlich ist auch die Frage wie Daten, die in Blockchains abgelegt sind, als Beweismittel zur Nachweisführung vor Gericht/Prüfinstanz dienen können und damit deren rechtlich notwendige Verkehrsfähigkeit gewährleistet wird. Ein Austauschformat für Daten in Blockchains – eine reine Übertragung Blockchain zu Blockchain – ist weder in DSGVO noch ZPO etc. vorgesehen.

Was steht der Anerkennung von digitalen Nachweisen als gleichwertig mit der Schriftform entgegen?

Bitkom Stellungnahme:

Sehr wenig, soweit eine Blockchain-Transaktion mit einer elektronischen Signatur verbunden ist. Durch die seit rund 22 Jahren bestehende qualifizierte elektronische Signatur, deren Nutzung durch remote und mobile Signaturen ohne Signaturkarte im Zuge der eIDAS-Verordnung erheblich erleichtert wurde und mit dem qualifizierten Elektronischen Siegel auch eine Authentizitätsbestätigung für juristische Personen inkl. Nutzung von einem Siegelzertifikat durch n-berechtigte Nutzer eines Unternehmens hinzugekommen ist, können rechtsverbindliche Transaktionen leicht und nutzergerecht abgeschlossen werden. In Europa sind, mit Ausnahme Deutschlands (aufgrund der Fokussierung auf die Signaturkarte bis zum Inkrafttreten der eIDAS-Verordnung), qualifizierte eSignaturen und teilweise Siegel etabliert. Die Standardisierung, Harmonisierung (verbindliche Formate, Sicherheitsvorgaben etc. für TrustServiceProvider) und Anerkennungspflichten der eIDAS ermöglichen vertrauenswürdige Transaktionen auf einfache Art und Weise im digitalen Binnenmarkt. Die Blockchain-Technologie muss demgemäß die bestehenden Lösungen integrieren.

Kann die Blockchain die Textform ergänzen und hierfür zusätzliche Sicherheit hinsichtlich der Identitäten bieten?

Bitkom Stellungnahme:

Die Textform erfordert einen geschriebenen Text bspw. in Form einer Email. Dies kann von Blockchain als verteiltem Register nicht erfüllt werden, sondern nur durch eine entsprechende Textdatei. Der Bezug zwischen Erfüllung der Textform und digitalen Identitäten ist unklar – die Formvorschrift erfordert nicht den Einsatz einer digitalen Identität. Bei entsprechender Ausgestaltung kann die Blockchain die Textform aber natürlich ergänzen.

Welche Beispiele gibt es, bei denen bereits von dem Erfordernis der Schriftform abgewichen wurde?

Bitkom Stellungnahme:

Ein Beispiel ist das Wartungsheft bei Autos. Gut nutzbar wäre die Blockchain-Technologie auch für das Führen eines elektronischen Fahrtenbuchs (§ 8 Abs. 2 S. 4 EStG).

Rechtliche Fragestellungen g) Steuern

Gerade weil die Blockchain-Technologie Möglichkeiten eröffnet, Vermögenswerte digital kopier- und manipulationssicher abzubilden, entsteht auch ein Potenzial für damit zusammenhängende wirtschaftliche Dienstleistungen. An diese Transaktionen knüpft die Besteuerung an. Die differenzierte und sich rasch verändernde Vielfalt von Geschäftsmodellen auf Blockchainbasis ist eine Herausforderung für die jeweilige steuerliche Einordnung. Eine Regulierung schafft auch Rechtssicherheit in den steuerlichen Konsequenzen.

Bitte geben Sie Ihre Stellungnahme zu Steuern ein:

Bitkom Stellungnahme:

In wieweit eine Regulierung der Blockchain Rechtssicherheit bei der steuerlichen Beurteilung schaffen soll, ist nicht nachvollziehbar. Die Nutzung der Blockchain-Technologie hat keinen Einfluss auf die Besteuerung der zugrundeliegenden Geschäftsmodelle und Transaktionen. Die Blockchain-Technologie kann zur Durchführung von Transaktionen genutzt werden, das Steuerrecht hat jedoch immer den zugrundeliegenden wirtschaftlichen Vorgang zu beurteilen, egal, ob dieser über eine Blockchain, in einem Laden, oder über das Internet abgewickelt wird. Das Steuerrecht erfordert jedoch in vielen Zusammenhängen eine lückenlose, nachvollziehbare und manipulationssichere Dokumentation von wirtschaftlichen Vorgängen. Hierfür scheinen Blockchain-Technologien geradezu prädestiniert.

Blockchains v.a. mit überprüftem, vertrauenswürdigem Teilnehmerkreis können den Gang der Bearbeitung von Aufzeichnungen inkl. Zeitstempeln papierlos mit hoher Manipulationssicherheit festhalten. Nützlich erscheint dies nicht nur für neuartige Geschäftsmodelle, sondern zur

Einsparung bislang aufbewahrungspflichtiger Begleitdokumente bei zugleich verbesserter Prüfbarkeit durch Verknüpfung mit in der Blockchain festgehaltenen Liefer- und Zahlungsvorgängen.

Werden Rechtsgeschäfte über Blockchain gesteuert, veranlasst oder dokumentiert, so bedarf dies keine gesonderte Besteuerung, da die Rechtsgeschäfte bereits besteuert sind.

Wie sind die – wirtschaftlichen – Ergebnisse der an (Trans)Aktionen Beteiligten umsatz- und ertragsteuerlich einzuordnen?

Bitkom Stellungnahme:

Die Nutzung der Blockchain-Technologie hat keinen Einfluss auf die Besteuerung der zugrundeliegenden Geschäftsmodelle und Transaktionen. Die Besteuerung erfasst wirtschaftliche Vorgänge und erfolgt unabhängig davon, auf welchem Weg diese wirtschaftlichen Transaktionen durchgeführt werden. Dabei hat das Steuerrecht zu untersuchen, ob im Rahmen einer Transaktion wirtschaftliche Werte oder vermögenswerte Vorteile übertragen werden oder entstehen. Verbessern und vereinfachen kann die Nutzung von Blockchain-Technologien v.a. die Erfüllung von Dokumentations- und Nachweispflichten, z.B. den Nachweis von Vollständigkeit und Manipulationsfreiheit von digitalen Aufzeichnungen, Unterlagen und Belegen: Kassenbücher und Lieferketten lassen sich so abbilden, dass z.B. Lücken und Karussellgeschäfte erschwert und somit einheitliche Steuererhebungen erleichtert werden, ohne Dokumentationspflichten und Haftung anderen Marktteilnehmern aufzubürden. Rechtliche Schwebezustände sind ausgeschlossen.

Insgesamt sollte die Blockchain technologieneutral behandelt werden, sodass Ergebnisse wie bei anderen Rechtsgeschäften zu besteuern sind.

Aus steuerrechtlicher Sicht ergibt sich vor allem die Frage der Erfüllung der Maßgaben nach GOBD und hier Z3 (Datenträgerüberlassung) gegenüber dem Steuerprüfer. Dies erscheint in Blockchain derzeit nur bedingt umsetzbar. In blockchainbasierten Transaktionen entstehende Daten dürften den Vorgaben nach §§ 147 AO und 238 ff. HGB unterliegen, womit sich die Frage der maschinellen Auswertbarkeit durch Drittverfahren stellt.

4 Praxisbeispiele

4 Praxisbeispiele

Zum Abschluss des Konsultationsprozesses haben Sie die Möglichkeit, auf Projekte hinzuweisen, bei denen die Blockchain-Technologie bereits erfolgreich genutzt wird:

Auf welche guten Beispiele aus der Praxis möchten Sie hinweisen?

Ort (inklusive PLZ), Organisation, Ansprechpartner, Kurzbeschreibung des Praxisbeispiels:

Bitkom Stellungnahme:

Neben den zahlreichen Praxis-Projekten, auf die im Zuge der Konsultation bereits verwiesen wurde, könnten an dieser Stelle beliebig viele weitere genannt werden. Es handelt sich demnach lediglich um eine Auswahl von Blockchain-Praxisbeispielen aus Unternehmen und Forschungseinrichtungen.

- Maersk und IBM, TradeLens: Intermodaler Transport von Containern und Prozessieren der Frachtpapiere über Blockchain: ↗https://www.tradelens.com/
- Bayreuth, Tennet, Einsatz der Blockchain zur Stabilisierung des Stromnetzes über die Einspeisung von Batteriespeichern: ↗https://www.tennet.eu/de/unsere-kernaufgaben/innovationen/blockchain-technologie/
- Daimler und LBBW, Blockchain Einsatz bei Schuldschein-Transaktion. Begebung eines Schuldscheindarlehens über Blockchain- Technologie in Höhe von 100 Mio. € mit Laufzeit von einem Jahr als Pilotprojekt für Kapitalmarkt-Transaktionen und Finanzprozesse: ↗https://media.daimler.com/marsMediaSite/de/instance/ko/Daimler-und-LBBW-setzen-erfolgreich-Blockchain-bei-Schuldschein-Transaktion-ein.xhtml?oid=22744703
- IBM »Foodtrust«, Blockchain Einsatz für die sicherer Lebensmittelkette in der Lieferkette, produktiv seit Oktober 2018: ↗https://www.ibm.com/de-de/blockchain/solutions/food-trust
- Mercedes-Benz Cars und Icertis, Transparenz in Bezug auf Arbeitsbedingungen, Menschenrechte, Umweltschutz, Sicherheit, Geschäftsethik und Compliance innerhalb der Lieferkette: ↗https://www.produktion.de/wirtschaft/wie-daimler-mit-blockchain-die-lieferkette-revolutioniert-109.html
- Köln, GS1 Germany, Dirk Freda, Digitalisierung des Palettenscheins. Basierend auf einem umfassenden Pilotprojekt im Jahr 2018 (Ergebnisbericht: ↗https://www.gs1-germany.de/innovation/trendforschung/blockchain/pilot/). 2019 soll eine produktive Lösung geschaffen werden.

- Plastic Bank, Einsatz der Blockchain für ein Anreizsystem und Bezahlung von Plastikmüllsammlung: ↗https://www.plasticbank.com/de/was-wir-tun/

- Northern Trust, Blockchain Einsatz zur Private Equity Fund Verwaltung ↗https://www.northerntrust.com/news-financial-statement/press-release?c=871cebb-9540c342982bc2280ef89af84

- Referenzkunde BAMF: »Blockchain powered Flüchlingsverfahren«-Projekt: Verbesserung der behördenübergreifenden Zusammenarbeit durch Sicherheit und Einheitlichkeit von Daten mittels Blockchain.

- Deutsche Telekom, City Pass Showcase: Der Telekom City Pass ist ein offenes und dezentrales Ökosystem für Smart Cities. Es vereinfacht die Nutzung von städtischen Diensten, indem es einen einheitlichen, standardisierten Zugang und Zahlung bietet. Die Nutzer können alle angebotenen Dienste (z.B. Bibliothek, Fahrradhaltung) über eine Smartcard oder mobile App nutzen und bezahlen.

Weitere Blockchain-Netzwerke und Projekte sind z.B. über das Unbounded Register zu finden, über welches auch Kontakt zu den Netzwerken aufgenommen werden kann: ↗https://unbounded.network/?Lang=de

Zudem sind auch am Ende der Bitkom-Studie »Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen« (2019) noch einige ausführliche Anwendungsbeispiele der Blockchain-Technologie in der Praxis näher vorgestellt.

Zahlreiche Praxisbeispiele und Projekte finden auch im Kontext von/in Zusammenarbeit Forschungseinrichtungen und Universitäten statt.

- Aachen, RWTH Aachen, Campus Cluster Smart Logistik, David Holtkemper, mehrere Projekte:
  1. Demonstrator mit Fischertechnik, welcher in eine reale Blockchain schreibt.
  2. Demonstrator mit mehreren ERP-Systemen, welche eine unternehmensübergreifende Wertschöpfung simulieren und über eine Blockchain kommunizieren (in Entwicklung).
  3. In Zusammenarbeit mit der e.GO Mobile AG, digitale Fahrzeugakte in welche Daten aus Produktion und After Sales geschrieben werden (Scheckheft gepflegtes Auto).

- Dortmund, IML Fraunhofer, Claas, Diebold Nixdorf, Ekol, Forschungsprojekt SOFiA (Smart Objects und Smart Finance), Ansprechpartner Dominik Sparer: Im Rahmen des Forschungsprojekt SOFiA zwischen dem Fraunhofer IML, Claas, Ekol und Diebold Nixdorf wurde bereits eine Blockchain-Testumgebung entwickelt und implementiert. Mit dieser Umgebung ist es möglich, sowohl den Material- als auch den Finanzfluss transparent und vor allem sicher darzustellen. Dies erlaubt die Automatisierung unterschiedlichster Prozesse über die Implementierung von Smart Contracts. Zur vollständigen Aufnahme und Auswertung des Prozessablaufs musste auch der Zahlungsvorgang über die Smart Contracts auswertbar sein. Da die Abwicklung der Vergütung über Kryptowährungen für die beteiligten Unter-

nehmen keine akzeptable Alternative darstellte, wurde eine Payment Cloud entwickelt, die über eine digitale Schnittstelle (EBICS) Transaktionen in Fiatgeld ermöglicht. Die dabei betrachteten Anwendungsfälle waren der Ernteprozess in der Landwirtschaft (Farming 4.0) und der Transportprozess in der Logistik.

- Dortmund, Fraunhofer IML, Commerzbank, Trade Finance Innovations Lab, Ansprechpartner Dr. Philipp Sprenger: Im »Trade Finance Innovations Lab« sollen neue Zahlungsverkehrs- und Finanzierungslösungen für das Handelsfinanzierungsgeschäft auf Basis innovativer Technologien wie zum Beispiel der Distributed-Ledger-Technologie (DLT), Smart Contracts und dem Internet der Dinge (Internet of Things, IoT) entwickelt und zur Marktreife gebracht werden. Gleichzeitig sollen Standards und Rahmenbedingungen für die Digitalisierung des internationalen Supply Chain Management und die entsprechenden Finanzierungsinstrumente aktiv mitgestaltet werden.

- Dortmund, Fraunhofer IML, Piel – Die technische Großhandlung, Forschungsprojekt TeHa DataBlock, Ansprechpartner Natalia Broza-Abut: Schnittstellenharmonisierung im technischen Handel mittels Blockchain. Unternehmensübergreifender elektronischer Datenaustausch mit Blockchain-basierter Lösung entlang kompletter Supply Chain eines KMU.

- Dortmund, Fraunhofer IML, Supply Chain Finance Community, Simon Hegele Gesellschaft für Logistik und Service, Europäisches Forschungsprojekt, Ansprechpartnerin Tanja Brink: Blockchain-basierte Finanzlösungen für Logistikdienstleister. Forschungsprojekt, in dem ein Blockchain-basiertes Supply-Chain-Finance-Konzept für Logistikdienstleister entwickelt wurde.

- Dortmund, Fraunhofer IML, Fraunhofer AISEC, Fraunhofer FIT, TrackChain Teilprojekt des Fraunhofer Dataspace (FDS), Ansprechpartner Sabine Jakob: Warenverfolgung mit gesicherten Orts- und Zustandsinformationen auf Basis der Blockchain. Lückenlose Verfolgung und manipulationssichere Speicherung ermöglicht unmittelbare Reaktion auf Vorfälle wie z.B. Beschädigung der Ware.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 400 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom