Bundesministerium
für Wirtschaft
und Energie

Bundesministerium
der Finanzen

Online-Konsultation zur Erarbeitung der Blockchain-Strategie der Bundesregierung

Einleitung

Die Bundesregierung hat sich zum Ziel gesetzt, eine umfassende Blockchain-Strategie zu erarbeiten. Um Hinweise und Expertenmeinungen in die Erstellung der Strategie einfließen zu lassen, wird eine Online-Konsultation durchgeführt. Schwerpunktmäßig werden die Stellungnahmen bundesweit arbeitender Verbände, Unternehmen, Organisationen und Institutionen berücksichtigt. Ein Anspruch auf Berücksichtigung aller Stellungnahmen besteht nicht. Um größtmögliche Transparenz zu gewährleisten, werden die Stellungnahmen unter Nennung der Organisation (ohne persönlichen Ansprechpartner) nach Ende des Konsultationsprozesses veröffentlicht, hierin willigen Sie stellvertretend für Ihre Organisation ein. Die finale Entscheidung über die Veröffentlichung einzelner Stellungnahmen obliegt den beiden Bundesministerien.

Inhalt

I. 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 Start-up- 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.

Möglichkeit zur Stellungnahme bezüglich der Relevanz der Blockchain-Technologie.

II. Blockchain-Technologie – Funktionsweise, Anwendungen, Potenziale

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 Kasten 1). 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)**, das heißt 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.

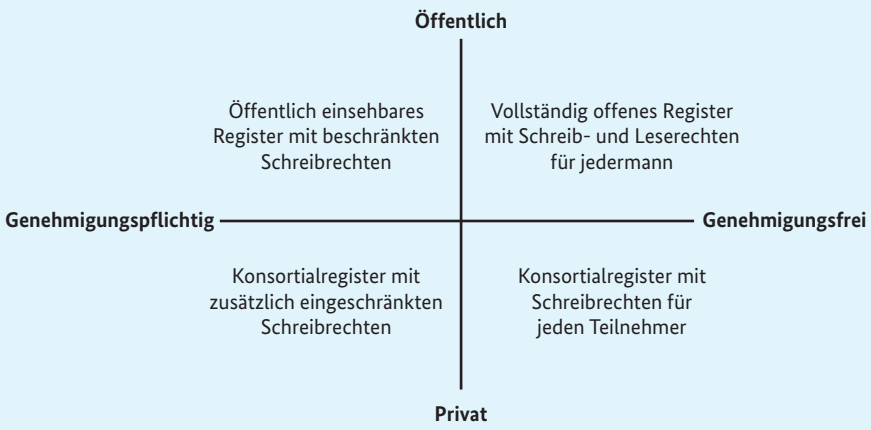
Smart Contracts sind ein wesentliches Merkmal der meisten Blockchain-Technologien, bei dem Transaktionen mit Programmcode zu sogenannten Smart Contracts verknüpft werden. Mit diesen lassen sich unter anderem Vertragsbeziehungen ganz oder teilweise abbilden und auch ganz oder zum Teil vollautomatisch 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.

Kasten 1: Blockchain-Baukasten

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:[1]

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.

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:

Möglichkeit zur Stellungnahme bezüglich der Anwendungsfelder.

a) Finanzsektor

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 Start-ups 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 Start-ups 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, d.h. 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 Handelbarkeit 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 diezugrundeliegenden 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 (z. B. 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.

Möglichkeit zur Stellungnahme bezüglich des Themengebietes Kryptowährungen, Token und ICOs.

Fragen:

- Gibt es – außerhalb der Spekulation – nachhaltige Anwendungsmöglichkeiten für Kryptowährungen?
- Ist die Token-Emission eine zukunftsfähige Form der Unternehmens- und Projektfinanzierung bzw. unter welchen Rahmenbedingungen könnte sie sich dazu entwickeln?
- Welcher Mehrwert und welche Hindernisse bestehen bei der Tokenisierung klassischer Wertpapiere?
- Teilen Sie die Einschätzung, dass sich ICOs mit Utility-Token und Kryptowährungen primär zur Finanzierung dezentralisierter Blockchainprojekte eignen? Welche weiteren sinnvollen Finanzierungsbereiche sehen Sie?
- Welche Tokenarten werden den Markt der ICOs in den nächsten 5 Jahren dominieren?
- Welche Missbrauchsrisiken bestehen? Welche Risiken bestehen für Kleinanleger?
- Sollte die Emission von Utility-Token und Kryptowährungen reguliert werden? Sollte diese Regulierung auf europäischer oder auf nationaler Ebene erfolgen?
- Welche inhaltlichen Aspekte (zum Beispiel Anlegerschutz, Marktintegrität (insbes. bzgl. Insiderhandel und Kursmanipulation), Handelstransparenz, Erlaubnispflichten für bestimmte Dienstleistungen) sollte eine etwaige Regulierung von Kryptowährungen und Token adressieren?
- Wie werden Potenziale von Kryptowährungen, die an Realwährungen gekoppelt sind, also sogenannte stable coins, bewertet?

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.

Möglichkeit zur Stellungnahme bezüglich der Anwendungen in der Finanzwirtschaft.

Fragen:

- In welchen Anwendungsbereichen im Finanzsektor sind Blockchain-Anwendungen bereits im produktiven Einsatz bzw. wo werden sie in absehbarer Zeit zum Einsatz kommen?
- Zu welchen Erkenntnissen hat die Erprobung geführt mit Blick auf den zukünftigen Einsatz der Blockchain als Alternative zu bestehenden Systemen?
- Wie ist die deutsche Finanzwirtschaft im Vergleich zur Finanzwirtschaft in Europa, USA und Asien im Bereich Blockchain-Technologie positioniert?

b) Energie

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.

Möglichkeit zur Stellungnahme bezüglich des Themengebietes Energie, insbesondere Stromhandel.

Fragen:

- Welche besonders relevanten/geeigneten Anwendungsfälle werden im Energiebereich gesehen?
- Welche Erfahrungen konnten mit Blockchain-basierten Anwendungen im Handel von Strom und Gas gewonnen werden?
- 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?
- Welche Regulierungsanforderungen bestehen an die Ausgestaltung der Blockchain-Technologie für einen Einsatz im Strommarkt?
- Mit welchen Maßnahmen könnte und sollte der Energiesektor auf die Dezentralisierung von Wirtschaftsbeziehungen ausgerichtet werden?
- Können energiewirtschaftliche Regulierungspflichten wie die Bilanzkreisverantwortung implementiert werden?
- Ist der Anbieterwechsel ein geeigneter Anwendungsfall für Blockchain? Gibt es Hindernisse? Gibt es weitere Anwendungsfälle?
- Welche Schätzungen gibt es zur Energie- und Klimabilanz des Einsatzes von Blockchain-Technologie im Energiesektor (auch im Vergleich mit alternativen Maßnahmen)?

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 (Redispatch). 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.

Möglichkeit zur Stellungnahme bezüglich des Themengebietes Stromnetze.

Fragen:

- Ergeben sich Risiken für kritische Netzinfrastrukturen durch dezentralen Stromhandel?
- Welche Auswirkungen werden durch den Einsatz von Blockchain auf die Bepreisung von Strom sowie die Finanzierung und die Regulierung der Netze gesehen?
- Welche Auswirkungen werden durch den Einsatz von Blockchain auf die Versorgungssicherheit und die Integration von erneuerbaren Energien gesehen?
- Welcher zusätzliche nationale Stromverbrauch ergäbe sich durch eine ausgeweitete Nutzung der Blockchain-Technologie? Wären Netzkapazitäten hierfür ausreichend ausgelegt?
- Können dezentrale Kleinspeicher mittels Blockchain zu einem virtuellen Großspeicher zusammengeschaltet werden?
- Kann eine lokale just-in-time Vermarktung von Strom zur Stabilität des Stromnetzes beitragen?

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 schutzwürdige Interessen der Patientinnen und Patienten im Vordergrund.

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Gesundheit/Pflege.

Fragen:

- Welche Anwendungsfälle gibt es im Bereich Gesundheit/Pflege?
- Zeigt die Blockchain-Technologie für diese Anwendungsfälle einen Mehrwert gegenüber herkömmlichen Technologien?
- Welche rechtlichen und organisatorischen Herausforderungen gibt es beim Einsatz in diesen Bereichen?
- Wie könnten datenschutzrechtskonforme Lösungen zur Anwendung von Blockchain aussehen, vor dem Hintergrund der besonderen Anforderungen im Umgang mit Gesundheitsdaten?
- Gibt es ethische Bedenken, die sich aus einer Ansammlung von Gesundheitsdaten in einer Blockchain ergeben?

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 zum Beispiel 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.

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Mobilität.

Fragen:

- Welche Anwendungsfälle im Bereich der Mobilität zeichnen sich ab (zum Beispiel im Bereich des automatisierten und vernetzten Fahrens, der Erhebung von Straßenbenutzungsgebühren, der intermodalen Transporte (Personen und Güter))?
- Wird gesetzlicher Handlungsbedarf im Bereich der Mobilität gesehen, um Blockchain-basierte Mobilitätslösungen massenmarktfähig einzusetzen?
- Inwiefern sollten Blockchain-basierte Mobilitätslösungen auf staatlichen Infrastrukturen aufsetzen? Welche Rolle könnte der geplanten europäischen Blockchain-Services-Infrastruktur dabei zukommen?
- Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?
- 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?

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.

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Lieferketten/Logistik.

Fragen:

- Welche Anwendungsfälle bzw. auch Projekte im Regeleinsatz gibt es für die Logistik?
- Welche Anreize und Hindernisse bestehen bei der Etablierung einer Blockchain im Lieferketten-Bereich sowohl national als auch international?
- Gibt es – wenn ja, welche – insbesondere rechtliche und organisatorische Herausforderungen beim Einsatz in diesem Bereich?
- 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?
- Welche Schnittstellen oder sonstigen technischen und rechtlichen Voraussetzungen werden benötigt, um anbieterübergreifende Bezahlvorgänge zu ermöglichen?

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.

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Internet der Dinge.

Fragen:

- Welche Technologien haben ähnliche Funktionalitäten wie die Blockchain, um im Bereich IoT eingesetzt zu werden?
- Welche rechtlichen und technologischen Hindernisse gibt es beim Einsatz von Blockchains im Bereich IoT?
- Welche Herausforderungen bestehen hinsichtlich der Interoperabilität?
- Sind Blockchains auf die großen Datenmengen im IoT-Bereich skalierbar? Falls ja, welche Varianten sind hierfür besonders geeignet?
- Wie kann sichergestellt werden, dass der Übertrag von nicht automatisch digitalisierten IoT-Daten auf die Blockchain und in Smart Contracts fehlerfrei erfolgt?
- Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

g) Identitäten-/Rechtemanagement

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.

Möglichkeit zur Stellungnahme bezüglich des Themengebietes Digitale Identitäten.

Fragen:

- Welche Aufgaben kann bzw. sollte der Staat bei der Bereitstellung rechtssicherer digitaler Identitäten übernehmen?
- Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?
- Welche Akzeptanzkriterien sind bei dezentralem Identitätsmanagement durch Bürgerinnen, Bürger und Unternehmen zu berücksichtigen?
- Wie kann ein eindeutiger, rechtssicherer Identitätsnachweis erfolgen und Missbrauch verhindert werden?

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 (zum Beispiel 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.

Möglichkeit zur Stellungnahme bezüglich des Themengebietes Urheberrechte.

Fragen:

- Gibt es konkrete Blockchain-basierte Lösungen im Bereich Urheberrecht?
- Sind diese Lösungen den herkömmlichen Lösungen überlegen?
- Welche Geschäftsmodelle stehen hinter den Lösungen?
- Könnte die Blockchain-Technologie zu einer Neudefinition der Rolle der Urheberrechtsintermediäre führen?

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.

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Verwaltung.

Fragen:

- Welchen Mehrwert und welche Nachteile bietet eine verteilte Datenbank bei öffentlichen Registern?
- Welchen Grad an Zentralisierung braucht eine von der öffentlichen Verwaltung eingesetzte Datenbank?
- Für welche Anwendungen (Kommunikation mit den Bürgern, Dokumente/Ausweise, interne Behördenprozesse) bestehen die größten Potenziale?
- Welche Restriktionen ergeben sich bei der Anwendung von Smart Contracts im Hinblick auf die automatisierte Entscheidung rechtsverbindlicher Verwaltungsakte?
- Schließt der Rechtsrahmen einen Einsatz in bestimmten Anwendungsbereichen derzeit aus?
- Ergeben sich neue strategische Überlegungen bei der IT-Konsolidierung öffentlicher Netze?
- Welche Governance-Aspekte sind bei internationalen Blockchain-Anwendungen mit öffentlicher Beteiligung zu beachten?

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).

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Plattformökonomie.

Fragen:

- 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?
- Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?
- Welches Geschäfts- bzw. Betreibermodell sollte hinter einer Blockchain-basierten Plattformlösung stehen?
- Welche Rolle spielt Blockchain für den Aufbau von digitalen Genossenschaften („platform cooperatives“)?

III. Zentrale Fragestellungen der Blockchain-Technologie

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.

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[2]. 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.

Möglichkeit zur Stellungnahme bezüglich der Herausforderung der Skalierbarkeit.

Fragen:

- Welche Lösungsansätze für das Skalierbarkeitsproblem von (öffentlichen) Blockchains sind erfolgversprechend?
- Inwiefern kann den Herausforderungen der Skalierbarkeit durch Interoperabilität von Blockchains begegnet werden?
- Welche Hindernisse (technisch und verfahrensrechtlich) müssen zur Skalierung von bestehenden bzw. potenziellen Pilotprojekten überwunden werden?

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.

Möglichkeit zur Stellungnahme bezüglich der Herausforderung der Ineffizienz durch Redundanz.

Fragen:

- In welchem Maße konkurriert die Blockchain mit anderen Datenbanklösungen?
- In welchen Szenarien überwiegen die Vorteile der redundanten Datenspeicherung die Nachteile?
- Welche Lösungsansätze für das Redundanzproblem von Blockchains sind erfolgversprechend?

2 Guter Überblick über verschiedene Vorschläge zum Umgang mit der Skalierbarkeit bei Croman et al. (2016)

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[3] 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[4] 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.

Möglichkeit zur Stellungnahme bezüglich der Herausforderung der technischen Anforderungen.

Fragen:

- Welche Anforderungen bestehen, um die Integration von Blockchain-Lösungen in die Unternehmenstätigkeit, v. a. vor dem Hintergrund bestehender zentralisierter Systeme, zu ermöglichen?
- Sollte es ein Zertifizierungsverfahren für Blockchain-Technologien im Hinblick auf die versprochenen Funktionalitäten geben?

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.

Möglichkeit zur Stellungnahme bezüglich der Herausforderung der Interoperabilität.

Fragen:

- Welche Lösungen bzw. Lösungsansätze gibt es, um die Interoperabilität von Blockchains herzustellen? Wie „marktfähig“ sind derartige Lösungsansätze?
- Bringen bestimmte Mindeststandards einen „Mehrwert“ für alle Teilnehmer? Welche „Standards“ könnten das sein?

3 Smarte Orakel sind Module für Drittanbieterschnittstellen, die es erlauben, Daten in die Blockchain zu schreiben.

4 www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/iblockchain

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.

Möglichkeit zur Stellungnahme bezüglich der Herausforderung der Irreversibilität.

Fragen:

- Reicht es zur Erfüllung von Löschansprüchen oder -pflichten aus, Daten, zum Beispiel 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?

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[5] 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.

Möglichkeit zur Stellungnahme bezüglich der Herausforderung der IT-Sicherheit.

Fragen:

- Welche Anforderungen an die IT-Sicherheit eines Blockchain-Systems stellen technologiebedingt eine besondere Herausforderung dar?
- Wo und wie könnten „klassische“ Sicherheitsansätze (wie zum Beispiel eine Public Key Infrastructure) die Blockchain-Technologie ergänzen?
- Sollte es eine Sicherheitszertifizierung für Blockchain-Produkte geben?

5 www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf

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

2. 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 anwendungsbezogen 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" (unter anderem 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).[6] 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 Start-ups im Bereich der Blockchain-Technologie – 80 Prozent in den Wirtschaftsbereichen Finanz- sowie Informations- und Kommunikationstechnologien (IKT). Die meisten Blockchain-Start-ups sind im Finanz- und Versicherungssektor zu finden. Neben diesen FinTech-Start-ups ist der nächstgrößte Anteil der Blockchain-Start-ups im Informations- und Kommunikationssektor tätig. In Deutschland gibt es insgesamt rund 170 Blockchain-Start-ups, die meisten davon sind in Berlin ansässig (Stand: Februar 2019).[7]

6 www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html

7 www.chain.de/blockchain-startups/

Wagniskapital: In die in obiger Studie genannten 1.140 Start-ups 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 Milliarden US-Dollar an Wagniskapital in die Blockchain-Technologie investiert.[8] Gemäß einer Studie von EY belief sich das Gesamtvolumen der Kapitalaufnahme 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)[9].

Möglichkeit zur Stellungnahme bezüglich des ökonomischen Potenzials.

Fragen:

- Wie schätzen Sie das ökonomische Potenzial der Blockchain-Technologie in den nächsten fünf Jahren ein?
- Wie schätzen Sie das ökonomische Potenzial von privaten Blockchains im Vergleich zu öffentlichen Blockchains ein?
- Welches sind die zentralen ökonomischen Herausforderungen für private Blockchain-Anwendungen bzw. Anwendungen auf öffentlichen Blockchains?

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.

Möglichkeit zur Stellungnahme bezüglich KMU.

Fragen:

- Wie kann das Potenzial der Blockchain-Technologie nicht nur in der Start-up-Szene, sondern auch bei mittelständischen Unternehmen, insbesondere kleinen und mittleren Unternehmen, gehoben werden?
- Welche Einsatzmöglichkeiten und Potenziale sehen Sie insbes. bei kleinen und mittleren Unternehmen?

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 u.a. 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.

8 https://news.crunchbase.com/news/with-at-least-1-3-billion-invested-globally-in-2018-vc-funding-for-blockchain-blows-past-2017-totals/

9 www.ipaustralia.gov.au/sites/default/files/reports_publications/acs-blockchain-report_0.pdf

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).[10] 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 i. d. R. 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 bieten.

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

Möglichkeit zur Stellungnahme bezüglich ökologischer Fragestellungen.

Fragen:

- In welchen Anwendungsfeldern werden zentrale ökologische Chancen bzw. Risiken durch die Nutzung der Blockchain-Technologie gesehen (Use Cases)?
- Welche Lösungsansätze für das Ressourcenproblem von (öffentlichen) Blockchains sind erfolgversprechend? Wann ist die Umsetzung solcher Lösungsansätze zu erwarten?
- Durch welche Regelungs-, Regulierungs- und Anreizsysteme könnte eine nachhaltige Nutzung der Blockchain-Technologie unterstützt werden? Welche europäischen oder internationalen Governance-Strukturen sind denkbar?
- Wie hoch wird der Stromverbrauch für Blockchain-Anwendungen heute und im erwarteten Trend eingeschätzt? Und wie verhalten sich demgegenüber mögliche Einsparungen?
- Welche Änderungen in der Konstruktion der Blockchain, zum Beispiel zugunsten der Transaktionsgeschwindigkeit und des Energieverbrauchs, unterwandern wiederum die Kerneigenschaften der Technologie wie zum Beispiel Transparenz und Manipulationssicherheit?
- Sollte es ein Zertifizierungsverfahren für Blockchain-Technologien im Hinblick auf Energie-/Ressourcenverbrauch geben?

10 https://digiconomist.net/bitcoin-energy-consumption

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.

Möglichkeit zur Stellungnahme bezüglich rechtlicher Fragestellungen.

Fragen:

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

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 (zum Beispiel 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.

Möglichkeit zur Stellungnahme bezüglich des anwendbaren Rechts.

Fragen:

- 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?
- Können Transaktionen, die verschiedenen Rechtsordnungen unterliegen, in einer Blockchain abgebildet werden und welche Herausforderungen stellt dies an die Blockchain?
- Wie können in Blockchains wesentliche Verbraucherschutzrechte und rechtsstaatliche Grundsätze (Rule of Law) sichergestellt werden?

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).[11]

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.

Möglichkeit zur Stellungnahme bezüglich rechtlicher Verantwortlichkeit und Rechtsdurchsetzung.

Fragen:

- Besteht Bedarf für ein technisches und regulatives Regime, mit dem auf der Blockchain festgehaltene Transaktionen rückgängig gemacht werden können?
- Ggf.: Wie könnte ein solches technisches und regulatives Regime aussehen?

c) Smart Contracts

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

11 Schrey/Thalhofer, Rechtliche Aspekte der Blockchain, NJW 2017, 1431

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.[12]

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.

Möglichkeit zur Stellungnahme bezüglich Smart Contracts.

Fragen:

- 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?
- Wie kann eine transparente Vertragsgestaltung und -abwicklung (insbesondere für Verbraucher) gewährleistet werden?
- Ggf.: Welche Fragen sollten gesetzlich geregelt werden? Gibt es bereits Orakel, die Gegebenheiten der realen Welt in der Blockchain abbilden können?
- Wie ist die grenzüberschreitende Wirksamkeit von Smart Contracts zu bewerten (zum Beispiel bei internationalen Lieferketten)? Ist eine Vereinheitlichung internationalen Rechts erforderlich?
- Sollte es ein Zertifizierungsverfahren für Smart Contracts im Hinblick auf die versprochenen Funktionalitäten und die Cybersicherheit geben?

12 Kaulartz/Heckmann, Smart Contracts – Anwendungen einer Blockchain-Technologie, CR 2016, 618

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 u. a. Marktintegrität und Anlegerschutz sichergestellt.

Möglichkeit zur Stellungnahme bezüglich der Ersetzbarkeit von Intermediären.

Fragen:

- Gibt es bereits Konzepte, wie dezentrale Handelsplattformen beaufsichtigt werden können?
- Welche Möglichkeiten gibt es, die Funktion von Intermediären anderweitig sicherzustellen?
- In welchen Bereichen sollte auf einen Intermediär nicht verzichtet werden und warum?

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.

Möglichkeit zur Stellungnahme bezüglich des Datenschutzes.

Fragen:

- Wie kann der Einsatz der Blockchain-Technologie kompatibel mit datenschutzrechtlichen Anforderungen (informationelle Selbstbestimmung) gestaltet werden?
- Durch welche Methoden können personenbezogene Daten hinreichend anonymisiert werden (Verschlüsselung, Verschleierung, Aggregieren etc.)?
- Gibt es eventuell auf indirektem Wege Berührungspunkte mit der DSGVO, selbst wenn alle personenbezogenen Daten „off-chain" gespeichert werden?

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, d. h. 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.

Möglichkeit zur Stellungnahme bezüglich Formvorschriften.

Fragen:

- Was steht der Anerkennung von digitalen Nachweisen als gleichwertig mit der Schriftform entgegen?
- Kann die Blockchain die Textform ergänzen und hierfür zusätzliche Sicherheit hinsichtlich der Identitäten bieten?
- Welche Beispiele gibt es, bei denen bereits von dem Erfordernis der Schriftform abgewichen wurde?

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 Blockchain-Basis ist eine Herausforderung für die jeweilige steuerliche Einordnung. Eine Regulierung schafft auch Rechtssicherheit in den steuerlichen Konsequenzen.

Möglichkeit zur Stellungnahme bezüglich Steuern.

Fragen:

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

IV. Praxisbeispiele

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