Fraunhofer FIT

Projektgruppe Wirtschaftsinformatik

UNIVERSITÄT BAYREUTH

Universität Bayreuth
Professor für Wirtschaftsinformatik und Nachhaltiges IT-Management
Prof. Dr. Gilbert Fridgen
Stellvertretender Leiter der Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT
Gründer des Fraunhofer Blockchain-Labors
Stellvertretender wissenschaftlicher Leiter des Kernkompetenzzentrum Finanz- & Informationsmanagement

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)024

Ansprechpartner Prof. Dr. G. Fridgen
Telefon +49 921 55 - 4711
E-Mail gilbert.fridgen@uni-bayreuth.de
Datum Bayreuth, 24. November 2018

Stellungnahme zu den Fragen zum Thema „Blockchain“ im Ausschuss für Digitale Agenda am 28. November 2018[1]

Prof. Dr. Gilbert Fridgen
Fraunhofer FIT / Universität Bayreuth

1. In welchem Zusammenhang stehen Distributed-Ledger-Technologien (DLT), das Blockchain-Verfahren und Bitcoin? Worin besteht der Unterschied zwischen öffentlichen und privaten Blockchains? Welche Auswirkung kann die Entscheidung für eine der beiden Arten haben?

Der Begriff *Distributed-Ledger-Technologie* (DLT) bezeichnet eine Form von Datenbanksystem, welches sich durch gemeinsame/synchronisierte Datenhaltung in einem Peer-to-Peer-Netzwerk und fortlaufende, kryptografische Verkettung der Daten auszeichnet. Dadurch werden Unveränderbarkeit, Transparenz und Redundanz der gespeicherten Daten ermöglicht. Blockchain stellt eine konkrete Ausgestaltungsform dieser Technologie dar, bei der die Daten in einer Kette aus mittels kryptografischer Verfahren miteinander verbundenen Blöcken gespeichert werden. Andere

[1] Ich bedanke mich für die Unterstützung meines Teams im Fraunhofer Blockchain-Labor an der Universität Bayreuth: Laurin Arnold, Martin Brennecke, Patrick Camus, Benedict Drasch, Florian Guggenmos, Jannik Lockl, Sven Radszuwill, Alexander Rieger, Vincent Schlatt, André Schweizer, Johannes Sedlmeir

Ausgestaltungsformen, die je nach Interpretation als Blockchain, DLT oder beides bezeichnet werden, sind z.B. gerichtete, azyklische Graphen (siehe z.B. den „Tangle“ von IOTA).

Im Folgenden werden primär die allgemeineren Begriffe Distributed Ledger (DL) und Distributed Ledger Technology (DLT) genutzt, außer es ist explizit eine Blockchain gemeint.

Der erste Anwendungsfall der DLT ist die Kryptowährung Bitcoin. Die der Bitcoin zugrundeliegende Technologie – die Bitcoin-Blockchain – ist bereits seit 2009 relativ unverändert im Einsatz. Die (veraltete) technische Ausgestaltung der Bitcoin-Blockchain hat u.a. einen hohen Energieverbrauch zur Folge. Dieser Energieverbrauch ist jedoch Bitcoin-spezifisch und nicht verallgemeinerbar auf andere DLTs. Es gibt bereits heute andere technische Ausgestaltungsvarianten, die mit deutlich geringerem Energieverbrauch auskommen (siehe auch Frage 28).

Aufgrund der stetigen Weiterentwicklung der gesamten Technologie über die letzten Jahre hinweg existieren heute bereits eine Reihe unterschiedlicher konzeptionelle Ansätze für DL-Lösungen. Eine DL-Anwendung kann so entweder öffentlich oder privat sein sowie verschiedene Mechanismen zur Konsensbildung (d.h. zur Bestätigung der Transaktionen) nutzen.

An einem öffentlichen DL-Netzwerk kann grundsätzlich jeder teilnehmen – es gibt keine Teilnahmevoraussetzungen (außer handelsüblichen PCs). Im Unterschied dazu können an einem privaten DL-Netzwerk nur die Nutzer teilnehmen, die dazu berechtigt sind. Dies hat weitreichenden Einfluss auf die technische Ausgestaltung und auf Aspekte der Governance. In privaten DL-Netzwerken – wie z.B. Unternehmenskonsortien – sind die Teilnehmer untereinander im Normalfall bekannt und vertrauen sich zumindest teilweise. Diese Unterscheidung hat wesentliche Auswirkungen auf den Konsensmechanismus.

Der Konsensmechanismus bestimmt hauptsächlich die Sicherheit und die Transaktionsgeschwindigkeit des Netzwerkes. In einem öffentlichen DL-Netzwerk sind die Sicherheitsanforderungen an den Konsensmechanismus sehr hoch da jeder (unbekannte) Teilnehmer potenziell schädliche Absichten hat. Diese Eigenschaft geht zu Lasten der Performanz und der Ressourceneffizienz, was bedeutet, dass weniger Transaktionen durchgeführt werden können und diese bspw. mit hohem Energieverbrauch belastet sind. Ein Beispiel hierfür ist die Bitcoin-Blockchain.

Der eingeschränkte Nutzerzugang in privaten DLs reduziert die Sicherheitsanforderungen an den Konsensmechanismus. Beispielsweise werden hier auch Verfahren gewählt, in denen die Teilnehmer zufällig abwechselnd die Korrektheit der Transaktionen bestätigen. Dies ist mit deutlich höheren Transaktionsraten und geringerem Ressourcenverbrauch verbunden. Möglichem schädlichem Verhalten würde Aufgrund der Transparenz im Teilnehmerkreis auch außerhalb des DL begegnet (notfalls gerichtlich).

2. Welche der DLT/Blockchain-Technologien sind aus Ihrer Sicht - mit Blick auf Aspekte wie Sicherheit, Skalierbarkeit, Wirtschaftlichkeit, Interoperabilität, Transaktions-Durchsatzgeschwindigkeit, Transaktionsmenge und Energieverbrauch - schon heute zuverlässig einsatzfähig und welche haben das größte Potential?

Nicht jeder Anwendungsfall stellt die gleichen Anforderungen an eine DLT. Deshalb ist von Anwendungsfall zu Anwendungsfall zu unterscheiden, welche Anforderungen gestellt werden und die damit verbundenen Auswirkungen dementsprechend abzuwägen (vgl. Frage 1). Wie unter Frage 1 erwähnt, ergeben sich der hohe Energieverbrauch sowie die geringe Durchsatzgeschwindigkeit und Transaktionsmenge der Bitcoin-Blockchain v.a. durch aufwendige Anforderungen an die Sicherheit des Konsensmechanismus und sind nicht inhärente DLT-Schwächen. Generell wird jedoch bisher keine DLT allen denkbaren Anforderungen in jedem möglichen Anwendungsfall gerecht.

Dominante DLT-Protokolle sind derzeit insbesondere Ethereum, Hyperledger Fabric und CORDA. IOTA gilt trotz einzelner Kritikpunkte als sehr potenzialreich und wird u.a. durch die deutsche Automobil(zuliefer)industrie prototypisch eingesetzt.

3. In welchen Anwendungsgebieten sehen Sie das größte Potenzial der DLT/ Blockchain-Technologie und welche Voraussetzungen müssen gegeben sein, um dieses zu nutzen, z.B. in den Bereichen eHealth, eGovernment, und Energiewirtschaft?

Grundsätzlich ist festzustellen, dass DLTs sich weder im Besonderen für einzelnen Branchen, noch für bestimmten Anwendungsgebiete eignen. Deshalb kann derzeit noch nicht abschließend vorhergesehen werden, ob DLT eine Technologie ist, welche besonders günstig für eHealth, eGovernment oder Energiewirtschaft sein wird. Sie ist aber überall dort sinnvoll einsetzbar, wo Daten oder Prozessabläufe fälschungssicher dokumentiert (vgl. Frage 4, Anwendungsmuster 5) oder Prozesse über Organisationsgrenzen hinweg organisiert werden müssen (vgl. Frage 4, Anwendungsmuster 3) – konkret also in Szenarien, in denen zahlreiche, auch unterschiedliche Beteiligte zusammenarbeiten (müssen). Üblicherweise werden in solchen Szenarien heute zentrale Plattformen eingesetzt, die durch einen einzelnen Plattformbetreiber bereitgestellt werden. Aus Gründen der Governance ist diese Variante allerdings oftmals nur schwer umsetzbar, da es in bestimmten Anwendungsgebieten keine zentrale Koordination gibt, keine zentrale Koordination geben soll oder aus ökonomischen Gründen keiner der Beteiligten einer anderen Partei die Koordination überlassen möchte („Winner takes all"-Prinzip der Plattformökonomie; vgl. Frage 4, Anwendungsmuster 1). Unter Zuhilfenahme der DLT kann unter diesen Umständen dennoch eine Lösung umgesetzt werden, in welcher es keinen zentralen Plattformbetreiber gibt, der vom Betrieb der Plattform profitiert und potenziell monopolistisch auftritt.

Im Bereich eHealth sind Potenziale beispielsweise in der Pharmaindustrie (Produktfälschungen) denkbar (vgl. Frage 4, Anwendungsmuster III), im Bereich des eGovernment in der Schaffung DLT-basierter, digitaler Identitäten (vgl. Frage 4, Anwendungsmuster II), im Bereichen der Energie in Roaminglösungen für E-Ladeinfrastruktur oder in Herkunftsnachweisen für Strom. Jedoch ist hier jeder Bereich selbst im Detail auf Potenziale hin zu analysieren, wie dies beispielsweise das Bundesministerium für Verkehr und digitale Infrastruktur gerade im Rahmen eines Grundgutachtens angeht.

4. Für welche aktuellen, real existierenden Anforderungen und Use Cases funktioniert eine DLT/Blockchain besser als etablierte Technologien? Welche Anwendungsfälle sind aus Ihrer Sicht gefährlich? Was sind die zentralen Schwächen der Technologie?

Die Entscheidung für den Einsatz einer DL-Lösung fällt in den meisten Fällen aus einer Mischung aus wirtschaftlichen/organisatorischen Gründen und nicht aus technischen Gründen. Wirtschaftliche Gründe beziehen sich meist auf eine effizientere Gestaltung (u.a. schneller und kostengünstiger) von Prozessen. Aus organisatorischer Sicht ist DLT eine vielversprechende Lösung, wenn dezentrale Prozesse und Systeme verknüpft werden sollen, dennoch aber eine dezentrale Datenhaltung wünschenswert ist (bspw. im Falle behördenübergreifender Verwaltungsprozesse, vgl. Frage 3).

Grundsätzlich konnten wir bisher die folgenden (nicht durchschnittsfremden) Anwendungsmuster identifizieren:

I. Neutrale Plattform (vgl. Frage 3): Neutrale Plattformen ermöglichen die bilaterale Abwicklung von Geschäftsprozessen auf einer neutralen technologischen Basis. Dabei steht im Vordergrund, dass für die Bereitstellung dieser Plattform kein zentraler Betreiber notwendig ist. Die DLT schafft durch ihre Dezentralität und Transparenz die Möglichkeit, dass die Plattform durch deren Teilnehmer koordiniert und verwaltet wird. Hierdurch wird es möglich Drittparteien, u.a. Prüfinstanzen, zu ersetzen und Vorgänge oder Prozesse auf direktem Wege zwischen den involvierten Parteien abzuwickeln. Darüber hinaus ermöglicht eine derartige Plattform die Automatisierung von Prozessen, bspw. durch den Einsatz von Smart Contracts. Somit können die Vorteile einer Plattformökonomie erschlossen werden, ohne die Nachteile eines potenziellen Monopolisten in Kauf nehmen zu müssen.

II. Digitale Identität / Digitaler Zwilling (vgl. Frage 3): DLT ermöglicht die Schaffung digitaler Identitäten oder digitaler Zwillinge, mit Hilfe derer Personen oder autonom agierende Objekte in der digitalen Welt repräsentiert werden können. Digitale Identitäten bzw. digitale Zwillinge bilden dabei Eigenschaften und Verhalten einer Person oder eines Objektes digital ab, so dass mit dieser Person oder diesem Objekt im Nachgang digital interagiert werden kann. Durch eineindeutige, validierte und souveräne Identitäten werden so Identitätsdiebstahl oder Manipulationen deutlich erschwert. Das Bundesamt für Migration und Flüchtlinge ist in dieser Thematik bereits aktiv und erörtert die Möglichkeit, eine eindeutige und für Verwaltungszwecke geeignete digitale Identität zu schaffen. Perspektivisch kann auch dem einzelnen Bürger die Souveränität über seine DLT-basierte digitale Identitäten gewährt werden.

III. Management organisationsübergreifender Geschäftsprozesse: DLTs bieten eine Infrastruktur, durch die sich Prozesse organisationsübergreifend koordinieren und zu einer großen Kette zusammenschließen lassen – wiederum ohne dass dafür eine zentraler Koordinator benötigt würde. Im Gegensatz zu bestehenden Technologien kann jedoch hierbei ein größeres Maß an Transparenz geschaffen werden, ohne dass einzelnen Organisationen ihre Systeme zu sehr miteinander verknüpfen müssen. Dennoch können wichtige Governance Rahmenbedingungen zwischen den Organisationen eingehalten und ein hohes Maß an Vertrauen in die Informationen der anderen Organisationen gewährleistet werden.

IV. Zahlungsverkehr: Der Einsatz eines Distributed Ledgers bietet die Möglichkeit, digitale Zahlungsmittel zu etablieren und diese zu handeln. Unter digitale Zahlungsmittel fallen bspw. Kryptowährungen, welche sich erst durch die DLT etablieren konnten. Ähnlich wie bei Tokens können digitale Zahlungsmittel sehr fein gestückelt werden (bspw. bis zu 18 Nachkommastellen). Außerdem bringen sie die Möglichkeit, Transaktionen mit geringen Kosten, in kurzer Zeit über Ländergrenzen und Währungsräume hinweg durchzuführen, mit sich.

V. Fälschungssichere Dokumentation: Durch den Einsatz eines Distributed Ledgers kann die nachträgliche Manipulation dort abgelegter Daten und Informationen (z.B. Dokumente, Verträge, Maschinenprotokolle) verhindert oder zumindest aufgedeckt werden. Dies führt zu einer sicheren, glaubwürdigen und für alle beteiligten Akteure einsehbare Datenhistorie, wodurch sich die abgelegten Daten u.a. für eine Auditierung eigenen. Um Originaldaten vor fremdem Zugriff zu schützen, werden dazu

aber meist nur so genannte Hashwerte (Prüfsummen) abgelegt, mit denen bestätigt werden kann, dass ein außerhalb des DL verfügbares Dokument bereits zu einem früheren Zeitpunkt in genau dieser Form vorlag.

VI. Ökonomisch autonome Maschine: DLTs bieten eine Infrastruktur, um die Interaktion und das Wirtschaften zwischen autonom agierenden Maschinen zu ermöglichen. Durch parallele Entwicklungen in den Bereichen *künstliche Intelligenz* und *Internet der Dinge* sind autonom agierende Maschinen in den kommenden Jahren in vielfältigen Anwendungsfeldern zu erwarten, so z.B. im Bereich der Mobilität (autonome Fahrzeuge), in Transport/Logistik (Drohnen), oder auch in der Industrie (Industrieroboter). Damit diese Maschinen auch wirtschaftlich interagieren können (beispielsweise Leistungen untereinander abrechnen), ohne dass es dafür eine zentrale Überwachung bräuchte, sind DLT notwendig.

VII. Allgegenwärtige Dienste: In einem DL einmal (in Form von Smart Contracts) verankerte digitale Dienstleistungen können – einmal veröffentlicht – ohne weitere Wartung oder Betrieb durch den ursprünglichen Entwickler verfügbar bleiben, solange das zu Grunde liegende DL durch die Allgemeinheit weiter betrieben, d.h. genutzt wird. Damit entstehen gewissermaßen Dienstleistungen ohne Dienstleister, was sich nicht in bisherigen ökonomischer Theorie wiederfindet.

VIII. Tokenisierung (vgl. Frage 4)*:* DLT ermöglicht die Abbildung von Objekten oder Vermögenswerten aus der Realwelt in Form eines Tokens. Ähnlich dazu wäre heute eine Urkunde. Im Rahmen der Tokenisierung werden dabei Eigenschaften eines Objektes digital abgebildet. Aus der Tokenisierung resultiert die Möglichkeit, Objekte (bspw. Vermögenswerte) (nahezu) beliebig zu stückeln und zu handeln. Tokenisierung bildet damit eine Alternative für papierbasierte Beurkundung, die bzgl. Fälschungssicherheit und Dokumentenlogistik schwer zu handhaben sind. Damit können sowohl neue Anwendungsfelder erschlossen werden, die heute zu viel Aufwand generieren würden als auch bisherige Anwendungsfelder effizienter oder betrugssicherer gestaltet werden (z.B. ggf. auch im Kontext der kürzlich wegen Steuerbetrugs in die Kritik geratenen American Depositary Receipts).

Die Transparenz, die durch die Nutzung eines Distributed Ledgers herbeigeführt werden, kann – muss aber nicht – Gefahren mit sich bringen, sofern sie nicht im Sinne eines europäischen Werteverständnisses und unter Berücksichtigung der digitalen Souveränität gestaltet wird. Es existieren bereits erste Ansätze, um dieser Gefahr entgegenzuwirken, wie bspw. die Nutzung von sogenannten Zero-Knowledge-Protokollen oder privaten Datenkanälen (z.B. Channels bei Hyperledger). Ein weiterer Ansatz ist, sensible Daten nur lokal vorzuhalten („off-chain“) und lediglich einen kryptographischen Hash zur Überprüfung der Nichtveränderung (Hash-Pointer) im Distributed Ledger abzulegen („on-chain“). Ohne diese Mechanismen könnten DL-Lösungen missbraucht und bspw. auch zur Überwachung genutzt werden. Demnach ist eine frühzeitige ökonomische, rechtliche und technische Analyse auf deutscher und europäischer Ebene unumgänglich, um eine Einhaltung unserer Werte und rechtlicher Grundsätze sicherzustellen (vgl. Frage 16). Andernfalls wäre zu befürchten, dass später Lösungen in Deutschland breit genutzt werden, die nicht europäischen Standards und Anforderungen genügen, denen man aber auch nur schwer regulatorisch entgegenwirken kann (vgl. die Fragen 9-13).

Aktuelle Herausforderungen der DLT liegen besonders in der Skalierbarkeit, der Integration mit bestehenden digitalen Infrastrukturen und der Vereinbarkeit mit dem bestehenden regulatorischen Rahmen in den jeweiligen Anwendungsbereichen. So erschwert u.a. die Datenschutzgrundverordnung (DSGVO) den Einsatz von DLT, da diese v.a. auf zentralisierte Lösungen zugeschnitten ist und eine Vereinbarkeit derzeit teilweise noch ungeklärt ist (vgl. Frage 9). Trotz vielversprechender Ansätze gibt es hier aktuell keine endgültig akzeptierte Einschätzung.

5. Welche gesellschaftliche, aber auch ökonomische, ökologische und soziale Möglichkeiten sind mit den verschiedenen Ansätzen (private Blockchain, öffentlich-genehmigungsbasierte Blockchain und öffentlich-genehmigungsfreie Blockchain) und entsprechenden Anwendungsmöglichkeiten verbunden und wie schätzen Sie diese Potentiale in ihrer grundlegenden Bedeutung ein?

Die gesellschaftlichen, ökonomischen, ökologischen und sozialen Möglichkeiten der DLT hängen vom konkreten Anwendungsfall ab. Die Auswahl der beschriebenen Ansätze (privates DL-Netzwerk, öffentlich-genehmigungsbasiertes DL-Netzwerk und öffentlich-genehmigungsfreies DL-Netzwerk) ergeben sich meist direkt aus den Anforderungen des Anwendungsfalls. Aufgrund der Vielzahl der möglichen Anwendungsfälle ist eine abschließende Auflistung und Analyse schwierig. Der gesellschaftliche Mehrwert ergibt sich insbesondere aus der Möglichkeit, eine *höherwertige digitale Infrastruktur* schaffen zu können (vgl. auch Fragen 3 und 4). Damit sind digitale Dienste mit Infrastrukturcharakter gemeint, die über reine Breitbandversorgung hinausgehen.

Die ökonomischen Möglichkeiten der DLT liegen primär dort, wo man die Vorteile einer Plattformökonomie nutzen möchte, man allerdings keinen monopolistischen Plattformbetreiber einsetzen kann oder möchte (vgl. Frage 4, Anwendungsmuster I). Zudem kann die DLT dazu dienen, eine Infrastruktur für die Interaktion zwischen autonom agierenden Maschinen bereitzustellen (z.B. Fahrzeuge, Drohnen), welche untereinander auch wirtschaftliche Transaktionen abwickeln (im Bereich der Mobilität beispielsweise E-Fahrzeug und Ladesäule, Fahrzeug und Mautstation, Fahrzeug im Platoon). Insbesondere vor dem Hintergrund eines zu erwartenden Internet der Dinge und Fortschritten in der künstlichen Intelligenz besitzt DLT zusätzliches Potenzial.

Ökologische Möglichkeiten ergeben sich z.B. bei Anwendungen im internationalen Warenhandel. Die Koordination und Abwicklung des internationalen Handels ist heute überwiegend noch papierbasiert und Aufträge, Verträge oder Abrechnungen werden oft in Papierform international teilweise per Luftpost von einer Vertragspartei zur anderen befördert. DLT könnten hier papierbasierte Prozesse in großem Stil ablösen und damit das Aufkommen von Luftfracht verringern. Hier existieren bereits eine Reihe an Initiativen großer Logistikkonzerne, Finanzdienstleister (bezogen auf Handels-finanzierung) und IT-Dienstleister.

Auch die sozialen Anwendungsfelder sind breit gestreut. So werden DLT bspw. bereits genutzt um die Verteilung von Hilfsgütern in Flüchtlingslagern zu koordinieren. Zudem könnten mit Hilfe von DLT auch in von Korruption und Bürgerkrieg gebeutelten Ländern bürokratische Strukturen wie z.B. ein vertrauenswürdiges Katasterwesen aufgebaut werden.

6. Welche Voraussetzungen müssen dafür erfüllt sein, damit DLTs/ Blockchain Intermediäre ersetzen? Welche Nachteile kann dies haben?

Es ist nicht davon auszugehen, dass durch DLT bereits erfolgreich etablierte Intermediäre ersetzt werden. Meist haben sich diese nicht nur bewährt, sondern auch weitere organisatorische Aufgaben übernommen. Zudem handeln sie im Gegensatz zu technischen Lösungen wirtschaftlich strategisch. Wie der Bankensektor zeigt, können Intermediäre DLT sogar gezielt für sich nutzen, um ihre eigene Prozesseffizienz (Geschwindigkeit/Kosten) zu verbessern, wovon dann wiederum andere Marktteilnehmer profitieren. Lediglich Intermediäre welche ihre Marktmacht

missbrauchen, könnten durch die Einführung einer DLT-Lösung effektiv verdrängt werden. DLT stellt somit ein potenzielles Korrektiv am Markt dar.

Der Einsatz von DLT ist in Anwendungsfeldern vielversprechend, in denen ein Intermediär nutzenstiftend wäre, Markt oder politisches Umfeld diesen aber nicht hervorbringen oder noch nicht hervorgebracht haben (vgl. die Frage 3 und 4, Anwendungsmuster I sowie Frage 5: Katasterwesen). So wäre es zwar auf absehbare Zeit nicht sinnvoll, das Grundbuchamt in Deutschland durch ein DL zu ersetzen. In Ländern, in denen solche Register jedoch nicht existieren oder nicht zuverlässig funktionieren (z.B. aufgrund von Korruption) kann es aber durchaus sinnvoll sein, ein entsprechendes System auf der Basis von DLT einzuführen.

7. Gibt es Strategien, um innerhalb eines dezentralen Systems einen gemeinsamen Konsens der User hinsichtlich Standards, Patches und Updates zu finden?

Diese Strategien sind von DL-Protokoll zu DL-Protokoll unterschiedlich. DL-Protokolle werden hauptsächlich durch eine dezidierte Community, von Start-ups oder Stiftungen entwickelt. Die Software ist meistens Open Source, sodass die gesamte DLT-Community immer eng in den Entwicklungsprozess eingebunden wird. Durch die unterschiedlichen Entwicklungsformen existieren aktuell dezentralisierte, teilzentralisierte und zentralisierte Governance-Strukturen. Dabei ist eine entscheidende Frage, ob das DL-Netzwerk öffentlich oder privat ist (vgl. Frage 1).

In einem privaten DL-Netzwerk ist der zu treffende Konsens über Änderungen am System deutlich einfacher zu finden, da nur eine überschaubare Anzahl an Entscheidern und Nutzern beteiligt ist, die in ihrem DL-Protokoll grundsätzlich jeden technisch abbildbaren Konsens vereinbaren könnten.

In der öffentlichen Bitcoin-Blockchain entsteht ein Konsens meist durch eine vorangegangene Diskussion innerhalb der Community sowie eine darauf aufbauende Mehrheitsentscheidung bezüglich eines Änderungsvorschlages. Grundsätzlich durchlaufen Änderungen einen mehrstufigen Prozess. Am Anfang steht eine Forschungsphase, in der an möglichen Lösungen für ein bestehendes Problem gearbeitet wird. Daran beteiligt sich die gesamte Community. Wurde eine mögliche Lösung gefunden, so wird sie als Bitcoin Improvement Proposal (BIP) öffentlich geteilt und anschließend in die Software übertragen. Die tatsächliche Akzeptanz der Änderung hängt von der Community ab. Je mehr Teilnehmer des Netzwerks (Miner und User) die geänderte Software übernehmen und akzeptieren, desto größer ist Wahrscheinlichkeit einer Änderung des gesamten Systems.

Eine etwas andere Governance-Struktur nutzt die öffentliche Ethereum-Blockchain. Hier existieren zwar ebenfalls eine Forschungs- und eine Diskussionsphase (Ethereum Improvement Proposal), doch die letztendlichen Entscheidungen zur Änderung des Protokolls werden deutlich zentralisierter durch ein Gremium getroffen. Einen der bekanntesten Standards stellt der ERC-20 Standard von Ethereum dar, der eine Schnittstelle für Smart Contracts zum Tokenaustausch oder zur Tokenimplementierung ist. Mit dem steigenden Bekanntheitsgrad von Kryptowährungen, dem sich zunehmend bewährenden Konzepts von Initial Coin Offerings (ICOs) und der Implementierung der ERC-20 Schnittstelle zur Durchführung eines technisch einfach realisierbaren ICOs folgte der Boom der Kryptowährungen und ICOs im Winter 2017/2018. Der ERC-20 Standard entstand durch keine anerkannte Standardisierungsstelle, sondern durch die allgemeine Akzeptanz innerhalb der Community.

An beiden Mechanismen bleibt zu kritisieren, dass die endgültigen Entscheidungen durch eine kleine Gruppe mit technischem Sachverstand und/oder großem (finanziellen) Anteil an hinterlegten Krpytowährungen getroffen wird und somit nicht gleichberechtigt von allen Entscheidern. Insbesondere staatliche DLT-Initiativen müssten sich hier deutlich stärker an demokratischen Strukturen orientieren.

8. Wie geht man mit irrtümlichen Falschbuchungen oder unveränderbar gespeicherten Falschmeldungen um? Wie geht man mit illegalen, auf der Blockchain gespeicherten Daten um, man kann sie schließlich nicht löschen?

In einem DL ist es grundsätzlich nicht möglich, Buchungen oder Falschmeldungen rückwirkend zu verändern. Die Unveränderbarkeit resultiert aus der fortlaufenden kryptografischen Verkettung der Daten (vgl. Frage 1). Auch Falschmeldungen oder illegale Daten werden unveränderlich gespeichert.

Soll in einem DL eine Transaktion (z.B. Buchung) berichtigt werden, muss eine Gegentransaktion (z.B. Gegenbuchung) durchgeführt werden, wie dies auch in zentralen Registern heute üblich ist. Um beispielsweise eine Falschmeldung zu korrigieren ist es so notwendig, die Meldung über eine neue Transaktion richtigzustellen. Anhand der Historie sind die Statusänderungen (ursprüngliche Falschmeldung und Berichtigung) dann nachvollziehbar.

Die Unveränderbarkeit und Transparenz stellt eine der wichtigsten Stärken der DLT dar. Die Idee einer rückwirkenden Löschung wäre die Unterwanderung von der Technologie inhärenten Grundsätzen. Nichtsdestotrotz ist auch dies nicht grundsätzlich ausgeschlossen: Prinzipiell ist es möglich, in DL Änderungen durch sogenannte Hard Forks vorzunehmen. Bei einer Änderung durch einen Hard Fork wird das DL bis zu dem Block zurückgesetzt, in dem der Fehler, bzw. die illegalen Daten enthalten sind.

Dieses Vorgehen gab es bereits in der öffentlichen Ethereum-Blockchain im Zusammenhang mit dem und dem Hack der Decentralized Autonomous Organization, bei dem viele Nutzer durch einen Programmierfehler einen Anteil ihrer Kryptowährungen verloren. In einem bisher einmaligen Prozess entschied das Gremium von Ethereum zusammen mit der Community, einen Hard Fork vorzunehmen. Dazu wurde der enthaltene Fehler in der Software korrigiert und diese als neue Version veröffentlicht. Ein Großteil der Community unterstützte diesen Fork, sodass das geänderte Distributed Ledger fortan als neuer Standard angesehen wurde. Teilnehmer, die sich nicht der Änderung angeschlossen haben, führen das Distributed Ledger, welche den Programmierfehler beinhaltet, allerdings weiter. Um eine tatsächliche Löschung von Daten zu erreichen müsste dieses alte DL-Netzwerk „abgeschaltet“ werden. Da allerdings jeder frei entscheiden kann, welches öffentliches DL-Netzwerk er unterstützen möchte, stellt die Löschung in einem öffentlichen DL-Netzwerk eine große Herausforderung dar und ist vor allem nach aktuellem Stand nicht staatlich herbeizuführen.

Auch in einem privaten DL könnten sich die Teilnehmer gemeinsam auf eine Änderung einigen und nur die „wahre“ Version unterstützen. Dies wäre prinzipiell einfacher, erfordert aber auch die Kooperation und Abstimmung zwischen allen Teilnehmern. Das Rücksetzen eines DL hat zudem immer zur Folge, dass alle nach dem Rücksetzzeitpunkt getätigten Transaktionen als ungültig angesehen werden und erneut durchgeführt werden müssen.

Vielversprechender wäre es, die Nutzung von DL für spezifische Zwecke soweit einzuschränken, dass illegale Inhalte gar nicht im Ledger gespeichert werden können und nur Transaktionen durchgeführt werden dürfen, für die man auch eine entsprechende Gegenbuchung vornehmen kann. Einfachere Wege um nicht gewünschte Daten zu löschen sind zudem aktuell in der Erforschung.

9. Inwieweit ist das offene und verteilte Design der Blockchain mit dem Datenschutz (insbesondere dem „Recht auf Vergessenwerden“ nach der DSGVO) vereinbar?

Herausforderungen bzgl. Datenschutz ergeben sich vereinfacht gesagt nur, wenn im Rahmen einer DL-Anwendung personenbezogene oder personenbeziehbare Daten tangiert werden. Für diese Anwendungen sind bereits vielversprechende technische Ansätze entwickelt worden. So wäre es denkbar, dass die personenbezogenen Daten ausschließlich außerhalb des DL („off-chain“) abgespeichert werden. Die Verknüpfung mit dem DL funktioniert dann durch einen entsprechenden auf der DL („on-chain“) gespeicherten Verweis (Link), der auf die off-chain-Daten referenziert. Eine Löschung der off-chain-Daten wäre genau wie in traditionellen Datenstrukturen leicht möglich. Der on-chain-Verweis würde dann ins Leere zeigen.

Im Rahmen unseres Grundgutachtens für das Bundesministerium für Verkehr und digitale Infrastruktur adressieren wir diese Fragestellung aktuell im Detail mit Kollegen der Rechtswissenschaftlichen Fakultät der Universität Münster. Im Rahmen unseres Projekts mit dem Bundesamt für Migration und Flüchtlinge diskutieren wir zudem mit Mitarbeitern der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, inwiefern auf der DL verbleibende abstrakte Informationen (z.B. Identifier einer Person) ein prinzipielles datenschutzrechtliches Problem darstellen können. Schließlich könnte man über Kombination mit anderen Datenquellen oder durch Kenntnis der einer Person zugeordneten Distributed Leder ID (Identifier) den Bezug wiederherstellen. Wenn allerdings alle off-chain Daten gelöscht wurden ist für die betrachtete Stelle in der Regel kein Personenbezug (bzw. nur mit unverhältnismäßig großem Aufwand oder kriminellen Absichten bereits vor dem Löschen) mehr reproduzierbar. Das Problem krimineller Handlungen existiert aber auch in allen gängigen nicht-DLT-Lösungen und besteht unter anderem in unrechtmäßig angefertigten Kopien (oder Screenshots) gespeicherter Daten.

10. Wie können bei Smart Contracts die im BGB verankerten Prinzipien bei der Behandlung von Irrtümern, wie beispielsweise das Anfechtungsrecht, gesichert werden?

Da mir die rechtswissenschaftliche Ausbildung und Expertise fehlen, möchte ich die Beantwortung dieser Frage Sachverständigen mit entsprechendem Hintergrund überlassen.

Sofern in einem DLT-Netzwerk rechtsstaatliche Entscheidungen und Prinzipien durchsetzbar sein sollen, so müsse dies bereits in der Gestaltung der DLT verankert sein. Sollen beispielsweise Gerichtentscheidungen auf einem Distributed Ledger durchgesetzt werden, so müssten Judikative und Exekutive entsprechende „Generalschlüssel“ zur Änderung von Transaktionen Dritter erhalten. Eine solche Lösung existiert heute noch nicht im Rahmen einer interdisziplinär besetzten Forschungsinitiative zunächst auf ihre Machbarkeit geprüft und ggf. im Folgenden umgesetzt werden (vgl. Frage 14).

11. Wie kann sichergestellt werden, dass beim Einsatz von Blockchain-Technologien zivilrechtliche Löschansprüche nicht gänzlich unterlaufen werden, etwa, weil Daten - unabhängig davon ob zufällig, fahrlässig oder absichtlich - in einer solchen Blockchain gespeichert wurden? (Die Nutzenden der Blockchain könnten sich ja ggf. auf eine Unzumutbarkeit der Löschung berufen vgl. § 275 II, III BGB).

Da mir die rechtswissenschaftliche Ausbildung und Expertise fehlen, möchte ich die Beantwortung dieser Frage Sachverständigen mit entsprechendem Hintergrund überlassen.

Für Fragen zur technischen Umsetzbarkeit nachträglicher Änderungen oder zur Vereinbarkeit mit der DSGVO vgl. die Fragen 8, 9, 10 und 11.

12. Wie kann sichergestellt werden, dass das strikte Abstraktions- und Trennungsprinzip des deutschen Rechts nicht umgangen wird - was in der Folge auch z.B. das Bereicherungsrecht zur Makulatur machen würde?

Da mir die rechtswissenschaftliche Ausbildung und Expertise fehlen, möchte ich die Beantwortung dieser Frage Sachverständigen mit entsprechendem Hintergrund überlassen.

Sofern auf einem DL jedoch rechtsstaatliche Entscheidungen und Prinzipien durchsetzbar sein sollen, so sollten diese bereits in der spezifischen Gestaltung der DLT-Lösung verankert sein (vgl. Frage 10).

13. Der Grundgedanke von Blockchain ist, dass Einträge nur hinzugefügt und niemals verändert werden können. Wie wollen Sie das Problem endlos wachsender Datenbanken lösen, die ja, um Konsistenz sicherzustellen, niemals bereinigt werden können? Falls die Lösung eine Trusted 3rd Party ist, die die Datenbank entleert, warum dann überhaupt eine Blockchain?

In der Tat ist eine Trusted-3rd Party nicht die Lösung für dieses Problem. Vielmehr gilt es, DL-Systeme so zu gestalten, dass dieses Problem in der Ausgestaltung der DL-Anwendung adressiert wird. Dies kann grundsätzlich auf mehreren Wegen erfolgen:

Erstens ist es sinnvoll, nur die für die Anwendung wirklich notwendigen auf der DL zu speichern. Dies ist auch im Sinne des Datenschutzes (Datensparsamkeit, vgl. die Fragen 8 und 9).

Zweitens ist es möglich, lediglich die Salden einer Vielzahl bilateraler Transaktionen zu bestimmten Zeitpunkten auf das DL zu schreiben. Dadurch wird die Fülle der gespeicherten Informationen im Sinne einer Aggregation reduziert. Hierbei existieren bereits Ansätze, um auch alte Teile zu saldieren, oder gar von Zeit zu Zeit zu löschen.

Drittens können Informationen gefiltert werden. Nicht alle Teilnehmer des DL-Netzwerks sind an allen Informationen interessiert oder dürfen diese einsehen. Durch sogenannte Channels teilen nur bestimmte Nutzerkreise Informationen teilen. Lediglich deren Konsistenz wird durch die Allgemeinheit bestätigt.

Viertens wäre denkbar, dass zur Speicherung die Daten geographisch geschickt verteilt werden. Der Gedanke dabei ist, dass nicht alle Informationen zu jedem Zeitpunkt an jedem Knoten im Netz vorgehalten werden müssen, sondern ein vollständiger Ledger in jeder Region rekonstruierbar ist.

14. Bei der Anwendung von BC / DLT kann niemand Transaktion verhindern oder rückabwickeln, auch sind Kontosperrungen unmöglich. Wie könnte ein regulativer Rahmen aussehen, ohne dass dabei die grundlegenden Eigenschaften von BC / DLT aufgegeben werden müssen? Wie können dann nachweisbare, rechtsgültige und einklagbare, gerichtsfesten Verträge, Haftungsregelungen und verbindlich beweisbare Zahlungen gestaltet werden?

Zu Fragen zur technischen Umsetzbarkeit von Transaktionsprüfungen, nachträglicher Änderungen oder zur Vereinbarkeit mit der DSGVO vgl. die Fragen 8, 9, 10 und 11.

Grundgedanke eines regulativen Rahmens sollte sein, DL-Anwendungen mit den Prinzipien unserer freiheitlich-demokratischen Ordnung und unseres Rechtsstaates in Einklang zu bringen (vgl. Frage 10). Dies ist besonders dort relevant, wo DL-Anwendungen den Charakter einer höherwertigen digitalen Infrastruktur besitzen.

Heutige DLT-Implementierungen bilden keine Gewaltenteilung ab und ermöglichen den entsprechenden Staatsorganen keine Zugriffsmöglichkeiten. Eine staatlich sanktionierte DLT müsste allerdings so gestaltet sein, dass sie beispielsweise die Entscheidung eines Gerichts bedingungslos umsetzt (vgl. Frage 10). Auch wenn Bitcoin dies nicht unterstützt, könnte eine Kryptowährung durchaus so gestaltet werden, dass der Judikative und Exekutive beispielsweise „Generalschlüssel“ vorliegen, mit Hilfe deren gerichtlich bestätigte Entscheidungen auf einem Distributed Ledger durchgesetzt werden können. Eine solche Lösung existiert heute noch nicht und müsste im Rahmen einer interdisziplinär besetzten Forschungsinitiative zunächst auf ihre Machbarkeit geprüft und ggf. im Folgenden umgesetzt werden (vgl. Frage 10).

Da mir die rechtswissenschaftliche Ausbildung und Expertise fehlen, möchte ich die detaillierte Beantwortung der letzten Teilfrage Sachverständigen mit entsprechendem Hintergrund überlassen. Gerichtsfeste Smart Contracts könnten meines Erachtens allerdings dazu beitragen, Divergenzen zwischen Vertragstexten und der prozessualen sowie technischer Umsetzung zu verringern. Zudem könnten sie die Beurteilung von rechtlichen Sachverhalten durch eine saubere Historisierung vereinfachen.

15. Welche vorrangigen Regulierungsfragen stellen sich aus Ihrer Perspektive in Zusammenhang mit dem Einsatz von Blockchain- und Distributed-Ledger-Technologien sowie durch die Ausgabe von Kryptowährungen und Finanzierung von Unternehmen durch ICOs? Wie kann neben Regulierungsfragen eine internationale Standardsetzung erfolgen, die die Technologien und damit die Innovationspotentiale sicherstellt?

DLTs befindet sich aktuell noch stark in der Entwicklung, sodass es viele verschiedene Ansätze und Richtungen gibt. Zu frühe und restriktive Regulierung oder Standardisierung kann aus meiner Sicht zum aktuellen Zeitpunkt auch innovationshinderlich sein. Es kommt erschwerend hinzu, dass es aufgrund der globalen Ausrichtung von DL-Lösungen technisch kaum möglich sein wird, strenge Regulierung durchzusetzen – insbesondere beim Endnutzer. Dies wäre vermutlich auch der falsche Ansatz: Am Beispiel illegaler Musik- und Filmtauschbörsen hat sich schon in der Vergangenheit gezeigt, dass diese nicht durch Verbote zu verdrängen waren, sondern dass diese erst durch legale und dennoch bezahlbare Alternativen wie die heutigen Streamingdienste (z.B. Spotify, Deezer) abgelöst wurden. Daher sollte die Regulierung eher das Ziel verfolgen, Nutzern für jeden Anwendungsbereich eine legale und dennoch nutzerfreundliche DL-Lösung zur Verfügung zu stellen.

In diesem Sinne sollte der Fokus einerseits auf einer behutsamen und internationalen Standardisierung liegen, wie sie aktuell die IEEE Standards Association, die ISO oder die Ethereum Enterprise Alliance verfolgen. Gleichzeitig sollten behutsame Regulierungsvorschläge in enger Abstimmung mit Vertretern aus Wirtschaft und Wissenschaft erarbeitet, sowie gezielte Versuchsumfelder und Förderinstrumente geschaffen werden. Dabei sind insbesondere auch die Interessen und Erfahrungen der gerade in Deutschland wachsenden Start-up-Szene zu berücksichtigen, von der im Moment die meiste Innovation ausgeht. Im Erfolgsfall wären Deutschland und Europa damit nicht nur Vorreiter in einer wirtschaftlich attraktiven Zukunftstechnologie, sondern gleichermaßen Exporteure unserer freiheitlich-demokratischen und rechtstaatlichen Grundprinzipien.

Eine sehr häufig genannte Herausforderung ist jedoch der mögliche Konflikt zwischen DLT und DSGVO. Auch wenn es hier bereits technische Ansätze gibt, existierende Probleme zu entschärfen oder gar zu lösen, scheinen beide Konzepte zunächst unvereinbar. Zur Bewertung dieses Konfliktes ist es zunächst sinnvoll, die Ziele der Technologie einerseits und der Gesetzgebung andererseits zu hinterfragen. Das Ziel der DSGVO ist es, die Souveränität des Einzelnen über seine Daten zu stärken. Damit sollen u.a. Plattformbetreiber, die asymmetrisch in den Besitz großer Datenmengen gelangen, daran gehindert werden, diese Daten ohne entsprechendes Einverständnis des Nutzers zu verwerten. Anwendungen von DLT verfolgen das gleiche Ziel auf anderem Wege: Die Daten stehen hier prinzipiell jedem (d.h. symmetrisch) zur Verfügung, können aber durch Verschlüsselung oder Anonymisierung zumindest vor Massenverarbeitung geschützt werden – und schützen so auch (oder sogar noch mehr) die Souveränität des Einzelnen. Die grundlegenden Ziele von DLT und DSGVO sind somit durchaus kompatibel. Erfahrungen zeigen jedoch, dass es in vielen Detailfragen rechtlichen Klärungsbedarf gibt, für den durch entsprechende Regulierung Rechtssicherheit geschaffen werden sollte (vgl. die Fragen 3 und 10).

Um durch internationale Regulierung zu einer positiven Entwicklung im Bereich der Tokens beizutragen, sollte insbesondere auf die Förderung vorhandener Kreativität und auf die Vorgabe transparenter (rechtlicher) Rahmenbedingungen gesetzt werden (vgl. die Fragen 16 und 25). Bei voreiliger oder unsachgemäßer Regulierung könnten ansonsten nicht-intendierte Innovationshemmnisse erzeugt werden.

16. Wie bewerten Sie die europäische Blockchain-Partnerschaft?

Die Kooperation im Rahmen der Europäischen Blockchain-Partnerschaft[2], die Einrichtung des EU Blockchain Observatory and Forum[3], die European Blockchain Services Infrastructure (EBSI) Initiative[4] sind wichtige Schritte in die richtige Richtung. Im Rahmen dieser Zusammenarbeit und Initiativen können gemeinsame Grundlagen und Rahmenbedingungen gelegt werden, die auch in Zukunft die Entwicklungen im Bereich der DLT innerhalb der EU nicht nur fördern, sondern auch gestalten. Wichtig ist, dieser Partnerschaft auch in juristischer, wirtschaftlicher und politischer Hinsicht Handlungen folgen zu lassen und die Zusammenarbeit in die Tat umzusetzen. So muss die

[2] Siehe https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership, abgerufen am 24.11.2018
[3] Siehe https://www.eublockchainforum.eu/, abgerufen am 24.11.2018
[4] Siehe https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-roundtable-supports-efforts-deploy-blockchain-technologies-eu, abgerufen am 24.11.2018

Zusammenarbeit auf den verschiedenen Ebenen weiter intensiviert werden, damit letztlich der notwendige Beitrag geleistet werden kann.

In diesem Sinne ist es zentral und werden die Entwicklungen im DLT-Bereich davon profitieren, wenn die Zusammenarbeit auf allen Ebenen weiter intensiviert wird. Die bereits über Ländergrenzen hinweg existierenden Start-ups, Initiativen und Organisationen sind darauf angewiesen, einen einheitlichen Rechts- und Handelsraum zu haben und sich an klaren Rahmenbedingungen zu orientieren.

17. Für den Fall anonymitätsbewahrender BC/DLT-Implementierungen im Zahlungsverkehr können Kriminalitäts-Problematiken entstehen, wie etwa Steuervermeidung, Geldwäsche, etc. Können diese Problematiken durch Einführung der BC/DLT noch zunehmen bzw. noch schwerer zu bekämpfen sein?

DLT ist keine Technologie, die Kriminalitätsproblematiken ausschließlich erschwert oder ausschließlich erleichtert. Vielmehr kommt es auf die Ausgestaltung der DL-Anwendung an. Durch die Möglichkeiten, Transaktionen pseudonym oder anonym zu gestalten, können die angesprochenen Problematiken natürlich verschärft werden. Entsprechend wichtig ist, dass diese Herausforderungen bereits in der Entwicklungsphase von DL-Anwendungen im Zahlungsverkehr diskutiert und technische sowie organisatorische Lösungsmöglichkeiten erarbeitet werden.

Ein Ansatz könnte die Einführung einer offiziellen Europäischen Digitalwährung (bspw. e€, Krypto-€) als rechtskonforme Basiseinheit für DL-Anwendungen sein. Dieser Vorschlag wurde kürzlich auch von der Direktorin des Internationalen Währungsfonds Christine Lagarde im Rahmen des Singapore Fintech Festivals in einer Rede eingebracht[5]. Diese Kryptowährungen könnte Anwendungen ermöglichen, welche die angesprochenen Kriminalitätsproblematiken sogar leichter bekämpfbar machen (vgl. Frage 9) und in ihrer Ausgestaltung unseren Ansprüchen an Sicherheit, Verbraucherschutz und Datenschutz gerecht wird. Ebenso wäre eine solche Digitalwährung mit unserem heutigen Währungssystem kompatibel und die Teilnahme nicht an bestimmte Zugangsvoraussetzungen knüpfen (wie etwa bei Bitcoin).

18. Wer sollte aus Ihrer Sicht eine Blockchain verwalten/betreiben? Der Staat, zivilgesellschaftliche Organisationen, private Unternehmen oder eine Partnerschaft aus den Bereichen?

Der DLT liegt die Idee zugrunde, dass für den Betrieb keine zentrale Partei benötigt wird. Im Grunde genommen können Governance-Strukturen so aufgesetzt werden, dass die Teilnehmer des DL-Netzwerks entscheiden, wie dieses weiterentwickelt und gestaltet werden soll. Dennoch ist es möglich, Teilnehmern verschiedene Rollen zuzuweisen und dementsprechend könnten auch staatlichen Einrichtungen die jeweiligen Berechtigungen zugewiesen werden.

DL-Lösungen weisen jedoch oftmals den Charakter einer höherwertigen digitalen Infrastruktur auf, welche es den Marktteilnehmer ermöglicht digital miteinander Wirtschaft zu treiben. Für solche Infrastrukturen könnte sich ein Staat entsprechend verantwortlich fühlen.

---

[5] Siehe https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency, abgerufen am 24.11.2018

Wie diese Verantwortung letztlich ausgestaltet ist, bleibt je nach Anwendungsfall zu entscheiden. So sind sowohl gezielte Förderungen als auch die Vergabe von Entwicklung und Betrieb an private Anbieter denkbar. Lediglich weder die komplett staatliche Entwicklung noch den reinen Verlass auf die Privatwirtschaft halte ich im Allgemeinen nicht für sinnvoll. Für eine rein staatliche Entwicklung fehlen vermutlich Ressourcen und Kompetenzen. Eine rein privatwirtschaftlich getriebene Entwicklung solcher Infrastrukturen steht nicht notwendigerweise im Einklang mit unserem Werte- und Rechtsverständnis (vgl. die Fragen 9-13, 23) – insbesondere, wenn sie aus dem Ausland getrieben wird.

19. In welchem Bereich der öffentlichen Verwaltung sehen Sie das größte Potential für einen Einsatz von Distributed-Ledger-Technologie? Wie kann die deutsche öffentliche Verwaltung davon profitieren? Welche Fähigkeiten braucht die öffentliche Verwaltung, um ein Instrument wie die Distributed-Ledger-Technologie effizient einzusetzen?

Das Potenzial besteht vor allem dort, wo Verwaltungsprozesse behördenübergreifende Kommunikation und Zusammenarbeit erfordern. Die aktuelle dezentrale Datenhaltung bei einer Vielzahl an Behörden erschwert bei all ihren Vorteilen allerdings auch die überbehördliche Zusammenarbeit, da oft die wechselseitige Daten- und technische Integration fehlt. In wirtschaftlich agierenden Unternehmen wäre dies ein Grund für eine Integration der Daten, in welcher sämtliche Informationen aller Behörden vorgehalten werden würden („Bundesdatenbank“).

Da wir in unserm föderalistischen Staat die zentrale Datenhaltung („der gläserne Bürger“) aber gerade vermeiden möchten, könnte die DLT dabei unterstützen, behördenübergreifende Prozesse abzuwickeln, ohne dass dafür eine zentrale Datenhaltung nötig wäre. Dies würde die Kommunikation erleichtern, die Zusammenarbeit unterstützen und gleichzeitig die Datensouveränität des einzelnen Bürgers stärken (vgl. die Fragen 3 und 5). Weiterhin gibt es Potenzial im Bereich der Besteuerung (z.B. Besteuerung von Roborterarbeit).

Die öffentliche Verwaltung benötigt für einen effizienten Einsatz von DLTs das organisationale Wissen bezüglich behördeninterner und behördenübergreifender Prozesse, Know-how im Bereich Prozessreorganisation vor dem Hintergrund der Möglichkeiten der DLT, rechtlichen Sachverstand (bspw. in Bezug auf die Speicherung von Daten), sowie das technische Verständnis in der Umsetzung (vgl. Frage 3). Die Begleitung solcher Projekte kann dabei von Einrichtungen mit entsprechender Expertise geleistet werden.

20. In welchen Bereichen ist es aus Ihrer Sicht wahrscheinlich, dass ein Zusammenspiel aus Künstlicher Intelligenz (Vorhersagen und Analyse) und Smart Contracts (Abwicklung) zukünftig die Abläufe der öffentlichen Verwaltung bestimmen wird?

Um Einsatzmöglichkeiten zu identifizieren ist ein detailliertes Verständnis für die Schnittstelle zwischen künstlicher Intelligenz (trifft die Entscheidungen), Smart Contracts (löst verbindliche Transaktionen aus) und DLT (ermöglicht Interaktion und dokumentiert Handlungen) notwendig, das je nach Anwendungsgebiet separat erörtert werden müsste. Beispielsweise besteht allgemein Potenzial die Entscheidungsfindung durch gezielte Analyse und Vorhersage zu unterstützen oder einfach Abläufe und Prozesse zu automatisieren.

Dennoch sind in vielen Prozessen der öffentlichen Verwaltung vollautomatisierte Entscheidungen nicht wünschenswert. Künstliche Intelligenz und DLT können zwar im Zusammenspiel durchaus wichtige Unterstützungsfunktionen übernehmen und Fehler oder Ineffizienzen in Verwaltungsprozessen aufdecken. Der Mensch als Ansprechpartner, der die Funktion einer Beschwerdestelle einnimmt und Entscheidungen nachvollziehen oder intellektuell prüfen kann, darf jedoch nicht verloren gehen. Eine vollautomatisierte Bürokratie, in welcher Maschinen entscheiden und diese Entscheidung in DLs direkt umsetzen hätte jedenfalls Eigenschaften einer Dystopie.

21. Ab wann werden heute angewendete Verschlüsselungsalgorithmen und Instrumente aus dem Bereich der IT-Sicherheit voraussichtlich unsicher? Wie kann angesichts der Weiterentwicklung von Quantenkryptografie bzw. -analyse auch zukünftig die Sicherheit von Blockchains sichergestellt werden? Welche Angriffsmuster sind bei einer Blockchain vorstellbar und wie kann man sich dagegen absichern?

Das wesentliche Versprechen der DLT beruht auf ihrer hohen Manipulationsresistenz durch den Einsatz bewährter und sicherer kryptographischer Verfahren. Ein Beispiel ist ihr asymmetrische Verschlüsselung, welche ebenfalls für Sicherheit im Internet, z.B. bei E-Mails, sorgt. Entsprechend stellen alle Ansätze und Angriffsvektoren, die diese Verfahren knacken können eine große Herausforderung für Angreifer dar.

Die abstrakte Fokussierung auf Quantenkryptographie und -analyse halte ich aus zwei Gründen für bedingt zielführend: Erstens wissen wir nicht, wann diese Verfahren tatsächlich zur Verfügung stehen, was Quantencomputer zu leisten vermögen und welche zukünftigen Verfahren auch Sicherheit vor Quantencomputern bieten. Zweitens werden Quantencomputer unsere bisher verwendeten Sicherheitsverfahren insgesamt auf den Prüfstand stellen, was eine viel umfangreiche Lösung der damit verbundenen Veränderungen nötig macht. Die heutige Herausforderung ist daher eher, DL-Anwendungen so zu gestalten, dass veraltete und angreifbar gewordenen Verfahren zu einem späteren Zeitpunkt durch neue, weiterhin sichere („quantum-safe“) ersetzt werden können.

Angriffsmuster auf DLTs sind von verschiedenen Faktoren abhängig (bspw. von der Wahl des Konsensmechanismus) und damit schwer verallgemeinerbar. Dennoch stelle ich im Folgenden theoretisch mögliche oder in der Vergangenheit aufgetretene Fälle dar:

Ein DL-Netzwerk, das den Proof-of-Work Konsensmechanismus verwendet (auch eingesetzt in der Bitcoin-Blockchain), wird u.a. durch eine sogenannte 51%-Attacke bedroht. Dabei muss ein Angreifer über mehr als 50% der Rechenleistung des Netzwerkes verfügen und kann so beispielsweise eigene Transaktionen vortäuschen. Verhindert wird ein derartiger Angriff durch die Größe des Netzwerkes und den dadurch notwendigen Einsatz von Rechenleistung, sodass ein Angriff auf die großen Kryptowährungen heute unrealistisch erscheint.

Beim „Double Spending“ nutzt ein Angreifer die Latenzzeit bis zu endgültigen Bestätigung einer Transaktion, um Geschäfte mit zwei verschiedenen Nutzern abzuschließen. Dieses Szenario wird durch die schnellere Transaktionsabwicklung neuerer DLTs erschwert und kann durch vorsichtige Nutzer (insb. bei großen Transaktionen) verhindert werden.

Ein weitläufig bekannt gewordenes Angriffsmuster ist der Diebstahl von Kryptowährungen im großen Stil. Die großen Diebstähle oder Angriffe waren stets darauf

zurückzuführen, dass Anbieter von Kryptobörsen angegriffen und die verwahrten Coins entwendet wurden (ein prominentes Beispiel ist hier der mittlerweile insolvente japanische Anbieter MtGox[6]). Diese Angriffe betreffen jedoch nicht die eigentliche DLT, sondern eher die IT-Sicherheit dieser Börsen – sie sind eher vergleichbar mit einem klassischen Bankraub.

Auch fehlerhafte Smart Contracts können durch Angreifer gezielt ausgenutzt werden. Dabei ist nicht das DL-Protokoll selbst betroffen, sondern der fehlerhafte Quellcode eines durch einen Nutzer hochgeladenen Programms. Bekannt wurde dieses Szenario durch den sogenannten DAO-Hack7. Die DAO (Decentralized Autonomous Organization) hatte zum Ziel, Kapital von Nutzern des Ethereum-Netzwerks zu sammeln und nach einem Abstimmungsverfahren als Risikokapital an Start-ups im Blockchain-Umfeld zu verteilen. Durch einen Fehler konnten die der DAO zugehörigen Adressen (Konten) jedoch bestohlen werden. Um solche Vorfälle zukünftig zu vermeiden, wird die Zertifizierung von Smart Contracts (beispielsweise durch tehchnische Prüforganisationen) diskutiert.

Schließlich bleibt die Schnittstelle zur Realwelt ein Schwachpunkt in der Sicherheit von DLs. Sollen beispielsweise Sensordaten fälschungssicher dokumentiert werden (vgl. Frage 4, Anwendungsmuster 5), so bleibt die Möglichkeit, den Sensor selbst zu manipulieren. Dies ist jedoch ein Angriffsszenario, welches nur zum Tragen kommt, wenn Nutzer sich dieser Möglichkeit nicht bewusst sind und folglich den im DL abgelegten Informationen vollständig vertrauen. Grundsätzlich mindert DLT hier die Möglichkeiten betrügerischer Angriff, kann dieser aber auch nicht völlig ausschließen.

22. Wie bewerten Sie im Vergleich mit anderen Staaten die bisherigen politischen Maßnahmen zur Förderung und Regulierung von Blockchain- und Distributed-Ledger-Technologien und inwiefern besteht hier ein Nachholbedarf? Wie schätzen Sie die aktuellen Bedingungen in Deutschland für die Ansiedlung von Blockchain-Startups ein? Welche finanziellen, strukturellen und regulatorischen Rahmenbedingungen im Bereich von Forschung und Entwicklung und Innovation sind in Deutschland notwendig, damit sich D zu einem Leitmarkt BC/DLT entwickeln?

Förderung und Regulierung der DLT in Deutschland stehen bisweilen noch in ihren Anfängen, insbesondere die Regulierung von Kryptowährungen rückt aber auch international zunehmend in den Fokus. Hier ist positiv hervorzuheben, dass diese Regulierungsmaßnahmen in den meisten Fällen aktuell nicht so weit gehen, dass sie die Innovationskraft der zugrundeliegenden DLT einschränkt. Derzeitig bietet vor allem der Standort Berlin ein attraktives Umfeld zur Ansiedlung von Start-Ups im Kontext von DLT. Dies gilt es durch eine enge Vernetzung zu Wirtschaft, Wissenschaft und Politik zu fördern. Deutschland besitzt mit der in Berlin ansässigen DLT-Szene eine der größten und wichtigsten weltweit. Insgesamt sind dort mehr als 70 DLT-Startups ansässig. Der Standort Deutschland steht jedoch in großer Konkurrenz zu aufstrebenden Standorten, wie z.B. Malta, die sich zum Ziel gesetzt haben mit einem regulatorischen Rahmen und einer DLT-Strategie junge Start-Ups anzuwerben. So wird dort aktuell an einem regulatorischen Rahmenwerk für DLTs und Kryptowährungen gearbeitet. Dieses soll für Transparenz und Rechtssicherheit sorgen. Mit der kürzlich geschaffenen Malta Digital

[6] Siehe https://www.mtgox.com/, abgerufen am 24.11.2018
[7] Für eine übersichtliche Beschreibung siehe https://www.zeit.de/digital/internet/2016-06/the-dao-blockchain-ether-hack, abgerufen am 24.11.2018

Innovation Authority, die sich u.a. mit DLT und KI beschäftigt, stehen digitale Innovationen weit oben auf der Agenda. Hier gilt es nicht den Anschluss und Standortvorteil zu verlieren.

In Bezug auf die strukturellen und finanziellen Rahmenbedingungen ist bedauerlicherweise zu verzeichnen, dass in Deutschland derzeit zu wenige Absolventen mit entsprechender DLT-Expertise aus den Universitäten auf den Arbeitsmarkt kommen. Nötig wäre hier aufgrund des Charakters der Technologie insbesondere eine Förderung von Programmen, welche die Schnittstelle mindestens zweier der Disziplinen Wirtschaft, Recht, Informatik und ggf. Ingenieurwissenschaften bedienen. Zudem Bedarf es projektbezogener Förderprogramme durch die Ministerien, die sich Explizit auf den Aufbau von DL-Infrastrukturlösungen beziehen, welche ohne diese Technologien gar nicht denkbar wären. Solche Förderprogramme müssten in der Zusammensetzung der Konsortien ebenfalls den interdisziplinären Charakter von DLT betonen.

23. Welche Gesetze müssen in Deutschland angepasst werden, um international den Anschluss an neue Geschäftsmodelle, die die Blockchain-Technologie ermöglicht, nicht zu verlieren? Wird die Geschwindigkeit der notwendigen Gesetzesanpassungen insb. bei der Innovationsgeschwindigkeit, die die Blockchain Community vorlegt, und allgemein im digitalen Zeitalter den Anforderungen der Innovationen gerecht und wie sollte der Gesetzgeber diesem schnellen Wandel begegnen?

Deutschland sollte sich um innovationsfreundliche Gesetzgebung und Forschungskultur bemühen. Andernfalls besteht die große Gefahr, dass Ökosysteme außerhalb des Zugriffs deutscher Rechtsprechung entstehen und sich Deutschland im Nachgang mit den geschaffenen Ökosystemen konfrontiert sieht (vgl. die Fragen 9-13, 18).

Eine Möglichkeit Innovation gezielt zu fördern und die Gesetzgebung schnell und zielgerichtet weiterzuentwickeln wäre ein unbürokratisches Genehmigungsverfahren, mit Hilfe dessen Wirtschaft und Wissenschaft in enger Abstimmung mit den Ministerien unbürokratisch isolierte Anwendungsfälle erproben. DL-Proof-of-Concepts, welche in einem solchen Umfeld entstehen, könnten anschließend evaluiert und bei entsprechender Einschätzung auch zu Produktivlösungen erweitert werden. Dieser Ansatz würde kein regulatorisches Sandboxing erfordern und könnte trotzdem Innovationshemmnisse abbauen.

Ein weiterer Ansatz könnte darin bestehen, die inhaltliche Expertise der einzelnen Ministerien einzusetzen. Konkret könnte der Gesetzgeber Leitplanken vorgeben, im Rahmen derer Verordnungen mit „Halbwertszeit“ erarbeitet werden können. Diese wären dann in regelmäßigen Abständen auf Aktualität zu überprüfen. Gerade wenn DLT breit in der öffentlichen Verwaltung zum Einsatz kommen, wären allgemein DLT-Verordnungen oder Gesetze wünschenswert, um Rechtsunsicherheiten zu vermeiden.

24. Inwieweit kann durch die Regulierung von Token-Emissionen zur Unternehmensfinanzierung ein positiver Standorteffekt entstehen? Welche Vorteile hat ein so genannter ICO gegenüber einem IPO? Kommt ein ICO nur für große Unternehmen in Betracht? Welche Unternehmen könnten aus Ihrer Sicht von Token-basierten Finanzierungsmöglichkeiten profitieren? Welche Risiken sehen Sie bei ICOs, insbesondere für die Verbraucherinnen und Verbraucher, aber auch für Unternehmen?

Zunächst ist die Ansiedlung von DLT-Unternehmen nicht vollständig von der Regulierung der Token-Emissionen abhängig. So ist trotz strengerer Regulierung ein starkes Ökosystem in Deutschland entstanden (vgl. Frage 22). Viele Unternehmen verlegen jedoch ihren Sitz oder den Sitz einer assozieerten Stiftung ins Ausland, um Token-Emissionen durchzuführen. Eine transparente Regulierung von Token-Emissionen würde daher Ansiedlung und Bindung junger DLT-Unternehmen weiter begünstigen.

Besonders Malta versucht bereits, einen regulatorischen Rahmen für Kryptowährungen, Kryptobörsen und ICOs zu schaffen. Diese regulatorische Offensive veranlasste bspw. jüngst das Unternehmen Binance (weltweit größte Kryptobörse nach Volumen), seinen Unternehmensstandort von Japan nach Malta zu verlegen. Im Zuge der Umsiedlung sollen u.a. direkt mehr als 200 hochqualifizierte Arbeitsplätze geschaffen werden. Mit der Schaffung eines Rechtsrahmens für Kryptowährungen, Kryptobörsen und ICOs könnte Deutschland seine führende Position in Bezug auf diese Zukunftstechnologie weiter festigen und ausbauen.

Token können nach ihrer Erzeugung über verschiedene Wege an Investoren ausgegeben werden. Der am weitesten verbreitete Ansatz sind dabei „Initial Coin Offerings“ (ICOs – oft auch als „Token Generating Events“ bezeichnet). Im Rahmen dieser werden Token durch Smart Contracts und gegen Bezahlung mit einer Fiat- (bspw. EUR, USD) oder Kryptowährung ausgegeben. Hierbei kommen anders als bei IPOs keine teuren Drittparteien (wie z.B. Banken) zur Vermittlung oder Abwicklung zum Einsatz. Die durch den ICO erzielten Erlöse stehen somit vollumfänglich zur Finanzierung des Entwicklungsvorhabens zur Verfügung. Grundsätzlich kann der Prozess eines ICOs in drei Schritte unterteilt werden. Im ersten Schritt erfolgt die Veröffentlichung eines Whitepapers, welches das zu finanzierende Vorhaben, den zugrundeliegenden Business Plan sowie die geplante technische Umsetzung detailliert beschreibt. Der Whitepaper-Prozess ermöglicht einen frühzeitigen Austausch mit späteren Investoren und Kunden und fördert eine gezielte Anpassung der entwickelten Konzepte und Ideen an deren Wünsche und Erwartungen. In einem zweiten Schritt wird dann eine vorgezogene Investitionsrunde für Großinvestoren und Partner durchgeführt (meist zu vergünstigten Konditionen). Durch diesen „Presale“ sollen gezielt Anreize geschaffen werden, um das Vorhaben gemeinsam zum Erfolg zu führen. Der eigentliche öffentliche ICO folgt dann etwas später in einem dritten Schritt und bietet auch externen Investoren die Möglichkeit, gezielt und frühzeitig in das Vorhaben zu investieren.

Anders als IPOs können ICOs deutlich früher in der Entwicklung eines Unternehmens durchgeführt werden, da sie mit geringeren Kosten und Auflagen verbunden sind. Zudem nimmt die Vorbereitung eines IPOs weniger Zeit in Anspruch. ICOs sind entsprechend v.a. für frühe Finanzierungsrunden von DLT-Start-ups interessant und sind eher mit dem Crowdfunding vergleichbar.

Aktuell ist für ICOs besonders das Stiftungsrecht der Schweiz interessant. Mit einer Strukturierung als Stiftung kann ein gemeinnütziger Steuerstatus beantragt werden, sodass das eingesammelte Geld als Spende behandelt werden kann und nicht an die ICO-

Investoren zurückgegeben werden muss. Verbraucher/-innen gehen bei einer derartigen Beteiligung ein besonders hohes Verlustrisiko ein, welches besonders durch einen Scam (=Vorschussbetrug) oder eine Preismanipulation der gehandelten Tokens auf einer Kryptobörse entstehen kann. Besonders die geringe Transparenz der ICOs wurde mehrmals von Betrügern ausgenutzt, sodass den „Investoren" meist nur die Akzeptanz des Totalverlusts blieb. Für Unternehmen besteht hauptsächlich das Risiko, dass die ausgegebenen Tokens nachträglich von der Behörde als Wertpapiere und dadurch als Sicherheit eingestuft werden. In einem derartigen Fall unterliegen die aus dem ICO hervorgegangenen Unternehmen bestimmten Kapitalmarktregulierungen. Darüber hinaus hat eine nachträgliche Einstufung des Tokens als Wertpapier einen Ausschluss von Kryptobörsen (die nicht für den Handel von Sicherheiten legitimiert sind) zur Folge, was üblicherweise wiederum einen starken Preisverfall des Tokens nach sich zieht.

25. Wie und in welchem Rahmen sollte eine verbindliche Normierung der Token-Typen (etwa in Currency, Equity, Utility, Asset und Reward) erfolgen und was braucht es sonst noch seitens Politik an Regulierung und Förderung oder Anreizsystemen, um schneller und breiter aus technologischen Ansätzen (Potentialen) konkrete Anwendungsideen und tatsächliche Anwendungsfälle zu generieren?

Token-Emissionen sind nach wie vor durch starke Entwicklungen gekennzeichnet. Die hier genannten Token Typen werden überhaupt erst seit wenigen Monaten diskutiert. Welche Ziele mit Token erreicht werden können und welche Einsatzmöglichkeiten sich daraus ergeben, ist noch lange nicht abschließend geklärt. Daher scheint es verfrüht, die derzeit stattfindenden Denkprozesse einzuschränken und durch Standardisierung oder voreilige Regulierung zu limitieren (vgl. Frage 14). Vielmehr sollte im Vordergrund stehen, die vorhandene Kreativität etwa mittels geeigneter Plattformen zur Vernetzung (bspw. Hackathons) oder durch Förderung (bspw. Start-ups) zu nutzen und gegebenenfalls grob in eine Richtung zu lenken, die in Zukunft einen gesellschaftlichen, wirtschaftlichen und ökologischen Beitrag leistet (vgl. die Fragen 23 und 24).

Eine regulatorische Möglichkeit die technologischen Ansätze positiv zu unterstützen könnte darin liegen, durch die Vorgabe juristischer Rahmenbedingung in Form einer Art Lösungsraumes den Gestaltungsspielraum vorzugeben. Da für das Verständnis und die Weiterentwicklung der DLT unterschiedliche Fachrichtungen zusammenarbeiten (müssen), ist eine interdisziplinäre Betrachtung der Themen zwingend notwendig und sollte im Rahmen von Förderungen gestärkt werden. Darüber hinaus könnte auch auf Bundesebene analysiert werden, welche sinnvollen Einsetzungsmöglichkeiten Tokens in der einer digitalen Verwaltung und spielen könnten.

26. Die Beschäftigung mit und die Anwendung der Blockchain-Technologie ist in keinem Bereich soweit fortgeschritten wie im Finanzbereich. Dementsprechend werden auch Regulierungsfragen in Bezug auf Blockchain-Anwendungen im Finanzbereich auf nationaler und internationaler Ebene intensiver diskutiert als in anderen Bereichen. Können die Erfahrungen im Verhältnis von Innovationen und Regulierung auch auf andere Anwendungsbereiche der Blockchain-Technologie übertragen werden?

Zunächst ist die Aussage, dass die Anwendung der DLT im Finanzbereich am weitesten fortgeschritten ist, durchaus strittig, da auch in anderen Sektoren (etwa dem internationalen Warenhandel) Anwendungen von hoher Relevanz, fortgeschrittenem Reifegrad und technologischem Anspruch zu finden sind.

Der Finanzbereich ist lediglich durch die Erstnutzung von DLT als Kryptowährungen früh in den Fokus gerückt. Dabei ist anzumerken, dass in der Regulierung in diesem Bereich mit Ausnahme weniger Länder, wie Japan oder China, in den letzten Jahren nur geringfügige Anpassungen vorgenommen wurden.

Dennoch werden im Finanzbereich bereits seit Einführung der Bitcoin-Blockchain Diskussionen geführt, die nun auch andere Branchen erreichen. Zu beachten ist jedoch, dass DLT-basierte Systeme typischerweise unabhängig von Landesgrenzen entstehen und daher schwer national regulierbar sind.

27. Wie kann die Finanzmarktaufsicht zu einem Enabler von Innovation im Blockchain-Bereich werden?

Durch das aktuelle Urteil des Kammergerichts Berlin, welches Bitcoins nicht als Finanzinstrumente einordnet, ist der Gestaltungsspielraum der BaFin im Kryptowährungsbereich geschwächt worden. Gleichzeitig besteht bei vielen weiteren Arten von Tokens das Erfordernis einzelfallbezogener Prüfungen.

Derzeit ist von außen nicht transparent erkennbar, dass maßgebliche Innovationen im Bereich der DLT in deren Handlungen einbezogen würden. Um zu einem Enabler von Innovation im DLT-Bereich zu werden, müssen die derzeit in der Entwicklung befindlichen Konzepte rund um Kryptowährungen, Token-Emissionen u.a. deutlich stärker in die Betrachtung und Handlungen der Finanzmarktaufsicht einfließen, sodass ein fruchtbarer Nährboden für technologische Weiterentwicklung unter klaren und konstruktiven Rahmenbedingungen geschaffen wird. Um einen Rechtsraum zu schaffen, der sich über Ländergrenzen hinweg erstreckt und sich daher analog zur DLT-Community nicht nach Landesgrenzen richtet, ist dabei eine internationale Vorgehensweise und ein übergreifendes Handeln notwendig (vgl. Frage 16). Beispielsweise besteht aktuell eine große Debatte hinsichtlich der Rechtmäßigkeit der Abwicklung von Transaktionen in Euro auf einem Distributed Ledger. Die zentrale Frage besteht dabei darin, ob Geschäftsbanken explizit damit beauftragt werden sollten oder ob dies eine Aufgabe für die europäische Zentralbank wäre. Wichtig ist grundsätzlich, rechtssicher in Fiat-Währungen (z.B. Euro) abrechnen zu können. Länder wie beispielsweise Schweden und China gehen an dieser Stelle sehr innovative Wege und lassen durch ihre Zentralbanken eigene Kryptowährungen entwickeln. Auch die Direktorin des Internationale Währungsfonds Christine Lagarde hat kürzlich durch ihren Vorschlag einer Digitalwährung in ebendiese Richtung argumentiert (vgl. Frage 17).

Spätestens, wenn in Industrie und Finanzbrache über den Einsatz konkreter, DLT-basierter Anwendungen nachgedacht wird, stellen sich sofort Fragen hinsichtlich derer Behandlung gegenüber der jeweiligen Aufsichtsbehörde. Diese Unsicherheit macht es Unternehmen derzeit äußerst schwer, die genannten Anwendungen in Unternehmensprozesse zu integrieren und entsprechende Business Cases zu rechnen.

Zuletzt wäre es geradezu im Interesse der Finanzmarktaufsicht, DLT zu fördern, da deren Transparenz und Nachvollziehbarkeit auch die Aufsichtsprozesse selbst vereinfachen könnte. Die Frage, welchen konkreten Institutionen hierbei welche Aufgabe zukommt, ist noch zu klären.

28. Bekanntermaßen geht die Anwendung der einiger Blockchain-Technologie mit einem großen Energieverbrauch einher. Gibt es Möglichkeiten und Ansätze, diesen zu begrenzen? Welche künftigen Entwicklungen sehen sie hinsichtlich künftigem Speicherplatzbedarf und Transaktionsraten? Wie könnte eine Massentauglichkeit der Technologie realisiert werden?

Die Assoziation der DLT mit einem hohen Energieverbrauch geht überwiegend auf die bereits 9 Jahre alte Bitcoin-Blockchain zurück. Die Bitcoin-Blockchain nutzt zur Absicherung des Netzwerkes einen Proof-of-Work-Konsensmechanismus, d.h. Teilnehmer am Netzwerk haben einen Anreiz, ein rechenintensives, kryptographisches Rätsel zu lösen, weil für die Lösung eine entsprechende Belohnung in Bitcoin ausbezahlt wird. Diese Problematik ist aus drei wesentlichen Gründen nicht auf andere DLTs übertragbar:

Erstens haben private DLTs üblicherweise einen deutlich geringeren Energieverbrauch als öffentliche DLTs. Der eingeschränkte und bekannte Nutzerkreis mindert Betrugsrisiken und damit auch die Anforderungen an Konsensverfahren.

Zweitens kann das Problem des hohen Energieverbrauchs durch die Wahl eines anderen Konsensmechanismus gelöst werden. Hier gibt es bereits mehrere Alternativen mit einem deutlich niedrigeren Energieverbrauch. Beispielsweise garantiert beim Proof-of-Stake-Verfahren jeder Teilnehmer am Netzwerk mit einem gewissen Anteil an Kryptowährung, dass er nur gültige Transaktionen validiert.

Drittens verwenden neuere DLTs gänzlich andere Architekturen (gerichtete azyklische Graphen), die deutlich höhere Transaktionsraten bei niedrigem Ressourcenverbrauch ermöglichen.

Sowohl der Speicherplatzbedarf als auch die maximale Transaktionsrate hängen maßgeblich von der Art und Weise ab, wie die DLT genutzt werden sollen. In Zeitverlauf wird der Speicherplatzbedarf eines Distributed Ledgers tendenziell wachsen, da wohl immer mehr Daten in einer Distributed Ledger gespeichert werden. Eine mögliche Lösung des Problems stellt dabei eine geschickte Kombination von „Onchain“- und „Offchain“-Speicherung dar (vgl. die Fragen 4 und 13). Die Höhe der maximalen Transaktionsrate hängt stark von der Interaktion mit dem Distributed Ledger ab. Auch hier ist die Wahl des Konsensmechanismus ausschlaggebend. Je nach Konsensmechanismus variiert die Transaktionszahl von variieren von 5-10 bis hin zu mehreren Zehntausend pro Sekunde. Eine Massentauglichkeit hängt stark von der technischen Weiterentwicklung, einem einfachen Zugang zur Technologie sowie der Schaffung eines rechtlichen Rahmens ab.

29. Hat die Blockchain-Technologie das Potential, zur Demokratisierung von Wahlen, Verwaltung, Identifizierung beizutragen?

DLT hat in der Tat das Potential, die digitale Souveränität der Bürger zu stärken. DLT kann gerade bei behördenübergreifenden Prozessen dazu beitragen, einen gemeinsamen Informationsstand unter den beteiligten Institutionen herzustellen, ohne dass es einen zentralen Datensatz für jeden Bürger bräuchte. Die Identifizierung könnte dabei außerhalb dieses Systems erfolgen, etwa durch biometrische Merkmale wie Retina-, Handvenen-, oder Fingerabdruck. Die Sicherstellung der Identifizierung ist somit kein Kern der DLT, sondern der Schnittstelle zum Nutzer. Hierbei ist jedoch besonders sorgfältig darauf zu achten, dass durch den Einsatz von DLT keine

(ungewollten) Überwachungsmöglichkeiten entstehen. Dies kann und muss bereits bei der Konzeption der DL-Anwendung berücksichtig werden.

Im Kontext von Wahlen sollten digitale Technologien aller Art nur mit größter Vorsicht zum Einsatz kommen. Sie sind ein zu attraktives Ziel für Manipulationen. Durch ihre Fähigkeit zur fälschungssichere Dokumentation können DLTs hier einen Beitrag leisten (vgl. Frage 4, Anwendungsmuster 5), die Schnittstelle zum Wähler bleibt allerdings ein möglicher Angriffspunkt (vgl. Frage 21). Daher sollte die Frage DLT-basierter Wahlen in Deutschland erst nach ausreichender Erfahrung mit der Technologie angegangen werden.