Deutscher Bundestag

Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)025

Stellungnahme

von Herrn Prof. Dr. Dr. Walter Blocher

– Universität Kassel, Blockchain-Center.eu –

zur öffentlichen Anhörung

des Ausschusses Digitale Agenda

zum Thema „Blockchain“

am 28. November 2018

Blockchain Center.eu | UNIKASSEL VERSITÄT

Fragen für das Fachgespräch zum Thema Blockchain im Ausschuss Digitale Agenda am 28. November 2018

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?

   Als Oberbegriff umfasst DLT alle Arten replizierter, geographisch verteilter, dezentralisierter Verzeichnisse, deren Konsistenz durch einen Konsens-Mechanismus bewirkt wird. Darauf beruht die Unveränderbarkeit, Zensurresistenz, Resilienz und die ohne gegenseitiges Vertrauen der beteiligten Akteure und vor allem auch ohne dieses Vertrauen substituierende Intermediäre auskommende Funktionalität solcher Verzeichnisse. Damit lässt sich u.a. das zuvor der digitalen Welt inhärente Problem des „double spending“ (das ist die Mehrfachverwendung ein und derselben digitalen Münze durch schlichtes, auf digitalem Weg mit gegen Null gehenden Grenzkosten mögliches Kopieren) lösen, ohne dafür auf Banken oder einen sonstigen „Buchhalter“ angewiesen zu sein. Sie stellen ein „Internet der Originale“ neben das vertraute „Internet der Kopien“ und damit ein „Internet der Werte“ neben jenes „der Information“.

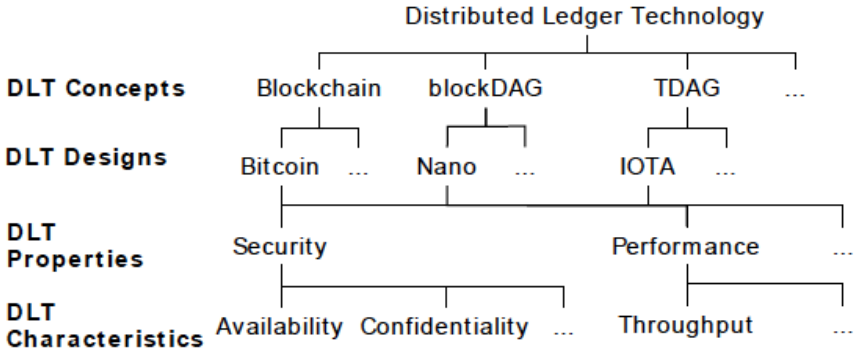

Abbildung 1 aus einer Publikation des am Blockchain-Center.eu angesiedelten Forschungsprojekts “Trusted Blockchain“: N. Kannengießer/S. Lins/T. Dehling/A. Sunyaev, What Does Not Fit Can be Made to Fit! – Trade-Offs in Distributed Ledger Technology Designs, Proceedings of the 52nd Hawaii International Conference on System Sciences (in Druck, erscheint im Januar 2019)

Blockchains sind wichtige Erscheinungsformen der DLT, bei denen Transaktionen in kryptographisch verketteten Blöcken gespeichert werden.

Bitcoin ist ein in mehrfacher Bedeutung verwendeter Begriff, der sich auf die Community, das Netzwerk, das Protokoll, die „Währung“ oder eine Einheit derselben beziehen kann. Auf einem Peer-to-Peer-Netzwerk werden Transaktionen über Satoshi (das ist ein Hundertmillionstel der Einheit Bitcoin) in Form einer auf dem Proof-of-Work-Konsens-Mechanismus beruhenden Blockchain gespeichert. Das so bewirkte global funktionierende digitale Bezahlsystem, das weder auf Staaten noch auf Zentralbanken oder gar auf Geschäftsbanken angewiesen ist, repräsentiert aber nur einen – wenn auch spektakulären – „Proof of Concept“ der Blockchain-Technologie, die für vielfältigste Anwendungen einsetzbar ist. Ihre Vorzüge kommen vor allem dann zur Geltung, wenn heterogene Akteure, die einander nicht kennen oder sich nicht „grün“ sind, zusammenwirken wollen, wobei keiner von ihnen die Führung übernehmen und etwa Transaktionen in einer proprietären Datenbank verzeichnen soll oder will.

Öffentliche Blockchains ermöglichen es erstmals in der Menschheitsgeschichte, Verzeichnisse zur Verfügung zu stellen, in die jeder Einblick nehmen und in die auch jeder schreiben darf, in denen aber nachträglich nichts geändert, gefälscht oder gelöscht werden kann.

Sog. „private Blockchains“ gewähren dagegen nur bestimmten Berechtigten die Befugnis, darin zu schreiben und/oder zu lesen. Ihre Proponenten sprechen oft undifferenziert von „*der* Blockchain“, die sie verwenden würden, ohne darzulegen, unter welchen Bedingungen sich die mit öffentlichen Blockchains untrennbar verbundenen Eigenschaften auf ihre „private Blockchain“ vererben. Je nach der Anzahl ihrer Knoten und der Art des eingesetzten Konsens-Mechanismus ist eine „private Blockchain“ auf einer Skala zwischen den Endpunkten „öffentliche Blockchain“ und „private IT“ anzusiedeln. Je weniger sie einer öffentlichen Blockchain ähnelt, desto wichtiger werden soziales Vertrauen der beteiligten Akteure und klassische IT-Sicherheit. Der Extremfall einer „privaten Blockchain“ mit bloß einem Knoten verwendet zwar möglicherweise dieselbe (Open-Source-)Software wie öffentliche Blockchains, weist aber im Vergleich zu herkömmlicher IT keinerlei erhöhte Zuverlässigkeit der darin verzeichneten Daten auf, da diese jederzeit durch den Betreiber des Knotens verändert werden können. Besteht eine sog. „konsortiale Blockchain“ beispielsweise aus neun Knoten, genügt es, fünf davon zu „hacken“ oder auf sonstige Weise unter seine Kontrolle zu bekommen, um die Daten nach Belieben zu verfälschen.

Die Entscheidung für eine der beiden Arten von Blockchains (in diesem Kontext sollen „private“ und „konsortiale“ Blockchains als eine einzige Art betrachtet werden) hängt davon ab, welche Herausforderungen durch den Einsatz der Blockchain zu bewältigen sind. Soll jedermann Schreibberechtigung haben und zugleich auf einen „vertrauenswürdigen Dritten“ (Intermediär, der rund um die Uhr zur Verfügung steht und für eine ordnungsgemäße Verbuchung der Transaktionen sorgt) verzichtet werden, lässt sich dies nur mit einer öffentlichen Blockchain bewerkstelligen. Sind alle Personen, die eine Schreibberechtigung erhalten sollen, zwar namentlich bekannt, aber hinsichtlich ihrer Vertrauenswürdigkeit und Zuverlässigkeit nicht hinreichend zu beurteilen, lässt sich die daraus resultierende Problematik mit einer „privaten Blockchain“ in den Griff bekommen.

Profitiert Ihr Projekt von einer Blockchain?

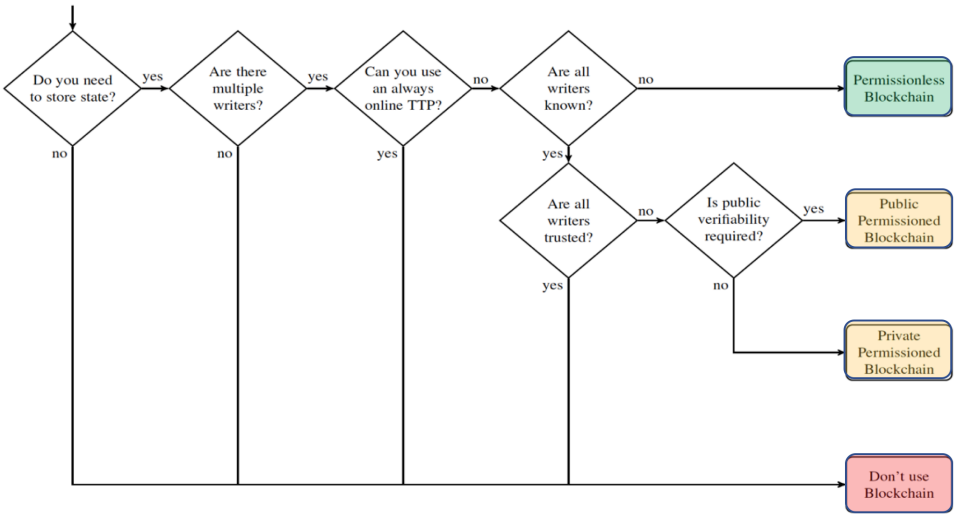

Abbildung 2: nach K. Wüst/A. Gervais, Do you need a Blockchain?, IACR Cryptology ePrint Archive 2017, 375.

Da zwischen den Eigenschaften unterschiedlicher Ausprägungen von Blockchains Zielkonflikte bestehen, wird mit der Entscheidung für eine bestimmte Blockchain-Art zugleich eine Prioritätensitzung hinsichtlich dieser Eigenschaften vorgenommen. So ist eine „private Blockchain“ kostengünstiger, skalierbarer, performanter und vertraulicher als eine öffentliche Blockchain, deren Fälschungssicherheit, Verfügbarkeit, Resilienz und Transparenz damit aber unerreichbar bleiben.

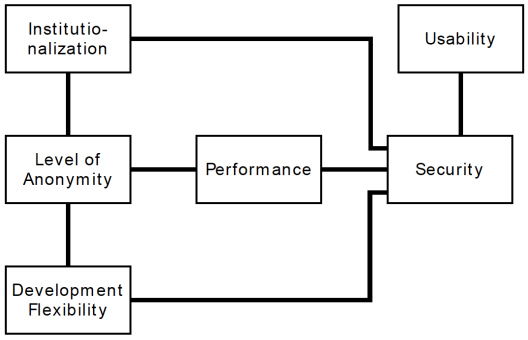

Abbildung 3: Schematische Darstellung der Zielkonflikte zwischen Blockchain-Eigenschaften aus N. Kannengießer et al. (oben, Abb. 1).

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?

Diese Frage lässt sich nur unter Verweis auf den bereits erwähnten Zielkonflikt beantworten: Für die Beurteilung der Einsatzfähigkeit einer bestimmten Ausprägung der DLT/Blockchain-Technologie kommt es auf die für die konkrete Anwendung vorgenommene Prioritätensetzung hinsichtlich der widerstreitenden Eigenschaften an.

Performance Characteristics of Blockchains

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Consistency	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less then 1 minute	P2P mirroring. Limited primarily by network I/O. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Consensus with probability one; Byzantine agreement, but attackers must control less than one-third
System Availability	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less then 1 minute	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Virtual voting; DoS resistant without proof-of-work, fast gossip
Failure Tolerance	Longest chain wins	Longest chain wins	Last balloted block always has consensus.	Content address hash. Highly resilient against network partitioning	Longest chain wins	Strong Byzantine fault tolerance
Scalability	Block size. 7 transactions per second	Block size. 7–20 transactions per second	Thousands to tens of thousands of transactions per second.	Thousands to tens of thousands of transactions per seconds. Scales linearly as nodes are added.	Block size. 7 transactions per second	Thousands to tens of thousands of transactions per seconds. Limited by bandwidth only
Latency	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Virtual voting; limited only by exponentially fast gossip protocol
Auditability	Full	Full	Full	Difficult	Full	Configurable
Liveliness	Full	Full	Full	Fails if nodes storing data fail	Full	Full
Denial of Service Resistance	Spend Bitcoin	Spend Ether	Spend Stellar	Files are only mirrored if requested	Spend Bitcoin	Signed State/ Proof-of-stake/ <1/3 attackers
System Complexity	Medium	High	Medium	Medium	Medium High	Low, but not full system

Abbildung 4 aus A. Anjum/M. Sporny/A. Sill, Blockchain Standards for Compliance and Trust, IEEE Cloud Computing (Juli 2017), DOI: 10.1109/MCC.2017.3791019.

Nach wie vor ist die Bitcoin-Blockchain die älteste, größte, bekannteste und stabilste unter allen Erscheinungsformen von DLT/Blockchain. Ihre Stabilität resultiert aus dem vergleichsweise einfachen ihr zugrunde liegenden Protokoll. Aus heutiger Sicht ist ihre überragende Zuverlässigkeit und vor allem „trustless trust“ nur mit dem Proof-of-Work-Konsens-Mechanismus und dem damit einhergehenden hohen Ressourceneinsatz erzielbar. Dafür stellt Bitcoin eine einzigartige, beeindruckende Infrastruktur zur Verfügung, die unabhängig von Staaten und Rechtssystemen die sichere Durchführung von Transaktionen aller Art (diese können auch Grundstücke, bewegliche Sachen oder immaterielle Güter wie Software-Lizenzen oder auch bloße Berechtigungen, etwa den Zugang zu einer Wohnung, repräsentieren) ermöglicht. Die derzeit mit 1 MB begrenzte Blockgröße beeinträchtigt die Skalierbarkeit. Eine so spektakuläre Einrichtung wie die Bitcoin-Blockchain sollte aber auch gar nicht zur Dokumentation einzelner Geschäfte am Point of Sales missbraucht werden. Sie ist vielmehr wie ein Granitfelsen zu sehen, in dem off-chain oder in einer Side-Chain abgewickelte Transaktionen, jeweils in großer Zahl gebündelt oder saldiert, „verankert“ und damit – mittelbar – abgesichert werden können.

Wird dagegen „trustless trust“ nicht benötigt, weil nur bestimmte oder bestimmbare Akteure untereinander Transaktionen schließen und dazu in das Verzeichnis schreiben können sollen, lässt sich auf der Basis anderer Konsens-Mechanismen (etwa Proof-of-Stake, Delegated Proof-of-Stake und Proof-of-Authority) auch unmittelbar ein wesentlich höherer Durchsatz bei unvergleichlich geringerem Ressourceneinsatz und ohne die mit Proof-of-Work einhergehenden Konzentrationstendenzen im Bereich des Minings (samt der damit verbundenen Gefahr eines sog. „51-Prozent-Angriffs“) erzielen. Die dann notwendig werdende Inanspruchnahme sozialen Vertrauens und die Abhängigkeit von der Zuverlässigkeit klassischer IT-Sicherheit (wie bereits ausgeführt, genügt es in diesem Fall, die Hälfte der beteiligten Knoten erfolgreich anzugreifen, um die gesamte Blockchain zu „übernehmen“) sind als (hoher) Preis für den Verzicht auf „trustless trust“ zu sehen.

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, Energiewirtschaft?

Die in der Frage beispielhaft aufgezählten Bereiche sind zweifellos zu jenen zu zählen, in denen DLT/Blockchain-Technologien großen Nutzen stiften können.

Dabei geht es stets auch um die Frage der Datensouveränität. Diesen Begriff sehen Datenschutzexpertinnen und -experten kritisch, weil er inzwischen von Teilen der Industrie usurpiert wurde. Richtig verstanden geht es aber darum, im Verhältnis Unternehmer/Verbraucher der Verbraucherin, im Verhältnis Gesundheitsdienstleister/Patient der Patientin und im Verhältnis Staat/Bürger der Bürgerin die Hoheit über den Zugriff auf personenbezogene Daten und deren Verwendung zurückzugeben. Das von Datenschutzgesetzen (insb. der DSGVO) geschaffene Schutzniveau ist aus der Sicht der Bürgerin und des Bürgers eine Blackbox. Sie hoffen, dass die Bestimmungen vom Staat sowie seinen Untergliederungen und überdies auch von Unternehmen eingehalten werden und stützen diese Hoffnung u.a. auf das Wirken der Datenschutzbehörden. Dessen, dass sich alle Mitarbeiterinnen von Versandhäusern oder Gesundheitskassen bzw. jede Beamtin und jeder Verwaltungsmitarbeiter einer Behörde im Umgang mit den Daten rechtskonform verhal-

ten, können sie sich allerdings nie ganz sicher sein. Hier könnte die DLT/Blockchain-Technologie dazu beitragen, die Verhältnisse vom Kopf auf die Füße zu stellen.

Selbstverständlich benötigt der Staat für den Erfüllung seiner Aufgaben den Zugriff auf manche personenbezogenen Daten der Bürgerinnen und Bürger. Diese sollten dann auf der Grundlage entsprechender gesetzlicher Verpflichtungen dazu angehalten werden, den Zugriff auf diese Daten zu gewähren, aber nie das Gefühl haben, die Daten würden „über ihre Köpfe hinweg“ erhoben. Mit DLT/Blockchain-Technologie könnte die Freigabe der Daten in die Hand der Bürgerin/Patientin/Verbraucherin gelegt werden. Unter diesen Umständen wäre auch jeder Zugriff auf die Daten transparent und, wegen der Begründungspflicht des zugriffnehmenden Beamten, eindeutig zweckgebunden. Bei einer Blockchain-gestützten Verkehrskontrolle würden dem amtshandelnden Polizeivollzugsbeamten nur der Fahrzeugschein und die Lenkerberechtigung elektronisch präsentiert, nicht dagegen das Geburtsdatum, der Geburtsort oder andere für den Zweck der Amtshandlung nicht relevante Daten.

So ließe sich etwa auch eine Welt vorstellen, in welcher es keines Dringlichkeitsvermerks des Hausarztes und keiner (von den Kassenärztlichen Vereinigungen gem. § 75 SGB V seit dem 23.01.2016 verbindlich zu betreibenden) verwaltungsaufwändigen Terminservicestelle bedarf, um nicht wochenlang auf einen Termin bei seiner Internistin warten zu müssen. Stattdessen würde der Patient über die Blockchain „in die Welt hinausrufen“, dass er am kommenden Freitagnachmittag im Zeitfenster zwischen 14 und 18 Uhr einen Termin bei einem beliebigen (oder mit durchschnittlich mindestens vier Sternen von seinen Patientinnen bewerteten) Internisten in Hamburg oder in einem Umkreis von 15 km Durchmesser benötigt. Der durch das automatische Matching gefundenen Fachärztin mit einem passenden Termin könnte der Patient nun z.B. Zugang auf die aus bildgebenden Verfahren gewonnenen Befunde der letzten zwölf Monate gewähren und damit das Problem der Portabilität von Gesundheitsdaten lösen. In ähnlicher Weise wäre es möglich, die für Finanzdienstleistungen erforderliche Legitimationsprüfung dadurch zu erleichtern, dass ein und dieselben KYC-Daten nicht wieder und wieder erfasst werden müssten, sondern durch den Kunden dem neuen Dienstleister gegenüber freigegeben werden könnten (vgl. hierzu W. Blocher, C2B statt B2C? – Auswirkungen von Blockchain, Smart Contracts & Co. auf die Rolle des Verbrauchers. In: P. Kenning & J. Lamla (Hrsg.), Entgrenzungen des Konsums, 87-107, [2017]).

In der Energiewirtschaft geht es vorrangig um ein Fundament für die dezentrale Energieversorgung, die ohne Blockchain-gestützte Abrechnungsverfahren kaum vorstellbar ist. Auch der Anbieterwechsel „on the fly“, der etwa die Elektromobilität ganz erheblich voranbringen könnte, wäre so zu realisieren.

Als weitere vielversprechende Einsatzgebiete für DLT-Blockchain-Technologien sind generell Finanzdienstleistungen (etwa Clearing sowie Settlement im Wertpapierhandel und Handelsfinanzierung aber auch P2P-Kredite ohne zentralen Kreditgeber und P2P-Versicherungen ohne zentralen Versicherer), die staatlichen Register, die Buchführung und Prüfung von Unternehmen, die Etablierung betrugsresistenter Steuererhebungsverfahren, die manipulationssichere Speicherung von Kilometerständen und eingehaltenen Service-Intervallen bei Fahrzeugen, das digitale Identitätsmanagement, die Verrechnung zwischen Telekom-Providern, die

Ausstellung von Herkunftszertifikaten aller Art (insb. im Zusammenhang mit Lebensmitteln), die digitale Bescheinigung von Ausbildungsabschlüssen, Vollmachten und sonstigen Befugnissen, die effizientere Gestaltung des Supply-chain-Managements, der Aufbau und die Adaptierung von Compliance-Systemen, die unternehmensübergreifende Verwaltung von Messdaten oder die Mensch-Maschine-Interaktion sowie die Maschine-zu-Maschine-Kommunikation in der Industrie 4.0, der multimodale Personen- und Güterverkehr, Petitionen und Abstimmungen, das Management und die Durchsetzung von Immaterialgüterrechten, sowie – last but not least – die Einführung digitalen Zentralbankgeldes zu nennen.

Das noch wenig erforschte Gebiet der Token-Ökonomie könnte u.a. Wege zur Lösung des Problems weisen, dass im E-Commerce der Markt von einigen wenigen Plattformen dominiert wird, weil Netzwerkeffekte, Skaleneffekte und Effekte der Datenökonomie den Marktzutritt von innovativen Ansätzen nahezu unmöglich machen. Durch die Verarbeitung und Speicherung sowohl der Stammdaten von Kunden als auch der von ihnen durchgeführten Transaktionen wurden diese zentralen Plattformen überdies zu „Datenkraken“, welche ihre Kunden nicht nur besser kennen, als diesen lieb sein kann, sondern durch die gefährliche Akkumulation von Benutzerprofilen als „Honeypots“ fungieren, von denen sich Hacker angezogen fühlen, wie Bären von Honigseim. Der Token-Ökonomie wird das Potenzial zugeschrieben, Märkte radikal zu verändern und neue zu schaffen. So werden sich die Machtverhältnisse zwischen den bisherigen Akteuren verändern und überdies neue Akteure (Maschinen, Software-Agenten) auf den Plan treten. So wird eine Verbesserung der Position des Verbrauchers erwartet, der künftig nicht nur aus unternehmerseitig zusammengestellten Angebotsbündeln aus Waren, Dienstleistungen und/oder Allgemeinen Geschäftsbedingungen zu mehr oder weniger feststehenden Preisen wählen („B2C“), sondern – etwa in Form von „Mini-Ausschreibungen“, die auf beiden Seiten von Software-Agenten abgewickelt werden – auf dem Markt seine tatsächlichen Bedürfnisse artikulieren kann (diese Veränderung der Machtverhältnisse ist Gegenstand des Forschungsprojekts „C2B“ am Blockchain-Center.eu). Zudem ist mit einer Öffnung von Märkten zu rechnen (u.a. – wie bereits erwähnt – auf dem Energiesektor oder im Transportwesen), wodurch die Grenzen zwischen Anbieterinnen und Verbraucherinnen zerfließen. Mittels auf DLT/Blockchain-Technologie beruhender „Tokens”, die Vermögensgegenstände aller Art digital repräsentieren können, lassen sich nicht nur Märkte unter Ausschaltung überkommener Intermediäre etablieren, sondern auch völlig neue Koordinationsformen entwickeln (dies ist u.a. Gegenstand des Forschungsprojekts „Crypto Assets“ am Blockchain-Center.eu).

Viele der gennannten Anwendungsbereiche für DLT/Blockchain-Technologie könnten von – weitestgehend noch zu leistender – Standardisierung profitieren. Manche Einsatzbereiche setzen die eine oder andere Anpassung des bestehenden rechtlichen Rahmens (z.B. die Berücksichtigung von Blockchains und Hashwerten in Formvorschriften) voraus, für andere wäre ein erst zu schaffender klarer Rechtsrahmen ein Kriterium der Investitionssicherheit und damit ein entscheidender Standortfaktor. Wesentliche Impulse könnten auch von einer deutlichen Verstärkung der einschlägigen personellen Ressourcen in Ministerien und Behörden (etwa BSI, BNetzA, BaFin) ausgehen.

Der Erfolg von DLT/Blockchain-Technologie hängt in hohem Maße von der Akzeptanz auf Unternehmerinnen- und Verbraucherseite ab. Daher wären Maßnahmen

zu deren Förderung (regionale Schaufenster, Vermittlung von Hands-on-Erfahrung, Berücksichtigung in Lehrplänen) hilfreich.

Nicht zuletzt bedarf die DLT/Blockchain-Technologie enormer multidisziplinärer Forschungsanstrengungen, um das von ihr erwartete Wachstumspotential zur Entfaltung bringen zu können. Da es dabei u.a. darum geht, den „First-mover advantage“ zu lukrieren sowie im Wettbewerb der Nationen und Wirtschaftsregionen möglichst viele Arbeitsplätze auf diesem Feld der digitalen Transformation zu attrahieren, ist hier eine Art „Windhundrennen“ zu beobachten. Möglichst rasch zur Verfügung gestellte Forschungsmittel dürften sich gesamtwirtschaftlich deutlich besser zu Buche schlagen, als mit der üblichen Zeitverzögerung erfolgende Zuwendungen.

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?

In der Antwort auf Frage 3 wurden bereits Anwendungsbereiche genannt, für die von DLT/Blockchain klar bessere (weil effizientere, transparentere, datenschutzkonformere oder den Marktzugang erleichternde) Ergebnisse als von etablierten Technologien erwartet werden. Festzustellen ist allerdings, dass in der noch frühen Phase des Technologielebenszyklus (Entstehungsphase, allenfalls in Teilbereichen bereits Wachstumsphase) noch wenige vorzeigbare Use Cases existieren.

Zuvorderst ist hier wohl nach wie vor Bitcoin als „Währung“ zu nennen, die innerhalb weniger Minuten sichere und kostengünstige Transaktionen „rund um den Globus“ zulässt, was die diesbezügliche Performanz herkömmlicher Finanzdienstleister deutlich in den Schatten stellt.

Als funktionierender Anwendungsfall im Bereich der Herkunftsnachweise kann das von De Beers etablierte System tracr.com präsentiert werden, das den Weg eines Diamanten von der Mine bis zum Endkunden dokumentiert und damit dazu beiträgt, den Handel mit sog. „Blutdiamanten“ zu bekämpfen.

Der Blockchain-gestützte Sekundärhandel mit Software erfüllt auch die strengen Anforderungen der deutschen Rechtsprechung hinsichtlich des Nachweises einer ununterbrochenen Rechtekette (https://www.softandcloud.com/de/blockchain/).

Die Hälfte der Führungskräfte der deutschen Energiewirtschaft gibt an, dass in ihrem Unternehmen mit Blockchain-Technologie zumindest bereits experimentiert wird (https://www.dena.de/newsroom/revolutioniert-blockchain-die-energiewirtschaft/).

Industrie 4.0 und IoT sind ohne Blockchain-Fundament kaum denkbar, da hierbei stets heterogene Akteure handeln, die sich nicht auf die Zuverlässigkeit eines Verzeichnisses verlassen wollen, das von einem anderen der Beteiligten geführt wird.

Es ist ein bekanntes Phänomen, dass Kriminelle zu den „Early adopters“ neuer Technologien zählen, da sie sich davon einen Vorsprung vor Strafverfolgungsbehörden und damit eine Reduktion ihres persönlichen Risikos erhoffen. So litt die bedeutende Entwicklung Bitcoin zunächst unter einem „halbseidenen“ Ruf, der auf ihre frühe Verwendung als Zahlungsmittel auf dem Darknet-Schwarzmarkt „Silk

Road“ zurückzuführen war. Bis heute ist Bitcoin ein im Darknet beliebtes Zahlungsinstrument, dem allerdings nicht oder zumindest wesentlich schwerer zurückzuverfolgende Coins wie Monero den Rang abgelaufen haben. Bei alledem sollte nicht übersehen werden, dass sich für Geschäfte in der Schattenwirtschaft, für Bestechung, internationale organisierte Kriminalität und Terrorfinanzierung Bargeld nach wie vor größte Beliebtheit erfreut. Dennoch ist es nicht der Grund für kriminelle Taten, auch wenn es wegen seiner relativen Anonymität und hohen Akzeptanz für die Verschleierung illegaler Transaktionen genutzt wird (H. Mai, Bargeld und Kriminalität, in: J. Lempp/T. Pitz/J. Sickmann (Hrsg.), Die Zukunft des Bargelds [2018], 134). Ebenso verhält es sich mit Bitcoin und anderen Kryptowährungen. In diesem Zusammenhang mag es sogar ein tröstlicher Gedanke sein, dass deren Übertragung – anders als jene von Bargeld – keinen persönlichen Kontakt erfordert, sodass zumindest daraus keine Gefahr für Leib und Leben der an der Transaktion Beteiligten resultiert.

Per se gefährliche DLT/Blockchain-Anwendungen sind dem Verfasser dieser Stellungnahme und den Angehörigen des Blockchain-Center.eu kaum bekannt. Zu denken wäre allenfalls an für strafbare oder sonst verpönte Zwecke unter Zuhilfenahme unaufhaltsamer Smart Contracts ausgesetzte Belohnungen oder die auf dieselbe Art und Weise bewirkte Steigerung der „Effizienz“ von Ransomware-Angriffen.

Sollte sich die Frage aber mehr auf allgemeine Grenzen und Herausforderungen der DLT/Blockchain-Technologie beziehen, wären – jedenfalls von einem „zentralistischen“ Standpunkt aus betrachtet – im Hinblick auf die Bitcoin-Blockchain und andere öffentliche Blockchains (wie Ethereum) insbesondere folgende Punkte zu nennen:

- die noch nicht ausreichend erforschten Bedingungen für die Stabilität des jeweiligen Ökosystems
- der mit öffentlichen Blockchains verbundene Ressourcenverbrauch
- die Tendenz zur Konzentration der Hashing Power
- die mangelnde Skalierbarkeit („block size debate“)
- das Fehlen eines Konsens-Mechanismus für Änderungen des der Blockchain zugrundeliegenden Protokolls
- die relative Regulierungsresistenz
- die fehlende Zurechenbarkeit (kein „Betreiber“ oder sonstiger Verantwortlicher)
- die derzeit noch fehlende Resistenz gegen künftig verfügbare Quantencomputer

Im Zusammenhang mit Smart Contracts geben derzeit u.a. folgende Aspekt Anlass zur Sorge:

- die wegen der grundsätzlich angestrebten Unveränderbarkeit zugleich gegebene mangelnde Korrigierbarkeit von Fehlern (vgl. “The DAO“, dessen katastrophaler Programmierfehler einem Angreifer das „Abziehen“ von 60 Mio. USD ermöglichte, was schließlich durch eine „Hard Fork“ ungeschehen

gemacht wurde, die der Ethereum-Blockchain in Gestalt des damit verbundenen Reputationsverlusts aber einen hohen Preis abverlangte)

- die fehlende Möglichkeit einer angemessenen Reaktion auf unvorhergesehene Ereignisse
- der fehlende Raum für die Interpretation von Code im juristischen Sinne
- bislang ungeklärte Haftungsfragen
- die wegen des grundsätzlich globalen Charakters von Smart Contracts an die Grenzen der Leistungsfähigkeit des Internationalen Privatrechts stoßenden Fragen nach dem darauf anwendbaren Recht
- die bereits erwähnten „kriminellen“ Smart Contracts
- bislang ungelöste Fragen des Verbraucherschutzes und weitere Regulierungsfragen

5. Welche gesellschaftlichen, aber auch ökonomischen, ökologischen und sozialen 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?

An dieser Stelle sei zunächst auf die Beantwortung der Fragen 1 und 2 verwiesen. „Private Blockchains“ sind danach mit einem vergleichsweise geringen Ressourcenverzehr verbunden und weisen einen hohen Durchsatz auf, setzen dafür aber soziales Vertrauen zwischen den Akteuren voraus und sind überdies von der Zuverlässigkeit klassischer IT-Sicherheit abhängig. Im Extremfall hat eine „private Blockchain“ annähernd dieselben Eigenschaften wie eine privat betriebene relationale Datenbank, ist aber wegen der verwendeten kryptographischen Komponenten etwas nachvollziehbarer sowie transaktionssicherer (vgl. S. Voshmgir, Blockchains, Smart Contracts und das Dezentrale Web [2016], 16; Internet-Quelle) und deshalb zugleich etwas weniger flott. Welche Blockchain-Art für eine bestimmte Anwendung in Betracht kommt, hängt im Wesentlichen von der Bekanntheit oder Anonymität der beteiligten Knotenbetreiber und von deren Vertrauenswürdigkeit ab:

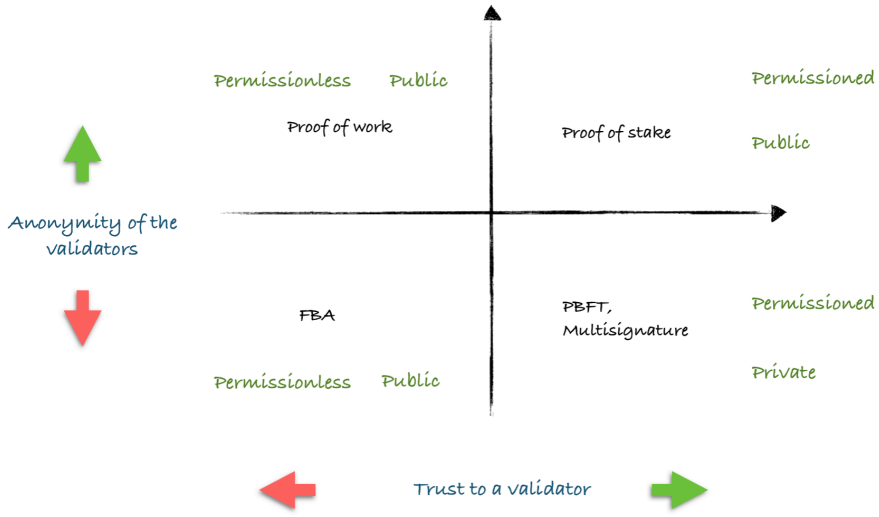

Abbildung 5 aus P. Kravchenko, Ok, I need a blockchain, but which one? (2016), https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100

Öffentlich-genehmigungsbasierte Blockchains erlauben nicht jedermann, sich mit einem Knoten zu beteiligen, weisen daher weniger Knoten sowie gesteigerte Vertraulichkeit auf und sind wegen der geringeren oder fehlenden Transaktionsgebühren auch weniger ressourcenintensiv und daher je Transaktion kostengünstiger als öffentlich-genehmigungsfreie Blockchains wie Bitcoin und Ethereum. Allerdings zeigen nur Letztere in uneingeschränkter Weise die Blockchains häufig zu pauschal zugeschriebenen Eigenschaften Unveränderbarkeit, „trustless trust“, Resilienz etc. Der mit der geringeren Anzahl von Knoten einer öffentlich-genehmigungsbasierten Blockchain erzielbare höhere Durchsatz wird um einen hohen Preis erkauft: Die relative Übersichtlichkeit des Netzwerkgraphen steigert die Vorhersehbarkeit von Kommunikationspfaden, was die gezielte Störung der Kommunikation ermöglicht und damit auch erfolgreiche Angriffe auf die Ausgewogenheit der Blockchain („balance attack“) mit dem Ziel, Forks zu provozieren, um das Verzeichnis in betrügerischer Absicht „umzuschreiben“, nämlich nur in dem nicht mehr weiterverfolgten Zweig der Blockchain eingebundene Transaktionen im Nachhinein „ungeschehen“ zu machen und damit „double spending“ zu bewirken (vgl. N. Kannengießer et al. [oben, Abb. 1]).

„Private Blockchains“ werden häufig innerhalb eines Unternehmens eingesetzt, um nicht mehr zeitgemäße papiergebundene oder sonst veraltete oder redundante Formen der Datenhaltung zu ersetzen. Der hierdurch arg verwässerte Modebegriff „Blockchain“ wird zuweilen auch dazu verwendet, längst fällige Modernisierungsschritte der unternehmenseigenen IT gegenüber den Mitarbeiterinnen und Mitarbeitern zu rechtfertigen („blockchain as an excuse“). Manche Beobachter sagen den „privaten Blockchains“ dasselbe Schicksal wie den „Intranets“ der 1990er-Jahre voraus, die – spätestens mit dem Aufkommen des Web 2.0 – fast vollständig vom Internet verdrängt wurden, zumal andere kryptographische Verfahren, wie digitale Signaturen und insbesondere das Zero-Knowledge-Protokoll hierfür deutlich geeigneter erscheinen als „private Blockchains“ (vgl. V. Buterin, On Public and Private Blockchains [2015]; Internet-Quelle).

Öffentlich-genehmigungsbasierte Blockchains betreibt ein Konsortium, weshalb man sie auch als „konsortiale Blockchains“ bezeichnet. Sie werden häufig von Finanzdienstleistern und im Bereich der Energiewirtschaft eingesetzt. Beispiele sind R3, The Energy Web und The Blockchain Insurance Initiative.

Grundsätzlich kommen konsortiale Blockchains auch für bestimmte Aufgaben der öffentlichen Verwaltung in Betracht, bei denen aus Gründen des Datenschutzes oder der Governance auf die überragende Zuverlässigkeit und Transparenz öffentlicher Blockchains verzichtet werden soll.

Öffentlich-genehmigungsfreie Blockchains (Synonym: „die Blockchain“) haben ihre Wurzeln in der Cypherpunk-Szene, also im Kreise jener meist jungen, gut ausgebildeten Aktivisten, die im verbreiteten Einsatz von Kryptographie und datenschützenden Technologien ein Mittel zur Herbeiführung sozialer Reformen und der Stärkung des für eine offene Gesellschaft unverzichtbaren Diskurses sehen. Auch wenn bis heute nicht aufgedeckt wurde, wer mit dem Pseudonym Satoshi Nakamoto als Mastermind hinter der Entwicklung von Bitcoin steckte, lässt sich auch die ein wenig „subversive“ Herkunft des ohne Finanzinstitutionen funktionierenden Bezahlsystems nicht verleugnen, dessen Whitepaper am 31. Oktober 2008 und damit ausgerechnet am Weltspartag unmittelbar nach dem Höhepunkt der Weltfinanz- und -wirtschaftskrise veröffentlicht wurde. Es hat unzweifelhaft das

Potential, Machtverhältnisse „bottom up“ zu verändern. Gerade deshalb werden sowohl Bitcoin als „die Mutter aller Blockchains“ als auch alle anderen öffentlich-genehmigungsfreien Blockchains vor allem von totalitären Regimen bekämpft oder zumindest mit Argwohn betrachtet. Aber auch jene Akteure in demokratischen Staaten, die ihre Macht der Existenz vertauensstiftender Intermediäre (wie Zentralbanken, Geschäftsbanken, Versicherungen, um nur einige zu nennen) verdanken, suchen nach Wegen, den Spieß umzudrehen und nun ihrerseits die Existenzberechtigung solcher Blockchains in Frage zu stellen. So werden sie etwa nicht müde, Bitcoin totzureden, aber die Blockchain-Technologie als solche zu preisen und dabei meist doch nur die konsortiale Blockchain, an der ihre Institution beteiligt ist, oder gar deren private zu meinen.

Bei Lichte betrachtet, sind jedoch öffentlich-genehmigungsfreie Blockchains die eigentlichen „Game Changer“. Sie können etwa bislang allenfalls durch das Vertrauen in Gütesiegel für Verbraucherinnen einigermaßen nachvollziehbare Aussagen über fair gehandelte Produkte auf jedem Punkt der Wertschöpfungskette bis hin zum Farmer oder der einzelnen Landarbeiterin nachprüfbar machen. Menschen aus Ländern der vierten Welt, die wir neudeutsch als „underbanked“ oder „unbanked“ bezeichnen, lassen sie nach dem Motto „be your own bank“ endlich auch an den Segnungen und nicht nur an den Herausforderungen der globalisierten Wirtschaft teilhaben. Mit Blockchain-gestützten Methoden ließe sich dort die Korruption bekämpfen, durch grundbuchartige Landregister das Ergebnis oft lebenslanger harter Arbeit eindeutig den Berechtigten zuordnen und durch digitale Wahlsysteme eine Grundvoraussetzung für demokratische Strukturen schaffen. Freilich ist zu erwarten, dass die derzeitigen Machthaber dem nicht tatenlos zusehen werden. DLT/Blockchain-Technologie könnte es ihnen aber bedeutend schwerer machen, die derzeitigen Zustände aufrechtzuhalten. Schon unter diesem Aspekt sollten demokratische Rechtsstaaten öffentlich-genehmigungsfreien Blockchains tendenziell mit Wohlwollen begegnen, statt ihre Anwendung und Fortentwicklung auf der Grundlage zu kurz greifender Argumente zu erschweren.

Vor der Anwendung öffentlich-erlaubnisfreier Blockchains zur „Auslagerung“ bisheriger Staatsaufgaben oder auch nur zur transparenteren Erfüllung solcher Aufgaben durch den Staat ist freilich sorgfältig zu analysieren, welchen Kriterien derartige Blockchains genügen müssen, um kein unkalkulierbares Risiko einzugehen (dies ist u.a. Gegenstand des Forschungsprojekts „Trusted Blockchain“ am Blockchain-Center.eu). So ist die Tendenz solcher Blockchains, die für den Proof-of-Work-Konsens-Mechanismus erforderliche Hash Rate auf relativ wenige potente Miners zu konzentrieren, besonders dann problematisch, wenn diese in Ländern ihren Sitz haben, die keinen Art. 14 GG (Eigentumsgarantie) kennen, sodass entweder die das Mining betreibenden Unternehmen oder deren Energielieferanten dem (fremden) staatlichen Zugriff ausgesetzt sind. Die spieltheoretische Absicherung solcher Blockchains greift nämlich nur dann, wenn rationale Akteuere monetäre Ziele verfolgen. Will ein mächtiger Akteuer (Staat) aus anderen, insbesondere politischen Gründen eine öffentlich-erlaubnisfreie Blockchain desavouieren und damit die davon abhängigen Verwaltungen und/oder Wirtschaftszweige (insbesondere anderer Länder) in Bedrängnis bringen, mag ihm dies gelingen. Auf der Grundlage solcher Überlegungen scheint es besonders lohnend zu sein, die Möglichkeit der Etablierung bundesländer- und staatenübergreifender oder gar europäischer Blockchains zu prüfen. Wegen der dann notwendigerweise begrenzten

Zutrittsmöglichkeit für weitere Knoten wären solche Blockchains i.S.d. derzeit üblichen Terminologie nicht als „öffentlich-erlaubnisfrei“ zu klassifizieren. Vor allem bei einer erheblichen Anzahl von Knoten, die überdies von Institutionen mit erheblicher Reputation betrieben werden, hätten sie aber ähnliche Eigenschaften ohne zugleich die geschilderten Nachteile mit sich zu bringen.

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

Hier als „öffentlich-genehmigungsfrei“ bezeichnete Blockchains werden immer und ohne weitere Voraussetzungen Intermediäre ersetzen. Dies wird allerdings weniger – wie von manchen erwartet – in „disruptiver“ Weise, sondern – je nach dem Grad der Akzeptanz durch Verbraucher und Unternehmerinnen – allmählich erfolgen. Zugleich sorgen Anpassungsprozesse dafür, dass die Angebote der bisherigen Intermediärer – jedenfalls der entsprechend flexiblen – innovativer und damit attraktiver werden. So hat schon die bloße Möglichkeit, mit Bitcoin in kürzester Zeit globale Finanztransaktionen abwickeln zu können, zur rascheren Entwicklung von Echtzeit-Bezahldiensten im Banken- und Kreditkartensektor beigetragen.

Umgekehrt werden auch Blockchain-basierte Koordinationsmechanismen, die etwa Funktionen der großen E-Commerce- und Social-Media-Plattformen wie Amazon, Facebook, YouTube, Instagram, LinkedIn, Twitter, Xing, Uber oder Airbnb übernehmen könnten, auf die Entwicklung und ständige Verbesserung benutzerfreundlicher Apps sowie auf entsprechendes Marketing angewiesen sein. Daher ist auch längerfristig nicht von der vollständigen Ersetzung von Intermediären auszugehen, sondern davon, dass es durch DLT/Blockchain-Technologie mehr Wettbewerb geben wird. Neben den verbleibenden (adaptiven) Platzhirschen, die z.B. mit ihrer Erfahrung und Reputation punkten können, werden jedenfalls – und deutlich leichter, als vor dem Hintergrund der derzeitigen Situation in der Plattform-Ökonomie – auch neue Anbieter eine Chance auf den Markteintritt erhalten.

Letztlich wird – wie im Laufe der Wirtschaftsgeschichte bereits wiederholt zu beobachten war – auf die Phasen der Intermediatisierung und der Disintermediatisierung eine solche der Reintermediatisierung folgen. Nachteile kann dies vor allem für zu wenig anpassungsfähige bisherige Intermediäre haben, die es nicht rechtzeitig schaffen, ihr Geschäftsmodell entsprechend anzupassen. Hier werden zweifellos auch Arbeitsplätze verloren gehen. Gesamtwirtschaftlich betrachtet sollte aber der aus der Steigerung des Wettbewerbs resultierende Nutzen deutlich überwiegen.

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

Hiermit wird das Problem der „Blockchain Governance“ angesprochen. Das von Satoshi Nakamoto (wer immer das sein mag) entworfene Design von Bitcoin ist bemerkenswert: Es kombiniert hinlänglich bekannte Funktionen und Entwicklungen auf dem Feld der Kryptographie (öffentliche und private Schlüssel, Hash-Werte, Merkle-Bäume) in genialer Weise mit spieltheoretischen Erkenntnissen und Konstrukten (Proof-of-Work). Was ihm allerdings fehlt, ist ein expliziter Mechanismus für die Anpassung an künftige Erfordernisse. Ein solcher ist aber nicht nur in der Evolution lebendiger Organismen wegen der Selektion i.S.v. „survival of

the fittest“ für längerfristigen Erfolg entscheidend. So scheint es auch für eine globale, dezentrale Blockchain unangemessen zu sein, dass Entscheidungen über die Fortentwicklung des sog. „Protokolls“, also der die „Spielregeln“ enthaltenden Software, „off-chain“, etwa über Mailing-Listen oder gar bei Besprechungen von Core-Entwicklern in Hotelzimmern, getroffen werden. Freilich hängt die Umsetzung dieser Entscheidung noch davon ab, ob diese auch von den Miners und letztlich auch von den Betreibern der Knoten mehrheitlich mitgetragen wird. Diese Form der „impliziten Governance“ bietet vor allem neu hinzukommenden Entwicklern nur geringe Anreize, innovative Vorschläge zu unterbreiten. Stattdessen konzentriert sich die Entscheidungsmacht zunehmend bei einer vergleichsweise kleinen und tendenziell an der Erhaltung des Status quo interessierten Gruppe von Core-Entwicklern aus der frühen Phase von Bitcoin. Aus der Kombination dieses Umstands mit der Konzentration eines großen Anteils an der Hash Rate bei relativ wenigen Miners resultiert die Gefahr der schleichenden Zentralisierung der Machtverhältnisse im Bitcoin-Netzwerk, das sich ja eigentlich der Dezentralisierung verschrieben hat.

Freilich besteht für Akteure, die mit der Entwicklung einer öffentlich-genehmigungsfreien Blockchain unzufrieden sind, stets die Möglichkeit, ihre Token abzustoßen oder – wenn sie davon überzeugt sind, es „selbst“ resp. zusammen mit ihren Gefolgsleuten besser machen zu können – eine Hard Fork zu bewirken, die alle bisherigen Eigenschaften der Ursprungs-Blockchain und deren Transaktionshistorie bis zum Tag des Forking übernimmt, aber hinsichtlich ihrer Fortentwicklung einem anderen Machtgefüge unterliegt.

Vergleichbares gilt für das hinsichtlich der in diesem Zusammenhang entscheidenden Punkte ähnlich aufgebaute Etherum-Netzwerk. Die geplante Umstellung von Proof-of-Work auf Proof-of-Stake als Konsens-Mechanismus könnte allerdings den geschilderten Konzentrationstendenzen entgegenwirken, da es das Gefälle zwischen Miners und Nutzern deutlich verringern oder gänzlich aufheben wird.

Jüngere Entwicklungen im Bereich der Blockchain-Technologie experimentieren mit Konzepten der „On-Chain-Governance“. Dabei wird etwa abhängig vom Ergebnis einer Abstimmung unter allen Nutzern eine neu vorgeschlagener Code-Sequenz zunächst getestet und im Fall eines erfolgreichen Tests dem auf diese Weise evolvierenden Protokoll hinzugefügt, was demjenigen, der die Änderung vorgeschlagen hat, zugleich eine Belohnung in der Form von Protokoll-Tokens (also von Einheiten der dieser Blockchain zugrundeliegenden „Währung“) verschafft.

So überzeugend derartige Entwicklungen auf den ersten Blick scheinen mögen, bergen sie doch erhebliche Gefahren in sich: Gewissermaßen auf der „Mikroebene“ werden Koordinationsprozesse erleichtert, was tendenziell zu mehr Gerechtigkeit führen sollte. Andererseits wird es auf der „Makroebene“ immer schwieriger, die Meta-Struktur der Governance – also gewissermaßen deren „Verfassung“ – zu ändern, was das System letztlich angreifbar macht.

Letztlich ist davon auszugehen, dass es für jede Ausformung der Blockchain-Governance passende Anwendungsbereiche gibt. Wenn es – wie bei Bitcoin – um die zuverlässige Aufzeichnung von Transaktionen über Werte geht, ist möglicherweise der eher konservative Ansatz vorzuziehen, während eine raschere Mutationen ermöglichende Governance mehr zu einem dynamischeren Umfeld passen

mag. (Vgl. zu allen hier angesprochenen und noch einigen weiterführenden Punkten den überaus lesenswerten Beitrag F. Ehrsam, Blockchain Governance: Programming Our Future [2017]; Internet-Quelle.)

Zum Stichwort „Standards“ ist anzumerken, dass sich diese häufig als „De-facto-Standards“ durch Marktmechanismen oder auf Grund ihrer Definition seitens mächtiger Stakeholders ergeben. Dagegen werden technische Standards durch Normengremien verabschiedet und De-jure-Standards durch den Gesetzgeber vorgegeben. Standards können aus Inkompatibilitäten resultierende Effizienzverluste vermeiden helfen, was einer noch jungen Technologie zum Durchbruch verhelfen mag. Dagegen wirken sie längerfristig tendenziell innovationshemmend, da Übergänge zwischen Standards meist schwierig sind, weil sich die Überlegenheit eines bisher nicht realisierten Standards schwer zeigen lässt.

Der Standards setzende Gesetzgeber läuft stets Gefahr, sich dem Vorwurf der Wissensanmaßung auszusetzen. Andererseits kann ein ausreichende Flexibilität erlaubender Standard einen Punkt in der Nähe des vermuteten Optimums definieren, von dem aus es dem Markt rascher gelingt, sich zum tatsächlichen Optimum „einzuschwingen“. Vor diesem Hintergrund sind grundsätzlich auch Bemühungen zur Definition von Standards für Blockchains zu sehen. Bei öffentlich-genehmigungsfreien Blockchains tritt allerdings noch die Problematik des Unterfangens hinzu, eine dezentrale Einrichtung mittels zentraler Normsetzung regulieren zu wollen.

Auf diesem Feld besteht noch viel ökonomischer und juristischer, vielleicht auch politikwissenschaftlicher, soziologischer und informationswissenschaftlicher Forschungsbedarf.

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?

Irrtümlich oder sonst ohne Rechtsgrund auf einer Blockchain verzeichnete Transaktionen sind mit der versehentlichen Übereignung gesetzlicher Zahlungsmittel vergleichbar: Auch diese lässt sich nicht rückgängig machen, aber man kann eine gegenläufige Transaktion (Rückübereignung, Rücküberweisung) durchführen und erforderlichenfalls mit den Mitteln der Zwangsvollstreckung erzwingen lassen. Diese fehlerbehaftete Transaktion kann sowohl auf der Blockchain als auch außerhalb derselben (etwa durch Übergabe oder Überweisung ihres in Euro ausgedrückten Werts) neutralisiert werden.

Auf „*der* Blockchain“ werden ausschließlich Transaktionen über Satoshi (s. die Beantwortung von Frage 1) verzeichnet. Allerdings gibt es einige Möglichkeiten, mittelbar auch andere Informationen unveränderbar auf der Blockchain zu „verewigen“. Dies kann z.B. durch Übertragung des geringstmöglichen Betrags (1 Satoshi) auf eine frei gewählte „Bitcoin-Adresse“ geschehen, zu der zwar niemand den passenden privaten Schlüssel hat, deren 26 bis 35 alphanumerische Stellen aber als „Nachricht“ interpretierbar sind. Auf diese Weise lassen sich pro Transaktion bis zu 32 Bytes an Nutzdaten transportieren, sodass es – mühselig und mit nicht zu unterschätzendem Aufwand – mit einer Vielzahl solcher „Fake-Überweisungen“ sogar möglich ist, Fotos oder kleine MP3-Tondateien permanent zu speichern. Vergleichsweise „praktischer“ ist da schon die Methode, das Standardskript „OP_RETURN“, das eingeführt wurde, um Metadaten für Transaktionen anderer Werte als

Bitcoin „huckepack“ auf der Bitcoin-Blockchain speichern zu können, zu verwenden. Damit lassen sich pro Transaktion (wohlgemerkt auf existierende Adressen, sodass die primär damit übertragenen Bitcoin-Einheiten nicht verloren sind) als sog. „Payload“ bis zu 80 Bytes „mitübertragen“ und für immer auf der Blockchain speichern. (Weiterführend A. Sward/I. Vecna/F. Stonedahl, Data Insertion in Bitcoin’s Blockchain, ledgerjournal.org, DOI 10.5915/LEDGER.2018.101.)

Daraus lässt sich erkennen, dass allenfalls ganz simple, bloß eine einzige „Fake-Adresse“ oder eine einzige Payload nutzende Kommunikationsakte unmittelbar mit üblichen Werkzeugen zur Untersuchung der Bitcoin-Datenbank (etwa Block Explorer) wahrgenommen werden können. Was einen größeren Umfang aufweist, lässt sich dagegen nur durch die Verknüpfung mehrerer Transaktionen nach bestimmten Regeln und damit gewissermaßen auf einer Anwendungsschicht oberhalb der Bitcoin-Blockchain „sichtbar“ oder „hörbar“ machen.

Diejenigen, die derartige Werkzeuge herstellen, anbieten oder konfigurieren sind daher zugleich jene, welche der interpretierbaren Nachricht ihre Wahrnehmbarkeit wieder nehmen können, obwohl die ihr zugrundeliegenden Daten nach wie vor in der Blockchain gespeichert sind.

An dieser Stelle ist auch an das Grundbuch zu erinnern, das eine Art „papiergebundene, staatlich betriebene Blockchain“ darstellt, aus der ebenfalls nichts gelöscht, sondern allenfalls „gerötelt“ wird, damit die Kette von Transaktionen nachvollziehbar erhalten bleibt. In ähnlicher Weise ist auch als solchen unveränderlichen Einträgen auf einer Blockchain durch später Verbuchtes ihre „Gültigkeit“ zu nehmen. So könnten insbesondere obsolete, falsche oder illegale Informationen gekennzeichnet werden. Wer sie dennoch verwendet, müsste evtl. mit Rechtsfolgen von Schadensersatz bis Strafe rechnen.

In ähnlicher Weise ließe sich mit in die Blockchain gesetzten Links auf außerhalb derselben befindliche Daten verfahren. Auch diese Links könnten durch spätere Transaktionen als „ungültig“ oder „illegal“ markiert, nicht jedoch als solche gelöscht werden. Primär wäre in diesen Fällen ohnehin beim Anbieter der verwiesenen Daten anzusetzen. Das in der digitalen Welt immer bestehende Risiko, dass man dessen nicht habhaft werden kann, wäre ggf. im Rahmen einer umfassenden Interessenabwägung mit dem Ziel einer rechtlichen Regulierung der Problematik entsprechend zu berücksichtigen.

Einschränkung: In privaten oder sehr kleinen Blockchains mit anderen Konsens-Mechanismen als Proof-of-Work oder anderen Mechanismen zur Absicherung der Zuverlässigkeit der verwendeten Zeitstempel ist die nachträgliche Änderung/Korrektur von Einträgen möglich. In der Definity-Blockchain ist die durch die Mehrheit beschließbare Änderung sogar expliziter Bestandteil des Protokolls. Das geht freilich zulasten der Verlässlichkeit der Datenspeicherung. Unklar ist noch, wie sich dies auf die Nützlichkeit solcher Ausprägungen der Blockchain-Technologie auswirkt. Wäre die Blockchain dann nur noch ein Mittel, um das Vertrauen, das in mehrere voneinander unabhängige, sich idealerweise (?) gegenseitig misstrauende Institutionen gesetzt wird, zusammenzuführen? In derartigen Protokollen könnte auch vorgesehen sein, dass kleiner Änderungen nur der einfachen Mehrheit bedürfen, während gewichtige Änderung eine qualifizierte Mehrheit oder eine gerichtliche Anordnung voraussetzen.

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

Die mit der DSGVO angestrebte Technologieneutralität (vgl. Erwägungsgrund 15) wurde nur in begrenztem Maße erreicht. Das Fehlen jeglicher Bezugnahme auf dezentrale Datenspeicherung ist im Hinblick auf die rasant zunehmende Bedeutung der DLT-Blockchain-Technologie eine gravierende Regelungslücke. So wird bereits die Meinung vertreten, öffentlich-genehmigungsfreie Blockchains seien vor allem wegen der nicht realisierbaren Löschungspflicht aber auch wegen der offensichtlichen Schwierigkeit, die dezentrale Datenverarbeitung einem greifbaren „Verantwortlichen“ zuzurechnen, nicht DSGVO-konform.

In der Tat kollidiert das auch als „Recht auf Vergessenwerden“ bezeichnete Recht auf Löschung mit den hervorstechenden Eigenschaften dieser Klasse von Blockchains, die insbesondere in deren Unveränderbarkeit, Zensurresistenz, Transparenz und Resilienz zu sehen sind.

Auf der übergeordneten verfassungsrechtlichen Ebene prallen aber auch grundrechtlich geschützte Positionen aufeinander, die auf der Grundlage umfassender Abwägungsvorgänge in praktische Konkordanz zu bringen sind.

So kann die Verwendung von DLT/Blockchain-Technologie durchaus im überwiegenden Interesse der/des von der Speicherung personenbezogener Daten Betroffenen liegen und überdies – ganz im Sinne von Privacy by Design – zur Verfolgung datenschutzrechtlicher Anliegen beitragen. So könnten solche Blockchains nicht auf Intermediäre angewiesene und damit ideale Plattformen für die Vergabe von Zugriffsrechten auf (in der Regel nicht auf einer öffentlichen Blockchain gespeicherte) Daten bilden. Damit sollte es schließlich möglich sein, die bereits in Beantwortung von Frage 3 als erstrebenswert dargestellte Rückübertragung der Datensouveränität an die „betroffene Person“ zu erreichen.

Aber selbst für den Fall, dass die Speicherung ganz und gar nicht im Interesse der betroffenen Person liegt, muss man sich für eine umfassende Interessenabwägung von der Vorstellung lösen, Art. 8 GRCh verpflichte den einfachen Normsetzer auf europäischer Ebene und auf der Ebene des jeweiligen Mitgliedstaates zur Schaffung eines Individualgrundrechts, das nur die Interessen der betroffenen Person in den Blick zu nehmen hat. Nach wohl zutreffendem Verständnis ebnet Abs. 2 den Weg für letztlich die Wohlfahrt optimierende Innovationen (vgl. dazu ganz umfassend und erhellend insb. die rezente Habilitationsschrift N. Marsch, Das europäische Datenschutzgrundrecht. Grundlagen – Dimensionen – Verflechtungen [2018]; speziell zu Blockchains bereits R. Böhme/P. Pesch, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD [2017], 473 ff.).

Daraus lassen sich Anforderungen an die einfachgesetzliche Ausgestaltung des Datenschutzrechts ableiten, für die selbst die sonst in dieser Hinsicht leider schweigende DSGVO in Gestalt des in Art. 23 Abs. 1 normierten Katalogs von Beschränkungen, insb. mit lit. e), eine Grundlage bereithält.

Die Pseudonymisierung und unter Umständen sogar die Anonymisierung lassen sich durch TLD/Blockchain-Technologie stärken. Dies gilt es durch legislative Maßnahmen zu fördern oder nutzen. In Anbetracht des Umstands, dass Daten, die nicht (mehr) gespeichert werden sollen oder dürfen, auf öffentlich-genehmigungsfreien Blockchains dennoch unveränderbar gespeichert bleiben, muss das Recht

die Realitäten akzeptieren: Es kann nur an der Speicherung ansetzen und hier Anreize schaffen, ggf. peinlichst darauf zu achten, keine unangemessenen Daten unveränderbar zu speichern. Außerdem könnten sich Lösungen entlang der zur Beantwortung von Frage 8 dargestellten Linien ergeben.

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

Entgegen ihrer etwas irreführenden Bezeichnung sind Smart Contracts per se weder „smart“ noch ohne weiteres als Verträge im rechtlichen Sinne aufzufassen. (Sie können wie folgt definiert werden: „Programmcode, der auf einer Blockchain läuft und dort digitale Assets oder Repräsentationen körperlicher Gegenstände auf der Grundlage von anderen – oft externen – Daten, die zum Zeitpunkt der Programmierung des Codes noch nicht feststanden, zwischen zwei oder mehreren Parteien in Form von Transaktionen neu zuordnet.“)

Vom Standpunkt des deutschen Zivilrechts aus betrachtet, wird ein Smart Contract in der Regel Gegenstand einer außerhalb desselben getroffenen vertraglichen Vereinbarung (i.S.v. „Verpflichtungsgeschäft“) sein und allenfalls das Verfügungsgeschäft oder zumindest Teilaspekte desselben beinhalten. Wie Transaktionsdaten auf der Bitcoin-Blockchain sind Zustandsdaten (sozusagen die Schaltzustände des dadurch repräsentierten „Welt-Computers“) auf einer Smart Contracts ermöglichenden Blockchain, wie insb. Ethereum, unveränderbar und die einmal gestarteten Smart Contracts unaufhaltsam.

So kann auch ein „irrtümlich“ in Gang gesetzter Smart Contract nur dann gestoppt oder korrigiert werden, wenn dies durch den vorsorglichen Einbau von Sicherungsmechanismen (z.B. die Verwendung des von der Programmiersprache „Solidity“ angebotenen Konzepts „Delegatecall“, welches das dynamische Nachladen von ausführbarem Code zur Laufzeit ermöglicht, durch Third-key-Lösungen, bei denen ein vertrauenswürdiger Dritter „die Reißleine ziehen“ kann, oder durch zur Verfügungstellung entsprechend interpretierbarer Daten durch ein sog. „Oracle“) explizit so vorgesehen wurde. Andernfalls wird der Smart Contract unweigerlich so ausgeführt, wie er programmiert wurde. Dies schließt selbstverständlich nicht aus, dass eine gegen den Willen des Erklärenden vorgenommene Verfügung (durch eine gegenläufige Transaktion auf der Blockchain oder außerhalb derselben) rückabgewickelt wird. Falls eine Ersatzvornahme nicht möglich ist, mag für die Durchsetzung eines derartigen Anspruchs die Festsetzung von Zwangsmitteln gem. § 888 ZPO erforderlich sein. Ein Problem kann allenfalls dadurch entstehen, dass sich die vom Smart Contract Beteiligten auf „trustless trust“ verlassen und daher über keine ladungsfähige Anschrift ihres Gegenübers verfügen.

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).

Vgl. hierzu die Beantwortung von Frage 8.

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?

Diese Frage beruht möglicherweise auf dem Missverständnis, Smart Contracts seien als solche Verträge oder umfassten den gesamten Inhalt einer vertraglichen Vereinbarung. Wie unter Nr. 10 ausgeführt, sind sie dagegen nach deutschem Recht in der Regel allenfalls als (Teile) des Verfügungsgeschäfts zu sehen, erfüllen also eine vertragliche Verpflichtung, anstatt diese zu begründen.

Das Bereicherungsrecht bietet u.a. die Lösung des aus dem Abstraktionsprinzip resultierenden Problems, dass Verfügungen unabhängig vom kausalen Verpflichtungsgeschäft zu beurteilen sind. Es schafft auf der Grundlage eines gesetzlichen Schuldverhältnisses schuldrechtliche Ansprüche auf rückabwickelnde Verfügungen, eben weil vorgenommene Verfügungen als solche nicht mehr aus der Welt geschafft werden können. Das Bereicherungsrecht und seine Wirksamkeit werden daher durch Smart Contracts nicht bedroht. Im Gegenteil: Es stellt ein Instrument zur Rückgängigmachung rechtsgrundloser Vermögensverschiebungen bereit und entschärft damit ein Problem, mit dem sich möglicherweise andere Rechtsordnungen im Umgang mit Smart Contracts konfrontiert sehen.

13. Der Grundgedanke von Blockchains 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?

Es ist davon auszugehen, dass die Speicherkapazität reichen wird. Jedenfalls auf der Bitcoin-Blockchain wächst die zu speichernde Datenmenge annähernd linear (derzeit etwas mehr als 190 GB bei einem Zuwachs von ca. 1 MB ungefähr alle 10 Minuten), während die verfügbaren Speicherkapazitäten (gem. dem „Mooreschen Gesetz“) exponentiell zunehmen. Überdies ist zu berücksichtigen, dass moderne Bitcoin-Core-Knoten zwar die gesamte Datenmenge der Blockchain im Zuge der Synchronisation herunterladen müssen, was eine entsprechende Bandbreite erfordert, dass sie aber unter Anwendung von „Pruning“, also dem Löschen bestimmter, für die Aufrechterhaltung der Funktionalität des Knotens nicht mehr erforderlicher Blöcke, Speicherplatz einsparen können.

14. Bei der Anwendung von BC/DLT kann niemand eine 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?

Zunächst sei auf die Beantwortung von Frage 8 verwiesen und überdies darauf, dass Transaktionen innerhalb einer Blockchain keine Rechte verändern, sondern tatsächliche Zustände. So ist diejenige, die über den zu einer Bitcoin-Adresse (Hashwert eines öffentlichen Schlüssels) gehörenden privaten Schlüssel verfügt, aus kryptographischen und damit aus technischen, nicht dagegen aus rechtlichen Gründen die Einzige auf dieser Welt, die weitere gültige Transaktionen über die dorthin transferierten Werte vornehmen kann. Damit ist eine Transaktion auf der

Blockchain eher mit der Übertragung des Besitzes (tatsächliche Herrschaft) als mit einer solchen des Eigentums (Rechtsposition) zu vergleichen, wobei freilich beide Vergleiche wegen der fehlenden Sachqualität von Kryptowährungen nicht ganz passen. Ansprüche auf Besitzeinräumung können, wenn die Sache (oder ein zu deren in Besitznahme erforderlicher Schlüssel) etwa vom bisherigen Besitzer versteckt gehalten wird, nur durch Zwangsmittel gem. § 888 ZPO durchgesetzt werden. Gleiches gilt für eine Transaktion auf der Blockchain.

Ausnahmen:

- Aufgrund der Nutzung eines (auch auf der Bitcoin-Blockchain verfügbaren) Multisig-Schemas wird vorgesehen, dass z.B. 2 aus insgesamt 3 Schlüsseln für die Bewirkung einer Transaktion erforderlich sind. Dann kann z.B. der Inhaber des Anspruchs gemeinsam mit einer als Schiedsfrau fungierenden Dritten signieren, sodass man für die Veränderung des tatsächlichen Zustands nicht auf den Verpflichteten angewiesen ist.
- Der die Transaktion auf der Blockchain steuernde Smart Contract wurde so aufgesetzt, dass er die Eingriffsmöglichkeit eines Dritten oder mehrerer Dritter vorsieht (vgl. hierzu die Beantwortung von Frage 10). Dadurch ließen sich Blockchains mit einer solchen Korrekturmöglichkeit etablieren. Es ist noch nicht klar, in welchem Umfang damit die Vorteile der Blockchain-Technologie beseitigt würden. Diese Unklarheit rührt auch daher, dass mit der Bitcoin-Blockchain als erster und bislang bedeutendster aller Blockchains die Unabhängigkeit von staatlichen Maßnahmen als dezidiertes Ziel verfolgt wurde. Davon abzugehen ist jedoch die normative Entscheidung der Entwickler einer neuen Blockchain oder einer Blockchain-basierten Anwendung. So sieht das bei der Beantwortung von Frage 4 erwähnte Blockchain-gestützte System für den Sekundärhandel mit Software vor, dass gerichtliche Entscheidungen über die rechtliche Zuordnung durch Korrekturbuchungen nachvollzogen werden können (vgl. W. Blocher/A. Hoppen/P. Hoppen, Softwarelizenzen auf der Blockchain, CR 2017, 337 ff.). Derartiges lässt sich leicht mit Smart Contracts oder auf Blockchains ohne Smart-Contract-Funktionalität, wie der Bitcoin-Blockchain, dadurch realisieren, dass eine oberhalb der eigentlichen Blockchain liegende Anwendungsschicht genutzt wird, um Rechte an Sachen oder immaterialgüterrechtliche Befugnisse durch Payload-Einträge in Transaktionen über Protokoll-Token (etwa Satoshi im Falle der Bitcoin-Blockchain) zu repräsentieren.

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?

Wie schon bei der Beantwortung von Frage 3 ausgeführt, wäre der noch zu schaffender klare Rechtsrahmen ein Kriterium der Investitionssicherheit und damit ein entscheidender Standortfaktor für Startups und die Entwicklung einer deutschen Blockchain-Industrie. Am ungünstigsten erscheint es, in einem Bereich der tenden-

ziell rund um den Globus operieren kann, mit der Regulierung zuzuwarten und damit Staaten, die frühzeitig für verlässliche Regeln und andere Anreize sorgen, das Feld zu überlassen.

Andererseits besteht die Gefahr, durch die Setzung falscher Anreize oder potentielle Überregulierung die Entfaltung der Marktkräfte zu hemmen. Daher bietet sich nicht nur auf dem Gebiet von DLT/Blockchain-Technologien, sondern generell für viele besonders dynamische Bereiche auf dem Weg der digitalen Transformation als zielführendes Instrument legislativer Vorhaben jenes des „adaptiven Rechtsrahmens“ an. So könnten in sog. „Real-Laboren“ oder in „regulatorischen Sandkästen“ Experimentierräume für neue Geschäftsmodelle geschaffen werden, in denen sich diese erproben und beobachtet lassen, ohne sie gleich allen Vorschriften zu unterstellen, deren Anwendungsbereich grundsätzlich eröffnet wäre. Zugleich können daraus Erfahrungen für anstehende Regulierungen gewonnen werden. Überdies sollten bereits in Kraft befindliche Regulierungen in einem dynamischen Prozess laufend auf ihre Geeignetheit und Zweckmäßigkeit hin überprüft werden, um bei Bedarf rasch neue Regelungsansätze ableiten und damit die Steuerungswirkung optimieren zu können.

Die Verwendung von Kryptowährungen als Zahlungs- oder Tauschmittel bedarf m.E. keiner besonderen Regulierung. Kritisch ist dagegen deren Umwechslung *von* gesetzlichen Zahlungsmitteln oder *in* diese. An diesen Punkten sind aber schon jetzt einschlägige und zum Teil im Rahmen der europäischen Union harmonisierte Regeln für KYC und AML zu beachten.

Auch in dieser Hinsicht hat die von EZB und BaFin geteilte Parole „Same business, same risks, same rule“ (das Zitat wird Sabine Lautenschläger, Mitglied des Direktoriums der EZB, zugeschrieben) gewiss ihre Berechtigung. Die BaFin irrt jedoch, wenn sie dabei von falschen Prämissen ausgeht. So ist etwa das mit einem „herkömmlichen“ Bankautomaten und dessen möglicher Manipulation einhergehende Risiko ungleich größer als jenes, das etwa von einem Bitcoin-ATM ausgeht. Während mit Ersterem ggf. das gesamte Bankkonto eines Nutzers einschließlich Überziehungsrahmen leergeräumt werden kann, ist der „schlimmste anzunehmende Unfall“ beim Einsatz des Letzteren darin zu sehen, dass die Nutzerin für die von ihr dem Automaten zugeführten Geldschein nichts erhält. Das kann auch bei Warenautomaten, mit denen Parfüms oder andere vergleichsweise hochpreisige Gegenstände verkauft werden, passieren, ohne dass für diese Art der Geschäftsabwicklung eine Banklizenz erforderlich wäre. Freilich sind auch für den Verkauf von Kryptowährungen über ATMs oder für den durch Kioske erfolgenden Vertrieb von Bons, die online gegen Kryptowährungen eingelöst werden können, geeignete KYC/AML-Prozesse vorzusehen. Dagegen scheint es im Hinblick auf das Ziel einer erfahrungs- und wissensbasierten Akzeptanz von DLT/Blockchain-Technologien durch die deutsche Bevölkerung nicht sinnvoll zu sein, dieser bloß bei Reisen ins benachbarte Ausland (Frankreich, Italien, Österreich) entsprechende Erfahrungen zu gönnen. In diesem Zusammenhang wäre auch die Klarstellung sinnvoll, dass Kryptowährungen keine „Rechnungseinheiten“ i.S.d. § 1 Abs. 11 S. 1 KWG und damit auch nicht als Finanzinstrumente zu qualifizieren sind.

Unter den unmittelbar anstehenden Regulierungsthemen kommt der Finanzierung durch ICOs bestimmt eine hohe Priorität zu. Zum einen bestehen hier ähnliche Anlegerschutzprobleme wie im Wertpapiergeschäft, sodass die Lösungen für sog. „Security Tokens“, die eine Beteiligung an einem Unternehmen oder an dessen

Erträgen vermitteln, ebenfalls vergleichbar sein sollten. Zum anderen ist inzwischen auch unter vergleichsweise unbedarften Anlegern weithin bekannt, dass ein besonders hohes Risiko eingeht, wer über den Erwerb von Token in Unternehmen investiert. Evtl. kann man diese Offensichtlichkeit des erhöhten Risikos nutzen, um den Anlegerschutz für diejenigen zu lockern, die weniger stark geschützt sein müssen, weil sie nachvollziehbar und wirklich offensichtlich ein höheres Risiko eingehen wollen. Damit ließe sich das grundsätzlich interessante Instrument alternativer Unternehmensfinanzierung zur Förderung des unterentwickelten deutschen Venture-Capital-Marktes nutzen.

Wichtig ist, und das sein an dieser Stelle bewusst wiederholt, jedenfalls eine rasche legislative Klarstellung, die notfalls vorläufig durchaus auf nationaler Ebene erfolgen sollte, wenn eine europäische Lösung zu lange auf sich warten ließe.

Kurzfristig sollte noch die bereits im Koalitionsvertrag angekündigte großzügige Überprüfung von Formvorschriften auch im Hinblick auf ihre mögliche Erfüllung oder Ablösung durch Blockchain-gestützte Verfahren angegangen werden.

In mittlerer Zukunft dürfte die Anpassung des Aktienrechts an Tokens zur Repräsentation von Entscheidungsrechten anstehen (wodurch evtl. auch komplexe Stimmrechtsübertragungen etc. ermöglicht werden könnten), und in etwas fernerer Zukunft jene des Sachenrechts an Tokens als Publizitätsmerkmal.

Bei allem hier angedeuteten Regulierungsbedarf sollte ein möglicherweise übergeordnetes Ziel der DLT/Blockchain-Regulierung nicht aus den Augen verloren werden: Die Anwendung der Technologie wird Arbeitsplätze vernichten und neue schaffen. Eine vernünftige, „Blockchain-freundliche“ Regulierung, die einige Freiheiten einschränkt, um am Ende das – nicht zuletzt auch verbraucherschützende – Potential zu entfalten, kann und sollte dazu fuhren, dass unter dem Strich eine ansehnliche schwarze Zahl stehen wird.

Zur Frage nach einer internationalen Standardsetzung sei vor allem auf die diesbezüglichen Ausführungen zur Beantwortung von Frage 8 verwiesen. Für umfassende Standardisierungen scheint der Markt für Blockchains noch deutlich zu jung zu sein. Zuvor muss sich noch viel Technologie im Wettbewerb entwickeln. Davon abgesehen stellt sich im Hinblick auf öffentlich-genehmigungsfreie Blockchains das oben unter Nr. 7 behandelte Problem der Governance. Zumindest vorläufig dürfte hier die Devise „Adapter statt Standards!“ lauten.

16. Wie bewerten Sie die die europäische Blockchain-Partnerschaft?

Beim „Internet der Information“ hat Europa das Feld völlig den US-amerikanischen und asiatischen Akteuren überlassen. Das durch DLT/Blockchain-Technologie ermöglichte „Internet der Werte“ weiß europäische Standortvorteile wie Erfahrung als Finanzplatz, politische Stabilität, grundrechtlich gewährleistete Eigentumsgarantie und Berufsfreiheit, IT-Sicherheit und vielleicht sogar den Datenschutz europäischer Provenienz zu schätzen. Wenn einem das Schicksal schon eine zweite Chance gibt, sollte man sie nützen! Überdies könnte (wie am Ende der Beantwortung von Frage Nr. 5 bereits angedeutet) eine gemeinsame Blockchain der Mitgliedstaaten der Europäischen Union nicht nur für die als „Digital natives“ aufgewachsene Generation den europäischen Gedanken versinnbildlichen, weil dabei alle bei der gemeinsamen Verfolgung von Zielen zusammenwirken, ohne dass einer von ihnen oder selbst einige „Große“ die anderen „overrulen“ könnten. Damit

wäre vor allem auch eine rasche Verdichtung und Verfestigung des europäischen Verwaltungsraums mit seinem europäischen Verwaltungsverbunds zu realisieren. So gesehen ist die Initiative einer „europäische Blockchain-Partnerschaft“ und die damit verbundenen Ideen (z.B. jene für die auch hier vertretene europäische Verwaltungsinfrastruktur auf Blockchain-Basis, vgl. hierzu Rehfeld, Government Blockchain Infrastructure – A Chance for Europe [2018], Internet-Quelle) sehr zu begrüßen. Zu bedauern ist allerdings, dass sie seit ihrer Gründung am 10. April 2018 nicht viel von sich hören ließ.

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?

Diese Frage wurde bereits unter Nr. 4 bejaht. Die Lösung der damit einhergehenden Problematik kann nicht darin bestehen, die Anwendung der DLT/Blockchain-Technologie verhindern zu wollen, weil das in einem demokratischen Rechtsstaat einerseits kaum möglich ist und ihm andererseits solche Anwandlungen auch nicht gut zu Gesicht stünden. Selbst wenn man die Technologie in vielen Staaten unterbände, könnten in einigen wenigen Staaten weiterhin die dafür nötige Infrastruktur (die im Übrigen relativ mobil ist) betrieben werden, auf welche über das Internet inkl. dem Darknet problemlos von allen Staaten mit freiem Internetzugang aus zugegriffen werden könnte. Auf diese Weise ließen sich somit nur die positiven Seiten der DLT/Blockchain-Technologie erfolgreich unterbinden, nicht dagegen die negativen.

Wie die meisten Technologien ist auch DLT/Blockchain grundsätzlich neutral, kann aber für legale ebenso wie für illegale Zwecke eingesetzt werden. Daher ist nach Wegen suchen, die sich faktisch ergebenden Probleme in den Griff zu bekommen. Z.B. konnte die unter Nr. 4 bereits erwähnte „Silk Road“ stillgelegt werden, weil es international kooperierenden Strafverfolgungsbehörden gelang, das dem Online-Schwarzmarkt zugrundeliegende Tor-Netzwerk zu infiltrieren.

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

Bei öffentlich-genehmigungsfreien Blockchains stellt sich diese Frage nicht, weil sie eben vollständig dezentral organisiert sind und daher keinen „Betreiber“ kennen. Es ist aber zu erwarten, dass es längerfristig nur wenige (deutlich weniger als 10) stabile Blockchains geben wird, die auf dem Proof-of-Work-Konsens-Mechanismus basieren, weil sonst die insgesamt verfügbare Hash Rate viel größer würde, als die in den einzelnen Blockchains eingesetzte „Power“, sodass die Gefahr einer 51%-Attacke zu groß würde. Unter bestimmten, noch näher zu untersuchenden Umständen könnten besonders stabile öffentlich-genehmigungsfreie Blockchains auch für den Gesetzgeber relevant werden, der etwa darauf gespeicherte Hash-Werte in Verbindung mit dem zugrundeliegenden Dokument mit besonderen Rechtswirkungen (vgl. etwa die §§ 371a und 416a ZPO) versehen könnte, ohne dafür die Einhaltung schwerfälligerer Formenvorschriften vorauszusetzen.

Bei anderen Formen von Blockchains (also konsortialen und privaten) kommt auf die Zielsetzung und schließlich darauf an, wie das Betreiberkonsortium zusammenzusetzen ist, damit ihm insgesamt viel Vertrauen entgegengebracht wird.

Sinnvollerweise werde Unternehmen Mitglieder sein, wenn es um die Absicherung von Supply-Chains geht, wie bereits oben zu Nr. 6 beschrieben, können dagegen staatliche Institutionen die passenden „Betreiber“ sein, wenn Legalität im Vordergrund steht oder wenn Blockchain-Protokolle dafür eingesetzt werden sollen, die Erreichung politischer Ziele, etwa die Nutzung CO_2-sparender Verkehrsmittel, durch Anreize für das unternehmerische Gewinnstreben abzusichern.

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?

Auch die Beantwortung dieser Frage hängt von der Zielsetzung ab. Öffentlich-genehmigungsfreie und – in eingeschränkter Weise – auch konsortiale Blockchains sind ideale Instrument zur Schaffung von Transparenz und Vertrauen. Beides kann sowohl im Verhältnis Bürgerin/Staat als auch zwischen einzelnen staatlichen Institutionen fehlen.

Was die mögliche Rückübertragung der Datenhoheit an personenbezogenen Daten an die Bürgerinnen und Bürger anbelangt, sei auf die Beantwortung der Frage 3 verwiesen.

Besonders vielversprechend erscheint die Einführung von Blockchain-gestützten Registern (etwa an bestimmten Mobilien oder Immaterialgütern) deren Führung bislang nicht effizient gewesen wäre.

Ähnlich wie auf der europäischen Ebene eine gemeinsame Verwaltungs-Blockchain der Mitgliedstaaten ein wirksames Instrument für Reformen sein könnte (vgl. hierzu die Beantwortung von Frage Nr. 16), ließen sich auch innerhalb Deutschlands länderübergreifende Verwaltungsprojekte leichter realisieren, wenn keines der Bundesländer mit seiner „effizienteren“ Lösung den Lead übernehmen müsste, sondern der erforderliche Datenaustausch über einen durch eine Blockchain zu schaffenden äquidistanten „Layer“ durchführbar wäre.

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?

Hiermit wird ein sehr großes Fass aufgemacht, das sich in diesem Rahmen schon wegen der vielfältigen ethischen Implikationen nicht adäquat beantworten lässt. Hierzu nur soviel: KI-Systeme sollen und dürfen grundsätzlich allenfalls zur automatisierten Umstürzung der Entscheidung herangezogen werden (Art. 22 DSGVO). Selbst dies setzt voraus, dass sich die Entscheidungsträgerin erläutern lassen kann, auf welcher Grundlage das System zu seiner Empfehlung kam. Wenn dies nicht möglich ist, müssen derartige Systeme als für den Bereich juristischer (und sonstiger) Hermeneutik ungeeignet betrachtet werden. Dabei geht es nämlich nie um eine Wahrheitsfindung im naturwissenschaftlichen Sinne, sondern um die zutiefst menschliche Angelegenheit, im diskursiven Prozess geäußerte Argumente gegeneinander abzuwägen. Wollten wir uns darauf verlassen, wenn uns eines Tages ein KI-System mitteilte: „Das kannst du, Mensch, mit deinem begrenzt leistungsfähi-

gen Gehirn nicht verstehen, aber glaube mir, so ist es richtig.“, fielen wir damit hinter die Errungenschaften der Aufklärung zurück und setzten an die Stelle von Vernunft und Streben nach Erkenntnis den Glauben an digitale Götzen.

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?

Hierzu sei insbesondere auf die Ergebnisse der öffentlichen Anhörung zum Thema „Quantencomputer“ verwiesen.

Als grobe Einschätzung mag reichen: Heute für wenige Hundert Euro erhältliche ASIC-Miners erledigen ihre Aufgabe um mindestens den Faktor 1:1000 schneller, als der derzeit verfügbare stärkste Quantencomputer. Wenn die ersten ausreichend leistungsfähigen Quantencomputer nicht – was äußerst unwahrscheinlich erscheint – heimlich vorbereitet und dann auch noch vor allem für Angriffe auf Blockchains eingesetzt werden, gibt es in dieser Hinsicht keine Probleme, weil die Verschlüsselungsmethode rechtzeitig durch eine „Quantencomputer-sichere“ ersetzt werden kann. Selbst – in dieser Hinsicht - „pessimistische“ Annahmen gehen davon aus, dass wir bis zu diesem Zeitpunkt noch mindestens ein Jahrzehnt Zeit haben werden. Der Proof-of-Work-Prozess lässt sich ohnehin auch mit künftigen Quantencomputern im Vergleich zur Verwendung „herkömmlicher“ Prozessoren nicht signifikant beschleunigen (vgl. D. Aggawald/G. Brennen/T. Lee/M. Santha/M. Tomamichel, Quantum attacks on Bitcoin, and how to protect against them, Quantum Physics, 28 Oct 2017, arXiv:1710.10377).

Möglicherweise müssten eines Tages sehr betagte Dateien neue gehasht werden, um ihre Integrität auch weiterhin beweisen zu können. Das damit verwandte Problem des „Nachsignierens“ ist aus der Forschung zur Langzeitarchivierung bekannt.

Außerhalb von Proof-of-Work stellen sich bei Blockchains aufgrund der Entwicklung von Quantencomputern keine anderen Sicherheitsprobleme, als bei anderen Technologien. Dabei geht es z.B. um die Erleichterung des Herausfindens von Passwörtern.

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 entwickelt?

Auch diese Frage kann im gegebenen Rahmen nicht umfassend beantwortet werden. Deutschland ist zwar kein Spitzenreiter im Bereich der Anwendung der DLT/Blockchain-Technologie, aber immerhin gibt es in Berlin und auch anderswo eine sehr rührige einschlägige Startup-Szene, die Grund zu entsprechenden Hoffnungen gibt.

Die Politik ist vor allem hinsichtlich der zügigen Schaffung einer klaren Regulierungen gefordert, zumal hier andere Staaten, etwa die Schweiz, Liechtenstein und

Malta, deutlich schneller waren. Insbesondere wird von Kreisen der Industrie eine eindeutige Lösung für das DSGVO-Problem erhofft.

Schließlich wäre da noch die freilich auch aus anderen Gründen allenthalben zu vernehmende Forderung nach besserer Netzabdeckung und höherer Bandbreite zu nennen. Gute, schnelle Datenleitungen sind für das Gelingen der digitalen Transformation elementar! Das bezieht sich nicht auf schnelles Internet für alle, auch in Thüringen, in Niederbayern und im Hochschwarzwald, sondern auf sehr schnelle Leitungen an den Hotspots der DLT/Blockchain-Wirtschaft.

Und last but not least gehören hervorragende Bedingungen sowohl für die Erforschung der Grundlagen von DLT/Blockchain-Technologien als auch für die anwendungsorientierte Forschung in Kooperation mit einschlägig tätigen Unternehmen zu den jedenfalls noch verbesserungsbedürftigen Erfolgsfaktoren für die Erreichung einer Spitzenstellung im europäischen wie im internationalen Vergleich. Wenn das in den meisten Kennzahlen um den Faktor 1:10 kleinere Österreich in einer einzigen Förderlinie 20 Mio. Euro für die Blockchain-Forschung zur Verfügung stellen kann, sollte es Deutschland gelingen, mindestens 200 Mio. Euro „in die Hand zu nehmen“, um vor allem abseits der klassischen Forschungsförderung, die viel zu lange benötigt, um wirklich innovativen und multidisziplinären Initiativen unter die Arme zu greifen, ein wahres Feuerwerk der DLT/Blockchain-F&E zu entfachen.

23. Welche Gesetze müssen in Deutschland angepasst werden, um international den Anschluss an neue Geschäftsmodelle, 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?

Hinsichtlich sämtlicher Teilaspekte dieser Frage wird auf die Beantwortung der Frage 15 verwiesen.

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 tokenbasierten Finanzierungsmöglichkeiten profitieren? Welche Risiken sehen Sie bei ICOs, insbesondere für die Verbraucherinnen und Verbraucher, aber auch für Unternehmen?

Zunächst ist wiederum auf die Beantwortung der Frage 15 zu verweisen. Security-Token-Emissionen = Crowdfunding = Risikokapital = positiver Standorteffekt (Beseitigung eines bisher bestehenden Nachteils). Wieder: klare Regeln schaffen!

ICOs und IPOs sind einander ähnlich, wenn auf sie die gleiche Regulierung angewandt wird. IPOs sind aber sehr aufwändig und daher i.d.R. nur größeren Unternehmen zugänglich. Von ICOs könnten daher vor allem kleine und junge Unternehmen profitieren, wenn die Regulierung mit diesem Ziel hinter den Anforderungen an einen IPO zurückbleibt.

Mit ICOs wird Risikokapital gesammelt, daher ist damit stets unternehmerisches Risiko verbunden. Durch entsprechende Regulierung *unter*bunden werden sollten dagegen betrügerische Konstruktionen und Versprechungen, die vor allem im Jahr

2017 zu einem massivem Reputationsverlust dieses dem Grunde nach interessanten Finanzierungsinstruments geführt haben.

Ein im Vergleich zu IPOs geringerer Bedarf an gesetzlich normiertem Anlegerschutz könnte evtl. daraus resultieren, dass resp. wenn man zunächst Euros in eine Kryptowährung wechseln muss, um damit im Zuge des ICOs ausgegebene Tokens zu erwerben. Dadurch wird dem Anleger deutlich, dass er etwas Außergewöhnliches und entsprechend Riskantes tut. Wenn das nicht (mehr) der Fall ist, gibt es in dieser Hinsicht keinen signifikanten Unterschied zu sonstigen Crowdfunding-Methoden.

Für Unternehmen als Anleger bestehen im Hinblick auf ICOs keine Besonderheiten, es sei denn es geht um Unternehmen mit ähnlichen Risiko-Präferenzen wie Verbraucher. Für mit das mit einem ICO kapitalbeschaffende Unternehmen besteht das hinlänglich bekannte, aus der Volatilität von Kryptowährungen resultierende Kursrisiko, gegen das freilich gehedget werden kann. Ein zusätzliches Risiko könnte mit einer ungeschickten Konstruktion von Entscheidungsbefugnissen im Unternehmen einhergehen, bis dato verhält es sich allerdings meist anders herum: Die Unternehmer reservieren sich im Zuge von ICOs sehr viel Macht.

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?

Hierzu darf abermals auf die Beantwortung der Frage 15 verwiesen werden.

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?

Allenfalls insofern: Regulierungsunsicherheit hemmt Innovationen. Aber das ist keine neue Erkenntnis.

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

Indem sie klare aber nicht zu sehr einengende Regulierungen durchzusetzen hat und hierbei rasch und auskunftsbereit arbeitet.

28. Bekanntermaßen geht die Anwendung einiger Blockchain-Technologien 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?

Der Verweis auf den hohen Energieverbrauch wird nicht zuletzt von Menschen, darunter auch von Politikern, als Killerargument missbraucht, um damit eine innovative Technologie abzutun, mit der sie sich nicht ausreichend beschäftigt haben, um sie hinsichtlich anderer Zusammenhänge zu verstehen.

Der hohe Energieverbrauch von Proof-of-Work ist „konstruktionsbedingt“ erforderlich, weil auf diese Weise Abstimmungsmacht im Konsensmechanismus teuer und dadurch beschränkt ist und damit zugleich die Zeitstempel verlässlich sind. Theoretisch könnte die „schwierige Aufgabe“ des Findens eines passenden „Nonces“ durch eine andere ersetzt werden, wenn diese ebenfalls den Nachweis des Einsatzes von Ressourcen erforderten, der notwendigerweise Zeit braucht und unmittelbar mit der jeweiligen Blockchain verbunden ist. Vielleicht wäre hier an „Proof-of-Storage“ zu denken, bei dem es darum geht, dadurch die Vorhaltung enormer Speicherkapazitäten zu beweisen, dass es einem in kürzester Zeit gelingt, den Inhalt einer vom System zufällig vorgegebenen Speicherzelle zu nennen. Da auch die Herstellung und der Betrieb von Speichern Energie kosten, wäre damit aber nicht sehr viel zu gewinnen.

Letztlich ist der Energieverbrauch von Proof-of-Work auch damit erklärbar, dass der Konsens-Mechanismus in einem bestimmten, engen Teilbereich das Rechtssystem mit dem dahinterstehenden Staat und seinen Rechtsdurchsetzungsorgangen ersetzt. Auch dieses System ermöglicht Transaktionen, obwohl es einen gewissen (niedrigen, auf 5 bis 10 geschätzten) Prozentsatz von nicht kooperierenden Menschen gibt. Überspitzt könnte man formulieren, dass wir uns diesen teuren Apparat dafür leisten, um trotzdem in effizienter Weise verbindliche Vereinbarungen mit uns nicht völlig vertrauten Menschen eingehen zu können. Die Bitcoin-Blockchain ermöglicht „trustless trust“!

Annährungsweise lässt sich der Energieverbrauch der Bitcoin-Blockchain übrigens wie folgt abschätzen:

Ø Hash Rate der Bitcoin-Blockchain zw. 01.01.2018 und 27.11.2018: **36 EH/s**
Leistung des aktuellen ASIC-Miners Bitmain Antminer S9i: **14,5 TH/s**
Stromberbrauch eines Bitmain Antminer S9i: **1,365 KW**
36*10^18 :14,5*10^12 = **2.482.758 Antminer S9i** mit einer Stromaufnahme von 2.482.758*1,365 = **3.388.965 KW**, was einen Stromverbrauch pro Jahr von 3.388.965*24*365 = 29.687.333.400 KW/h = **30 TW/h** bedeutet.
Unter Berücksichtigung eines Aufwands von ¼ der Anschlussleistung für die Kühlung und eines Aufschlags wegen der weiterhin eingesetzten älteren und daher weniger effizienten Mining-Hardware von einem weiteren ¼ kommen wir zu einer Schätzung von 1,5*30 = **45 TW/h** pro Jahr, was ungefähr **0,19 %** des für 2018 geschätzten weltweiten Stromverbrauchs von 24.000 TW/h und damit ungefähr jenem von **Hong Kong** oder **Singapur** entspricht.

Der Energieverbrauch könnte evtl. besser genutzt werden. Dabei ist aber nicht an den Einsatz für ökonomische Zwecke aus der Perspektive des Miners zu denken (entgeltliches Einspeisen in ein Fernwärmenetz, Beheizung eines eigenen Glashauses etc.), da die eingesetzte Energie sonst unter dem Strich bloß billiger würde, was einen noch größeren Energieverbrauch nach sich ziehen würde. Evtl. könnte man aber eine Blockchain so aufsetzen oder regulieren, dass von ihr öffentliche Güter geschaffen werden (dabei wäre schon an die kostenlose Beheizung von Gemeinschaftseinrichtungen zu denken), die sonst nicht geschaffen werden könnten. Das reduziert nicht den Energieverbrauch, macht ihn jedoch (noch) sinnvoller.

Von diesem „Problem“ sind allerdings nur die großen öffentlich-genehmigungsfreien Blockchains betroffen, die auf dem Proof-of-Work-Konsens-Mechanismus basieren. Das werden weltweit nicht mehr als ein, zwei Handvoll sein.

Wahrscheinlich braucht man diese großen Blockchains als den festen Grund für das Setzen von Vertrauensankern durch andere Blockchains, weil sie diesen die Möglichkeit geben, das Vorhandensein von Daten zu einem bestimmten Zeitpunkt zu beweisen (perfekter Zeitstempel, der keine einzelne vertrauenswürdige Institution voraussetzt).

Speicherbedarf ist kein Problem (s. dazu die Beantwortung der Frage 13).

Transaktionsraten sind in (einzelnen) Alternativen resp. Ergänzungen zu Bitcoin (z.B. bei Anwendung des Lightning Networks als Second-Layer-Bezahlsystem) kein Problem, wobei die Sicherheit der Alternativen durch die Einbettung von Hash-Werten in die Payload einer Transaktion auf der Bitcoin-Blockchain gewährleistet werden kann.

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

Blockchain-gestützte Wahlen könnten zuverlässiger sein und damit zur Stärkung demokratischer Strukturen beitragen. Damit verbunden ist aber das Problem, dass es hierbei um das für die Demokratie entscheidende Instrument geht, weshalb politische Wahlen nicht bloß aus verfassungsrechtlichen Gründen keine guten Kandidaten für den Blockchain-Einsatz sind. Einfache Abstimmungen könnten dagegen von der mit Blockchain-Technologie einfach realisierbaren problemspezifischen Delegation von Entscheidungsmacht profitieren.

Auch Verwaltungsreformen könnten Blockchain-gestützt einfacher und besser gelingen (s. die dazu die Beantwortung der Frage 16). Ob dagegen eine „Demokratisierung“ der Verwaltung anzustreben ist, scheint schon unter dem Aspekt der Gewaltenteilung fraglich.