

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

Antworten von Jürgen Geuter

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)023

Frage 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?

Rein technisch ist "Distributed Ledger Technologie" der Oberbegriff zu Blockchains, d.h. Alle Blockchains sind Distributed Ledger aber nicht alle Distributed Ledger müssen auch eine Blockchain sein.

Bitcoin ist eine spezifische öffentliche Blockchain neben vielen anderen.

In der Blockchain Community hat sich seit einigen Monaten - weil der Begriff Blockchain wegen diverser Skandale und insbesondere Problemen wie dem exorbitanten Stromverbrauch von Bitcoin etwas verbrannt war - etabliert, statt Blockchain, Distributed Ledger zu sagen, um einen unbelasteten Begriff zu benutzen.

Öffentliche Blockchains sind Blockchains auf denen sich beliebige Teilnehmer einklinken und nach den definierten Regeln auf die Funktionen der Blockchain zugreifen können. Bitcoin und die meisten anderen Cryptocurrencies sind öffentliche Blockchains. Private Blockchains sind Blockchains, an denen nur ein durch eine Instanz autorisierter Teilnehmer Funktionen auf der Blockchain ausführen kann.

Die Auswirkung ist wie bei jedem anderen technischen System, welches mit Berechtigungen oder ohne Berechtigungen benutzt werden kann: Eine private Blockchain kann benutzt werden, wenn die zu speichernden Daten nicht einer unbeschränkten Öffentlichkeit zur Verfügung stehen sollen oder dürfen. Die Zahl der Teilnehmenden kann in einer privaten Blockchain eingeschränkt werden und zum Beispiel ein Verfahren zur Identitätsüberprüfung verknüpft werden, so dass keine anonymen Aktionen auf der speziellen privaten Blockchain möglich wären.

Frage 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?

Es gibt außerhalb von Prototypen und Cryptowährungen heute keine nennenswerten Blockchains. Alle bisher getesteten Systeme haben extreme Probleme beim Durchsatz (insbesondere bei einer großen Anzahl beteiligter Rechner, weil die Synchronisation des aktuellen Standes extremen Aufwand an Traffic und Datenspeicherung auf allen Rechnern erzwingt). Selbst die großen Blockchains wie Bitcoin und Ethereum haben aufgrund ihrer technischen und ökonomischen Struktur und Konsensmechanismen (Proof of Work) große Probleme, nennenswerte Transaktionsmengen in akzeptablen Reaktionszeiten abzubilden.

Blockchains verbrauchen aufgrund ihrer dezentralen Struktur immer mehr Datentransfer und Speicherplatz als etablierte Alternativen, die meisten öffentlichen Blockchains haben des Weiteren mit extremen Stromverbräuchen zu kämpfen, um den Konsensmechanismus (Proof of Work) abzubilden. Alternative Konsensmechanismen sind in der Theorie angedacht, aber nicht at scale im Betrieb und haben mit anderen Problemen zu kämpfen (insbesondere Fairness und Verlässlichkeit).

Zur Interoperabilität tragen Blockchains nichts bei, Interoperabilität hat etwas mit Kompatibilität von Datenformaten zu tun, dabei ist egal, ob die Daten in Blockchains oder etablierten Datenbanksystemen liegen.

Zum heutigen Zeitpunkt sind Blockchains nicht in der Lage mit etablierten Datenbank und Kommunikationssystemen zu konkurrieren, weder wenn es um Skalierbarkeit noch Sicherheit noch Datendurchsatz und insbesondere nicht wenn es um Wirtschaftlichkeit geht. Die existierenden minimalen Prototypen, die am Markt sind, haben bisher in nahezu keinem Fall einen Mehrwert in einer der Kategorien im Vergleich zu etablierten Technologien gezeigt.

Das zeigt sich auch daran, dass die Investitionen in Blockchain in den USA und China wieder rückläufig sind. Die Prototypen haben die großen Versprechungen bisher nicht ansatzweise einhalten können.

Frage 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?

Ausgehend von den bisher vorgelegten Blockchain Implementierungen halte ich die Technologie für wenig Erfolgsversprechend für alle angesprochenen Bereiche. Da in Blockchains Löschvorgänge nicht möglich sind, schließt sich die Ablage personenbezogener Daten (wie im Bereich Health) grundsätzlich aus. Die Vorteile, die eine dezentrale Technologie wie Blockchains theoretisch haben, können in den angesprochenen Bereichen im Vergleich zu etablierten Technologien und Protokollen keinesfalls die großen Nachteile (junge, fehleranfällige Technologie, stetig wachsende Datenverbräuche mit jedem teilnehmenden Player und potentiell extrem aufwändige Konsensmechanismen sowie die ungelöste Frage, wie mit Fehlern/Korrekturbedarf umgegangen werden soll) aufwiegen.

Frage 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?

Mir ist - außerhalb der Spekulation mit Kryptowährungen - kein real existierender Usecase bekannt, der nicht statt mit einer Blockchain besser mit etablierten Technologien abgebildet werden kann.

Jeder Anwendungsfall, der personenbezogene Daten betrifft, schließt sich per Definition (und DSGVO) aus: Personenbezogene Daten können nicht gelöscht werden. Alle Anwendungsfälle, bei denen eine strenge Regulierung und Aufsicht nötig ist, sollten auch nicht in eine Blockchain verschoben werden, da wie schon angemerkt, Daten nicht korrigiert oder entfernt werden können.

Grundsätzlich sind alle Fälle, die mit der physikalischen Welt interagieren schwierig: Das so-genannte Orakelproblem, also das Problem in einer digitalen Welt festzustellen, ob ein spezielles Ereignis woanders eingetreten ist (z.B. Paket ist angekommen) kann nicht sicher innerhalb des digitalen Systems abgebildet werden. Das ist bei traditionellen Systemen nicht so problematisch, weil Korrekturen und Anpassungen grundsätzlich vorgesehen sind. Blockchains schließen das aus, weshalb auch ökonomische und logistische Transaktionen stark gefährdet sind. Blockchains und ihre Automatismen funktionieren passabel in privaten Blockchains in denen keine Konflikte auftreten. Sobald man Probleme at scale angehen würde, wäre diese einfache Weltsicht hinfällig.

Frage 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 sind schätzen Sie diese Potentiale in ihrer grundlegenden Bedeutung ein?

Blockchains können in kleinen, vertrauenswürdigen Kontexten wie eine dezentrale Datenbank arbeiten und damit alle die Vorteile ausspielen, die Datenbanken und Automatisierung haben. Sie sind in ihrer aktuellen Form nur schlicht nicht wirtschaftlich im Vergleich zu anderen Datenbanktechnologien.

Direkt Blockchain-Verbundene Potenziale bestehen vor allem für die Firmen, die Blockchain Beratung verkaufen.

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

Intermediäre sind mehr als nur eine Datenbank. Von daher ist der Vergleich hier nicht sinnvoll. Man müsste zusätzlich zu einer Blockchain noch diverse Regelsysteme aufbauen, damit etwas als Intermediär auftreten könnte, welches auf einer Blockchain aufsetzt. Blockchains selber alleine können das nicht: Es gibt schlicht keine sinnvolle Art, wie Konflikte sinnvoll ausgetragen und vor allem verbindlich entschieden werden können. Das könnte man auslagern an eine Art "Gericht" - zu mindest für private Blockchains - das hat aber wiederum mit der Art wie Daten gespeichert werden (Blockchain oder nicht) nichts mehr zu tun: Die zentrale Gerichtsbarkeit - der ja alle vertrauen müssten, damit sie schlichten kann - könnte genau so gut eine normale Datenbank hosten, ohne all den Blockchain Overhead.

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

Ja, die Open Source Community, aus der Software wie Linux, Firefox und viele weitere Standardsoftware entstanden ist, hat diverse Konsensmodelle entwickelt, die eine zielgerichtete Produktentwicklung ohne eine Entscheidungsinstanz erlauben. Die Bandbreite hierbei reicht von basisdemokratischen bis hin zu meritokratischen Systemen.

Frage 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 der Bitcoin Blockchain sind diverse illegale Inhalte gespeichert: Man kann sie nicht entfernen und es wäre spannend zu untersuchen, ob sich nicht jeder Teilnehmende an der Bitcoin Blockchain in Deutschland strafbar macht.

Es gibt aus technischen Gründen keine Möglichkeit einen Falscheintrag zu korrigieren. Man kann ein "Update", d.h. Einen neuen, berichtigen Eintrag in die Blockchain

hängen, der den falschen ersetzen soll, aber der alte Eintrag bleibt immer bestehen. Das ist insbesondere bei personenbezogenen Daten nicht nur problematisch sondern illegal. Es gibt keinen Weg das zu adressieren.

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

Gar nicht. Weder das Recht auf Vergessenwerden noch das Recht auf Datenkorrektur sind in einer Blockchain umsetzbar.

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

Smart Contracts sind irreführend benannt, denn sie sind keineswegs “Verträge” (und auch nicht “Smart”). Smart Contracts sind klassische Datenbanktrigger, die auf Operationen auf der Datenbank (zum Beispiel einem neuen Block in der Blockchain) reagieren können.

Das Gesetz ist mehr als nur die Zeichen im Text, es ist komplex und manchmal mehrdeutig und widersprüchlich, Konflikte können oft erst in einer Güterabwägung auf Basis der konkreten Situation und den betroffenen Rechten und Pflichten gelöst werden.

Man kann Anfechtungsrechte in Smart Contracts durchaus abbilden, aber wie dann in einem dezentralen System eine Güterabwägung und Konfliktlösung funktionieren soll, ist völlig unklar.

Frage 11) Wie kann sichergestellt werden, dass beim Einsatz von Blockchain-Technologien zivilrechtliche Löschanträge 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).

Kann es nicht.

Frage 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?

Das ist innerhalb einer Blockchain selbst mit Smart Contracts nicht belastbar zu realisieren.

Frage 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?

Das ist genau die Frage, zu der die Blockchain Community bisher noch keine Antwort geben kann. Die Datenbank muss immer wachsen. Wenn eine Instanz sie bereinigen darf, dann kann ich mir den ganzen Budenzauber mit der Blockchain auch sparen und diese Instanz einfach eine sichere Datenbank hosten lassen für einen Bruchteil der Kosten.

Frage 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?

Das wäre in einer private Blockchain möglich. Wenn zum Beispiel die Bundesrepublik Zugänge zu einer Blockchain mit einem Personalausweis verknüpfen würde, wären Sperrungen durch klug gebaute Smart Contracts möglich. Natürlich würde man dadurch automatisch eine Form von zentraler Freigabeinstanz schaffen, wodurch sich wieder die Frage des Mehrwertes einer Blockchain stellt.

Smart Contracts sind keine Verträge und dürfen auch nicht verwechselt werden. Zahlungen ließen sich auch über Escrow und Smart Contracts abbilden mit den oben schon angedeuteten Zentralisierungskonsequenzen.

Frage 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?

Kryptowährungen und ICOs sind heute unreguliertes Glücksspiel: Es gibt keinerlei Sicherheiten für Investoren und die Anzahl der Betrugsfälle ist immens. Da sich die groben Blockchains, auf denen solche ICOs stattfinden wie Ethereum bewußt Regulierung entziehen, stellt sich hier die erste Frage: Wer ist überhaupt zuständig? Welche Finanzaufsicht ist zuständig für die Regulierung des Investitionsroulottes auf der Blockchain? Und wie kann Regulierung hier überhaupt angreifen? Man könnte eine

Standardisierung und eine Zertifizierung von ICOs etablieren, aber diese könnte nur freiwillig passieren. Der Investorenschutz bliebe weiterhin auf der Strecke.

Frage 16) Wie bewerten Sie die europäische Blockchain-Partnerschaft?

Eine solche Partnerschaft ist ja erst mal in Ordnung, um auch Forschung zu begleiten. Das Problem ist, dass diese Organisation eine Tendenz hat, Blockchain als Lösung zu präsentieren, egal wie das Problem beschaffen ist. Eigentlich sollte es anders herum funktionieren.

Frage 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?

Ja, auch wenn man sich bewusst sein muss, dass Bitcoins usw. ja kein Geld sind: Man kann sich für alle diese Währungen nicht wirklich etwas kaufen, sie müssen daher immer in Geld zurückgetauscht werden, um die Werte in der realen Welt nutzen zu können. Daher wird sich denke ich eher keine Vergrößerung des bestehenden Problems entwickeln, da die Straftäter im Zweifel beim Tausch der Kryptowährung in Echtgeld gefunden werden können.

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

Bis es echte Usecases für Blockchains gibt, maximal Forschungsinstitute. Kritische Daten und Prozesse sollte schlicht niemand auf Blockchains auslagern. Gerade der Staat sollte viel mehr über offene Datenbanken nachdenken, die Bürger*innen und anderen Entitäten Zugriff bieten, aber trotzdem die gesetzesmäßige Verwendung der Daten sicherstellen.

Frage 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?

Wenn eine zentrale Instanz wie die öffentliche Verwaltung Daten zum Zugriff anbieten will oder eine Schnittstelle zu diesen Daten bereitstellen möchte, dann sollte hier eine etablierte Datenbanktechnologie eingesetzt werden: Eine Blockchain/DLT würde hier schlicht ihre Vorteile nicht ausspielen können.

Frage 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?

In keinem Bereich. Smart Contracts sind schlicht nicht für solche Prozesse geeignet.

Frage 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?

Angriffsmuster bei Blockchains sind heute nicht so sehr potentielle Quantenkryptoangriffe sondern viel mehr schlecht programmierte Blockchain Implementierungen, gerade wenn es um Smart Contracts geht. Wenn Quantenkryptographie oder andere Angriffsmethoden es erlauben, die spezielle Hash-Art einer Blockchain, die die Integrität der Blöcke sicherstellt, anzugreifen, dann könnte einer Blockchain ein falscher Block untergeschoben werden, d.h. Die Vergangenheit umgeschrieben werden.

Heutige Angriffe sind oft auch gar nicht technisch sondern gehen eher auf den Konsensmechanismus: Einige wenige Entitäten haben einen Großteil der "Mining Power" von Bitcoin und könnten - so sie wollten - bestimmte Accounts einfach aus dem Netz ausschließen, indem deren Transaktionen nicht mehr bearbeitet würden. Hier hilft auch kein technischer Trick.

Frage 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?

Der Blockchain Hype kühlt weltweit gerade ab, die Versprechen haben sich in keiner Situation erfüllt. Deutschland hat also in diesem Fall Glück gehabt und nicht viel Geld in die Erforschung einer Nischentechnologie gesteckt. Es sollte hier keine besonderen Aktivitäten geben, insbesondere wenn man betrachtet, dass andere Länder schon groß angelegte Studien zu Blockchains durchgeführt haben und (wie zum Beispiel im Falle

Australiens) feststellten, dass eigentlich nur die Verkäufer von Blockchains diese überall pushen, aber es eigentlich keine wirtschaftlich oder inhaltlich sinnvollen Anwendungsbereiche gibt.

Frage 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?

Ich bezweifle, dass die Blockchain Technologie überhaupt neue Geschäftsmodelle ermöglicht und wenn, sollten dazu keine gesetzlichen Anpassungen notwendig sein. Gesetzesanpassungen, die sich ganz konkret auf eine Technologie beziehen, werden immer durch kurzfristige Entwicklungen überholt werden und ins leere Laufen. Gesetzgebung für die Digitale Sphäre muss sich eher an Grundrechten und politischen Zielen ausrichten.

Frage 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?

ICOs sind zur Zeit für verbraucher und auch Investoren eine zu risikoreiche Investition. Es gibt keine Standards, keine Sicherheit und oft nicht mal die Möglichkeit, das, in das investiert wird, wirklich zu begutachten.

Die einzigen Unternehmen, die von ICOs profitieren, sind die, die Geld für die Ausgabe wertloser Bits bekommen.

Frage 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 müssten reguliert werden, wie traditionelle Aktien und Investitionen. Wenn sie dann noch gute Rendite abwürfen, wäre das das Anreizsystem. Da eine Regulierung

von Token auf den großen öffentlichen Blockchains wie Ethereum aber unmöglich ist, sollten aus Investorenschutz gar keine Anreize geschaffen werden dort zu investieren. Eher das Gegenteil.

Frage 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?

Ja. Regulierung öffentlicher Blockchains schlägt fehl, daher sollten hier keine Incentives gesetzt werden. Das lässt sich genau so übertragen.

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

Warum sollte sie das tun? Bei all den aufgezeigten Problemen der Blockchain muss die Community überhaupt erst einmal zeigen, dass das Produkt es wert ist, enabled zu werden. Hier sollte man nichts übers Knie brechen.

Frage 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 künftigen Speicherplatzbedarf und Transaktionsraten? Wie könnte eine Massentauglichkeit der Technologie realisiert werden?

Man könnte andere Konsensmethoden (proof of Stake zum Beispiel) einsetzen. Diese verbrennen weniger Energie, haben dafür andere Probleme (bei Proof of Stake zum Beispiel entscheiden letzten Endes einfach die, die am meisten haben, was passiert, was jeden Markt unterläuft).

Methoden, die die Anzahl der Transaktionen erhöhen sollen wie das Lightning Network bei Bitcoin sind letzten Endes nur Rezentralisierungen des Netzwerks. Diese machen es leistungsfähiger, allerdings stellt sich dann wieder die Frage, warum man es nicht gleich leistungsfähig ohne Blockchains baut.

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

Nein. Blockchains lösen keines der diversen Probleme, die elektronische Wahlen plagen und die dazu geführt haben, dass in der Bundesrepublik nicht elektronisch gewählt wird. Und personenbezogene Daten, wie sie die Identifizierung von Personen braucht, dürfen nicht in Blockchains geschrieben werden, weil sie nicht korrigiert werden können (DSGVO).