BOTLABS GmbH | Keithstraße 2-4 | 10787 Berlin

**Deutscher Bundestag**
**Ausschuss Digitale Agenda**
Platz der Republik 1
11011 Berlin

**Deutscher Bundestag**
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)027

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

## Ingo Rübe – Founder & CEO, BOTLabs GmbH

**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?**

Zur Unterscheidung DLT/Blockchain/Bitcoin

a) **Distributed-Ledger-Technologien** beschreiben Verfahren, bei denen ein Kontenbuch oder eine Datenbank nicht zentral von einer Instanz (wie beim Bankkonto, beim Grundbuch oder bei einem Kassenbuch), sondern von mehreren Instanzen geführt wird. Im Gegensatz zum zentralen Ansatz ergeben sich folgende Vorteile:
   - Mehr Sicherheit, da Angreifer mehr als eine Instanz angreifen müssen,
   - Schutz vor Korruption, da sich mehrere Instanzen auf die Wahrheit einigen müssen und eine betrügerische Instanz keine Mehrheit finden wird,
   - Mehr Transparenz, da die Inhalte der Datenbank allen bekannt sind, die für die Führung der Datenbank verantwortlich sind.

   Es ergeben sich aber auch folgende Nachteile:
   - DLT speichern die Datenbank mehrfach. Sie sind also im Betrieb immer teurer als zentrale Systeme,
   - Zwischen den Instanzen muss immer wieder ein Konsens gefunden werden. Dies braucht Zeit. Deshalb sind DLT meist langsamer als vergleichbare zentrale Systeme.

b) **Blockchains** sind eine Möglichkeit, Distributed-Ledger-Systeme umzusetzen. Blockchains sind kontinuierlich erweiterbare Listen von Datensätzen (Block), die mittels kryptografischer Verfahren miteinander verkettet (Chain) sind. Diese Kette von Blöcken kann als verteilte Datenbank verwendet werden. Sie bietet folgende Vorteile:

- Blockchains vergessen nicht. Durch die die Verkettung der Liste sind alle Transaktionen bis zum Beginn der Blockchain von jedem einsehbar. Dies verhindert eine Reihe von Angriffsvektoren und macht Blockchains sehr sicher gegen Angriffe,
- Diese systeminhärente Sicherheit kann mehr Vertrauen herstellen als zentrale Instanzen. Blockchains eignen sich damit zur Ablösung von Intermediären,
- Blockchains sind eigene Ökosysteme, die keine zentrale Instanz zum Betrieb und zur Pflege benötigen. Sie ermöglichen auf diese Weise die Demokratisierung von Vorgängen.

Es ergeben sich aber auch folgende Nachteile:

- Da Blockchains ohne zentrale Instanz auskommen, sind Fehler (sowohl in der Programmierung als auch in der Datenbank) sehr schwer zu korrigieren. Hier benötigen Blockchains ein komplexes Governance-Modell.

c) **Bitcoin** ist ein Blockchain-Protokoll, das vor gut 10 Jahren entwickelt wurde. Es kann als die erste Blockchain bezeichnet werden, obwohl große Teile der Technologie bereits vorher in anderen Systemen verwendet wurden. Bitcoin hatte im Jahr der Finanzkrise 2008 das Ziel, eine rein elektronische Währung (den Bitcoin) als Alternative zu den von Banken kontrollierten FIAT-Währungen zu etablieren und diese langfristig zu ersetzen. Während dieses Ziel klar verfehlt wurde, hat Bitcoin es geschafft, dass ein neuer Industriezweig (Blockchain und DLT) entstanden ist, durch den ein hoher volkswirtschaftlicher Nutzen und zahlreiche Arbeitsplätze geschaffen wurden.

Dies sollte man stets bedenken, wenn man die Langsamkeit, den Energieverbrauch, die unzureichende Governance und die mangelnde Benutzerfreundlichkeit von Bitcoin kritisiert. Denn Bitcoin ist lediglich ein Prototyp der Blockchain.

<u>Zur Unterscheidung öffentliche/private Blockchains</u>

a) **Öffentliche Blockchains** sind insofern mit dem Internet vergleichbar als dass jeder Teilnehmer jede Rolle im Netzwerk annehmen kann ohne einen Antrag oder ein Genehmigungsverfahren. Insbesondere kann jeder beschließen, einer der Buchhalter, die die Blockchain führen, zu werden. Dies ist ein wichtiger Aspekt des Vertrauens und der Demokratisierung. Bitcoin und Ethereum sind öffentliche Blockchains. Genau wie das Internet nie eine Erfolgsgeschichte geworden wäre, wenn es von einer Firma oder einem Staat betrieben worden wäre, beruht der Erfolg und die enorme Wertschöpfung dieser Blockchains auf ihrer Offenheit. Im gesamten Blockchain-Ökosystem machen öffentliche Blockchains den Löwenanteil der Wertschöpfung aus.

b) **Private Blockchains** sind mit einem Intranet in einer Firma oder Behörde oder mit dem BTX-System vergleichbar. Hier können nur ausgewählte Personen teilnehmen und insbesondere der Kreis der Buchhalter ist beschränkt. Es sind Anwendungen zur innerbetrieblichen Leistungsverrechnung und zum Nachvollziehen von geschlossener Lieferketten denkbar. Diese wären aber prinzipiell meist auch mit zentralen Systemen umsetzbar. Private Blockchains verwenden die Blockchain-Technologie, um eine „ganz normale“ Software darzustellen. Sie bedürfen weder einer Regulierung noch der Aufmerksamkeit der Politik, da sie maximal betriebswirtschaftlichen Nutzen haben.

**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 nicht pauschal beantworten, da sie nicht nur auf einzelne Blockchains abzielt, sondern auch zugrundeliegende Technologien, wie z.B. Konsens-Algorithmen, erörtert werden müssten. Allerdings lässt sich grundsätzlich sagen, dass sich die Blockchain-Technologie als enorm zuverlässig herausgestellt hat. Sowohl die großen Blockchains wie Bitcoin oder Ethereum als auch neue Varianten wie Ripple oder ZCash laufen zuverlässig und mit sehr hoher Sicherheit. Neuere Technologien, wie die in Deutschland entwickelte BigChainDB, erlauben eine sehr hohe Transaktions-/Durchsatzgeschwindigkeit. Das Thema der Interoperabilität wird insbesondere von der (in Deutschland entwickelten) Blockchain Polkadot aufgegriffen. Der hohe Energieverbrauch von Proof-of-Work-Algorithmen, wie sie bei Bitcoin und Ethereum im Einsatz sind, ist bei moderneren Verfahren wie Proof-of-Stake nicht mehr relevant.

Unser Unternehmen setzt für die Entwicklung neuer Blockchains auf das (in Deutschland entwickelte) Framework Parity Substrate, auf dem auch Polkadot basiert.

Über die Wirtschaftlichkeit entscheidet letztlich immer der Use Case: So ist Sicherheit beispielsweise immer eine Funktion aus größtmöglichem Schaden und Investitionsbereitschaft in dessen Verhinderung.

**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?**

Das größte Potenzial der Blockchain-Technologie liegt in der Evolution des Internets hin zu einem Web 3.0, in dem nicht mehr monopolistische US-Konzerne wie Facebook und Google allein profitieren. Dies kann mit Blockchain-Technologie erreicht werden, indem Dienste wie Identität, Suche und Bezahlung (aber auch das Buchen von Taxis oder Übernachtungsmöglichkeiten) auf Protokollebene implementiert werden. Die zugrundeliegenden Daten wären nicht mehr in den privaten Daten-Silos einiger weniger Firmen gefangen, sondern stünden jedem zur Verfügung, der Mehrwertdienste anbieten möchte.

Das zweite große Potenzial der Blockchain-Technologie liegt darin, Daten handelbar zu machen. Dies ist ein für Regierungen enorm wichtiger Aspekt, da dieser Markt in einigen Jahren vermutlich dem Volumen einer der größten sein wird und die Besteuerung eine der wichtigsten Einnahmequellen der Staaten werden könnte.

Bereiche wie eHealth, eGovernment und Energiewirtschaft sind darüber hinaus ebenfalls wichtige Anwendungsfelder. Notwendige Voraussetzungen für die Nutzbarmachung von DLT/Blockchain für diese Bereiche sind:

- **Technologisch**: Blockchain-Technologien müssen so gestaltet sein, dass sie für Wirtschaft und Verwaltung verständlich und leicht nutzbar sind. Es müssen SKDs (Software Deveopment Kits) für normale Anwendungsentwickler geschaffen werden, auf denen sich leicht Applikationen entwickeln lassen. An einer solchen Blockchain mit SDK arbeitet derzeit unter anderem BOTLabs.

- **Basistechnologien**: Es müssen Standards für Identität, Micropayments, Urheberrechte usw. etabliert werden.
- **Rechtssicherheit**: Herstellung und Betrieb von Blockchains müssen rechtssicher möglich sein, damit Unternehmen und Verwaltung investieren und Blockchains für geschäftskritische Prozesse anwenden können.

**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?**

Der Einsatz einer Blockchain ist immer dann sinnvoll, wenn durch dezentrale Datenhaltung Vertrauen oder Geschäftsgrundlagen geschaffen werden können, die zentral nicht oder nur eingeschränkt existieren. Use Cases entstehen nur selten im betriebswirtschaftlichen Denken eines Unternehmens, sondern eher, wenn man sich eine ganze Branche ansieht. Einige Beispiele:

- Für den elektronischen Zahlungsverkehr sind Blockchains geeigneter als Banken, da keine zentrale Instanz mehr angegriffen werden kann.
- Die Aufbewahrung einer elektronischen Patientenakte im Besitz des Patienten könnte durch eine Blockchain realisiert werden. Dies würde die Datensouveränität der Patienten erhöhen.
- Die Inhalte auf sozialen Netzwerken könnten ebenfalls durch Blockchain-Technologie in den Besitz der Nutzer übergehen. Dies würde den Missbrauch von Daten, beispielsweise durch Facebook, verhindern. Das gilt gleichermaßen auch für Kaufhistorien, Suchverläufe und alle anderen „Spuren im Internet“.
- Ticketing im ÖPNV, Bahn, Flugzeug usw. ist mit Blockchains effizienter umzusetzen. Auch hier gilt es Branchenlösungen zu entwickeln, um die Potenziale von Blockchains voll zu heben.
- Dienste wie Uber und AirBnB verlören ihre Monopolstellung, wenn Mitbewerber ähnliche Angebote auf Blockchain anbieten würden.
- Datenhandel (und damit das Aufbrechen der Datensilos) wird wahrscheinlich auf der Blockchain entstehen.
- Self-Owned-Devices (also beispielsweise Autos, die eine eigene rechtliche Einheit darstellen, sich selbst beim Hersteller leasen, sich dann streckenweise vermieten und die Einnahmen versteuern) sind ohne Blockchains fast nicht denkbar.

Grundsätzlich bringen Blockchains folgende Gefahren mit sich:

- Blockchains und Künstliche Intelligenz stellen eine neue Technologieklasse, „Opionated Technologies“, dar. Das heißt, wir haben es mit Technologien zu tun, die sich selbst Meinungen bilden und aufgrund dieser Meinungen, meist ohne Eingriffsmöglichkeit von Menschen, Entscheidungen treffen und handeln. Insbesondere im Zusammenspiel zwischen K.I. und Blockchain entstehen hier Risiken.
- Blockchain Governance ist bisher weitgehend unerforscht. Da Blockchains ein eigenes Ökosystem mit eigenen Regeln erstellen, können kleine Fehler in der Governance große Auswirkungen haben. Beispiel: Es wäre sicher sinnvoll, den Proof-of-Work-Algorithmus von Bitcoin durch einen moderneren Konsens zu ersetzen, der nahezu keine Energie verbraucht. Über solch eine Änderung stimmen (gemäß Bitcoin Governance) aber ausschließlich diejenigen ab, die in die Hardware investiert haben, die heute die Energie verbraucht. Aus Gründen des Investitionsschutzes

wird diese Gruppe niemals einem neuen Algorithmus zustimmen, der ohne ihre Rechenleistung auskommt.

Daraus ergibt sich aus meiner Sicht die Forderung, Blockchains nur dort einzusetzen, wo man auf die Entscheidung einer zentralen Instanz verzichten kann. So können beispielsweise nur sehr begrenzte Teile unseres Rechtssystems über Smart Contracts in Blockchains dargestellt werden.

**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?**

Die meisten privaten und genehmigungsbasierten Blockchains werden langfristig weder gesellschaftliche, noch ökonomische, noch ökologische oder soziale Auswirkungen haben. [Siehe Frage 1]

Öffentlich-genehmigungsfreie Blockchains haben hingegen das ökonomische Potenzial, das Ungleichgewicht, das im Internet zwischen Europa und den USA entstanden ist, auszugleichen. Es handelt sich in dieser Hinsicht wahrscheinlich um die wichtigste Technologie für die Zukunft Europas.

Aus sozialer Sicht kann man erwarten, dass im Falle einer klugen Regulierung Blockchain-Entwicklungen als neuer Wirtschaftszweig in Deutschland entstehen. Wir haben als weltweites Zentrum der Blockchain-Entwicklung (Ethereum, die erste DAO, Polkadot, Ocean-Protocol, Kilt-Protocol, …) die besten Voraussetzungen und enormes Potenzial. Andererseits werden in den Bereichen Internetplattformen und Finanzwirtschaft zahlreiche Arbeitsplätze verloren gehen, im Bereich der Plattformen allerdings hauptsächlich in den USA. Da es sich bei Blockchain um ein internationales Phänomen handelt, ist es unmöglich, die deutschen Arbeitsplätze im Bereich der Finanzwirtschaft zu schützen, indem man Blockchain-Entwicklungen in Deutschland behindert. Sie finden dann andernorts statt und haben dieselben negativen Auswirkungen als wäre sie hier entwickelt worden (mit Ausnahme der positiven Effekte).

Aus ökologischer Sicht können Blockchains nur Vorteile haben, da sie es erlauben, den Energieverbrauch besser und kontinuierlicher zu messen und zu regeln.

Die wichtigste gesellschaftliche Auswirkung wird vermutlich ein Umdenken beim Besitz von Daten sein. Wir gehen heute wie selbstverständlich davon aus, dass zentrale Instanzen wie Facebook der Eigentümer unserer persönlichen Daten sind, gleichzeitig schockieren uns Skandale wie Cambridge Analytica. Blockchains werden die Gesellschaft fragen lassen, wo genau ihre Teilhabe ist und gleichzeitig die Rechte des Individuums an seinen Daten stärken. Dies führt zu mehr Datenmündigkeit und zu einer demokratischeren Gesellschaft.

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

Blockchains können Intermediäre nur zum Teil ersetzen. Ein Vergleich zur „analogen Welt“: Ein Medienhaus ist ein klassischer Intermediär. Es steht einerseits zwischen den Lesern und den Akteuren (Politiker, Stars, …), andererseits zwischen dem Leser und dem Werbetreibenden. Die Wertschöpfung des Medienhauses ist aber die Produktion und Publikation von Inhalten. Sicherlich lassen sich einige Abläufe, wie

der Einkauf von Bildern bei Agenturen und sogar die Wertermittlung von Medienmarken über Blockchains abwickeln. Artikel schreiben und diese veröffentlichen werden Blockchains aber nie.

Das Beispiel zeigt: Blockchains können Intermediäre nur dann ersetzen, wenn die einzige Wertschöpfung des Intermediärs der exklusive Zugriff auf einen Datenpool ist, der durch die Blockchain öffentlich gemacht wird, oder wenn er lediglich als „vertrauenswürdiger Dritter" in Transaktionen benötigt wird.

Das Ersetzen von Intermediären, die ihr Geschäftsmodell auf exklusiver Nutzung von Daten aufgebaut haben, hat sicher keine Nachteile. Im Gegenteil: Es schafft durch die Offenlegung der Daten einen offenen Markt für neue Anbieter. Mit anderen Worten, das Ersetzen von vertrauenswürdigen Dritten durch vertrauenswürdige Technologie erscheint lediglich für den vertrauenswürdigen Dritten als nachteilig. Volkswirtschaftlich wird mehr Wert geschaffen, da eine monopolistische Struktur aufgebrochen wird. Dies ist auch zum Wohle des Verbrauchers.

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

Mit dieser Frage setzt sich das Forschungsfeld Blockchain Governance auseinander. Es gilt, Strategien zu entwickeln, die einerseits demokratisch sind, andererseits aber die Interessen von Stakeholdern wie Minern ausreichend zu berücksichtigen. Auch ist darauf zu achten, dass sich keine ungeregelte Marktwirtschaft entwickelt, in der das Recht des Reicheren gilt. Hier wird derzeit viel geforscht, dabei gibt es durchaus verschiedene Ansätze.

**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?**

Blockchain ist eine Basistechnologie und keine fertige Software wie beispielsweise MS-Word. Es steht jedem frei, vor- und nachgelagerte Prozesse zu implementieren, die mit auftretenden Problemen umgehen. So könnte eine Buchung beispielsweise erst nach einer sorgfältigen Überprüfung auf einer Blockchain gespeichert werden. Auch könnte im Falle einer Falschmeldung die Korrektur gespeichert werden. Im Gegensatz zu einer herkömmlichen Datenbank wäre bei der Blockchain dann die komplette Historie sichtbar.

Sollte es aber eine wichtige Anforderung sein, dass irrtümliche Falschbuchungen erst gespeichert und später rückstandsfrei wieder gelöscht werden müssen, so sollte für diesen Use Case keine Blockchain verwendet werden.

Das Thema illegale Daten ist komplexer. Bekanntgeworden ist eine winzige Bilddatei, die mutmaßlich kinderpornografisches Material enthielt, und die Teil der Bitcoin-Blockchain geworden ist. Hierzu ist anzumerken, dass die Bitcoin-Blockchain eigentlich Finanztransaktionen verwaltet. Es ist einem „normalen" Nutzer also lediglich möglich, Geldbeträge zu versenden; es lässt sich jedoch kein illegales Material speichern. Der Nutzer, der die fraglichen Daten eingestellt hat, verwendete dafür ein Datenfeld, das ausschließlich Miner beschreiben können. Um die Daten zu schreiben, musste er also erst einmal einen Block gewinnen – eine erhebliche Investition. Dazu kommt, dass das Datenfeld nur wenige Byte groß ist und das vermeintliche Bild deshalb nur wenige Pixel enthalten kann. Um es aus der Bitcoin-Blockchain

zu extrahieren und anzuzeigen, benötigt man detaillierte Fachkenntnisse über die Bitcoin-Blockchain. Das Bild ist also sehr sicher vor versehentlichem Anschauen geschützt. Leider greifen Medien immer wieder solche Themen auf und vermitteln den Eindruck, das Blockchains gut zum Verbreiten illegaler Daten geeignet sind. Das Gegenteil ist der Fall: Es gibt keinen teureren Speicher als eine Blockchain. Die Verbreitung illegaler Daten auf anderen Wegen ist wesentlich einfacher und kostengünstiger.

Beim Design einer Blockchain sollte man allerdings immer darauf achten, dass diese möglichst wenig Daten speichert. Das erschwert nicht nur die Ablage illegaler Daten, es macht auch den Betrieb der Blockchain wesentlich günstiger.

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

Die DSGVO wurde bereits im Jahre 2012 konzipiert und betrachtet Blockchains nicht. Das führt dazu, dass sich Blockchain und DSGVO in Teilen widersprechen, obwohl beide die Datensouveränität des Einzelnen zum Ziel haben. Das „Recht auf Vergessenwerden“ beispielsweise zielt auf Anbieter von Suchmaschinen und sozialen Netzwerken. Es wird davon ausgegangen, dass diese Anbieter Datensilos mit persönlichen Daten anlegen und regelt die Pflicht auf Löschung persönlicher Daten auf Verlangen des Nutzers.

Hier kollidiert DSGVO und Blockchain-Technologie, da Blockchains nicht vergessen. Beim Design einer Blockchain, die im Bereich personenbezogener Daten arbeitet, sollte man also stets darauf achten, nicht die Daten selbst, sondern lediglich Hash-Werte der Daten oder Zeiger auf Datenspeicher, auf der Blockchain zu halten und niemals die Daten selbst.

Um den Betreibern von Blockchains hier Rechtssicherheit zu geben, wäre eine übergreifende, möglichst europaweite Interpretation der DSGVO sehr sinnvoll. Es ist beispielsweise zu klären, inwieweit ein Hash-Wert noch personenbezogen ist und mit welcher Menge von nicht-personenbezogenen Daten ein Datensatz anzureichern ist, damit sein Hash-Wert nicht mehr als personenbezogen gilt.

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

Zur Beantwortung dieser Frage ist eine juristische Bewertung notwendig.

**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).**

Zur Beantwortung dieser Frage ist eine juristische Bewertung notwendig.

**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?**

Zur Beantwortung dieser Frage ist eine juristische Bewertung notwendig.

**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?**

Bei der Entwicklung der Blockchain sollte darauf geachtet werden, dass diese so wenig Daten wie möglich hält. Dies wird ökonomisch dadurch sichergestellt, dass die Transaktionskosten einer Blockchain mit vielen Daten so hoch sein würden, dass sie niemand benutzen würde.

Wenn die Blockchain hingegen sinnvoll konzipiert ist und beispielsweise nur Hash-Werte von Transaktionen enthält, ist dieses Problem zu vernachlässigen. Die Bitcoin-Blockchain beispielsweise hat heute nach 10 Jahren im Betrieb eine Größe von 200GB. Die kleinste Festplatte, die man im Internet kaufen kann, hat 500GB und kostet weniger als 70 Euro. Da die Blockchain linear wächst, reicht diese Festplatte dann noch für weitere 15 Jahre.

**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?**

Um eine Transaktion zu verhindern oder rückabzuwickeln, wäre eine genehmigungsbasierte / private („permissioned“) Blockchain notwendig. Damit würde man die grundlegenden Eigenschaften der Blockchain (Offenheit und Demokratisierung von Prozessen) aufgeben.

Blockchain / DLT im Allgemeinen (und die permissionless-Blockchain im Speziellen) ermöglichen eine neue Art von Transaktionen, die eine Vielzahl von Vorteilen hat.

**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?**

15.1 Die Token-Klassifizierung sollte europaweit vereinheitlicht werden. Einheitlich ist nur die Gruppe der wertpapierähnlichen Token, die auf europäischem Recht basiert. Die von der BaFin vertretene Gruppe der sog. Rechnungseinheiten (Finanzinstrumente nach KWG) für Kryptowährungen existiert auf europäischer Ebene nicht und verursacht eine Benachteiligung des deutschen Marktes von Dienstleistern, die hier, anders als im europäischen Ausland, einer Erlaubnis bedürfen.

15.2 Erforderlich ist eine Diskussion über die regulatorische Behandlung solcher Projekte, die ohne Gewinnerzielungsabsicht eine öffentlich verfügbare, digitale Infrastruktur zu schaffen beabsichtigen. Hierfür ist eine neue Klasse der Gemeinnützigkeit erforderlich sowie regulatorische Erleichterungen zur Förderung dieser gesellschaftlich sinnvollen Projekte.

15.3 Es besteht dringender Handlungsbedarf zur Schaffung transparenten und fairer Märkten für alle Token-Klasse, auch der bislang nicht regulierten Token. Erforderlich sind europäische Regeln für Insider Tradings über alle liquiden Token Klassen hinweg

15.4 Das veraltete Konzept von papierbasierten Wertpapiere sollte aufgegeben werden.

15.5 Wünschenswert wäre ein zentraler Ansprechpartner im öffentlichen Bereich für Unternehmen, der die vielfältigen Themen koordiniert (Finanzaufsicht, Steuern, Verbraucherschutz).

15.8 Die BaFin sollte deutlich mehr, spezialisiertes Personal erhalten, um mit der technologischen Entwicklung Schritt halten zu können und in Zeiträumen auf Anfragen antworten zu können, die auch für schnell agierende Startups noch vertretbar sind.

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

Die europäische Blockchain-Partnerschaft zeigt, dass die Mitgliedsstaaten die Relevanz der Blockchain erkannt haben. Auch ist es positiv zu bewerten, dass sich die Bundesregierung aktiv beteiligt, Use Cases gesammelt hat und die jeweils zuständigen Ressorts miteinbeziehen wird. Wichtig ist dabei, dass die konkreten (Pilot-)Projekte politische Unterstützung erfahren, um auch auf europäischem Level sich als Vorreiter positionieren zu können.

**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?**

Derzeit sind Kryptowährungen für kriminelle Aktivitäten unattraktiv. Illegale Geschäfte, Schwarzarbeit und Geldwäsche lassen sich wesentlich einfacher anonym mit Bargeld abwickeln. Daher wird nur ein sehr kleiner Teil der kriminellen Geschäfte über Kryptowährungen getätigt. Das liegt insbesondere daran, dass die Blockchains alle Transaktionen für Dritte nachvollziehbar zur Verfügung stellen. Sollte ein Krimineller beispielsweise an einem Drogengeschäft verdient haben und den Gewinn gegen ein Luxusgut tauschen wollen, so muss er spätestens bei der Bezahlung seine Kryptowährung in Fiatgeld umtauschen, wodurch nicht nur seine Krypto-Adresse (Public Key) bekannt und mit seiner Person assoziierbar wird, sondern auch die Adressen seiner Klienten öffentlich würden.

Grundsätzlich ist es wichtig, dass Krypto-Börsen gute und einheitliche Prozesse zur Identifizierung von Teilnehmern („KYC/AML“) durchführen. Hierfür sollte ein internationaler Standard geschaffen werden.

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

Jede der genannten Optionen ist möglich und kann sinnvoll sein. Wichtiger als die Betreiber-/Verwaltungsstruktur einer Blockchain ist die Frage, ob diese genehmigungsfrei („permissionless“) ist. In genehmigungsfreien Blockchains kann jeder Teilnehmer partizipieren und die Blockchain weiter gestalten. Auf diese Weise wird Vertrauen generiert.

Das Kilt-Protokoll ist beispielsweise eine genehmigungsfreie Blockchain. Sie bildet eine technische Grundlage, auf der jeder eigene Anwendungen aufbauen kann – der Staat, zivilgesellschaftliche Organi-

sationen, private Unternehmen oder eine Partnerschaft aus den Bereichen. Wäre Kilt eine genehmigungspflichtige („permissioned“) Blockchain – vergleichbar mit einem Intranet – könnten andere Akteure nicht teilnehmen.

**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?**

In der öffentlichen Verwaltung ist der Einsatz von Blockchains etwa bei öffentlichen Registern sinnvoll. Das bietet sich insbesondere dann an, wenn Dienste bereits heute dezentral geführt werden, wie beispielsweise ein Grundbuch.

Die öffentliche Verwaltung profitiert von Blockchain-Technologien, da sie mehr Transparenz und Vertrauen schaffen können. So kann etwa Korruption effektiv bekämpft und Vorgänge nachvollziehbarer ausgestaltet werden.

Zu den notwendigen Fähigkeiten: Die öffentliche Verwaltung muss nicht in der Lage sein, eine eigene Blockchain zu entwickeln. Es genügt, eigene Applikationen zu entwickeln und auf die Blockchain aufzusetzen. Dafür gibt sogenannte Software-Development-Kits. Für unser Kilt-Protokoll haben wir einen solchen Bausatz veröffentlicht, mithilfe dessen Entwickler – etwa aus der öffentlichen Verwaltung – eigene Anwendungen schreiben und auf Kilt aufsetzen können.

**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?**

Zur Beantwortung dieser Frage wird auf die Antwort zu Frage 4 verwiesen.

**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?**

Die Sicherheit der Assets in einer Blockchain hängt von dem verwendeten kryptografischen Verfahren ab. Alle diese Verfahren werden irgendwann unsicher. Jedoch besteht die Möglichkeit des Austauschens der Instrumente und demnach ein dauerhafter Schutz.

Zur Quantenkryptografie: Es ist davon auszugehen, dass alle heute verwendeten Verfahren dann unsicher werden, wenn Quantencomputer wirksam eingesetzt werden können. Spätestens zu diesem Zeitpunkt sollten die kryprografischen Verfahren in Blockchains durch quantensichere ersetzt werden – mit ausreichendem zeitlichem Vorlauf kann die Umstellungsinnvoll vorbereitet werden.

**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?**

Für die Beantwortung der Frage verweisen wir auf Frage 23.

**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?**

Die Fragen 22 bis 23 werden gemeinsam beantwortet.

Der Trend, dass eine Vielzahl an Blockchain-Startups zumindest für ICOs in andere europäische Länder oder nach Asien abwandern, zeigt, dass in Deutschland keine genügenden Rahmenbedingungen gegeben sind.

Bewusst ist uns dabei, dass die Politik sich auf die relevantesten Themen erstmal konzentrieren muss und nicht alle Bereiche auf einmal angehen kann. Als dringendste Bereiche sehen wir folgende Regulierungsfelder:

- **ICO/Currencies** Für ICOs wäre es ein enormer Standortvorteil für Deutschland, wenn es eine einfache Checkliste (vergleichbar mit dem Standard in Singapur) geben würde, die ausschließt, dass es sich bei ICOs um Securities/Wertpapiere handelt.

- **Steuern:** Da insbesondere Pre-Sales (aber auch ICOs) nicht dem Profit, sondern der Entwicklung und Weiterentwicklung des Netzwerks dienen sollen, wäre es wichtig, wenn Einnahmen aus Pre-Sales über bis zu drei Jahre als Gewinnvortrag in der Gesellschaft belassen werden könnten.

- **DSGVO/Personenbezogenen Daten:** Alle Cryptocurrency-Netzwerke verwalten Kontostände. Das ist systeminhärent und nicht vermeidbar. Wenn die Kontostände jedoch als personenbezogene Daten klassifiziert werden, kann es keine Cryptocurrencies geben. Hier müsste eine Ausnahme her, um Rechtssicherheit zu schaffen.
  Hashes (kryptografisch sichere Streuwerte) sollten als nicht-personenbezogene Daten anerkannt werden, wenn sie neben personenbezogenen Daten auch andere Daten enthalten (ebenfalls notwendig für die Rechtssicherheit).
  Betreiber von full nodes (Programme, die die Gültigkeit von Blöcken/Transaktionen gewährleisten) in permissionless-Netzwerken brauchen Rechtssicherheit: als Betreiber von Infrastruktur, die keinen Einfluss auf die von ihnen gespeicherten Daten haben und deshalb auch nicht im Sinne der DSGVO zur Rechenschaft gezogen werden können.

- **Rechtsformen (u.a. für Smart Contracts):** Nach deutschem Recht haben Vermögenswerte zu jedem Zeitpunkt einen Besitzer. Dieser kann entweder eine natürliche oder eine juristische Person sein. In der Blockchain kann das zu Schwierigkeiten führen, denn ein Smart Contract stellt keines von beidem dar. Dies verhindert moderne Blockchain-Systeme in Deutschland. Hierfür müsste eine Lösung erarbeitet werden.

**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?**

Eine sinnvolle Regulierung von Token-Emission schafft Rechtssicherheit für Investoren, erleichtert somit ICOs in Deutschland und schafft Arbeitsplätze.

Bei einem IPO werden Unternehmensanteile an Investoren verkauft. Bei einem ICO hingegen werden Produkte der betreffenden Firma in Form von Token an Investoren weitergegeben. Dementsprechend ändert sich die Aufteilung der Firmenanteile nicht; die Gesellschafteranteiler bleiben gleich. Das macht es für Investoren attraktiver, in die betreffende Firma zu investieren. Zusätzliche Kapitalaufnahme schmälert seinen Anteil nicht, gleichzeitig vergrößert sich der potentielle Gewinn. Gerade für Deutschland, wo es vergleichsweise wenig „Seed Capital"-Investoren gibt, die eine Anschubfinanzierung leisten, sind ICOs daher interessant.

Ein ICO kommt insbesondere für kleinere Unternehmen mit Anschubfinanzierung in Betracht. Allerdings ist ein ICO immer noch ein großes logistisches Unterfangen, das viel Geld kostet. Insbesondere Startups können von token-basierten Finanzierungsmöglichkeiten profitieren.

Zu den Risiken im Zusammenhang mit ICOs für VerbraucherInnen und Unternehmen: ICOs sind nur dann prospektbehaftet, wenn es sich um Security Token handelt. Im Normalfall handelt es sich bei ICOs jedoch um Kryptowährungen, die – ebenso wie Utility Token – nicht der Prospektpflicht unterliegen.

**25. Wie und in welchem Rahmen sollte eine verbindliche Normierung der TokenTypen (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?**

Zur Beantwortung dieser Frage wird auf die Antwort zu Frage 15 verwiesen.

**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?**

Wir glauben, dass der Anwendungsbereich der Blockchain-Technologie im Nicht-Finanzbereich wesentlich größer ist als im Finanzbereich. Der Vorteil, Intermediäre durch die Blockchain auszuschalten, spielt beispielsweise außerhalb des Finanzbereiches eine wesentlich größere Rolle.

Fest steht aber auch, dass die Blockchain-Technologie zuerst im Finanzsystem angewendet wurde, die Technologie auf Basis dessen weiterentwickelt wurde und diese Lernfortschritte (z.B. die Vermeidung eines hohen Energieverbrauches) in anderen Anwendungsfeldern von elementarer Bedeutung sind.

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

Die BaFin hat im Bereich der Blockchain-Technologien große Kompetenzen aufgebaut, allerdings in viel zu geringer Personenzahl. Zudem fehlt ihr ein politisches Mandat und ein klarer Auftrag für den Bereich DLT, um die Verantwortung für die Aufsicht dieser Technologien zu widmen.

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

Zur Beantwortung der Frage zum Energieverbrauchs wird auf Frage 2 verwiesen.
Zur Beantwortung der Frage zum Speicherplatzbedarfs wird auf Frage 13 verwiesen.

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

Sicher birgt die Blockchain-Technologie ein enormes Potential für gesellschaftliche Veränderung. Inwiefern DLT seine positiven Effekte entfalten kann, hängt davon ab, ob Blockchains als genehmigungsbasierte („permissioned“) oder öffentliche („unpermissioned“) Blockchains gefördert und entwickelt werden. Wie in der frühen Phase des Internets waren es die offenen Strukturen – nicht die Intranets –, auf denen sich neue Systeme und Geschäftsmodelle aufbauten.