



**Deutscher Bundestag**  
Ausschuss Digitale Agenda  
  
Ausschussdrucksache  
**19(23)028**

# Stellungnahme des Blockchain Bundesverband

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

Sachverständiger: RA Florian Glatz, Präsident

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?*

Das **Blockchain-Verfahren**, welches zuerst **Bitcoin** - eine dezentrale digitale Währung - möglich machte, ist eine Technologie, deren Anwendung weit über den elektronischen Zahlungsverkehr hinausreicht. Die **Computerprotokolle**, die den dezentralen Währungsnetzwerken wie Bitcoin oder Ethereum zugrunde liegen, machen Transaktionen über beliebige Vermögenswerte möglich, erlauben es Maschinen autonom über Gelder zu verfügen und verleihen Menschen weltweit die Fähigkeit, sich verbindliche Regeln zur Zusammenarbeit zu geben – ohne Mitwirkung von Intermediären wie Juristen, Buchhaltern, Banken, Gerichten oder überhaupt einem Rechtssystem.

Die technische Basis dieser revolutionären Technologie sind **Peer-to-Peer-Netzwerke**, also Kommunikationsnetze, die Informationen nicht über eine zentrale Vermittlungsstelle (etwa eine Plattform wie Facebook oder Google) senden, sondern als „Schwarm“ Nachrichten von Nachbar zu Nachbar übertragen. Für Endnutzer stellt sich der Umgang mit der Technologie wie ein gewöhnlicher „Cloud-Service“ dar - einen Dienst, der über das Internet universell zugänglich ist. Im Hintergrund agieren aber Algorithmen (sog. **Konsensverfahren**), die eine zentrale Vermittlungsstelle als Diensteanbieter überflüssig machen.

In **öffentlichen Blockchain-Netzwerken**, die dem ganzen Internet offenstehen (wie Bitcoin und Ethereum), ermöglicht die Technologie dezentrales, anonymisiertes Interagieren. Vertrauen in Mittler, zum Beispiel in Banken, wird durch anonymisiertes Vertrauen auf technischer Basis ersetzt. Kollaborative Entscheidungsfindung in Gremien, Organisationen und Unternehmen kann auf der Blockchain abgebildet werden. Lieferketten lassen sich transparenter gestalten. Für Musik und Texte eröffnen sich neue Vertriebswege.

Die Nachteile öffentlicher Blockchain-Netzwerke liegen aus Sicht der etablierten Wirtschaft aber gerade in der radikalen Transparenz, die sie von ihren Nutzern einfordert. Deshalb formen sich um das Stichwort **“Distributed Ledger Technology”** (DLT) zunehmend Betreiberkonsortien aus Großunternehmen wie Banken und Versicherungen, die lediglich Teile der bewährten Blockchain-Protokolle nutzen. Dementsprechend verändert sich auch das **Vertrauensmodell**, auf dem eine solche Blockchain basiert. Der Anspruch einer universellen Vertrauensinfrastruktur weicht einer kleiner gefassten Automatisierungsplattform im zwischenbetrieblichen oder -behördlichen Bereich.

Statt anonymer Interaktionen, welche in dem Distributed Ledger Modell nicht vorgesehen sind, steht hier die **Standardisierung von Transaktionen** auf technischer Basis im Vordergrund. Anstelle isolierter, deal-basierter

Austauschbeziehungen könnten in Zukunft ganze Industriesektoren - möglicherweise auch Behörden und Staaten - eine Blockchain-basierte **Vertrauensinfrastruktur** in Form verschiedener Konsortien betreiben, auf welcher dann wirtschaftlicher Austausch weitgehend standardisiert und dadurch automatisiert werden kann. Die Silos existierender innerbetrieblicher Datensysteme werden aufgebrochen und in einer gemeinsam betriebenen Dateninfrastruktur vereint.

Die Wahl für eine **öffentliche oder private Blockchain** ist stets Use-Case bezogen. Für eine öffentliche Blockchain sprechen die „soziale Skalierbarkeit“, d.h. eine potenziell unbegrenzte Vielzahl von Teilnehmern kann auf transparente Art und Weise auf sicherer technischer Basis miteinander in wirtschaftlichen Austausch treten, Ressourcen teilen und sich verbindliche Regeln zur Zusammenarbeit geben. Für eine private Blockchain sprechen das gesteigerte Maß an Kontrolle darüber, wer welche Art von Tätigkeit auf der Infrastruktur ausüben darf, wer Einblick in die Daten erhält die über eine Blockchain ausgetauscht werden und ggf. auch welche rechtlichen Anforderungen über eine solche Infrastruktur überhaupt umgesetzt werden können (man denke etwa an das Recht auf Vergessenwerden aus der DSGVO).

**In Zukunft** wird es eine Vielzahl von Blockchain-Netzwerken unterschiedlichen Typs geben, die koexistieren. Dass diese wiederum nicht zu Daten-Silos werden, entsteht derzeit das sog. **Internet of Blockchains**, wo wiederum Protokolle dahinterstehen, welche Blockchainnetzwerke unterschiedlichen Typs miteinander verbinden, sodass auch zwischen Blockchain-Netzwerken Informationen und Werte sicher ausgetauscht werden können.

- 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?*

Der Blockchain Bundesverband ist technologieneutral aufgestellt und fördert grundsätzlich **alle auf Kryptografie basierenden dezentralen Technologien**, die ähnlich zur Blockchain-Technologie im Vergleich zu den heute genutzten zentralisierten IT-Diensten eine grundlegende infrastrukturelle Innovation darstellen.

Obwohl das Bitcoin Whitepaper dieses Jahr seinen zehnjährigen Geburtstag feiert, handelt es sich bei dem darin entdeckten Blockchain-Verfahren um eine unheimlich junge Technologie. Erst in den Jahren 2016 und 2017 fanden nennenswerte Investitionen in die Entwicklung innovativer Lösungen auf Basis des Blockchain-Verfahrens statt. **Mithin ist es noch zu früh einen klaren Marktführer zu identifizieren.**

Eine **stetige Marktbeobachtung** und eine **frühzeitige Auseinandersetzung** mit entstehenden Lösungen ist heute die wichtigste Aufgabe privater und staatlicher Akteure. Auch **Eigenentwicklungen** sind naheliegend, da die meisten bestehenden Blockchainprojekte auf Basis quelloffener Software arbeiten und damit Innovationen in einem Projekt schnell von anderen übernommen werden können.

Besonders erwähnenswert ist hier das Ethereum-Projekt, welches schon seit dem Jahr 2014 quelloffen entwickelt wird und eine große Community an Entwicklern um sich scharen konnte, die das heute vermutlich größte Software-Ökosystem im Blockchainbereich erschaffen haben. Viele neuere Blockchain-Projekte übernehmen Teile der Software, Konzepte (etwa Smart Contracts) und Schnittstellen (Ethereum Virtual Machine) die von Ethereum entwickelt wurden. IBM hat etwa im Jahr 2015 eigene Blockchainentwicklungen auf Basis des Ethereum Quellcodes begonnen, mittlerweile aber auf eigene Protokolle umgestellt.

Ebenfalls erwähnenswert ist das Projekt ZCash, weil es die erste öffentliche Blockchain ist, die auf einem sog. **Zero-Knowledge-Proof** Verfahren basiert. Dieses Verfahren eröffnet auch öffentlichen Blockchain-Netzwerken die Möglichkeit, Privatsphäre zu garantieren, ohne dabei die Transparenz und Nachvollziehbarkeit des Gesamtsystems zu reduzieren (im Gegensatz zu privaten Blockchain-Netzwerken, welche schlichtweg nicht öffentlich zugänglich sind).

Zusammenfassend spricht man heute von **drei Generationen** von Blockchains. Bitcoin und entsprechende Klone (etwa Litecoin) bilden die erste Generation. Smart Contract Plattformen wie Ethereum die zweite, und Systeme mit grundlegend abweichenden Datenstrukturen und Konsensverfahren wie etwa IOTA die dritte Generation.

**Layer One Skalierungslösungen** ersetzen das aus Bitcoin bekannte Proof-of-Work Konsensverfahren und ggf. auch die dahinterstehende Datenstruktur der Blockchain zugunsten effizienterer Verfahren, welche in kürzerer Zeit einen ähnlich stabilen Konsens unter den Netzwerkknoten herstellen können. Das Konsensverfahren einer Blockchain, welches einen zentralen Betreiber überflüssig macht, ist gleichzeitig ihr größter Nachteil. Denn die Konsensfindung in einem verteilten System kostet Zeit und Geld. Neuere Verfahren brechen deshalb mit dem Prinzip eines „globalen“ Konsens im Netzwerk. Ebenfalls wird das teure Verbrennen von Energie im Rahmen des Proof-of-Work-Verfahrens zunehmend durch energieneutrale Verfahren wie Proof-of-Stake und Proof-of-Authority ersetzt.

**Layer Two** Skalierungslösungen bauen auf bestehenden Blockchain-Netzwerken auf. Nicht immer lohnt es sich, vollständig neue Blockchain-Protokolle und damit letztlich auch Netzwerke zu entwickeln und aufzubauen. Gerade direkte und indirekte Netzwerkeffekte, die auch im Blockchain-Bereich Geltung haben, begünstigen Konzentrationseffekte. Die Nützlichkeit einer Blockchain beruht neben der Fähigkeit zur Programmierung und Automatisierung in der Verfügbarkeit von anderen Transaktionspartnern.

Mithin macht es Sinn, auf bestehende Blockchain-Netzwerke zusätzliche Protokolle zu bauen, die eine Skalierung des Transaktionsdurchsatzes ermöglichen, ohne dabei das ursprüngliche Netzwerk ersetzen zu müssen. Vielmehr kann die schon bestehende Nutzerbasis eines Blockchain-Netzwerks die zusätzlichen Protokolle als Skalierungslösung verwenden.

Als wichtigster Kandidat in diesem Bereich gilt die **Payment- bzw. State-Channel-Technologie**. Sie ist eine Skalierungslösung, um den Transaktionsdurchsatz gängiger Blockchain-Netzwerke zu erhöhen. In kürzeren Zeitintervallen können Transaktionen bestätigt werden. Nennenswertprojekte sind das Raiden Netzwerk und das Bitcoin Lightning Netzwerk.

- 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?*

## **Energie**

Wir erleben gerade in der energiewirtschaftlich ausgerichteten Blockchain-Szene enorme Innovationsschübe und unternehmerische Aktivität. Gerade Berlin hat derzeit den Ruf die Welthauptstadt für „Blockchain in Energy“ zu sein. Die Kerninnovationen in dem Bereich drehen sich um die Stichworte **Herkunftsnachweise, Prosumenten sowie Innovationsbilanzkreise**.

### ***Herkunftsnachweise***

Herkunftsnachweise wurden 2013 im Rahmen der Stromkennzeichnungspflicht eingeführt, um Ursprung und Echtheit von Grünstrom zu zertifizieren. Die Ziele waren einerseits der Schutz vor Falschabrechnungen gegenüber Verbrauchern, zum anderen belastbarere Daten über erzeugte erneuerbare Energien zu erhalten. Die Zertifikate werden vom Umweltbundesamt im Herkunftsnachweisregister (HKNR) erfasst und verwaltet. Es stellt die Herkunftsnachweise aus, überträgt, importiert, exportiert und entwertet sie. Dies wird den ursprünglichen Zielen der Herkunftsnachweise durchaus gerecht, nutzt aber kaum die Möglichkeiten der Digitalisierung für eine effiziente Verwaltung.

Wie fast alle Bereiche der Gesellschaft, besteht auch im Energiesektor ein enormer Bedarf zur weiteren Digitalisierung, um auf die Bedürfnisse von CO<sub>2</sub>-Reduktion und Nachhaltigkeit, staatliche Regulierungsanforderungen und kommerzielle Interessen kleiner wie großer Akteure im Energiemarkt effektiver und effizienter reagieren zu können. Damit ergeben sich neue Möglichkeiten in allen Bereichen, so z.B. für die Erfassung von Detailinformationen zum Stromfluss auch bei Kleinanlagen, eine Steigerung und Verbesserung von Prozessautomatisierung, mehr Transparenz

gegenüber Verbrauchern und Regulatoren, Kostensenkung, Abbau von Markteintrittsbarrieren und neue Möglichkeiten der Sektorenkopplung, insbesondere mit Blick auf den wachsenden Markt der Elektrofahrzeuge. Hinzu kommen neue Möglichkeiten der lokalen, kommunalen Wirtschaftsförderung, wenn detaillierte Energieerzeugungs- und Verbrauchsdaten Rückschlüsse auf die lokale bzw. regionale Bruttowertschöpfung erlauben.

Für diese Zwecke, die komplexe Prozessabläufe im Minuten- bis Sekundentakt erfordern, ist die derzeitige Verwaltung von Herkunftsnachweisen weder ausgelegt noch dauerhaft in der Lage, wodurch der Energiesektor undurchsichtig, teuer und für die meisten kleineren Teilnehmer unzugänglich bleibt – was sowohl der Energiewende als auch der Innovationsentwicklung in Deutschland im Weg steht. Denn diese analogen, weitgehend manuellen Strukturen können keine übergeordneten Funktionen unterstützen, wie beispielsweise transparente und sofortige Abrechnung nach Stromverbrauch, Stromanbieterwahl nach automatisch zertifizierten CO<sub>2</sub>-Emissionen oder die Verwendung von kleinsten Flexibilitätsmengen aus erneuerbaren Energien, um den Stromkreislauf stabil zu halten. Sehr verknappt ausgedrückt werden die derzeitigen Lösungen auf zukünftige, zunehmend komplexere Anforderungen nicht mehr reagieren können.

Hier bietet sich, mehr als jedes andere Lösungskonzept, der Einsatz von Blockchain und anderen dezentralisierten Technologien an. Die Informationen, die auf einer Blockchain gespeichert werden, und zwar Hashwerte und/oder digitale Signaturen, die Daten verifizieren, sind lückenlos und unwandelbar. Somit werden Manipulationen von Informationen zu Stromquellen oder CO<sub>2</sub>-Emissionen erschwert bis unmöglich gemacht. Über sogenannte Smart Contracts können an diese belastbaren Informationen Prozessautomatisierungen geknüpft werden, was großes Potenzial für Effizienzsteigerungen und Kosteneinsparungen in sich birgt. Zudem können aus den detaillierteren Daten und Effizienzgewinnen auch Optimierungen und Einsparungen für den Netzausbau abgeleitet werden. Darüber hinaus lassen sich, je nach Wahl der Architektur der Blockchain, sowohl komplexe Datenschutzanforderungen als auch Transparenzbedürfnisse von Zivilgesellschaft, Gesetzgebern und Regulatoren erfüllen und befriedigen.

Um den Einsatz von Blockchain-Technologie in diesem Bereich zu ermöglichen, bedarf es technologieneutraler Regulatorik sowie Zugangs- und Kooperationsmöglichkeiten innerhalb der Energiewirtschaft, die auch neuen Akteuren wie Start-Ups eine Partizipation in den bisher geschützten und oligopolistischen Bereichen der Energiewirtschaft erlaubt. Erstrebenswert sind daher beispielsweise Pilotprojekte zusammen mit dem Umweltbundesamt, um die neu eingeführten Regionalnachweise mittels Blockchain-Technologie effizienter zu erstellen und zu verwalten.

### ***Prosument***

Die zunehmend saubere, jedoch fluktuierende Energieerzeugung erfordert eine flexible Einbindung dieser dezentral erzeugten Strommengen in das Netz. Die Blockchain-Technologie kann dabei helfen, die zugehörigen Informationsflüsse sicher und kosteneffizient abzubilden und so dazu beitragen, Versorgungssicherheit und Netzstabilität in Zeiten der Energiewende zu gewährleisten. Wir sehen großes regionales Wertschöpfungspotenzial durch den sog. Blockchain-basierten Peer-to-Peer-Handel, sprich: den kleinteiligen Handel von grünem, regionalem Strom und Flexibilitäten (z.B. Speicher bzw. Verbrauchsverschiebung) zwischen sogenannten Prosumenten.

Im vergangenen Jahr wurden bereits entsprechende Pilotprojekte erfolgreich etabliert, wie z.B. Allgäuer Überlandwerke (Konsortialführer bei "Pebbles" - Plattform für Nachbarschaftsstrom und digitale Dienste), Wuppertaler Stadtwerke mit einem Pilotprodukt "Tal.Markt" in Kollaboration mit Elblox. Und obwohl das Geschäftsmodell bei Nutzern gut ankommt, haben es Start-Ups deutlich schwerer, da sie erst entsprechende Marktbarrieren zu überwinden haben.

Im Mittelpunkt dieses Geschäftsmodells steht der sog. Prosument. Der Begriff bezeichnet vor allem dezentrale Stromproduzenten, die den erzeugten Strom nicht nur selbst verbrauchen, sondern auch an Dritte (im Quartier, in der Nachbarschaft, in der Kommune oder der Region) verkaufen und damit sowohl Erzeuger („Produzent“) als auch Verbraucher („Konsument“) von Energie sind. Klassischerweise handelt es sich hierbei um Betreiber von Solaranlagen auf Wohnhäusern. Zunehmend sind auch Ressourcen wie Speicher als auch Energieeffizienzmaßnahmen des Konsumenten als Beitrag, und der aktive Verbraucher ebenfalls als Prosument zu werten. Jedoch ist ein kurzfristiger Wechsel zwischen Eigenverbrauch, Einspeisung nach EEG, Spot-Markt und Regelleistung heute regulatorisch nicht vorgesehen.

Der Prosument agiert hinter dem Zähler und damit faktisch außerhalb des energiewirtschaftlichen Systems. Aus Sicht des aktuellen Systems sind Prosumenten keine handelnden Akteure, sondern lediglich passiv. Das, was den Konsumenten zum Prosumenten macht, also die Produktion und die Vermarktung von Strom und Flexibilitäten, liegt weiterhin in der Hand von Aggregatoren wie dem Netzbetreiber oder dem Direktvermarkter. Trotz ihrer medial zentralen Stellung in der Energiewende sind Prosumenten damit im eigentlichen Marktgeschehen derzeit nicht repräsentiert.

Mit Blick auf die technologischen Möglichkeiten, die der Blockchain-basierte Peer-to-Peer-Handel solchen Prosumenten bietet und die zunehmende Dezentralisierung von Erzeugung und Vermarktung plädieren wir dafür, den Prosumenten als eigenständigen Marktakteur anzuerkennen. Der liberalisierte Energiemarkt kann es durch seine hohe Granularität und den leichten Markteintritt ermöglichen, dass jeder noch so kleine Akteur – der Handwerksbetrieb, der Solaranlagenbesitzer, die Wohnungsmieterin – sich die benötigte elektrische Energie auf den entsprechenden (dezentralen, ggf. lokalen bzw. regionalen) Märkten beschafft und/oder vermarktet.

Der Begriff des Prosumers könnte vor diesem Hintergrund deutlich erweitert werden. Es wären eben nicht mehr nur diejenigen, die auch selbst Strom produzieren, sondern all diejenigen, die aktiv am Marktgeschehen beteiligt sind, technologiegestützt darauf reagieren können und wollen. Prosumenten können sich mit den neuen technischen Möglichkeiten immer mehr vom passiven Verbraucher zu selbstbestimmten Akteuren weiterentwickeln. Um einen solch aktiven Prosumenten etablieren zu können, die einen wichtigen Beitrag zur Energiewende leistet, bedarf es aus unserer Sicht einer klaren regulatorischen Einordnung des Prosumenten, der eben nicht nur Anlagenbetreiber, Lieferant oder Letztverbraucher ist, sondern unterschiedliche Markttrollen innehat

Heute droht das Modell des Prosumenten an rechtlichen, bürokratischen und tatsächlichen Hürden zu scheitern womit dem Energiemarkt der Zukunft ein entscheidender Akteur verloren ginge. Die Schaffung einer separaten Markttrolle für den Prosumenten stünde auch im Einklang mit den Bestrebungen auf europäischer Ebene: Der EU-Entwurf der Erneuerbaren-Energien-Richtlinie (RED II) sieht eine – technologie neutrale – Legaldefinition des Peer-to-Peer-Geschäfts vor und berücksichtigt dabei insbesondere auch die unterschiedlichen Markttrollen der Teilnehmer.

### ***Der “Innovationsbilanzkreis” als flexibles, jedoch regional eingegrenztes Reallabor***

Der geltende energierechtliche Rahmen mit seinen über 10.000 Regelungen ist über die vergangenen 100 Jahre im Wechselspiel von Technologie, Wirtschaft und Markt entstanden. Er ist insbesondere ausgelegt auf den Einsatz zentraler, großer und kapitalintensiver Kraftwerke und den damit verbundenen Netzen. In ihrer Komplexität sind diese Rahmenbedingungen derzeit nur durch große Akteure beherrschbar und zementieren damit die gegenwärtigen Strukturen. Die für den weiteren Fortschritt der Energiewende wie auch für den Klimaschutz insgesamt unbedingt notwendigen Innovationen haben es in einem solchen Umfeld schwer.

Um technische Innovationen im Wechselspiel mit der Praxis entwickeln, testen und optimieren zu können, sind daher **regulatorische Freiräume** für neue Produkte aus unserer Sicht entscheidend. Das im Rahmen des SINTEG-Programms geschaffene **Reallabor** begrüßen wir ausdrücklich und ist ein Schritt in die richtige Richtung.

Die nur sehr begrenzte Anwendung der regulatorischen Ausnahmen zeigt dort aber auch, dass es nicht ausreicht, nur einzelne Details des rechtlichen Rahmens auszusetzen, um Innovationen anzureizen. Kern von Innovationsprozessen ist es ja gerade, dass am Anfang noch nicht sicher feststeht, wie sich das Zusammenspiel von Innovationen und regulatorischen Instrumenten entwickelt. Weiterhin entstehen Innovationen auch im Wechselspiel mit der Praxis. Dementsprechend lässt sich auch nicht abschließend im Voraus formulieren, welche der vielen und komplexen

Regelungen des geltenden Energierechts die Umsetzung der Innovation behindern bzw. fördern.

Wir schlagen daher konkret vor, die Idee des Reallabors zu „**Innovationsbilanzkreisen**“ weiterzuentwickeln, in denen Verbraucher, Prosumenten, Erzeuger und Lieferanten frei mit Energie handeln können. Eine institutionelle Zwischenschicht bindet die Innovationsbilanzkreise an die bestehende Energiewelt, Netze und Märkte an und sichert die Rechtskonformität nach außen. In solchen Innovationsbilanzkreisen können neue, z.B. Blockchain-basierte Geschäftsmodelle entwickelt und getestet werden, gleichzeitig erlaubt die institutionelle Zwischenschicht auch die Digitalisierung von bestehenden Prozessen, etwa die Digitalisierung des Herkunftsnachweises auf Basis der Blockchain-Technologie. Auf diese Weise werden die umfassenden Vorteile der ausgelösten Innovationen in ihrer Gesamtheit deutlich werden. Es können damit letztlich auch rechtliche Innovationen angestoßen werden, ohne dass die technisch-ökonomische Effizienz oder Stabilität des Gesamtsystems gefährdet wird. Mit der Wahl des Bilanzkreises als Organisationseinheit wird an bestehende Strukturen angeknüpft und diese erlaubt es sowohl angestammten wie neuen Akteuren, Innovationen im Wechselspiel mit der Praxis zu entwickeln und zu erproben.

### **E-Government**

Die Digitalisierung der Verwaltung gehört zu den großen Herausforderungen unserer Zeit. Gerade im öffentlichen Sektor bietet die Blockchain-Technologie viele Anwendungsmöglichkeiten. Ihr intelligenter Einsatz kann die Transparenz und Effizienz von Verwaltungsprozessen stärken.

Gesetze sind Regeln und Regeln drängen ins Digitale. Das gilt auch für die Verwaltung. Die Blockchain bietet die Möglichkeit dazu. Die Stichworte lauten: Automatisierung, Vertrauen und Ausschluß von Mittelsmännern – kurz: ein Verfahren, das den Bürgerinnen und Bürgern wieder zu ihrem „Recht“, dh zu Autonomie verhilft. Deswegen muss die Blockchain, wie im Koalitionsvertrag angedeutet, genutzt werden, um die traditionellen Qualitäten deutscher Verwaltung ins 21. Jh zu übersetzen.

Der CIO des Landes Nordrhein-Westfalen hat eine Initiative ins Leben gerufen – **Blockchain in der Verwaltung Deutschland (BiVD)** - die versucht, das Thema „Blockchain“ Verwaltungsebenen übergreifend zu betrachten und insbesondere im Hinblick auf einen Einsatz in der Verwaltung zu bewerten. Neben der CIO-Abteilung des nordrhein-Westfälischen Wirtschafts- und Digitalisierungsministeriums konnten VITAKO zusammen mit RegioIT Aachen, das Bundesamt für Migration und Flüchtlinge (BAMF) sowie der Bundesblock (Blockchain Bundesverband) als Initiativpartner gewonnen werden. Mittlerweile sind auch die Bundesdruckerei sowie NExT (Netzwerk Experten digitale Transformation der Verwaltung) eingebunden und engagiert. Weitere Teilnehmer werden in Kürze verkündet.

Der BiVD erwarten von der Technologie insbesondere folgende Vorteile:

- **Once-only-Prinzip (Bürger und Unternehmen müssen bestimmte Standardinformationen der Verwaltung nur noch einmal mitteilen)**
- **Selbstsouveräne Identität**
- **Mehr Sicherheit durch Dezentralisierung**
- **Gemeinsame Standards, behördenübergreifender und länderübergreifender Datenaustausch, auch im europäischen Kontext**

Deutschland ist im Bereich der Verwaltung (noch) weltweit führend oder wird zumindest als führend wahrgenommen. Markenkern Deutschlands war für Jahrzehnte eine moderne, regelbasierte und –gerechte sowie transparente Verwaltung. Darauf gründet der Erfolg unserer Wirtschaft, darauf gründet zu einem guten Teil auch unser Ansehen in der Welt.

Doch die Realität ist eine andere oder droht sehr schnell eine andere zu werden, wenn wir den technologischen Anschluss weiter verpassen. Der Koalitionsvertrag bietet die Chance, von einem Nachzügler wieder zu einem Vordenker und –macher zu werden. Wenn wir sein Potential energisch nutzen.

Das Potential ist riesig – für mehr Effektivität, Vereinfachung und Transparenz in Deutschland und birgt die Möglichkeit, internationale Standards zu setzen. Wir stehen vor einer grundlegenden Weichenstellung: lassen wir uns von der digitalen Entwicklung treiben oder nehmen wir sie selbst in die Hand? Als herausragende Aufgabe in offenen, und agilen Strukturen – Strukturen, die in erster Linie nicht wirtschaftliche Eigeninteressen sondern den Bürgern und dem Gemeinwohl-orientierten Rechtsrahmen dienen.

- Experimentelle Anwendungen, agile Demonstrationsprojekte und Pilotanwendungen lassen sich in Wochen entwickeln - mit politischem Willen. Sie können als parallele Lösung zum herkömmlichen Verwaltungsvorgang getestet werden, statt sich in jahrelangen Pilotversuchen zu ermüden. Große Technik-Investitionen sind hierfür nicht erforderlich. Nur beherztes Handeln.
- Das Thema „Change Management“ im öffentlichen Sektor ist ein wichtiges Thema, wenn die Blockchain-Technologie das demokratische Fundament erhalten soll, dass sie eröffnet.
- So wie bereits unsere Kommunikation in Silos und Filterblasen amerikanischer Technologieunternehmen steckt, so wie unser Wissen in wenigen Kanälen zu zentralisieren droht, so wird ein Nichthandeln der Verwaltung weitere Silos statt offener Strukturen entstehen lassen
- Wir müssen Digitalisierung gestalten. Und damit jetzt anfangen.

Je komplizierter die Regelungen des Staates sind, umso eher verlangen sie nach Digitalisierung. Sowohl die Verwaltung als auch die Normadressaten, Unternehmen und Bürger, ächzen unter der Last der Vollziehung auf der einen Seite und der

Compliance auf der anderen Seite. Eine richtig verstandene digitale Infrastruktur gibt die Möglichkeit, beiden zu helfen.

Das bedeutet, dass in einer deutschen bzw. europäischen Blockchain Services Infrastruktur, Regeln und Institutionen des Staates als „Protokoll“ etabliert werden müssen. Die Blockchain ist kein rechtsfreier Raum, sondern idealerweise läuft der staatliche Rechtsrahmen als technisches Protokoll auf der Blockchain und ermöglicht so Transaktionen eine „legal transaction finality“. Die Alternative, dass der Rechtsrahmen und die digitale Struktur der Blockchain eine mühsame Koexistenz führen und das Schicksal der Interpretation traditionellen Juristen ohne Technikverständnis oder Entwicklern ohne Rechtsverständnis überlassen wird, ist nicht erstrebenswert. Es gilt in einem Kraftakt die staatlichen Regelanforderungen auf Blockchain-Technologien rechtssicher zu implementieren.

Hierzu sollte ein in einem Pilotprojekt untersucht werden, wie eine Brücke geschlagen werden kann zwischen dem demokratisch legitimierten Institutionengefüge unseres Rechtsstaats und dem neuartigen Medium „Blockchain“. Das ehrgeizigste staatliche Pilotprojekt hat keine Chance auf Erfolg, wenn die digitale Infrastruktur, auf die es aufsetzt, keinen rechtsstaatlichen Unterbau hat. Die Regeln wie auch die Checks and Balances des Rechtsstaats müssen als konkrete digitale Infrastruktur im Alphabet des Mediums Blockchain reimplementiert werden. Hier sind Juristen aller Disziplinen gefragt, insbesondere auch Staatsrechtler und Verwaltungsrechtler.

Bei vielen Anwendungsszenarien für Blockchainlösungen in der öffentlichen Verwaltung stellt sich die Frage, auf welcher konkreten Blockchain - welchem Protokoll - denn nun etwa diverse Eigentumsverhältnisse registriert und Prozesse transparent berechnet und abgebildet werden können. Nicht in allen Fällen ist eine öffentliche Blockchain iSv. Bitcoin und Ethereum geeignet. Die Länder, der Bund und die übrigen Mitgliedsstaaten sollten deshalb eine gemeinsame Blockchaininfrastruktur für die öffentliche Verwaltung betreiben.

Die zwei zentralen Problemkomplexe die es bei der Bereitstellung einer derartigen Infrastruktur zu lösen gilt, sind einerseits das Thema Governance, sprich wie wird eine solche Infrastruktur in der Praxis bereitgestellt; wo liegt Technik-Kompetenz auf Seiten der Behörden und ggf. Bürger heute schon vor, wo muss diese durch gezielte Schulung und Ausbildung gefördert werden? Andererseits das Thema Rechtsstaatlichkeit: in welcher Form können demokratische Prinzipien wie Gewaltenteilung, Bürgerbeteiligung, Eigentumsrechte und andere grundlegende Errungenschaften moderner Demokratien in ein solches geteiltes, öffentliches Buchführungs- und Transaktionssystem einfließen?

Konkrete Anwendungsfelder und Pilotprojekte für Blockchain in oder mit Bezug zu der öffentlichen Verwaltung sind:

- Identitätsmanagement
  - o Europaweit standardisierte Identitäten

- Bürgerkonto bleibt sonst ein nutzloses Datensilo
- Registerführung, etwa
  - Führerscheinregister
  - Organspenderregister
  - Einheitliches europäisches Register für Geflüchtete
  - Handelsregister
  - Grundbuch
- Und Schaffung neuer Register
  - Register für Sicherheiten an Fahrnissen
  - Drohnenregister
- Vergabeprozesse; öffentliche Ausschreibungen
- Herkunftsnachweis für globale Handelslieferketten
- Digitale Unternehmensgründung und -leitung via Blockchain
- Digitalisierung von Unternehmensanteilen
- Digitales Gesetzesblatt (Veröffentlichungsorgan mit dezentralem Zeitstempel)
- Digitale Gesundheitsdaten
- Papierlose Buchführung in Unternehmen
- Digitales Testament
- Dezentrale Streitbeilegungsverfahren
- Sozialhilfe und andere staatliche Hilfszahlungen

### **Startup- und Mittelstandsfinanzierung**

Im Kontext der Blockchain-Technologie bieten Token-Emissionen zur Unternehmensfinanzierung ein großes Anwendungspotential. Es sind nur wenige Gesetzesanpassungen notwendig, um deutschen Unternehmen diese Art der Finanzierung zu ermöglichen. Die Möglichkeit der agilen und kostengünstigen Unternehmensfinanzierung verschafft deutschen Unternehmen einen Wettbewerbsvorteil und steigert die Attraktivität Deutschlands als Gründungsstandort, insbesondere, weil eine unmittelbare Investitionsmöglichkeit auch für Kleinanleger geschaffen wird.

In den vergangenen Jahren hat sich Deutschland, insbesondere Berlin, zu einem der attraktivsten und dynamischsten Standorte für die Ansiedlung von internationalen DLT-Startups entwickelt. Diese Entwicklung kann mit einer Regulierung der tokenbasierten Unternehmensfinanzierung weiter gefördert werden. Derzeit weichen in Berlin angesiedelte Unternehmen für Token-Emissionen insbesondere nach Malta und Lichtenstein aus, die sich bei der Token-Regulierung stark engagieren.

Neben Blockchain Startups sind auch Investmentfonds sowie der Markt für Schuldverschreibungen, Anleihen und ähnliche Kapitalmarktinstrumente geeignet für die Tokenisierung. Allein das durch Investmentfonds verwaltete Vermögen belief sich 2017 innerhalb der EU auf 15,6 Billionen Euro.

Auf Innovationen in der Unternehmensfinanzierung folgen regelmäßig Innovationen in der Realwirtschaft. Die tokenbasierte Unternehmensfinanzierung hat das Potential, eine solche Innovationskette in Gang zu setzen

### **E-Health**

Das Blockchain-Verfahren macht eine Emanzipation des Nutzers möglich. Das kann im Gesundheitssystem zu einer technologischen Privilegierung des Dateninhabers führen: Nur der Patient und der berechtigte Datennutzer haben Zugang zu den Daten.

Weiterhin ermöglicht Blockchain die Entkopplung von Service/Hardware und Daten - d.h. derjenige, der einen Service oder eine Infrastruktur anbietet, hat dadurch allein keine Kontrolle mehr über die Daten. Insbesondere bei Betrachtung der möglichen Gründe, die eine bisherige Vernetzung von Gesundheitsdaten verhindert hat, wird klar, dass Blockchain-Technologie neuen Wind in das komplizierte Multistakeholdersystem bringen kann.

Es ergeben sich weitere Anwendungen im Gesundheitssystem

- In der Gesundheitsforschung könnten durch Blockchain-basierte Verfahren neue Möglichkeiten in der Privatsphärensicherung ermöglicht werden. So können durch Blockchain-abgesicherte multiparty-computation alle Gesundheitsdaten ohne Verluste der Privatsphäre zur Versorgungsforschung verfügbar gemacht werden.
- Die Blockchain kann zur Verfolgung kritischer Produkte in der Produktionskette (Pharma, Blutersatzprodukte) sowie von Organspenden und Organtransport genutzt werden.
- Die Nachvollziehbarkeit von Leistungen und deren Abrechnung kann durch die systemimmanente Transparenz der Blockchain verbessert werden. Wir schlagen vor, den Einsatz der Blockchain zur Datenzugriffskontrolle und Vernetzung in Pilotprojekten im Gesundheitssystem zu erforschen und zu unterstützen.
  - o Die möglichen Auswirkungen der Datenautonomie auf die Patientenemanzipation soll evaluiert werden. Die rechtlichen Umgebungen für den Patientendatenschutz sollen unter den neuen Aspekten der Blockchain geprüft werden.
  - o Es sollen Anknüpfungspunkte an bisherige Lösungen (z.B. Gesundheitskarte) gesucht werden. Dies sollte in enger Kooperation mit den Interessengruppen geschehen. 2. Die Möglichkeiten im Rahmen der Gesundheitsversorgungsforschung sollen evaluiert werden. Blockchain-basierte Lösungen zur pseudonymen Verfügbarmachung von allen Gesundheitsdaten sollen erforscht werden.

- Der Einsatz in weiteren Bereichen der Gesundheitsversorgung (bspw. Pharmaproduktverfolgung, Organspende) soll evaluiert werden.
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?*

### **Positive Use Cases**

Bereits heute funktionieren Blockchain basierte Lösungen im Bereich **Supply Chain Monitoring** sehr zuverlässig und ermöglichen es anbieterunabhängig gesamte Lieferketten nachzuvollziehen.

Auch im Bereich der **Unternehmensfinanzierung** hat sich die Blockchain schon als taugliches Mittel etabliert, um weltweit Kapital von Kleinanlegern und professionellen Investoren einzusammeln. Im Bereich der **Wertpapieremissionen** geschehen derzeit erste Gehversuche. Der Vorteil der Blockchain liegt auf der Hand: anstelle einer Vielzahl von Intermediären zu involvieren welche in den Emissionsprozess eingeschaltet sind (Banken, Verwahrer, Zahlstelle), können Emittenten und Investoren direkt miteinander kontrahieren und Zahlungen abwickeln. Schon im Jahr 2017 hat die LBBW zusammen mit Daimler eine **Schuldverschreibung** digital auf der Blockchain begeben und abgewickelt.

Im Bereich der **Registerdigitalisierung** haben erste Länder schon erfolgreiche Pilotprojekte etabliert, wie etwa Schweden mit dem Grundbuch und Vergabepattformen in Ukraine und Georgien. Im Kanton Zug in der Schweiz wird blockchainbasiertes Identitätsmanagement erprobt und das Handelsregister auf einer Blockchainlösung digital verfügbar gemacht.

Im **Energiesektor** wurden bereits vergangenes Jahr erfolgreich Pilotprojekte etabliert, wie z.B. Allgäuer Überlandwerke (Konsortialführer bei "Pebbles" - Plattform für Nachbarschaftsstrom und digitale Dienste) und die Wuppertaler Stadtwerke mit einem Pilotprodukt "Tal.Markt" in Kollaboration mit Elblox.

Im **Mobilitätssektor** hat die RWE Tochter Innogy mit dem Share&Charge Projekt eine funktionierende Lösung zur Elektromobilität geschaffen, die Nutzern ermöglicht reibungslos Strom zu tanken und mit einer eigens geschaffenen Kryptowährung zu bezahlen.

### **Gefährliche Use Cases**

Gefährlich wird die Blockchain dort, wo ein unregulierter Kapitalmarkt Geldwäsche ermöglicht und Verbraucher ein übermäßiges Betrugsrisiko erwartet. Diese potentiellen Probleme wurden aber durch Banken größtenteils verhindert, indem sie

aus Risikogründen kaum Möglichkeiten eingeräumt haben, Krypto- in Fiatgelder umzutauschen. Daneben hat eine Konsolidierung der Märkte dazu geführt, dass die im Jahre 2017 bekannt gewordene Investitionsblase in eine rationalere Phase übergegangen ist, wo auch die Möglichkeiten zur Geldwäsche nicht mehr besonders ausgeprägt gegeben sind. Die Gefahr der Steuerhinterziehung ist im Rahmen der Blockchain eher gering, da jeder Übergang vom Krypto- ins Fiatsystem unwiderlegliche Spuren hinterlässt. Auch innerhalb einer Blockchain ist jede Geldbewegung sichtbar und permanent dokumentiert. Insofern reduziert das Blockchain-Verfahren in der Tendenz eher die Möglichkeit, Gelder zu verstecken.

### **Zentrale Schwächen**

- Beim Blockchain-Verfahren handelt es sich um eine „klassische“ Netzwerktechnologie. Die Technologie hat nur dann einen echten Mehrwert, wenn alle Parteien einer Transaktion und die Güter über die disponiert werden soll, auf dieser Infrastruktur verfügbar sind. Das ist streng genommen keine Schwäche, macht aber den Aufbau einer jeden blockchainbasierten Lösung zu einer Herausforderung, da das klassische „Henne Ei Problem“ gelöst werden muss.
- Die Blockchain-Technologie ist in einer naiven Implementierung schwer vereinbar mit der Datenschutzgrundverordnung, da darauf gespeicherte Daten in der Tat praktisch unlöschar sind. Mithin sind Unternehmen die auf Blockchainlösungen bauen, gehalten, sich zuvor ein Privacy-by-Design Konzept zu überlegen und auf dessen Einhaltung streng zu achten. Richtig eingesetzt, ist auch die DSGVO kein Problem für die Blockchain.
- Die Blockchain hat das Potenzial unser wirtschaftliches und gesellschaftliches Zusammenleben fundamental zu verändern, da sie einen Paradigmenwechsel einläutet. Deshalb müssen wir uns heute überlegen, wie wir die Entwicklung der digitalen Gesellschaft und des digitalen Staats gestalten wollen. Wir dürfen uns nicht länger von der Digitalisierung treiben lassen, sondern müssen sie aktiv mitgestalten. Blockchain kann entweder ein emanzipierendes Werkzeug für Deutschland, Europa und seine Bürgerinnen und Bürger werden, oder aber eine dystopische Zukunft einläuten. Es liegt an uns dies zu entscheiden und zu gestalten.

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?*

*[Grundgedanke: Die öffentliche Hand hat den Aufbau der digitalen Infrastruktur gänzlich der Privatwirtschaft überlassen, die aufgrund der systemimmanenten Monopolisierung solcher Angebote zu den heutigen Internetgiganten geführt hat. Blockchainbasierte Modelle ermöglichen die Schaffung von Nutzer-getragener, öffentlicher, digitaler Infrastruktur, die nicht einseitig von privatwirtschaftlichen Zwecken eines einzelnen, gewinnorientierten Unternehmens geprägt ist.]*

Blockchaintechnologie stellt eine infrastrukturelle Innovation dar welche es ermöglicht die bestehenden Monopolisierungs- und Zentralisierungsdynamik im Markt digitaler Angebote zu unterbinden. Durch Blockchain/DLT basierte Lösungen lassen sich in vielen Bereichen wieder **innovationsförderliche Wettbewerbsbedingungen** aufbauen. Anstatt wie heute Daten in abgeschlossenen Systemen (zumeist auf geschlossenen Plattformen) vorzuhalten ermöglicht die Blockchain Technologie eine geteilte Speicherung dieser Daten und somit die Entstehung offener Plattformen. Solche offenen Plattformen sind nicht auf Basis Ihrer Datenschätze erfolgreich, sondern aufgrund ihres innovativen Angebots auf Basis geteilter Daten.

Gerade in **datengetriebenen Märkten** ist es wichtig, dass wieder Wettbewerb *im* Markt und nicht *um* den Markt entsteht. Anstelle einer rein rechtlich vorgeschriebenen *Datenalmende* bzw. *Data Sharing Policy* können mit einer Blockchain schon technisch die Probleme von Datenmonopolen gelöst werden und zugleich der technische Standard festgelegt werden, wie Mitbewerber Daten austauschen.

Die Plattformökonomie, welche das Web 2.0 hervorgebracht hat, stellt den Staat vor Herausforderungen, die mit den Mitteln des Rechts allein nur schwer zu lösen sind. Die Blockchain eröffnet erstmals seit der Erfindung des Webs eine neue Vision, wie **Plattformen in Zukunft nutzerzentrierter und partizipativer ausgestaltet werden** können. Im Wege des *more technological approach* ist zu fragen, welche Herausforderungen der digitalen Transformation unserer Gesellschaft im Wege eines technologiebasierten Ansatzes mithilfe der Blockchain effizienter und langfristiger gelöst werden können.

Der **more technological approach** fragt, ob das gesellschaftspolitische Ziel, etwa die Steigerung der Konsumentenwohlfahrt, durch eine Regulierung mit den klassischen Mitteln des Rechts (Gesetze und Steuern) effektiv möglich ist. Falls etwa die ökonomischen Kosten den Nutzen übersteigen, oder wenn eine Handhabe mit den Mitteln des Rechts gar nicht greifbar erscheint, kann ein technologiebasierter Regulierungsansatz die Werkzeuge des Rechtsstaats sinnvoll ergänzen. Wie eine technologiebasierte Umsetzung ordnungspolitischer Ziele aussehen kann, demonstriert derzeit die Blockchain. Anstatt einen abstrakten Regelkatalogs mit einem separaten Zwangsvollstreckungsapparat zu paaren, wie es der Rechtsstaat

hervorgebracht hat, werden Protokolle, Vereinbarungen und Leistungsaustausch in einer homogenen, vernetzten Infrastruktur vereint.

Im World Wide Web findet die Wertschöpfung auf dem **Application Layer** statt. Nur dort können die wirtschaftlich wertvollen Daten wie beispielsweise Nutzerprofile durch den jeweiligen Diensteanbieter gespeichert, abgerufen und damit monetarisiert werden – sei es durch Werbung oder gegen Bezahlung. Auf der Blockchain hingegen wandert ein Großteil der Wertschöpfung auf die Ebene der Protokolle ab. Dadurch können Daten wie Nutzerprofile, Reputation im Netzwerk sowie andere kritische Daten auf der dezentralen, geteilten Blockchain-Datenbank persistent gespeichert werden. Diese Daten sind grundsätzlich für alle Teilnehmer im Netzwerk verfügbar. Wer mit den Daten interagieren möchte, muss über die netzwerkeigene Kryptowährung verfügen. Dadurch wird Wertschöpfung schon auf Protokollebene möglich. Der wirtschaftliche Wert eines Netzwerks kann in Form der Kryptowährungen direkter abgebildet, eingefangen und fairer verteilt werden.

Auch aus Sicht der Nutzer ergeben sich viele Vorteile. Anstatt in den **Datensilos** eines Diensteanbieters auf dem Application Layer gefangen zu sein, liegen ihre Nutzerdaten auf einer offenen Dateninfrastruktur. Dadurch reduziert sich der Möglichkeitsraum für Diensteanbieter, technische Lock-In-Effekte auf Anwendungsebene zu erzeugen um damit den Wechsel zu Mitbewerbern zu erschweren. Mehr Wettbewerb bedeutet für den Verbraucher mehr Auswahl und niedrigere Preise. Ebenfalls ist eine Partizipation der Nutzer am Erfolg der Dienste auf einfache Weise möglich. Das Token, das den Wert des Netzwerks repräsentiert, steigt im Wert, je erfolgreicher das Netzwerk wird. Nutzer können gemäß dem Protokoll durch das Beisteuern von Daten und Arbeit in Form solcher Token belohnt werden. Ebenfalls können insbesondere die frühen Nutzer selbst in die Token investieren und damit vom langfristigen Erfolg profitieren.

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

Damit DLTs/Blockchain Intermediäre ersetzen können ist häufig eine entsprechende Regulierung notwendig, da das Gesetz heute häufig die Existenz von Intermediären festschreibt. So etwa im

- Identitätsmanagement (eIDAS-Verordnung erfordert Vertrauensintermediäre)
- Datenschutz (DSGVO erfordert Verarbeiter und Verantwortliche)
- Telemedien (TMG erfordert Diensteanbieter)
- Kapitalmarktrecht

Eine Dezentralisierung mittels Blockchain und der ersatzlose Wegfall von Intermediären ist heute zwar technisch schon häufig möglich, aus regulatorischen

Gründen können dadurch aber keine Kostenersparnisse an die Kunden und Verbraucher weitergeleitet werden, weil einerseits durch Rechtsunsicherheit andererseits durch die rechtlich erzwungene Aufrechterhaltung von Intermediären noch hohe Kosten entstehen.

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

Alle relevanten Projekte im Bereich der Blockchain-Entwicklung basieren auf quelloffener Software. Mithin werden neue Entscheidungsstrukturen um die Weiterentwicklung dieser Plattformen möglich. Im Bereich der Bitcoin Blockchain und der Ethereum Blockchain haben sich sogenannte Improvement Proposals etabliert, wo jede/r neue Vorschläge zur Weiterentwicklung einbringen kann und diese dann offen diskutiert werden.

Innovative Projekte wie die Tezos Blockchain und das EOS Projekt ermöglichen ihren Nutzern aktiv mit der Benutzung des Systems darüber abzustimmen, wie das zugrundeliegende Protokoll fortentwickelt werden soll (sog. on chain governance).

*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?*

Grundsätzlich stehen den Nutzern einer Blockchain die gewöhnlichen Mittel des Rechts offen, wenn etwa trotz fehlenden rechtlichen Grunds an eine Person geleistet wurde. Im Gegensatz zu herkömmlichen Zahlungssystemen, erlaubt eine Blockchain keine Rückabwicklung einer einmal bestätigten Transaktion. Mithin besteht die heute im Internet gängige Variante der Rückerstattung über Anbieter wie Paypal gerade nicht. Jedoch ergeben sich hierdurch auch enorme Kosteneinsparungen. Seit der Entwicklung von Smart Contract Plattformen wie der Ethereum Blockchain, ist die Unwiderruflichkeit von Transaktionen losgelöst von der darüber liegenden Logik einer Anwendung: d.h. auf Ethereum könnte eine Zahlung rückabgewickelt werden, wenn es die Entwickler des darauf basierenden Zahlungssystem so vorgesehen haben.

Das größte Problem einer Rechtsverfolgung in einem dezentralen peer-to-peer System ist die Identifikation der Parteien. Praktisch ist aber davon auszugehen, dass in einer massentauglichen Applikation der Blockchain eine Identifizierung der Teilnehmer sichergestellt sein würde.

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

Datenschutz ist im Kontext einer öffentlichen Blockchain durch eine Kombination von unterschiedlichen Technologien und einem bewussten, datensparsamen Einsatz der Blockchain möglich.

Heute ist es gängig, auf einer öffentlichen Blockchain lediglich die Quersumme (Hash) der eigentlichen Informationen zu speichern. Die Quell-Informationen (etwa persönliche Daten) werden in einem dezentralen Datenspeicher verschlüsselt gespeichert. Somit bleiben die Daten auf der Blockchain anonym. Jedoch kann stets der Nachweis erbracht werden, dass die Quelldaten nicht nachträglich verändert wurden (Echtheit).

In Zukunft werden durch neuere Verschlüsselungsformen auch weitere Use Cases möglich, wo dann mehr als nur Quersummen auf einer öffentlichen Blockchain hinterlegt werden können, ohne dabei das Recht auf Privatsphäre einzelner Teilnehmer zu gefährden.

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

Konfliktlösungsmechanismen sind der Blockchain nicht fremd. Schon die Bitcoin Blockchain, die älteste und damit technisch „unterentwickelste“ Blockchain (im Vergleich zu komplexeren Blockchainsystemen wie etwa Ethereum) kann das Prinzip eines Schiedsrichters in Zahlungsabwicklungen integrieren, womit auch Leistungsstörungen, Anfechtungen und Vertragsrückabwicklungen adäquat abgebildet werden können. Bei Bitcoin erfolgt dies mittels sog. 2-von-3 Multisignatur Adressen, wo ein Schlüssel von einem unabhängigen Dritten gehalten wird, welcher im Konfliktfall darüber entscheiden kann, an welche Partei eine Zahlung fließen soll. Ethereum kann wiederum noch deutlich komplexere Entscheidungsstrukturen abbilden. Es ist denkbar, das Leistungsstörungsrecht des BGB mittels Smart Contracts auf Ethereum abzubilden. Alles was automatisierbar ist, kann mittels einer Smart Contract Plattform wie Ethereum automatisiert werden. Wo menschliche Werturteile notwendig sind, können diese transparent in einen Prozess eingefügt werden.

Dem benannten unabhängigen Dritten (Schiedsrichter) muss dank der Treuhandfunktion einer Blockchain kein gesteigertes Maß an Vertrauen entgegengebracht werden. Nur mit Zustimmung mindestens einer Partei kann dieser über die zur Disposition gestellten Gelder verfügen.

11. *Wie kann sichergestellt werden, dass beim Einsatz von Blockchaintechnologien 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).*

Grundsätzlich sollte in öffentlich-genehmigungsfreien Blockchains ausgeschlossen werden, dass die Betreiber von Nodes für eine solche Speicherung haftbar gemacht werden. Sonst würden wir in Deutschland ähnlich wie bei der WLAN-Betreiberhaftung viele Jahre beim Aufbau essentieller Infrastruktur verlieren.

Eine Beantwortung der Frage ist letztlich nur im Kontext des jeweiligen Anwendungsfalls möglich. Im Fall der Blockchain basierten Identität (Self-sovereign Identity) muss zum Beispiel zwischen der Speicherung von persönlichen Daten (im Sinne von Attributen: Name, Adresse, Telefonnummer) und „Identifizieren“ (nicht personalisierte Hashwerte) unterschieden werden. Während persönliche Daten auf keinen Fall in der Blockchain gespeichert werden sollten, besteht bei Identifizieren eine Notwendigkeit diese öffentlich in der Blockchain zu referenzieren um damit die anbieterunabhängige dezentrale Identität erst möglich zu machen. Der Identifier selbst enthält jedoch keine weiteren Informationen über die Identität der Person.

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 Blockchain-Verfahren umgeht nicht das Trennungs- und Abstraktionsprinzip.

**Siehe hierzu auch die Antwort auf Frage 10.**

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?*

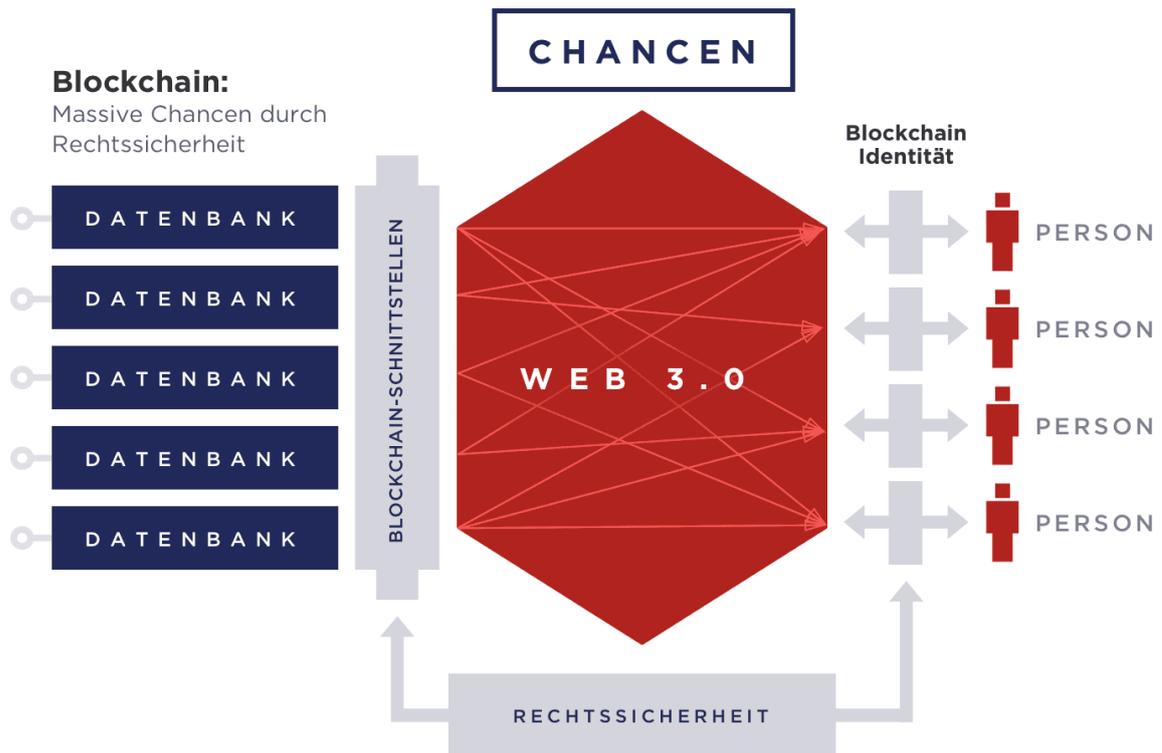
Grundsätzlich sinken die Kosten der Speicherung großer Datenmengen deutlich schneller als das Wachstum einzelner Blockchain Datenbanken. Für Nodes mit begrenztem Speicherplatz gibt es bereits Lösungen (sog. „pruning“) wo lediglich Teile einer Blockchain lokal gespeichert werden. Letztlich werden sich die einzelnen

Nodes in den Blockchain-Netzwerken ausdifferenzieren nach unterschiedlichen Aufgaben. Storage-Nodes, welche die komplette Blockchain speichern, werden dafür bezahlt, von denjenigen, die lediglich Teile der Blockchain vorhalten um Speicherplatz zu sparen. Dank kryptographischer Verfahren kann dennoch das Vertrauensmodell (trustless trust) aufrecht erhalten werden.

*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?*

Gemäß dem „more technological approach“ (siehe die Antwort auf Frage 5) ist hier ein moderner Regulierungsansatz zu wählen, um den Spagat zwischen Innovationsförderung und Rechtsstaatlichkeit zu meistern. Die Aufgabe des Regulators ist es nicht, Konzepte aus der analogen Welt 1:1 auf die Blockchain zu übertragen, sondern stattdessen Wege zu finden, eine dem Medium Blockchain angemessene Lösung zu finden.

Konkret bedeutet dies, dass es Aufgabe des Staates ist, die regulatorische Grundlagen für rechtssichere Identitäten auf einer Blockchain zu legen (insb. Anpassung der eIDAS Verordnung bzw. deren Umsetzung davon auf nationaler Ebene) sowie sichere, digitale Schnittstellen zu den staatlich verwalteten bzw. regulierten Registern zur Verfügung zu stellen (bspw. Handelsregister, Grundbuch, Aktienbücher, u.v.m.). Dadurch folgt dann ganz von allein die Umsetzung der gewünschten gesellschaftspolitischen Zielvorstellungen. Gleichzeitig entsteht eine Basis für innovationsgetriebenen Wettbewerb auf deutschem bzw. europäischem Boden.



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?

- Notwendig ist die europaweite Vereinheitlichung der Token-Klassifizierung, In Deutschland herrscht die Dreiteilung von Wertpapieren, Kryptowährungen als KWG-Finanzinstrumenten (Rechnungseinheiten) und Utility Token (realwirtschaftnahe Produkte laut BaFin, also Gutscheine/Club-Modelle). EU-weit gibt es nur eine Zweiteilung: Wertpapiere und (nicht beaufsichtigter) sonstige Token.
- Die Einordnung von Kryptowährungs-Token als Rechnungseinheiten sollte aufgegeben werden, da die damit einhergehende Einstufung als Finanzinstrumente der europarechtlichen Definition von Finanzinstrumenten widerspricht und damit zu etlichen Wertungswidersprüchen führt. Die durch die Qualifikation als Rechnungseinheit erreichte Erlaubnispflicht für Dienstleister greift nur isoliert für Deutschland, wodurch eine Ansiedlung von Krypto-Dienstleistern in Deutschland erschwert wird und der Wirtschaftsstandort Deutschland einseitig benachteiligt wird. Die deutsche Sonderklasse der

Rechnungseinheiten (=Kryptowährungen) ist eher zufällig historisch entstanden durch eine extensive Auslegung der BaFin. Sie ist rechtlich umstritten (s. Berliner Bitcoin Urteil, in dem das Kammergericht der BaFin eine grundgesetzwidrige Überschreitung ihrer Kompetenzen als Exekutive vorwirft) und auch konzeptionell fragwürdig. Die regulatorische Behandlung der Nicht-Wertpapier Token sollte grundsätzlich neu überdacht werden: Token, die ausgegeben werden, um auf non-profit Basis eine freie, öffentliche Infrastruktur zu etablieren, sollten begünstigt werden. Sie erfüllen den wünschenswerten gesamtgesellschaftlichen Zweck der Schaffung von nicht profit-orientierten, öffentlich zugänglichen Plattformen, die eigentlich die öffentliche Hand zur Verfügung stellen müsste. Die öffentliche Hand hat den Aufbau der digitalen Infrastruktur gänzlich der Privatwirtschaft überlassen, die aufgrund der systemimmanenten Monopolisierung solcher Angebote zu den heutigen Internetgiganten geführt hat. Die Förderung von gemeinnützigen (oder aktuell mangels passender Gemeinnützigkeits-Kategorie nur gemeinwohlnaher) Plattformen wäre daher das Mindeste, was ein Staat dieser ungesunden Entwicklung entgegen setzen könnte.

In diesem Zusammenhang fordern wir die Einführung einer entsprechenden, steuerlich anerkannten Gemeinnützigkeits-Kategorie.

- Wir empfehlen ebenfalls die Einführung von Regeln zur Sicherstellung von transparenten und fairen Märkten für alle Arten von Token, auch der Utility Token, auf europäischer Ebene. Aus unserer Sicht sind die Service Provider (die über die Rechnungseinheiten-Argumentation reguliert werden) nicht die Ursache für die hohe Volatilität auf den Krypto-Märkten und die damit einhergehenden Verluste der Nutzer. Das Problem entsteht durch die massiven Insider Tradings und Schneeballsysteme in diesem Markt, der nur mit einer vernünftigen Regelung von Insider Tradings (Secondary Market) über alle liquiden Token Klassen hinweg begegnet werden kann – also insbesondere durch strafbewehrte Offenlegungspflichten für Halter von Token. Gängige Praxis ist es, gering bewertete Token anzukaufen, anschließend in diversen Social Media Channels den Wert von Token pushen, um die eigenen Bestände anschließend gewinnbringend zu veräußern und die Kurse abstürzen zu lassen. Diesen missbräuchlichen Praktiken muss effektiv begegnet werden.
- Hiermit einhergehen sollte eine Regulierungsrahmen für Krypto-Börsen, die den Handel aller nicht-Wertpapier Token (sowohl von Kryptowährungs-Token sowie von Utility Token) regelt. Dabei sollte insbesondere der jungen Technologie und den daraus entstehenden Möglichkeiten aber auch den Risiken Rechnung getragen werden. Eine Ausdehnung der existierenden Regeln für MTFs auf Kryptowährungs-Token (wie in Deutschland durch ihre Erfassung als

Rechnungseinheiten) sowie auf (die u.E. nicht erfassten) Utility Token halten wir aufgrund der hohen Infrastrukturanforderungen für nicht geeignet für Krypto-Börsen.

- Entmaterialisierung der deutschen Wertpapiere und Herauslösung dieser tokenisierten Wertpapiere aus dem Zentralverwahrsystem. Siehe hierzu auch Antwort auf Frage 24.
- Der französische Vorschlag der Schaffung der Möglichkeit des Opt-in für Nicht-Wertpapier Token (also für Kryptowährungs-Token sowie Utility Token) für einen freiwilligen, von der Aufsicht zu billigenden Prospekt, für den dann die gesetzliche Prospekthaftung statt des deutlich weitreichenderen zivilrechtlichen Haftungsregimes (sogenannte enge Prospekthaftung) greift. Hierdurch würde einen Anreiz geschaffen, die mit einem Prospekt einhergehende Transparenz tatsächlich zu nutzen.
- Wir halten die Schaffung eines eigenen Anhangs für Wertpapier-Token-Verkäufe im Rahmen der EU-ProspektVO für dringend erforderlich. Daran angelehnt sollten deutsche Annexe für Nicht-Wertpapier Token bei Einführung der oben angeregten Opt-in Möglichkeit eingeführt werden (bis sich das Konzept auf EU-Ebene durchgesetzt hat, idealerweise in Abstimmung mit Frankreich und bei gegenseitiger Anerkennung solcher freiwilliger Prospekte).
- Schaffung eines zentralen Ansprechpartners zur Koordinierung der zuständigen öffentlichen Stellen für Fragen der Kryptoökonomie (Steuern, Verbraucherschutz, Aufsicht), der Widersprüche beseitigt und für eine konsistente Linie über alle Bereiche hinweg sorgt. Dies gilt auf EU-Ebene wie auch auf nationaler Ebene.
- Deutliche Aufstockung des Personals bei der BaFin für Anfragen aus dem Kryptobereich, um die Bearbeitungszeiten deutlich zu verkürzen. Nach unserer Kenntnis sind für diesen Bereich bislang keine neuen Stellen geschaffen worden, trotz der massiven Häufung von Anfragen und zusätzlicher Belastung durch erforderliche Zuarbeit zu nationalen wie internationalen Gremien sowie dem beaufsichtigenden Bundesministerium der Finanzen. Um mit dem technologischen Fortschritt mithalten zu können, ist eine deutliche Aufstockung der Kapazitäten erforderlich.

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

Die Europäische Blockchainpartnerschaft hat sich im Lauf der letzten Monate zu einem konstruktiven Arbeitsrahmen inter-europäischer Zusammenarbeit entwickelt. Der Aufbau einer Europäischen Blockchaininfrastruktur war als Ziel zwar sehr ambitioniert angesetzt, trägt aber im Anwendungsbereich der Digitalen Identität bereits erste Früchte. Das Bündnis BiVD (Blockchain in der Verwaltung Deutschland) hat sich hier strategisch positioniert und arbeitet gemeinsam mit Belgien und den Niederlanden daran Gruppe von Mitgliedsländern für die Arbeit im Projekt eSSIF (European Self-Sovereign Identity Framework) zu gewinnen. Ziel dieses Frameworks ist es die aufstrebende Technologie (Self-Sovereign Identity) in Europa so zu ermöglichen, so dass langfristig ein innovativer und vor allem offener Wettbewerb am Identitätsmarkt entsteht. Die Einhaltung von Rechtsvorgaben (eIDAS, DSGVO, PSD2, etc.) wird dabei vorausgesetzt und soll durch das eSSIF unterstützt werden. Zudem verfolgt die Initiative das Ziel Datensouveränität zu ermöglichen und Datenmärkte zu erschließen.

*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?*

Ganz im Sinne der neueren auch und vor allem europäischen Regelungen ist Privatsphäre ein grundsätzlich schützenswertes Gut (DSGVO).

Steuererhebung ist ein Thema, das sich in Zukunft mit Sicherheit wandeln muss und auch wandeln wird, denn die Digitalisierung ist nicht aufzuhalten. Selbst man einzelne BC/DLT Projekte zensieren könnte, sind die Ideen in der Welt. Es gilt also für Nationalstaaten neue Möglichkeiten zu finden. Wenn nach einer Quantifizierung gefragt ist, dann lässt sich das mangels Vergleichbarkeit nur schwerlich konkret beantworten.

Denkt man eine Finanztransaktionssteuer, so gab es wohl historisch gesehen nie eine bessere Opportunität diese einzuführen als mit der Umstellung auf BC/DLT.

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

Vor allem die Bürger selbst. Das Blockchain-Verfahren ermöglicht erstmals eine partizipative Systemarchitektur der kritischen Infrastruktur eines Staates. Diese Chance sollte angesichts zunehmender Politikverdrossenheit und Wandlung von Bürgern zu „Nutzern“ in einer sich schnell digitalisierenden Welt mutig ergriffen werden.

Unterstützend sollten dann auch Behörden, zivilgesellschaftliche Organisationen und private Unternehmen die Infrastrukturen mitbetreiben. Allerdings ohne darin notwendigerweise eine gehobene Position einzunehmen.

Soweit es um konsortial betriebene Blockchain-Infrastrukturen geht (private Blockchains), ist es auch hier wichtig die Bürger miteinzubinden. Der Zugewinn an Transparenz und Eigenverantwortung ist ein notwendiger Schritt hin zu mehr Demokratie. Ebenfalls ist die Technologie hervorragend dafür geeignet, den in Deutschland gelebten Föderalismus zu stärken. Anstatt auf Bundesebene zentralisierte Datenbasen zu schaffen, können auch die Länder stärker zum Betrieb einer deutschen bzw. europäischen Blockchaininfrastruktur beitragen.

*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?*

**Ausführlich siehe Antwort auf Frage 3.**

**Zusammengefasst:**

- **Once-only-Prinzip (Bürger und Unternehmen müssen bestimmte Standardinformationen der Verwaltung nur noch einmal mitteilen)**
- **Selbstsouveräne Identität**
- **Mehr Sicherheit durch Dezentralisierung**
- **Gemeinsame Standards, behördenübergreifender und länderübergreifender Datenaustausch, auch im europäischen Kontext**

**Nicht abschließende Auswahl an Use Cases:**

- Identitätsmanagement
  - o Europaweit standardisierte Identitäten
  - o Bürgerkonto bleibt sonst ein nutzloses Datensilo
- Registerführung, etwa
  - o Führerscheinregister
  - o Organspenderregister
  - o Einheitliches europäisches Register für Geflüchtete

- Handelsregister
- Grundbuch
- Und Schaffung neuer Register
  - Register für Sicherheiten an Fahrnissen
  - Drohnenregister
- Vergabeprozesse; öffentliche Ausschreibungen
- Herkunftsnachweis für globale Handelslieferketten
- Digitale Unternehmensgründung und -leitung via Blockchain
- Digitalisierung von Unternehmensanteilen
- Digitales Gesetzesblatt (Veröffentlichungsorgan mit dezentralem Zeitstempel)
- Digitale Gesundheitsdaten
- Papierlose Buchführung in Unternehmen
- Digitales Testament
- Dezentrale Streitbeilegungsverfahren
- Sozialhilfe und andere staatliche Hilfszahlungen

#### **Kernkompetenzen:**

Das Potential ist riesig – für mehr Effektivität, Vereinfachung und Transparenz in Deutschland und birgt die Möglichkeit, internationale Standards zu setzen. Wir stehen vor einer grundlegenden Weichenstellung: lassen wir uns von der digitalen Entwicklung treiben oder nehmen wir sie selbst in die Hand? Als herausragende Aufgabe in offenen und agilen:

- Experimentelle Anwendungen, agile Demonstrationsprojekte und Pilotanwendungen lassen sich in Wochen entwickeln - mit politischem Willen. Sie können als parallele Lösung zum herkömmlichen Verwaltungsvorgang getestet werden, statt sich in jahrelangen Pilotversuchen zu ermüden. Große Technik-Investitionen sind hierfür nicht erforderlich. Nur beherztes Handeln. Das Thema „Change Management“ im öffentlichen Sektor ist ein wichtiges Thema, wenn die Blockchain-Technologie das demokratische Fundament erhalten soll, dass sie eröffnet.
- So wie bereits unsere Kommunikation in Silos und Filterblasen amerikanischer Technologieunternehmen steckt, so wie unser Wissen in wenigen Kanälen zu zentralisieren droht, so wird ein Nichthandeln der Verwaltung weitere Silos statt offener Strukturen entstehen lassen
- Wir müssen Digitalisierung gestalten. Und damit jetzt anfangen.

*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?*

Gesetze sind Regeln und Regeln drängen ins Digitale. Das gilt auch für die Verwaltung. Die Blockchain bietet die Möglichkeit dazu. Die Stichworte lauten: Automatisierung, Vertrauen und Ausschluß von Mittelsmännern – kurz: ein Verfahren, das den Bürgerinnen und Bürgern wieder zu ihrem „Recht“, dh zu Autonomie verhilft.

Je komplizierter die Regelungen des Staates sind, umso eher verlangen sie nach Digitalisierung. Sowohl die Verwaltung als auch die Normadressaten, Unternehmen und Bürger, ächzen unter der Last der Vollziehung auf der einen Seite und der Compliance auf der anderen Seite. Eine richtig verstandene digitale Infrastruktur gibt die Möglichkeit, beiden zu helfen. Häufig wird sich das Recht, einmal in digitale Strukturen übersetzt, einbetten lassen.

Es entsteht Embedded Law: Recht vollzieht sich in jeder Transaktion mit und ist gleichzeitig jederzeit transparent und nachvollziehbar. Das ist die große Chance, nicht in der Bürokratie zu ersticken.

Das bedeutet, dass in einer europäischen Blockchain Services Infrastruktur Regeln und Institutionen des Staates als „Protokoll“ etabliert werden müssen. Die Blockchain ist kein rechtsfreier Raum, sondern idealerweise läuft der staatliche Rechtsrahmen als technisches Protokoll auf der Blockchain und ermöglicht so Transaktionen eine „legal transaction finality“. Die Alternative, dass der Rechtsrahmen und die digitale Struktur der Blockchain eine mühsame Koexistenz führen und das Schicksal der Interpretation traditionellen Juristen ohne Technikverständnis oder Entwicklern ohne Rechtsverständnis überlassen wird, ist nicht erstrebenswert. Es gilt in einem Kraftakt die staatlichen Regelanforderungen auf Blockchain-Technologien rechtssicher zu implementieren.

Hierzu sollte ein in einem Pilotprojekt untersucht werden, wie eine Brücke geschlagen werden kann zwischen dem demokratisch legitimierten Institutionengefüge unseres Rechtsstaats und dem neuartigen Medium „Blockchain“. Das ehrgeizigste staatliche Pilotprojekt hat keine Chance auf Erfolg, wenn die digitale Infrastruktur, auf die es aufsetzt, keinen rechtsstaatlichen Unterbau hat. Die Regeln wie auch die Checks and Balances des Rechtsstaats müssen als konkrete digitale Infrastruktur im Alphabet des Mediums Blockchain reimplementiert werden.

Zum einen muss zwischen Wet Code, also dem Recht, und Dry Code, dem digitalen Code, eine Brücke ermöglicht werden. Juristen, Programmierer und Prozessverantwortliche brauchen eine gemeinsame Verständigungsmöglichkeit. Hier bietet sich als visuelle Möglichkeit die bereits im Bundesministerium für Justiz bei der Reform des Versorgungsausgleichs und anderen Gesetzen etablierten Methode des Rulemappings an. Existiert eine einfache visuelle Repräsentation von Regelstrukturen, die es den Experten aus unterschiedlichen Hintergründen ermöglicht, eine gemeinsame Verständnisebene zu finden, wird eine kontinuierliche interdisziplinäre Zusammenführung von Wissen, Ideen und Evaluation möglich: Recht und Prozesse werden durch eine intelligente Visualisierung durchsichtig. Ist

eine Verständigung über Inhalt und Prozess hier einmal herbeigeführt, haben sich unterwegs überflüssige Regeln und Komplexität in der gemeinsamen Sicht verabschiedet. Das entstandene, möglichst vereinfachte Bedingungsgefüge lässt sich mit den richtigen Werkzeugen in Computer Code übersetzen. Gleichzeitig ermöglicht die visuelle Repräsentation jedoch Laien zu jedem Zeitpunkt nachzuvollziehen, welche Regeln im Computer Code implementiert sind.

Auf dieser Basis ist die Standardisierung auf hohem Niveau (Industrialisierung) von jeder Form von Verwaltung / Textproduktion möglich. Das heißt nicht, dass sich alles automatisieren lässt. Dort, wo es notwendig ist, bleibt der Raum für individuelle Entscheidungen. Bürokratische Monster, wie etwa das Asylbewerberleistungsgesetz lassen sich jedoch zum größten Teil industrialisieren.

*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?*

Es ist davon auszugehen, dass die praktische Implementierung von Quantenalgorithmen etwa zur effizienten Faktorisierung von Primzahlen wie sie in der asymmetrischen Verschlüsselung verwendet werden noch einige Jahre dauern wird. Bis heute sind große ungelöste Probleme gegeben. Sobald sich hier eine Entwicklung abzeichnen sollte, die darauf hinweist, dann in den nächsten zwei Jahren eine Lösung ersichtlich ist, können bestehende Blockchain-Systeme auf neuere Verschlüsselungsalgorithmen umgestellt werden. Im Übrigen wären auch klassisch betriebene Systeme, wie etwa das heutige Online Banking, heute nicht sicher vor derartigen Attacken. Die asymmetrische Verschlüsselung auf Basis gängiger Verfahren wie auch im Bereich der Blockchain verwendet ist Grundlage der Sicherheit des gesamten Internets, nicht lediglich der Blockchain.

Darüber hinaus gibt es viele denkbare Angriffsvektoren auf eine Blockchain. Im Gegensatz zu klassisch betriebenen Systemen sind diese Angriffsvektoren allerdings sehr klar definierbar und werden im Moment einer Attacke transparent. Ebenfalls gibt es schon heute einen großen Anreiz derartige Attacken durchzuführen, da potenziell hohe Summen als Belohnung auf einen Angreifer warten. Das Ausbleiben derartigen Attacken etwa auf Bitcoin oder Ethereum belegt, dass diese de facto nicht existieren bzw. praktisch umsetzbar sind.

Grundsätzlich sind Blockchain-Systeme sehr widerstandsfähig, aufgrund der hohen Redundanz der gespeicherten Daten.

*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?*

S.o. Frage 15 zu den notwendigen Maßnahmen im regulatorischen Bereich. Deutschland hat bislang aktiv noch keine Maßnahmen zur Förderung ergriffen und so besteht dringend Aufholbedarf.

Eines der großen Probleme weltweit, damit auch in Deutschland, ist die Unsicherheit bei der Rechnungslegung und Besteuerung von digitalen Werten (Crypto Assets). Deutschland könnte eine Vorreiterrolle übernehmen und diese Unsicherheiten mit einer eindeutigen Klassifizierung dieser digitalen Werte unter Anwendung der gegebenen handelsrechtlichen und steuerrechtlichen Bilanzierungs- und Bewertungsmaßstäbe adressieren. Ausgangspunkt einer solchen Klassifizierung könnte und müsste eine "Substance over Form" Betrachtungsweise sowie eine Orientierung am True and Fair View Grundsatz sein. Eine eindeutige und klare Lösung der Erfassungsproblematik digitaler Werte sowohl für bilanzielle als auch steuerrechtliche Fragestellungen behindert momentan viele institutionelle Anleger bei Investitionsentscheidungen aber auch Unternehmen und Privatanleger. Die momentane Situation, dass von den Finanzverwaltungen keine verbindlichen Aussagen zu vielen offenen Fragestellungen (handels- und steuerrechtliche Einordnung der digitalen Werte) getroffen werden (Beispiel: steuerliche Erfassung von Mitarbeiterprogrammen,..) ist unhaltbar. Diese Vorreiterrolle Deutschlands müsste dazu genutzt werden um die entwickelten Ansätze in der handelsrechtlichen und steuerrechtlichen Erfassung der digitalen Werte auf europäischer Ebene voranzutreiben.

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

Folgende rechtliche Hürden müssen abgebaut werden, damit Deutschland eine führende Rolle im neuen, dezentralen Internet einnehmen kann. **Siehe hierzu auch Antwort auf Frage 15.**

### **Formvorschriften**

Wann immer Formerfordernisse in der deutschen und europäischen Gesetzgebung, wie z.B. im Verbraucherschutzrecht oder im Gesellschaftsrecht, festgelegt sind, müssen diese Anforderungen geprüft werden, ob sie eine Blockchain-Anwendung daran hindern, den gleichen oder einen besseren Dienst zu erbringen als ein nicht-digitaler oder klassisch erbrachter Dienst. Es sollte anerkannt werden, dass die Blockchain-Technologie manchmal ein anderes, aber oft überlegenes Sicherheitsmodell verwendet, um die gleichen Ziele zu erreichen, die die gesetzliche Regelung anstrebt.

### **Digitale Identität und Signaturen**

Dezentrale Identitäten, mehr Datenhoheit für Bürger und digital signierte staatliche Beglaubigungen relevanter personenbezogener Attribute, sind die Grundlage der nächsten digitalen Infrastruktur Europas. Das gesamte digitale Leben ließe sich dadurch an einem einzigen Ort verwalten. Die neu gewonnene digitale Autonomie kann so zum Beispiel für die Identifikation bei E-Government Diensten genutzt werden, für die Nutzung von Carsharing Angeboten, in Sozialen Netzwerken, zum Abschluss einer Versicherung, zum Online Einkauf und bei vielem mehr.

Insbesondere sollte die Nutzung selbst-souveräner digitaler Identitäten in Deutschland und Europa ermöglicht und gefördert werden. Ebenfalls sollte das in Entwicklung befindliche Bürgerkonto in der öffentlichen Verwaltung mit einem parallel existierenden internationalen Identitätssystem basierend auf dezentraler Blockchain-Technologie kompatibel sein.

### **Energiemarkt: Smart Grids und Smart Meters müssen Blockchain-kompatibel werden**

Die Einführung von Smart Meters und die Liberalisierung der Energienetze muss im Dialog mit Blockchain-Experten geführt werden, um sicherzustellen, dass die neuen Normen und Regeln, die derzeit erarbeitet werden, Blockchain-Anwendungen nicht verhindern. Smart Meter sind die Datenquellen für dezentrale Energiemärkte, die von Smart Contracts angetrieben werden. Ihre Schnittstellen müssen digital und offen sein, sodass eine einfache Verbindung mit Blockchain-Anwendungen möglich ist. Ebenfalls muss berücksichtigt werden, dass Verbraucher und möglicherweise sogar elektronische Personen selbstbestimmte Marktteilnehmer sein werden.

### **Rechtspersönlichkeit und Rechtsformen in Dezentralen Autonomen Organisationen (DAOs)**

Das deutsche Gesellschaftsrecht sollte die positiven Aspekte von Blockchain für die Zusammenarbeit und weltweite Kollaboration anerkennen. Durch den Einsatz transparenter Regeln in dezentralen Blockchain-Netzwerken (Smart Contracts) sind neue Governance-Modelle möglich, die es einer Vielzahl von Individuen ermöglichen, sich in Unternehmensstrukturen zu organisieren, die keine rechtliche Ähnlichkeit oder Rechte nach geltendem Recht haben. Die Gewährung der Rechtspersönlichkeit, der beschränkten Haftung und des Zugangs zu Waren und Dienstleistungen auf dem europäischen Markt würde ein wachsendes Ökosystem fördern.

### **Intermediäre im Zentrum von Regulierung**

In vielen Fällen regeln Gesetze Märkte über Intermediäre. Dazu zählen etwa der "Diensteanbieter der Informationsgesellschaft" im Telemediengesetz oder ein Finanzintermediär im Rahmen des Kapitalmarktrechts (MiFID II). Im Gegensatz dazu ermöglichen Blockchains die Entfernung von Vermittlern aus vielen Transaktionen. Die bisher von vertrauenswürdigen Dritten gebotene Sicherheit wird durch vertrauenswürdige Software-Ausführungsumgebungen in dezentralen Netzwerken (Blockchain und DLT) ersetzt. Anstatt die niedrigen Transaktionskosten an Verbraucher weiterreichen zu können, erhöht der Mangel von Mittelsmännern die Rechtsunsicherheit und damit die Kosten von Transaktionen.

Für Deutschland ist es von entscheidender Bedeutung, neue regulatorische Möglichkeiten im Bereich der dezentralen Netze durch Soft Governance, Standardisierung, digitale öffentliche Dienste und intelligente Regulierung zu entwickeln, die in das digitale Gefüge unserer gemeinsamen Transaktionsinfrastruktur eingebettet sind. "Embedded Law" erfordert ausgefeilte technische Standards und Strategien, um diese Standards in der digitalen Welt zur Geltung zu bringen. Im Gegensatz zur heutigen zentralen digitalen Infrastruktur sind Blockchain-Netzwerke keine "Black Boxes". Sie können in der Tat teilweise durch Standards und Best Practices "reguliert" werden, die wiederum einen breiteren Marktzugang ermöglichen, wenn sie von den Marktteilnehmern einbezogen 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 tokenbasierten Finanzierungsmöglichkeiten profitieren? Welche Risiken sehen Sie bei ICOs, insbesondere für die Verbraucherinnen und Verbraucher, aber auch für Unternehmen?*

Token-Emissionen zur Unternehmensfinanzierung haben für Deutschland ein großes Anwendungspotential. Es sind nur wenige Gesetzesanpassungen

notwendig, um deutschen Unternehmen diese Art der Finanzierung zu ermöglichen. Die Möglichkeit der agilen und kostengünstigen Unternehmensfinanzierung verschafft deutschen Unternehmen einen Wettbewerbsvorteil und steigert die Attraktivität Deutschlands als Gründungsstandort, insbesondere, weil eine unmittelbare Investitionsmöglichkeit auch für Kleinanleger geschaffen wird.

Berlin ist zu einem der attraktivsten und dynamischsten Standorte für die Ansiedlung von internationalen DLT-Startups geworden weltweit. Diese Entwicklung kann mit einer Regulierung der tokenbasierten Unternehmensfinanzierung weiter gefördert werden. Derzeit weichen in Berlin angesiedelte Unternehmen für Token-Emissionen insbesondere nach Malta und Lichtenstein aus, die sich bei der Token-Regulierung stark engagieren.

Neben Blockchain Startups sind auch Investmentfonds sowie der Markt für Schuldverschreibungen, Anleihen und ähnliche Kapitalmarktinstrumente geeignet für die Tokenisierung. Allein das durch Investmentfonds verwaltete Vermögen belief sich 2017 innerhalb der EU auf 15,6 Billionen Euro.

Auf Innovationen in der Unternehmensfinanzierung folgen regelmäßig Innovationen in der Realwirtschaft. Die tokenbasierte Unternehmensfinanzierung hat das Potential, eine solche Innovationskette in Gang zu setzen

*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?*

**Siehe Antwort auf Frage 15.**

*26. Die Beschäftigung mit und die Anwendung der Blockchaintechnologie ist in keinem Bereich soweit fortgeschritten wie im Finanzbereich. Dementsprechend werden auch Regulierungsfragen in Bezug auf Blockchainanwendungen 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 Blockchaintechnologie übertragen werden?*

Für Deutschland ist es von entscheidender Bedeutung, neue regulatorische Möglichkeiten im Bereich der dezentralen Netze durch Soft Governance, Standardisierung, digitale öffentliche Dienste und intelligente Regulierung zu

entwickeln, die in das digitale Gefüge unserer gemeinsamen Transaktionsinfrastruktur eingebettet sind. “Embedded Law” erfordert ausgefeilte technische Standards und Strategien, um diese Standards in der digitalen Welt zur Geltung zu bringen. Im Gegensatz zur heutigen zentralen digitalen Infrastruktur sind Blockchain-Netzwerke keine “Black Boxes”. Sie können in der Tat teilweise durch Standards und Best Practices "reguliert" werden, die wiederum einen breiteren Marktzugang ermöglichen, wenn sie von den Marktteilnehmern einbezogen werden

*27. Wie kann die Finanzmarktaufsicht zu einem Enabler von Innovation im Blockchainbereich werden?*

Aufgrund der engen Verwandtschaft zwischen der Blockchaintechnologie und Finanztechnologien (FinTech), kommt der BaFin eine gesteigerte Bedeutung im Bereich der technischen Innovation und der Entwicklung neuer Geschäftsmodelle zu.

Die Behörde muss deshalb personell so ausgestattet werden, dass die wachsenden Anfragen zeitgerecht bearbeitet werden können.

Um die Zugänglichkeit zur Regulierung zu fördern, sollte die BaFin einen Leitfaden herausgeben, der Unternehmen die Finanzierung via einer Token-Emission anstreben, die für eine Billigung des Prospektes notwendigen Schritte verständlich erläutert; auf Deutsch und Englisch. Das verschafft die nötige Transparenz und schafft Einigkeit innerhalb der BaFin über die entsprechenden Prozesse.

Darüberhinaus ist die Schaffung von „Sandboxes“ denkbar, wo Unternehmen mit innovativen Geschäftsmodellen eine Erlaubnis erteilt wird, solange die Unternehmensumsätze unter einer gewissen Schwelle bleiben. In dieser Hinsicht hat Singapur bzw. die dortige Aufsicht MAS einige innovative Konzepte entwickelt, von denen auch Deutschland lernen kann.

*28. Bekanntermaßen geht die Anwendung der einiger Blockchaintechnologie 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?*

Schon heute verwenden die meisten neuen Blockchainprojekte kein Proof-of-Work (PoW) Verfahren mehr zur Sicherung ihrer Infrastruktur. Das PoW Verfahren ist historisch einmalig und wird letztlich auf Bitcoin beschränkt sein, während alle anderen Netzwerke hin zu Proof-of-Stake Verfahren wechseln, welche energieneutral sind.

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

Im Bereich der digitalen Identitätstechnologien stellen Blockchain basierte Systeme eine signifikante Verbesserung zu klassischen Identitäts Providern dar. Eine Demokratisierung und Dezentralisierung ist hier erstmals möglich. Die Speicherung sensibler Daten kann unter Zuhilfenahme von Blockchain Technologie in die Hände der Nutzer gelegt werden. Die Prinzipien der Datenschutzgrundverordnung und eIDAS lassen sich damit sehr gut vereinbaren. Mehrere Deutsche Unternehmen arbeiten bereits aktiv an interoperablen Self-Sovereign Identity Lösungen und koordinieren Ihre Arbeit dazu im Blockchain Bundesverband, sowie in internationalen Standardisierungsorganisationen (DIF, W3C, ISO). Das Bündnis BiVD (Blockchain in der Verwaltung Deutschland) hat sich hier strategisch positioniert und arbeitet gemeinsam mit Belgien und den Niederlanden daran Gruppe von Mitgliedsländern für die Arbeit im Projekt eSSIF (European Self-Sovereign Identity Framework) zu gewinnen. Ziel dieses Frameworks ist es die aufstrebende Technologie (Self-Sovereign Identity) in Europa so zu ermöglichen, so dass langfristig ein innovativer und vor allem offener Wettbewerb am Identitätsmarkt entsteht. Die Einhaltung von Rechtsvorgaben (eIDAS, DSGVO, PSD2, etc.) wird dabei vorausgesetzt und soll durch das eSSIF unterstützt werden. Zudem verfolgt die Initiative das Ziel Datensouveränität zu ermöglichen und Datenmärkte zu erschließen.

Darüber hinaus können in Zukunft auch Wahlen über ein Blockchain-Verfahren sicher digital gestaltet werden. Hierzu sollte allerdings noch weitere Forschung und Entwicklung – bestenfalls in Deutschland – stattfinden. Grundsätzlich ist es jedoch klar, dass wenn digital, eine Wahl nur über ein Blockchain-Verfahren stattfinden sollte, da nur hier eine vollständige Nachvollziehbarkeit für Bürger und Staat garantiert werden kann. Klassische IT-Systeme sind „black boxes“, die vielfältigen Manipulationen zugänglich sind und letztlich nicht vertrauenswürdig sein können.

Zur digitalen Verwaltung siehe Antworten auf die Fragen 19 und 3.