BearingPoint GmbH
Erika-Mann-Straße 9
D-80636 München
Postfach 20 03 29
D-80003 München

T +49 89 54033 0
F +49 89 54033 7900

www.bearingpoint.com

BearingPoint®

Deutscher Bundestag
Finanzausschuss
z. H. Bettina Stark-Watzinger, MdB
Platz der Republik 1
11011 Berlin
Per E-Mail

07.03.2019

Persönliche schriftliche Stellungnahme zur öffentlichen Anhörung als Sachverständiger zum Antrag „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ der Fraktion der FDP (Drucksache 19/4217) im Finanzausschuss des Deutschen Bundestages

Sehr geehrte Abgeordnete des Finanzausschusses im Deutschen Bundestag,

am Tag des 11.03.2019 beschäftigten wir uns hier im Finanzausschuss des Hohen Hauses gemeinsam mit der Blockchain-Technologie bzw. Distributed-Ledger-Technologie in Bezug auf den Antrag 19/4217 der FDP Bundestagsfraktion vom 11.09.2018 an die Bundesregierung. Die Bundesregierung hat sich im Koalitionsvertrag bereits am 12.03.2018 u. a. dazu verpflichtet, die Blockchain-Technologie als *Forschungsschwerpunkt* zu stärken, ihr *Potenzial* zu erschließen, eine *umfassende Blockchain-Strategie* und einen *angemessenen Rechtsrahmen* bereitzustellen sowie die Technologie selbst zu *erproben*. Die zehn Punkte des von uns zu behandelnden Antrags weisen auf Optimierungspotenziale hin, die die Bundesregierung im Rahmen ihrer grundsätzlichen Ausrichtung zur Blockchain umsetzen kann. Folgendes Grundverständnis leitet mich bei der Beantwortung Ihrer Antragspunkte und Fragen.

(1) Technologieführerschaft und Wertgestaltungsmöglichkeiten zurückerlangen

Wer jetzt den richtigen Rechtsrahmen für die Blockchain-Technologie freilegt und schafft, kann im Bereich der Digitalisierung wieder die Technologieführerschaft und damit Wertgestaltungsmöglichkeiten erlangen. Wir hören aus allen Fraktionen und auch aus den durch diese repräsentierten breiten Schichten der Bevölkerung die Kritik an Massenüberwachung, etwa durch den amerikanischen Geheimdienst NSA und am gläsernen Bürger, etwa durch das digitale Sozialkredit-System in China.

Fakt demgegenüber ist, dass wir ohne die fortschrittlichsten intellektuellen und technologischen Mittel in Deutschland und Europa nicht über die erforderlichen Werkzeuge verfügen werden, unsere Werte auch geltend zu machen. Ob sich die Ressourcen, die dazu erforderlich sind, bei uns ansiedeln und entwickeln, hängt ganz entscheidend vom regulatorischen Fundament ab, das wir dazu bereitstellen.

Da Innovation sprunghaft verläuft und zudem ganz entscheidend von sich selbst verstärkenden Netzwerk- und Spillover-Effekten abhängt, haben wir jetzt mit dem Aufkommen der Blockchain-Technologie die Chance, durch ein gutes regulatorisches Fundament wieder die Technologieführerschaft zurückzuerlangen. Zugleich besteht das Risiko, durch eine unsachgemäße Regulierung das Fundament für diese Entwicklung zu entziehen und so technologisch weiter abgehängt zu werden.

Dies ist umso wichtiger, da viele unserer Schlüsselindustrien, wie z. B. der Maschinenbau, die Energiewirtschaft, die Gesundheitsbranche und sogar unsere Währung ohne den Zugang zu einer rechtssicher funktionierenden digitalen Infrastruktur und ohne die digitale Integration in den Weltmarkt ihre Alleinstellungsmerkmale und damit ihren Wert verlieren könnten.

(2) Drei grundlegende technischen Eigenschaften

Für die Blockchain-Technologie haben sich drei mehr oder minder synonym verwendete Namen durchgesetzt: „Blockchain“ als eher umgangssprachlich genutzter Name, „Distributed Ledger“ als eher wissenschaftlich korrekter Begriff und Krypto-Währungen, bzw. -Tokens in Hinblick auf den konkreten Einsatz als Tausch, Gebrauchs- oder Anlage-Gut (Payment-, Utility- oder Security-Token). Diese drei Namen beinhalten zugleich die drei entscheidenden Eigenschaften dieser Technologie:

- *Verkettung* von Daten („Chain“)
- *Verteilung* von Daten („Distributed“)
- *Verschlüsselung* von Daten („Crypto“)

Diese drei Eigenschaften hat es so schon immer und auch für nicht-digitale Informationstechnik gegeben; man denke nur an die versiegelte Bindung und bedruckte Seitennummerierung eines notariellen Kaufvertrages („Verkettung“), das Ablegen dieses Kaufvertrages in mindestens dreifacher Ausfertigung jeweils beim Käufer, Verkäufer und beim Grundbuchamt als neutralem Dritten („Verteilung“) sowie die Kryptographie von besonders vertraulichen Botschaften in mündlichen wie schriftlichen Geheimsprachen, die es schon seit dem Altertum gibt („Verschlüsselung“).

(3) Ökonomischer und sozialer Wert der Blockchain

Das Neue an der Blockchain ist das nahtlose und automatisierte Zusammenwirken ihrer genannten Eigenschaften auf Basis der Eindeutigkeit des Digitalen und der Echtzeitvernetzung durch das Internet. Dadurch wird ein Novum in der bisherigen Geschichte der Informationstechnologie erreicht, die *Vereinbarkeit von Verfügbarkeit und Dokumentenfestigkeit* von Daten.

Bisher standen diese Eigenschaften in einem Trade-off-Verhältnis, waren hinsichtlich der Erreichung ihres jeweiligen Optimums also unvereinbar:

- Je verfügbarer bzw. auch übertragbarer die Daten waren, wie z. B. eine E-Mail oder eine beliebige Internetseite, desto manipulationsanfälliger, also weniger dokumentenfest waren sie.
- Je dokumentenfester die Daten waren, wie z. B. eine notariell beglaubigte Urkunde im Papier-Archiv, desto weniger zweitnahe und dezentral verfügbar waren sie.

Die Vereinbarkeit der Eigenschaften Allgemeinverfügbarkeit und Dokumentenfestigkeit auf der Blockchain steht für demokratisierte Wahrheit. Eine solche Technologie deckt sich hervorragend mit unseren Ansprüchen gegen „Fake News“ und für Gerechtigkeit wie auch ökonomische Nachhaltigkeit. Mittels natürlicher Identifikationsmerkmale (z. B. Kohlenstoffgehalt von Rohmetallen) ist zudem die Verlinkung der Blockchain als solide Datenbasis mit der realen Welt hin zum Internet der Dinge möglich.

(4) Ökonomische und soziale Wirkweise der Blockchain

Die Wirkweise der Blockchain beruht auf dem bewährten ökonomischen und sozialen *Prinzip des öffentlichen Statements*. Wenn zwei Menschen heiraten, geschieht dies z. B. öffentlich, damit das Wissen über das eingegangene Vertragsverhältnis *verteilt* in allen an der Gemeinschaft beteiligten Köpfen abgespeichert ist. Öffentliche Gerichtsverhandlungen, die öffentlichen Sitzungen des Bundestages, wichtige öffentliche Ankündigungen der Geschäftsführung vor der Belegschaft bei Richtungsentscheidungen im Betrieb, alles das funktioniert nach dem gleichen Prinzip.

Weicht das Verhalten eines Individuums von den öffentlich getroffenen Vereinbarungen später als Teil der Mehrheitsmeinung (*Konsens*) ab, wird es entsprechend sozial sanktioniert und nicht zugelassen. Diese Transparenz und soziale Kontrolle schaffen mehr Rechtsakzeptanz und Rechtssicherheit. Dadurch werden die Durchsetzbarkeit von Verträgen, das Gelingen von Tauschakten und somit die gesamtwirtschaftliche Wohlfahrt entscheidend verbessert.

Die Blockchain-Technologie überträgt dieses Prinzip des öffentlichen Statements in die digitale Welt des Internets und macht es auf globaler Ebene in der Interaktion zwischen Menschen und auch Maschinen in Echtzeit nutzbar. Zudem wird durch die Technik eine unbestechliche Objektivität geschaffen, die beim rein sozialen Prinzip der Mehrheitsmeinung nicht immer gewährleistet ist. Dadurch werden Effizienz und Effektivität sowie die Skalierbarkeit dieses Prinzips massiv verbessert und somit auch die mit ihm einhergehenden positiven ökonomischen und sozialen Effekte.

Genau wie in den genannten Beispielen der nicht-digitalen Welt liegt die Transaktionshistorie auf der Blockchain bei verschiedenen Teilnehmern des Netzwerkes in redundanten Kopien vor. Nur wenn eine von einem Nutzer neu angewiesene Transaktion zur Mehrheitsmeinung und den in dieser beschriebenen gemeinsamen Regeln aller Knotenpunkte im Netzwerk passt, wird sie zugelassen und in die Blockchain eingetragen. Manipuliert ein Nutzer seine Version der Blockchain, wird er dadurch inkompatibel mit dem Netzwerk und ist von der Teilnahme daran ausgeschlossen.

(5) Was ist die richtige Regulierung der Blockchain?

Wie wir gesehen haben, beinhaltet die Blockchain-Technologie keine grundsätzlich neuen Komponenten, sondern basiert auf bekannten sowie erklärbaren technischen, ökonomischen und sozialen Umständen. Es gibt bereits heute zahlreiche Gesetze, die diese Umstände erfassen. Der Schlüssel zum Erfolg liegt daher darin, die Blockchain-Technologie richtig zu verstehen, um ihr gegenüber die richtigen Gesetze passend zuordnen und anwenden zu können. Öffentlich gut kommunizierte uns sachgerechte *Verwaltungsvorschriften* sind hier die erste Wahl, um durch Rechtssicherheit eine solide Entwicklung der Technologie in unserem Staatsgebiet zu schaffen. Sondergesetzgebungen die speziell auf die Blockchain-Technologie zielen, werden die Technik in jedem Fall entweder unnötig blockieren oder unnötig auf Kosten besserer Verfahren übervorteilen. Beides wäre für eine nachhaltige technologische, ökonomische und soziale Entwicklung nachträglich.

Zielführend ist eine *technologieneutrale* und damit *ordnungspolitisch korrekte* Regulierung.

Mit meinen besten Grüßen

Ralph Bärligea

Anlage: Stellungnahme zu den einzelnen Antragspunkten

Zu I.:

Die Distributed-Ledger-Technologie fand zuerst breite Anwendung am Finanzmarkt. Dies liegt meines Erachtens daran, dass Geld – wie auch unsere staatliche Währung – als nichtstoffliches, rein virtuelles Gut funktionieren kann, wodurch es ohne Medienbruch direkt auf der Blockchain verbucht werden kann. Auch digitale Güter (wie z. B. Software-Lizenzen) können direkt auf der Blockchain gehandelt werden. Nicht digitale Güter und Akteure können referenziert werden, indem auf der Blockchain auf natürliche und manipulationssichere Identifikationsmerkmale (z. B. Handvenenabdruck) verwiesen wird.

In Zukunft könnte ein über die Blockchain abgewickelter Zahlungsverkehr Verwaltungskosten in Milliardenhöhe sowohl für den öffentlichen als auch den privaten Sektor einsparen, wenn auf blockchain-basierten Datenbanken alle Komponenten eines Wirtschaftsgeschäfts ohne Medienbruch und vollintegriert darstellbar werden:

- Identitäten der Geschäftspartner
- Vertrag
- Gehandeltes Gut
- Rechnungsstellung
- Bezahlung
- Buchhaltung
- Versteuerung

Möglich war ein solches Szenario bisher nicht, da eine dazu erforderliche zentrale Datenbank ein zu großes Sicherheits- und Missbrauchsrisiko für alle Beteiligten dargestellt hätte. Indem die Blockchain den dezentralen und zugleich vollintegrierten Datenbankbetrieb ermöglicht und zudem eine bisher nicht überwundene Manipulationssicherheit bietet, löst sie dieses Vertrauensproblem und schafft neue Möglichkeiten.

Indem auf der Blockchain ein Handelsgeschäft über sogenannte Smart-Contracts automatisiert abgewickelt wird, kann die vereinbarte Gegenleistung für eine Leistung technisch exekutiert und synchron erfolgen, bei gleichzeitig automatisierter Prüfung der Bonität der Geschäftspartner. Hierdurch steigt die Rechtssicherheit, während gleichzeitig die Transaktionskosten sinken. Bisher ging erhöhte Rechtssicherheit durch Schrift- oder Notarerfordernis hingegen mit höheren Transaktionskosten einher.

Zu II.:

Durch die Genehmigung des Wertpapierprospektes für das Security-Token-Offering (STO) der Bitbond Finance GmbH als erstes seiner Art in Deutschland hat die BaFin Pionierarbeit geleistet. Dieses STO wird bezeichnender Weise genau am Tage unserer Ausschusssitzung lanciert.

Zudem hat die BaFin bewiesen, dass sie in der Lage ist, ein Security-Token-Offering rechtssicher zu genehmigen und entsprechend von anderen Token-Klassen zu unterscheiden.

Zur Unterscheidung von Token:

- Es ist im Sinne der Technologieneutralität als sinnvoll zu betrachten, wenn für ***Security-Token***-*Offerings* (einem auf der Blockchain verbrieften Anspruch auf Eigen- oder Fremdkapital) die gleiche Gesetzgebung wir für alle anderen Wertpapiere gilt.

- ***Payment-Tokens*** (Tokens, die rein als Zahlungsmittel dienen) werden entsprechend korrekt bereits seit 2013 als Rechnungseinheit im Sinne des Kreditwesengesetzes eingeordnet, was richtigerweise positiv hervorgehoben wird.
- ***Utility-Tokens*** (Tokens, die rein als Gebrauchsgut bezogen auf eine bestimmte Funktion innerhalb eines digitalen Ökosystems funktionieren) könnten entsprechend dem Sachenrecht des BGB zugeordnet werden.

Herausfordernd sind hybride Formen der drei genannten Token-Klassen. Ein von Banken auf einer Blockchain verbuchtes Euro-Giralgeld würde z. B. sowohl die Kriterien eines Payment-Tokens (weil damit bezahlt wird) als auch die eines Security-Tokens (weil es sich um eine Fremdkapitalforderung handelt) erfüllen. Viele Utility-Tokens (wie z. B. die innerhalb des geschlossenen Marktplatzsystems Golem rein zum Kauf- und Verkauf von Rechenleistung gedachte Token GNT) sind nicht mehr oder minder liquide als reine Payment-Tokens, sodass sie grundsätzlich auch als solche eingesetzt werden können.

Zu III. 1., 2.:

Als ersten Schritt einen objektiv nachvollziehbaren Kriterienkatalog zu veröffentlichen, der es Marktteilnehmern ermöglicht zumindest bei eindeutigen Tokens diese zweifelsfrei einer bestimmten Klasse zuzuordnen, wäre eine sinnvolle Maßnahme.

Umgekehrt könnte bei hybriden Formen ein Kriterienkatalog ergänzt um eine Sammlung an Fallbeispielen veröffentlicht werden, die objektiv nachvollziehbar machen, welche Bestandteile welchen Rechtes für diesen Token unter welchen Umständen gelten.

Fallbeispiel für den rechtssicheren Umgang mit hybriden Tokens: Ein bilanzierungspflichtiges Architekturbüro tauscht einen bestimmten Betrag Euro gegen GNT, um damit im Bedarfsfall zusätzliche Rechenleistung zum Betrieb eines aufwändigen CAD-Programms (Computer-Aided-Design) hinzuzukaufen. Zudem besitzt das Architekturbüro einen betriebsinternen Server, der nachts nicht genutzt wird und seine Rechenleistung in dieser Zeit automatisiert über das Golem-Netzwerk gegen GNT verkauft. → Folge: Das Architekturbüro darf den dauerhaft bestehenden Kassen-Bestand an GNT als langfristiges Anlagevermögen werten und damit stets zu Anschaffungskosten in die Bilanz einfließen lassen. Im Umkehrschluss müsste ein Handelsunternehmen, dass den GNT rein als Payment-Token für beliebige Handelsgeschäfte wertet, diesen zum Umlaufvermögen zählen und somit nach dem Niederstwertprinzip in die Bilanz einfließen lassen.

Fallbeispiele zu regulatorischen Zusammenhängen zu veröffentlichen ist gängige Praxis, so z. B. im AnaCredit Reporting Manual Part III der Europäischen Zentralbank.

Zu III. 3.:

Wenn ICOs die Lancierung von Utility-Tokens betreffen und es sich nicht um Payment- oder wie bei STOs Security-Tokens handelt, wäre die Zuständigkeit der BaFin in Frage zu stellen. Bei reinen Utilty-Tokens könnten zudem Organisationen wie Verbraucherschutzverbände oder Technische Überwachungs-vereine eine führende Rolle bei der Bewertung der technischen Güte der Produkte übernehmen.

Zu III. 4.:

Eine kompetente und sachgerechte sowie stringent exekutierte Besteuerung ist gegenüber sachlich heterogenen Einzelfallentscheidungen zu begrüßen, da sie für die Akteure kalkulierbare Kosten und somit Rechts- und Investitionssicherheit schafft.

Zu III. 5.:

Siehe Beantwortung zu III. 1., 2.

Zu III. 6. und 7:

Die Vertragsfreiheit sollte grundsätzlich auch die freie Wahl des Mediums beinhalten, über den der Vertrag geschlossen und dokumentiert wird.

Je nach möglichem Ausmaß eines Rechtsgeschäfts für die Betroffenen kennt das BGB jedoch Formerfordernisse, die vom mündlich über den schriftlich bis hin zum notariell zu beurkundenden und zu schließenden Vertrag reichen. Hiermit soll ein entsprechend höheres Level an Dokumentenfestigkeit und Rechtssicherheit in angemessener Relation zum Ausmaß des Rechtsgeschäfts sichergestellt werden.

Dieser Gedanke kann beibehalten werden, wenn „Schriftlich“ und „Notariell“ frei vom Medium Papier und damit technologieneutral verstanden werden. Auch eine rechtssachgemäße Einordnung beispielsweise des Fax-Briefes ist basierend auf diesem Gedanken bereits gelungen.

Nach technischer Beurteilung ist eine Transaktion über die Blockchain-Technologie hinsichtlich ihrer Dokumentationsgüte je nach Ausgestaltung mit einem schriftlich bis hin zu einem notariell beglaubigt festgehaltenen Dokument vergleichbar.

Zu III. 8.:

Die Ergebnisse der DIN NA043-02-04AA und ISO TC-307 Arbeitsgruppen zu Blockchain sowie der DIN SPEC 4997 Projektes „Privacy by Blockchain Design: Ein standardisiertes Verfahren für die Verarbeitung personenbezogener Daten mittels Blockchain-Technologie“ sollten im politischen Diskurs berücksichtigt und begleitet werden.

In der öffentlichen Wahrnehmung herrscht hierzu ein widersprüchliches Bild: Einerseits gibt es Vorurteile, dass Datenschutz und DS-GVO im Widerspruch zur Blockchain-Technologie stünden, oder das Recht auf Löschung auf der Blockchain nicht umsetzbar sei. Andererseits gibt es gegenüber der Blockchain-Technologie den Vorwurf, dass sie uneingeschränkte Anonymität und damit zunehmende Kriminalität ermöglichen würde. Tatsächlich hängen diese Umstände jedoch lediglich von der Ausgestaltung der Technologie ab.

Zur Löschung:

- ***Bloße Referenzierung von Daten auf der Blockchain:*** Die eigentlichen Dateninhalte werden in einer herkömmlichen Datenbank abgespeichert und dort nach herkömmlichen Methoden gelöscht. Die Daten werden durch einen ihnen eineindeutig zuordenbaren sog. Hashwert als digitaler Fingerabdruck (ohne den eigentlichen Dateninhalt) auf einer Blockchain eingetragen und referenziert, um Dokumentenfestigkeit zu erreichen. Die Daten in der herkömmlichen Datenbank können jetzt nicht mehr verändert werden, ohne dass sie nicht mehr zum referenzierten Fingerabdruck auf der Blockchain – welche selbst nicht geändert werden kann – passen. Diese Methode eignet sich v. a. bei großen Datenvolumina (Filme, Computertomografien, etc.), die man auf Grund ihrer Größe ohnehin nicht im verteilten Register der Blockchain redundant abspeichern möchte, um Speicherplatz zu sparen.
- ***Unwiderrufliche Verschlüsselung von Daten auf der Blockchain:*** Dieses Verfahren ist erforderlich, wenn die Blockchain über einen autonomen Datenhaushalt verfügen muss, um zu funktionieren.

Das Verfahren ist bei ICOs gängige Praxis, um zum Emissionspreis nicht veräußerte Tokens der Vernichtung zuzuführen und die Teilnehmer der Emission so vor einem Preisverfall zu schützen. Der Zugangsschlüssel (Private-Key) auf die nicht veräußerten Tokens wird lediglich vernichtet, wodurch die Tokens unbrauchbar gemacht werden. In diesem Fall geht es nur um das Zugriffsrecht auf die Tokens, der eigentliche Dateninhalt bleibt sichtbar. Sind die Daten jedoch auch selbst verschlüsselt auf der Blockchain abgelegt, verliert man durch die Vernichtung des Zugangsschlüssels auch die Lesemöglichkeit der Daten unwiderruflich. Die DIN 66398 definiert Löschung als „Prozess, durch den pbD derart irreversibel verändert werden, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können“. Dennoch gibt es Bedenken in der Wirtschaft hierzu, weil die Daten physisch auf der Blockchain verbleiben. Beim herkömmlichen Löschen wird jedoch genauso verfahren. Die Daten werden lediglich nach einer später nicht mehr nachvollziehbaren Zufallslogik überschrieben, die später faktisch nicht mehr rückgängig abgewickelt werden kann. Bei dem Vernichten eines zuvor rein zufällig generierten Private-Keys zu verschlüsselten Daten ist die Rückabwicklung durch Ausprobieren aller Kombinationsmöglichkeiten (wie bei einem Zahlenschloss) mit roher Gewalt (Brute-Force-Methode) ebenso als defacto unmöglich, bzw. wirtschaftlich undurchführbar anzusehen. Die Datenschutzbehörden sollten darum in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik klarstellen unter welchen Bedingungen eine Vernichtung von Private-Keys zu verschlüsselten Daten auf der Blockchain dem herkömmlichen Löschen gleichkommt. Andernfalls werden sinnvolle Geschäftsmodelle, die eine Blockchain mit autonomem Datenhaushalt und personenbezogenen Daten (pbD) benötigten wegen Unsicherheit beim Thema Löschen verhindert.

- ***Löschung einer privat betriebenen Blockchain im Zeitscheibenverfahren:*** Tragen z. B. zwei Geschäftspartner ihre Geschäfte auf einer Blockchain ein (z. B. Verträge, Eingangs- und Ausgangsrechnungen, Zahlungen, bzw. Zahlungsbestätigungen), können sie eine private Blockchain unterhalten, zu der nur sie beide jeweils einen Knotenpunkt betreiben. Nach Ablauf eines Jahres nehmen sie die zum Jahresanfang begonnene Blockchain außer Betrieb, legen diese zur Erfüllung der zehnjährigen gesetzlichen Aufbewahrungspflicht ab Ende Kalenderjahr entsprechend HGB und AO in ein Archiv ab und beginnen eine neue Blockchain. Nach Ablauf von zehn Jahren wird die jeweilig abgelegte Blockchain gesamthaft gelöscht. Dieses Verfahren eignet sich nur für privat betriebene Blockchains, da andernfalls die Löschung auf Grund der zu starken Verteilung der Daten organisatorisch nicht durchsetzbar ist. Zudem eignet sich dieses Verfahren nur, wenn jährliche bzw. angemessen lange Zeitscheiben auf Grund der gewählten bzw. rechtlich verbindlichen Löschregeln möglich sind. Bei einer täglichen Löschung wäre die dargestellte Variante z. B. nicht sinnvoll.

Richtig eingesetzt könnte die Blockchain den Datenschutz und die Umsetzung der DS-GVO verbessern und gleichzeitig für Unternehmen leichter umsetzbar machen. Die Datenweitergabe auf der Blockchain könnte von Betroffenen an Verarbeiter über standardisierte Smart-Contracts erfolgen, die Zweck und Rechtsgrundlage, eine sich selbst exekutierende Löschregel, sowie die Erfüllung aller Informationspflichten zwingend enthalten (Privacy by Design). Unternehmen könnten ihr Verzeichnis über Verarbeitungstätigkeiten aus den von ihnen getätigten Transaktionen automatisiert generieren. Nutzer mit digitaler Identität könnten über eine App oder ein Web-Portal einen Überblick über ihre weitergegebenen Daten erhalten sowie u. a. ihr Recht auf Beauskunftung oder Berichtigung geltend machen. Die DS-GVO selbst fordert in Erwägungsgrund 63: „Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.“ Der Grund warum es solche Lösungen auf Basis der Blockchain noch nicht gibt, sind m. E. nicht technische Restriktionen, sondern die bisher dafür fehlende Rechtssicherheit sowie die Tatsache, dass es stets Zeit braucht, bis sich über schwer planbare soziale Prozesse und Netzwerkeffekte gemeinsame Standards etablieren.

Zu III. 9.:

Dieser Punkt ist essenziell, da Banken andernfalls eine Kontoführung für Payment-Tokens auf Grund unkalkulierbarer Risiken für den Fall des Verlustes oder Diebstahls von privaten Zugangsschlüsseln bei gleichzeitig stark schwankendem Marktwert nicht anbieten können. Analog der Depositenverfahrung von Gold oder Bargeld im Tresor sollte klargestellt werden, dass Banken über das Garantieren geeigneter fest definierter technischer und organisatorischer Maßnahmen hinaus – anders als bei Giralgeld, das eine Forderung darstellt – nicht unbegrenzt in die Haftung zu nehmen sind, bzw. diese unbegrenzte Haftung vertraglich analog der Depositenverwahrung ausschließen können.

Zu III. 10.:

Für Privatpersonen sollte ohne Wahlmöglichkeit einheitlich die First-In-First-Out-Regel gelten und zwar sowohl mehrere Wallets als auch Markt- und Börsenplätze übergreifend. Diese Regelung ist die einfachste und setzt Privatpersonen daher möglichst wenig dem Risiko aus, sich auf Grund mangelnden Wissens oder mangelnder Fähigkeiten unnötig straffällig zu machen.

Für alle Wirtschaftsteilnehmer, für die das Handelsgesetzbuch gilt, sollten die dort dargelegten Wahlmöglichkeiten zwischen First-In-First-Out- und Last-In-Last-Out-Regel analog mit ihrer Maßgeblichkeit für die Besteuerung auch für Tokens aller Art gelten.

Bemerkung zum Stromverbrauch auf Rückfrage von Abgeordnetenbüros verschiedener Fraktionen:

Proof-of-Work: Dieses Verfahren soll sicherstellen, dass ein Verarbeiter von Transaktionen von Token, in denen er zugleich für das Verarbeiten der Transaktion vergütet wird, auf Grund der vorher investierten Stromkosten wirtschaftlich kein Missbrauchsinteresse hat. Würde ein Verarbeiter nämlich Fehlbuchungen tätigen, würde dies das Vertrauen in den betroffenen Token erschüttern und so seine eigene Vergütung entwerten. Der Stromverbrauch wird dabei über das für das reine Verarbeiten der Transaktion erforderliche Maß durch zusätzliche gestellte Rechenaufgaben „künstlich“ nach oben getrieben. Dieses auch beim mittlerweile über 10 Jahre alten „Ur-Bitcoin“ bis heute angewandte eher brachiale Verfahren hat als Preis für Sicherheit und als Ausgangsgrundlage des ökonomisch autarken Funktionierens der Blockchain eine gewisse Berechtigung. Das stromintensive Proof-of-Work-Verfahren ist mittlerweile um Verfahren ergänzt worden, die die gleiche oder sogar höhere Sicherheit bei weniger Stromverbrauch bieten.

***Proof-of-Stake*:** Verarbeiter mit einem großen Anteil der Tokens im Netzwerk müssen ob ihrer dadurch bewiesenen Glaubwürdigkeit weniger Rechenleistung investieren.

Proof-of-Authority: Nur vertrauenswürde Stellen, etwa registrierte Firmen, Regierungsstellen, oder Akteure mit einer auf der blockchain dokumentierten Reputationshistorie, werden als Verarbeiter zum Betrieb der Blockchain zugelassen.

***Tangle-Verfahren**:* Bei diesem unter anderem von IOTA mit Sitz in Berlin praktizierten Verfahren basiert die Vergütung für das Verarbeiten von Transaktionen auf Gegenseitigkeit (Reziprozität). Jeder Nutzer der eine Transaktion tätigen will, muss zugleich zwei Vorgänger-Transaktionen selbst verarbeiten bzw. bestätigen. Dies bewirkt zugleich eine mit steigender Nachfrage nach Transaktionen automatisch mitskalierendes Angebot an Hardware-Ressourcen. Die „Blockchain“ ist hier zudem nicht streng chronologisch als lineare Kette, sondern als eine verkettete Gitternetzstruktur aufgebaut, was jedoch am grundsätzlichen Funktionsprinzip der Synchronisation von Daten wenig ändert.

Da den Kombinationsmöglichkeiten und Arten der verschiedenen Verfahren keine Grenzen gesetzt sind und ihr optimaler Einsatz von den Erfordernissen des jeweiligen Anwendungsfalles abhängt, kann nicht pauschal vorherbestimmt werden, welches Verfahren das Beste ist. Welcher Stromverbrauch hierbei angemessen ist, entscheiden die Verbraucher bzw. Nutzer in diesem Kontext selbst.

Verfahren mit niedrigerem Stromverbrauch regulatorisch zu befördern und solche mit höherem Stromverbrauch regulatorisch zu sanktionieren könnte bspw. sicherheitstechnisch suboptimale Verfahren begünstigen und so dem Ziel des Datenschutzes entgegenstehen oder den Innovationsprozess anderweitig unvorhersehbar behindern. Zudem ist bereits heute absehbar, dass sich die Verfahren mit dem höchsten Stromverbrauch langfristig nicht durchsetzen werden. Selbst für den Bitcoin gibt es hier bereits ergänzende Lösungen, wie diverse Forks oder das Lightning-Netzwerk, die den Stromverbrauch und damit auch die Kosten reduzieren.

Ordnungs- und umweltpolitisch entscheidend für eine optimale Entwicklung ist, dass der Strom selbst aus Quellen stammt, die keine negativen externen Effekte verursachen, indem die tatsächlichen Kosten (auch Umweltkosten) der Stromerzeugung voll im Strompreis der Endverbraucher enthalten sind.

Zur effizienteren Energienutzung bietet die Blockchain-Technologie zwei Chancen:

- Durch den flexiblen Betrieb kann in Phasen der Überproduktion überschüssige und günstige Energie aus regenerativen Energiequellen für das Verarbeiten von Transaktionen verwendet werden. Dadurch entsteht eine Sockelnachfrage nach regenerativen Energien, was diese für die Betreiber wirtschaftlicher und somit attraktiver und breiter einsetzbar macht. Diese Logik gilt für andere Energiequellen wie etwa günstigen Nacht-Strom aus Kohlekraftwerken ebenso (darum kosten selbst Bitcoin-Transkationen mit vergleichsweise sehr hohem Stromverbrauch i. d. R. umgerechnet nur wenige Cent. Kurzfristig hohe Kosten von umgerechnet bis zu 100,- EUR je Transaktion hingegen resultieren als Marktpreis bei kurzfristig starkem Nachfrageanstieg und gleichzeitig kurzfristig nicht erweiterbarem Angebot an Hardware-Ressourcen, also mangelnder Skalierbarkeit).
- Es besteht die Möglichkeit, durch die Blockchain-Technologie Angebot und Nachfrage, bzw. Erzeugung und Verbrauch von Strom über kostengünstige Marktplätze gestützt durch digitale Infrastruktur besser zu zusammenzuführen. Obwohl Wind- und Sonnenenergie in Hochphasen der Erzeugung bekanntlicherweise deutlich günstiger bis hin zum Nulltarif zu haben ist, kann sich die Nachfrage diesem attraktiven Angebot nicht adaptieren. Dies liegt daran, dass vertrauenswürdige, intelligente, kostengünstige und automatisierte Informations-, Marktplatz- und Bezahlsysteme hierzu fehlen, wodurch die bestehenden Transaktionskosten des Marktes prohibitiv wirken. Die Blockchain-Technologie hat jedoch das Potenzial, diese Infrastruktur-Lücke zu schließen.

Abschließende Empfehlung:

Neben allen dargestellten technologischen Raffinessen der Blockchain-Datenbank werden auch Netzwerkeffekte und leicht bedienbare Benutzeroberflächen entscheiden, welche Varianten der Blockchain sich durchsetzen. An diesem Prozess sollten sich alle Akteure überlegt beteiligten.

Weder unüberlegtes Bejahen und Fördern noch unüberlegtes Ablehnen und Verbieten, nicht Euphorie und auch nicht Ängste, sondern schlicht der richtige Einsatz der Technologie innerhalb unseres *bestehenden gültigen Rechtsrahmens* sind der Schlüssel zum Erfolg. Beim Einsatz der Blockchain-Technologie sollten sowohl private als auch öffentliche Stellen sich nicht von negativen oder positiven Vorurteilen leiten lassen, sondern den konkreten Nutzen für sich gegenüber herkömmlichen IT-Systemen abwägen. Hierzu gebe ich Ihnen abschließend zwei Hilfsmittel zur Hand.

Bewertungsmatrix zum Einsatz der Blockchain-Technologie in Ihrer Organisation:

	A: Entweder Dokumentenfestigkeit oder Verfügbarkeit von Daten sind gefordert (nur eines v. beiden)	**B: Sowohl Dokumentenfestigkeit als auch Verfügbarkeit von Daten sind gefordert**
1: Vertrauen in einen zentralen Verantwortlichen ist leicht etablierbar	**Schlechtester Anwendungsfall:** z. B. individuelle Notizen in einem Word-Dokument (nur ein Nutzer mit Vertrauen in die eigene IT)	
2: Vertrauen in einen zentralen Verantwortlichen ist schwer oder nicht etablierbar		**Idealtypischer Anwendungsfall:** z. B. Digitale Identität, Durchführung und Tracking int. Zahlungsverkehrs- und Handelsströme (viele Nutzer, die zentraler IT schwer vertrauen können)

Einordnung der Blockchain-Technologie innerhalb möglicher IT-Infrastrukturlösungen:

		Physikalische Betriebsumgebung	
Nutzergruppe		**beim Anwender selbst (on-premise)**	**bei Drittanbieter (off-premise)**
	Private	Private-Cloud	Virtual Private Cloud
	Community	Community Cloud	Virtual Community Cloud
	Public	Peer-to-Peer Cloud	Public Cloud

Hybrid Cloud

Private, Hybrid u. Public Blockchain