19. Wahlperiode

Deutscher Bundestag
Finanzausschuss

# Wortprotokoll
der 34. Sitzung

**Finanzausschuss**
Berlin, den 11. März 2019, 13:30 Uhr
Berlin, Paul-Löbe-Haus Sitzungssaal 2 600

Vorsitz: Bettina Stark-Watzinger, MdB

## Öffentliche Anhörung

**Einziger Tagesordnungspunkt** **Seite 13**

Antrag der Abgeordneten Frank Schäffler, Christian Dürr, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP

**Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen**

**BT-Drucksache 19/4217**

**Federführend:**
Finanzausschuss

**Mitberatend:**
Ausschuss Digitale Agenda

# Unterschriftsliste der Sachverständigen

Öffentliche Anhörung zu dem Antrag der Fraktion der FDP
**„Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“**
**(BT-Drucksache 19/4217)**

Montag, den 11. März 2019 (13:30 bis 15:45 Uhr)

**Bärligea, Ralph**

BearingPoint GmbH

**Blockchain Bundesverband e. V.**

Dr. Keding, Sebastian

Resas, Daniel

Himmer, Klaus

**BOTLabs GmbH**

Rübe, Ingo

**Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)**

Fußwinkel, Oliver

**Deutsche Börse AG**

Hachmeister, Jens

**Deutsche Bundesbank**

Dr. Diehl, Dr. Martin

**Die Deutsche Kreditwirtschaft**

Kohlhase, Miye

Christmann, Hagen

Zuther, Dr. Friedrich

Schreiber-Handschug, Frank

**Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.**

Prinz, Prof. Wolfgang

**Fries, Dr. Martin**

Ludwig-Maximilians-Universität München

**Immutable Insight GmbH**

Gehra, Katharina

**Otto, Claudia**

COT Legal

**Romba, Eric**

lindenpartners (Partnerschaft von Rechtsanwälten mbH)

Siedler, Nina

**Siedler, Dr. Nina-Luisa**

DWF Germany Rechtsanwaltsgesellschaft mbH

.....

**SAP SE & Co. KG**

Uhde, Thomas

**Zoppei, Dr. Verena**

## Sitzung des **Finanzausschusses (7. Ausschuss)**
Montag, 11. März 2019, 13:30 Uhr

| Ordentliche Mitglieder des Ausschusses | Unterschrift | Stellvertretende Mitglieder des Ausschusses | Unterschrift |
|---|---|---|---|
| **CDU/CSU** | | **CDU/CSU** | |
| Brehm, Sebastian | | Brehmer, Heike | |
| Brodesser Dr., Carsten | | Dött, Marie-Luise | |
| Feiler, Uwe | | Durz, Hansjörg | |
| Güntzler, Fritz | | Helfrich, Mark | |
| Gutting, Olav | | Hirte Dr., Heribert | |
| Hauer, Matthias | | Jung, Andreas | |
| Maizière Dr., Thomas de | | Lenz Dr., Andreas | |
| Michelbach Dr. h. c., Hans | | Middelberg Dr., Mathias | |
| Müller, Sepp | | Müller (Erlangen), Stefan | |
| Radwan, Alexander | | Nick Dr., Andreas | |
| Steiniger, Johannes | | Riebsamen, Lothar | |
| Stetten, Christian Frhr. von | | Steffel, Frank | |
| Tebroke Dr., Hermann-Josef | | Vries, Christoph de | |
| Tillmann, Antje | | Wiesmann, Bettina Margarethe | |

| Ordentliche Mitglieder des Ausschusses | Unterschrift | Stellvertretende Mitglieder des Ausschusses | Unterschrift |
|---|---|---|---|
| **SPD** | | **SPD** | |
| Arndt-Brauer, Ingrid | | Hartmann, Sebastian | |
| Binding (Heidelberg), Lothar | | Lauterbach Dr., Karl | |
| Daldrup, Bernhard | | Mindrup, Klaus | |
| Esdar Dr., Wiebke | | Post, Florian | |
| Hakverdi, Metin | | Post (Minden), Achim | |
| Kiziltepe, Cansel | | Schwarz, Andreas | |
| Ryglewski, Sarah | | Stein, Mathias | |
| Schrodi, Michael | | Ziegler, Dagmar | |
| Zimmermann Dr., Jens | | | |

| Ordentliche Mitglieder des Ausschusses | Unterschrift | Stellvertretende Mitglieder des Ausschusses | Unterschrift |
|---|---|---|---|
| **AfD** | | **AfD** | |
| Glaser, Albrecht | | Braun, Jürgen | |
| Gminder, Franziska | | König, Jörn | |
| Gottschalk, Kay | | Kotré, Steffen | |
| Hollnagel Dr., Bruno | | Malsack-Winkemann Dr., Birgit | |
| Keuter, Stefan | | Münz, Volker | |
| **FDP** | | **FDP** | |
| Herbrand, Markus | | Dürr, Christian | |
| Hessel, Katja | | Ebbing, Hartmut | |
| Schäffler, Frank | | Mansmann, Till | |
| Stark-Watzinger, Bettina | | Müller-Rosentritt, Frank | |
| Toncar Dr., Florian | | Solms Dr., Hermann Otto | |

| Ordentliche Mitglieder des Ausschusses | Unterschrift | Stellvertretende Mitglieder des Ausschusses | Unterschrift |
|---|---|---|---|
| DIE LINKE. | | DIE LINKE. | |
| Cezanne, Jörg | | Barrientos, Simone | |
| De Masi, Fabio | | Riexinger, Bernd | |
| Leutert, Michael | | Wagenknecht Dr., Sahra | |
| Zdebel, Hubertus | | | |
| | | | |
| BÜ90/GR | | BÜ90/GR | |
| Bayaz Dr., Danyal | | Andreae, Kerstin | |
| Paus, Lisa | | Dröge, Katharina | |
| Schmidt, Stefan | | Kekeritz, Uwe | |
| Strengmann-Kuhn Dr., Wolfgang | | Kindler, Sven-Christian | |
| | | | |

**Unterschriftsliste der Teilnehmer mitberatender Ausschüsse**

Öffentliche Anhörung zu dem Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN
**„Entwurf eines Gesetzes zur steuerlichen Förderung von Forschung und Entwicklung kleinerer und mittlerer Unternehmen (KMU-Forschungsförderungsgesetz)"**

Montag, den 11. März 2019 (13:30 bis 15:45 Uhr)

**Ausschuss Digitale Agenda**

.....

.....

.....

**Weitere Ausschüsse:**

.....

.....

.....

| Ministerium bzw. Dienststelle (bitte in Druckschrift) | Name (bitte in Druckschrift) | Unterschrift | Amtsbezeichnung |
|---|---|---|---|
| BMF | Dr. Müller | S. Müller | RD |
| BMJV | Höhfeld | Höhfeld | MR'n |
| BMF | Hai: | Shfa | RD |
| BRH | PLEYER | | VAK |
| BMF | KLETZ | | RDi |

| Bundesrat<br>Land | Name (bitte in Druckschrift) | Unterschrift | Amtsbezeichnung |
|---|---|---|---|
| Baden-Württemberg | | | |
| Bayern | SCHELDT | | RD |
| Berlin | | | |
| Brandenburg | | | |
| Bremen | Bodmann | | Ref. |
| Hamburg | | | |
| Hessen | Brauer | Brauer | RDin |
| Mecklenburg-Vorpommern | | | |
| Niedersachsen | Haudt | Fthaudt | RD'in |
| Nordrhein-Westfalen | Marlit | Marlit | RR |
| Rheinland-Pfalz | B. Wiegs | Wiegs | RV |
| Saarland | | | |
| Sachsen | | | |
| Sachsen-Anhalt | | | |
| Schleswig-Holstein | Dr KELLER | Keller | Ltd |
| Thüringen | | | |

11.03.2019 **Unterschriftsliste** 13.30
Fraktionsmitarbeiter
öff

| Name | Fraktion | Unterschrift |
|---|---|---|
| Dr. Florian Meyerhöfer | CDU/CSU | |
| Britta Hannemann | CDU/CSU | |
| Dr. Martin Hiermeyer | CDU/CSU | |
| Stephan Rochow | CDU/CSU | |
| Udo Weber | CDU/CSU | |
| Jan-Peter Wißborn | CDU/CSU | |
| Silke Klix | SPD | |
| Stephan Teuber | SPD | |
| Gerald Steininger | SPD | |
| Moritz v. Seefried | AfD | |
| Ralf Olheide | AfD | |
| Philipp Iza Schilling | FDP | |
| Benjamin Schulz | FDP | |
| Andreas Koenig | FDP | |
| Steffen Dähne | FDP | |
| Christoph Sauer | DIE LINKE. | |
| Sandra Schuster | DIE LINKE. | |
| Stefan Herweg | DIE LINKE. | |
| Ralph Kummer | DIE LINKE. | |
| Daniel Detzer | B90/GR | |
| Henry Scheel | B90/GR | |

Beginn der Sitzung: 13:30 Uhr

**Einziger Tagesordnungspunkt**

Antrag der Abgeordneten Frank Schäffler, Christian Dürr, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP

**Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen**

**BT-Drucksache 19/4217**

Vorsitzende **Bettina Stark-Watzinger**: Liebe Kolleginnen und Kollegen, ich begrüße Sie zur 34. Sitzung des Finanzausschusses.

Ganz besonders begrüße ich die Experten, die dem Finanzausschuss heute ihren Sachverstand zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ (BT-Drucksache 19/4217) zur Verfügung stellen.

Soweit Sachverständige davon Gebrauch gemacht haben, dem Finanzausschuss vorab eine schriftliche Stellungnahme einzureichen, ist diese an alle Mitglieder des Ausschusses verteilt worden. Die Stellungnahmen werden auch Bestandteil des Protokolls der heutigen Sitzung.

Ich begrüße die Kolleginnen und Kollegen aus den mitberatenden Ausschüssen. Für das Bundesministerium der Finanzen begrüße ich Frau Ministerialdirigentin Dr. Wimmer und Herrn Ministerialdirigenten Dr. Pleyer. Ebenso darf ich weitere Fachbeamte begrüßen. Ferner begrüße ich die Vertreter der Länder.

Das Thema der heutigen Anhörung ist der eben genannte Antrag der FDP Fraktion, der verschiedene Vorschläge zur Verbesserung der Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt enthält.

Zum Ablauf der Anhörung: Für die Anhörung ist ein Zeitraum von 2 Stunden und 15 Minuten angesetzt, das heißt wir tagen bis circa 15:45 Uhr.

Ziel ist es, möglichst vielen Kolleginnen und Kollegen die Möglichkeit zur Fragestellung zu geben.

Um dieses Ziel zu erreichen, hat sich der Finanzausschuss in dieser Legislaturperiode für ein neues Modell der Befragung entschieden, d. h. die vereinbarte Gesamtzeit wird entsprechend der Fraktionsstärke in Einheiten von jeweils 5 Minuten unterteilt. In diesem Zeitraum müssen sowohl Fragen als auch Antworten erfolgen. Je kürzer die Fragen formuliert werden, desto mehr Zeit bleibt für die Antworten. Wenn mehrere Sachverständige gefragt werden, bitten wir, fair darauf zu achten, den folgenden Experten ebenfalls Zeit zur Antwort zu lassen.

Um Ihnen ein Gefühl für die Zeit zu vermitteln, wird nach 4 Minuten und 30 Sekunden ein Signalton ertönen. Dann verbleiben noch 30 Sekunden für die Antwort. Unsere bisherigen Anhörungen haben gezeigt, dass dies bei etwas gutem Willen und gegenseitigem Verständnis gut möglich ist.

Die fragestellenden Kolleginnen und Kollegen darf ich bitten, stets zu Beginn ihrer Frage die Sachverständigen zu nennen, an die sich die Frage richtet, und bei einem Verband nicht die Abkürzung, sondern den vollen Namen zu nennen, um Verwechslungen zu vermeiden.

Zur Protokollführung: Zu der Anhörung wird ein Wortprotokoll erstellt. Zu diesem Zweck wird die Anhörung mitgeschnitten. Zur Erleichterung derjenigen, die unter Zuhilfenahme des Mitschnitts das Protokoll erstellen, werden die Sachverständigen von mir noch einmal namentlich aufgerufen, damit keine Verwechslung entsteht.

Ich darf Sie alle bitten, die Mikrofone zu benutzen und sie im Nachgang wieder auszuschalten, damit es zu keinen Störungen kommt.

Wir beginnen mit der ersten Fragerunde, mit den Kolleginnen und Kollegen von der CDU/CSU. Herr Hauer, bitte.

Abg. **Matthias Hauer** (CDU/CSU): Die Fraktion der CDU/CSU erwartet mit Hochspannung die Blockchain-Strategie der Bundesregierung. Dazu möchte ich unsere Erwartungshaltung klar machen: Wir erwarten, dass sie zu einer Initialzündung für diese Technologie in Deutschland wird und ihr einen echten Anschub verleiht. Wir erleben, dass schon jetzt eine Abwanderung ins Ausland stattfindet, die wir nicht weiter hinnehmen wollen. Wir wollen, dass die Strategie die Basis für einen angemessenen Rechtsrahmen für den Handel mit Kryptowährungen und Token bildet.

Daher meine Frage an die Deutsche Kreditwirtschaft: Welche Aspekte des Regelwerkes, zum Beispiel bestehende Regelungslücken und Überlegungen zur Verbriefung von Besitzrechten, haben aus Ihrer Sicht eine besondere Relevanz?

Darüber hinaus gibt es ein aktuelles Eckpunktepapier aus dem Bundesministerium der Finanzen (BMF), welches deutlich macht, dass deutsches Recht generell für elektronische Wertpapiere geöffnet werden soll. Es wird weiter ausgeführt, dass sich diese Öffnung zunächst auf elektronische Schuldverschreibungen beschränken soll. Die Einführung der elektronischen Aktie soll erst in einem zweiten, späteren Schritt geprüft werden. Wie ist Ihre Einschätzung dazu? Ist das ein sinnvolles Vorgehen?

Vorsitzende **Bettina Stark-Watzinger:** Für die Deutsche Kreditwirtschaft, Frau Kohlhase.

Sve **Miye Kohlhase** (Deutsche Kreditwirtschaft): Ja, wir sehen das tatsächlich so. Wir haben mit Interesse gesehen, dass dieses Konsultationspapier letzte Woche veröffentlicht wurde. Der Bankenverband hat heute zum Thema der DLT (Distributed Ledger Technologie)-Wertpapiere ein Diskussionspapier veröffentlicht, welches sich auf DLT-Wertpapiere und deren rechtliche Einordnung bezieht.

Um es so zu beschreiben: Die DLT ist eine neue Technologie, welche die Anwendung von neuen Verfahrensabläufen ermöglicht. Mit Blick auf den Finanzmarkt können Daten über Rechte und Berechtigte mittels einer Eintragung in einem verteilten Register erfasst werden. So wird dann auch die Weitergabe solcher Rechte an andere Berechtigte als Transaktion erfasst. Diese Überlegung ist Wertpapierrechtlern nicht ganz neu. Bislang ist es so, dass Rechte und die Möglichkeit der Übertragung von Rechten in Form von Wertpapierurkunden erfasst werden. Diese Rechte und Übertragungen werden zu Sachen und sind damit dem Sachenrecht zugänglich, weil sie in Wertpapierurkunden verbrieft sind. Das heißt, Unternehmenskredite werden durch Verbriefung zu Anleihen. Die Vorschriften des Sachenrechts finden darauf Anwendung, obwohl in der Praxis tatsächlich keine Urkunden mehr übergeben werden, sondern eine Übertragung mittels Depotbuchungen stattfindet. Die Vorteile des Sachenrechts liegen auf der Hand: Buchungssicherheit durch Zu- und Abbuchung, Gutglaubens- und Insolvenzschutz.

Wir gehen davon aus, dass eine Verbriefung nicht mehr notwendig ist und eine andere Lösungsmöglichkeit besteht. Im Konsultationspapier wird eine Analogie zum Bundesschuldenwesengesetz (BSchuWG) als Lösungsmöglichkeit angesprochen und weiterverfolgt. In unserem Diskussionspapier führen wir das weiter aus, speziell durch die Anwendung der DLT.

Die Alternative wäre, nicht den Weg der DLT zu gehen, sondern den Blick darauf zu richten, wie eine Dematerialisierung der Wertpapiere erreicht werden kann. Das Schweizer Bucheffektengesetz kann dafür als Vergleich herangezogen werden.

Zu beiden Wegen wird die Deutsche Kreditwirtschaft Stellung nehmen und sie mit Blick auf die DLT weiter verfolgen. Als ersten Ansatzpunkt hatten wir den Weg des BSchuWG gewählt, weil das dortige öffentliche Register eine Funktion erfüllt, welche die DLT als verteiltes Register auch erfüllen kann.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der SPD, Herr Dr. Zimmermann.

Abg. **Dr. Jens Zimmermann** (SPD): Meine Frage geht an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), da wir im Kontext von DLT und anderen Innovationen auf den Finanzmärkten sehr häufig Anfragen von Verbänden über die Rolle der BaFin und die Geschwindigkeit von Auskünften bekommen.

Wie ist insgesamt die Einschätzung der BaFin zu den Entwicklungen und Innovationen, die im Antrag der FDP genannt sind? Wie ist Ihre aktuelle Haltung dazu? Im vergangenen Jahr haben wir im Kontext des sogenannten ICO (Initial Coin Offering) Äußerungen der BaFin zur Kenntnis genommen. Deshalb wäre die aktuelle Einschätzung interessant.

Welche Projekte gibt es bei der BaFin, um mit den Veränderungen des Marktes umzugehen und gegenüber neuen Akteuren als Dienstleister aufzutreten?

Wie ist die Einschätzung der BaFin zum Eckpunktepapier des Bundesministeriums der Finanzen?

Vorsitzende **Bettina Stark-Watzinger**: Für die Bundesanstalt für Finanzdienstleistungsaufsicht, Herr Fußwinkel.

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)): Die BaFin beobachtet die technologischen Entwicklungen auf den Finanzmärkten seit vielen Jahren. Schon 2011 hat sie sich mit der Blockchain-Technologie auseinandergesetzt, indem sie seinerzeit eine Verwaltungspraxis zur Einordnung von Bitcoins als Rechnungseinheiten im Sinne des Kreditwirtschaftsgesetzes verkündet hat, was auf viele andere Kryptowährungen (old coins) übertragbar ist. Damit haben wir sehr zeitnah und frühzeitig auf damals erkannte potentielle Risiken im Bereich der Geldwäscheprävention und auf Geschäfte, welche die Marktintegrität potentiell beeinträchtigen können, reagiert.

Wir haben den Ansatz, den Markt zu beobachten und Entwicklungen zu verfolgen, in den letzten Jahren institutionalisiert. Dafür steht unter anderem das Referat, welches ich in der BaFin leite. Dieses schaut sich finanztechnologische Innovationen jenseits der einzelnen Verwaltungsvorgänge an. Zudem unterhält es ein internes und externes Netzwerk, in dem wir uns über die Thematik und die technischen Hintergründe intensiv austauschen. In diesem Netzwerk haben wir fast die Hälfte des hier anwesenden Kreises von Sachverständigen kennengelernt und vertiefende Gespräche geführt. Das hilft uns, im Rahmen der Aufsicht relativ nah an den technologischen Entwicklungen zu bleiben und möglichst nachhaltige Finanzinnovationen am Finanzmarkt zu identifizieren.

Das führt mich dazu, wie wir im Moment die Blockchain-Technologie einschätzen: Es gibt diverse Veröffentlichungen der BaFin, die das Potential der Blockchain-Technologie betonen. Die Risiken habe ich eben schon angesprochen. Die Kernpotentiale sind die Verringerung der Transaktionskosten durch die Anwendung von Blockchain-Modellen, die tendenziell eher „private“ und „permissioned“ sind, also von bestimmten Anbietern vorgehalten und entwickelt werden. In diesem Bereich spielen sich sehr viele Use Cases (Anwendungsfälle), Proof of Concepts (Nachweis der Machbarkeit) und Erprobungsmodelle von diversen Anbietern auf dem Kapitalmarkt ab. Das kann positive Auswirkungen auf den Finanzmarkt und die Finanzintegrität haben. Insbesondere bei der Hebung von Liquidität oder bei Prozessen, die derzeit noch als ineffizient bezeichnet werden. Zu nennen sind hier Bereiche mit Informationsasymmetrien, beispielsweise bei der Handelsfinanzierung, bei Commercial Papers oder Schuldschein-Darlehen. Das sind interessante Prozesse, die wir verfolgen.

Es gibt aber noch weitere Potentiale. Zum einen besteht ein natürliches Potential als Basistechnologie für den Kapitalmarkt in der etwas ferneren Zukunft. Zum anderen kann die Blockchain-Technologie zur Refinanzierung eingesetzt werden – dabei sind viele Rechtsfragen aber noch zu klären. Wir sehen auch Potential bei dezentralen Netzwerken, die dezentrale Plattformen unterstützen können. Das Potential eines Open-Source-Gedankens mit der Monetarisierung von Beiträgen durch Teilnehmer in einem Netzwerk und der Nutzung von Schwarmintelligenz kann gehoben werden. Aber hier besteht noch ein relativ hohes Prüfungs- und Entwicklungserfordernis.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der AfD, Herr König.

Abg. **Jörn König** (AfD): In dem Antrag der Fraktion der FDP ist viel von dem Begriff der Rechtssicherheit die Rede. Daher meine Frage an BearingPoint, Herrn Bärligea. Wie sehen Sie den Begriff der Rechtssicherheit, wie sollte er ausgestaltet sein? Sollte dieser Begriff nicht auch den Schutz vor wirtschaftlichen Risiken beinhalten?

Vorsitzende **Bettina Stark-Watzinger**: Herr Bärligea von BearingPoint.

Sv **Ralph Bärligea** (BearingPoint GmbH): In meiner schriftlichen Stellungnahme habe ich die groben Leitlinien, die ich persönlich sehe, festgehalten. Die Rechtssicherheit besteht für mich in erster Linie darin, die verschiedenen Erscheinungen, die es im Rahmen der Blockchain-Technologie gibt, den bestehenden Rechten und Gesetzen richtig zuzuordnen. Zum größten Teil gibt es noch Begriffsunklarheiten. Wir sehen das in dem Antrag bei der Klassifikation der verschiedenen Token. Da sehe ich primär Verbesserungsbedarf. Ich bezweifl, dass neue Gesetze notwendig sind. Alle Phänomene, die bei der Blockchain-Technologie auftreten, gibt es auch in der Nicht-Blockchain-Welt. Die Blockchain ist letztendlich nur ein Medium.

Bei der Gesetzgebung plädiere ich für technologieneutrale Regelungen, sodass nicht eine bestimmte Technologie behindert oder bevorteilt wird. Denn sobald versucht wird, Rechtssicherheit über eine

Sondergesetzgebung zu schaffen, besteht die Gefahr, dass ein Blockchain-Hype künstlich verstärkt wird oder sinnvolle Innovationen, die sich durch die Blockchain-Technologie ergeben könnten, künstlich behindert werden. Hierzu möchte ich Ihnen ein Beispiel geben:

Im Zusammenhang mit ICOs (Initial Coin Offering) wird häufig von ICO-Scams, also von Betrug gesprochen. Betrug ist ein Straftatbestand. Wenn jemand einen tollen ICO plant, öffentlich verkündet, was er mit dem Geld machen will, dieses Geld einsammelt und verschwindet, also die angekündigte Geschäftsidee nicht umsetzt, bietet bereits die bestehende Rechtslage genügend Möglichkeiten, dem Herr zu werden.

Zur Frage, wie können Verbraucher geschützt werden? Aus meiner Sicht ist es ordnungspolitisch sinnvoll, wenn diejenigen, die Geschäfte auf der Blockchain eingehen, die Risiken selbst tragen. Das heißt, sowohl auf Angebots- als auch auf Nachfrageseite. Zunächst geht es darum, den bestehenden Verbraucherschutz richtig anzuwenden. Wenn über den bestehenden Verbraucherschutz hinaus zusätzliche Regularien geschaffen werden, wird den Marktakteuren eine Scheinsicherheit gegeben. Das könnte befördern, dass Risiken eingegangen würden, die sonst nicht eingegangen würden. Es ist ohnehin schon schwierig, diese Technologie im Detail zu beurteilen und ihre Qualität und Güte für den Einzelfall zu bestimmen. Umso schwieriger wird es für den Gesetzgeber, wenn er versucht, einen Verbraucherschutz zu schaffen, der über das bestehende Maß hinausgeht.

Eine kleine Ergänzung: Bei der Finanzkrise gab es ein ähnliches Problem. Die Banken haben sich in Sicherheit gewogen. Sie gingen davon aus, dass sie im legalen Rahmen handelten und sahen die Perspektive, gerettet zu werden. Auch die Verbraucher waren der Meinung, dass sie Verträge bei privaten Banken oder einer Sparkasse abschließen könnten und es so etwas wie absolute Sicherheit gäbe. Im Endeffekt stellte sich heraus, dass es diese Sicherheit nicht gab. Dieser Fehler sollte bei der Blockchain-Technologie nicht wiederholt werden.

Vorsitzende **Bettina Stark-Watzinger**: Die nächste Frage kommt von den Kollegen der Fraktion der CDU/CSU, Herr Steiniger.

Abg. **Johannes Steiniger** (CDU/CSU): Meine Frage geht an Herrn Rübe von BOTLabs. Berlin ist ein großer Blockchain-Hub mit großem Potential. Bei Betrachtung der Finanzierung, sprich ICO (Initial Coin Offering), sehen wir die Tendenz, dass diese in letzter Zeit vornehmlich im Ausland stattfindet. Stichwort: Singapur oder Malta. Wie kommt es zu diesem Trend? Was müsste Politik machen, damit sich dieser Trend dreht – die Regierung mit ihrer Blockchain-Technologie, aber auch das Parlament in der Gesetzgebung? Damit wir nicht etwas erleben, was wir bei anderen Technologien erlebt haben. Dort hatte Deutschland ein gutes Potential, aber nun wird woanders das Geld verdient.

Vorsitzende **Bettina Stark-Watzinger**: Für BOT-Labs, Herr Rübe.

Sv **Ingo Rübe** (BOTLabs GmbH): Wir können tatsächlich beobachten, dass in den letzten ein, zwei Jahren sehr viele Unternehmen aus Deutschland abwandern und in andere Länder gehen. Singapur ist sicherlich der Hauptmagnet, aber es sind auch die Schweiz oder die Niederlande. Diese Unternehmen sind dann nicht mehr hier in Deutschland. Das ist schade, weil ein riesiges Potential in dieser Technologie liegt, die ursprünglich zum großen Teil aus Deutschland kam.

Die Gründe dafür liegen insbesondere in der Perspektivlosigkeit, die in Deutschland über die letzten Jahre generiert wurde. Es ist sehr schwierig, Geschäfte mit der Blockchain zu machen. Es geht hier nicht um Scam-ICOs, sondern um Firmen, die nachhaltige Geschäftsmodelle machen wollten. Wir haben den Eindruck, dass auf politischer Seite wenig Verständnis dafür besteht, welche Potentiale die Blockchain-Technologie bietet. Insbesondere geht es hier um die permissionless Blockchains und nicht um die permissioned Blockchains. Letztere sind relativ leicht einzugrenzen, da sie im Endeffekt nur Datenbanken sind. Die permissionless Blockchains sind von völlig neuer Qualität, da es in Richtung Token Curated Registry (TCR) und verteilte autonome Organisationen geht. Das sind schwierige technologische Themen, die politisch besser eingefangen werden könnten, als es heute der Fall ist.

Ich vergleiche das gerne mit dem Internet. Das Internet haben wir in Deutschland ein wenig verpasst. Die großen Internetfirmen sind nicht in Deutschland ansässig, sondern in den USA. Die USA haben Anfang der 1990er Jahre ein sehr gutes

Umfeld für die Entwicklung des Internets geschaffen. Sie haben es geschafft, dass sehr viel Geld in die Universitäten floss. Es wurde durch Staatsaufträge sehr viel Geld in kleine Unternehmen investiert. Dadurch wurde eine Sicherheit geschaffen, die Venture Capital angezogen hat. Zudem wurden damals die Netze sehr intensiv ausgebaut. Diese drei Dinge und das Ziel, Angebot und Nachfrage gemeinsam zu schaffen, haben dazu geführt, dass sich damals kleine Unternehmen in einem sehr angenehmen Umfeld ansiedeln konnten.

Das haben andere Länder besser verstanden als Deutschland. Singapur versucht momentan, ein Mekka für die Blockchain-Szene zu werden. Dort bauen sie sogenannte Sandboxes, in denen Blockchain-Unternehmen rechtssicher arbeiten können. Man könnte aber noch mehr tun: Man könnte darüber hinaus die Grundlagenforschung durch die Schaffung von Professuren besser unterstützen, insbesondere im Bereich Mathematik, nicht im Bereich BWL. Auch kleine Firmen müssten durch Kooperationen in Deutschland gehalten werden. Das müssen nicht unbedingt Kooperationen mit dem Staat sein. Das können auch Public Private Partnerships sein. Hier kann die Politik viel leisten, um die Player zusammenzubringen. Das passiert heute noch zu wenig. Das sind die Gründe dafür, warum die Leute abwandern. Dazu kommt, dass das Geld in China gerade etwas lockerer sitzt und Chinesen ihr Geld nach Singapur schaffen, um in Blockchain-Projekte zu investieren.

Der Hauptgrund sind jedoch die Rahmenbedingungen. Blockchain-Unternehmen fühlen sich in Deutschland nicht zu 100 Prozent willkommen. Das sage ich als Blockchain-Unternehmen, das in Deutschland ist und auch in Deutschland bleiben möchte.

Vorsitzende **Bettina Stark-Watzinger:** Die nächste Frage kommt von der Fraktion der FDP, Herr Schäffler.

Abg. **Frank Schäffler** (FDP): Meine Frage geht an Herrn Romba von lindenpartners und an den Blockchain Bundesverband. Wo stehen wir heute mit der Distributed-Ledger-Technologie in Deutschland im internationalen Vergleich? Wo sehen Sie regulatorischen oder gesetzgeberischen Handlungsbedarf?

Vorsitzende **Bettina Stark-Watzinger**: Herr Romba für lindenpartners.

Sv **Eric Romba** (lindenpartners, Partnerschaft von Rechtsanwälten mbH): Wo stehen wir in Deutschland? Gesamt gesehen, stehen wir in der Blockchain-Technologie und DLT (Distributed Ledger Technologie) am Anfang, nicht nur in Deutschland. In meiner Stellungnahme habe ich einen Vergleich zur Smartphone-Entwicklung aufgestellt; wir sind gerade beim iPhone 1, iPhone 2. Das heißt, das große Potential kommt noch. Wir werden noch eine Weile brauchen, bis es unser Leben so radikal verändert, wie andere Technologien das getan haben.

In Deutschland nehmen wir in der Beratungspraxis wahr, dass viele Unternehmen nach Deutschland zurückkehren, die sich in ausländischen Jurisdiktionen versucht hatten, beispielsweise in der Schweiz oder in Liechtenstein. Warum kommen sie zurück? Der Hintergrund ist oftmals, dass ein erfolgreiches Geschäft in Deutschland interessanter für Investoren ist, da hier eine Aufsicht mit strengen Rahmenbedingungen besteht. Insofern ist Deutschland mit seinen gesetzlichen Grundlagen ein Asset.

Stichwort gesetzliche Grundlagen: Bei vielen Themen hindert die mangelnde Technikneutralität des Rechts. Im Finanzaufsichtsrecht ist die Technikneutralität weitestgehend gegeben, im Zivilrecht jedoch nicht. Die Kreditwirtschaft hat das bereits angesprochen. Um Ihnen das bewusst zu machen: Wenn wir von einem Urkundserfordernis sprechen, betrifft dies Technik bzw. Technikneutralität. Denn wenn wir von Technik sprechen, reden wir nicht nur von digitaler, sondern auch von analoger Technik. Dieses Erfordernis der Technikneutralität müssen wir herstellen. Wenn das gelingt, können viele Bereiche der Technologie noch besser genutzt werden, gerade hier in Deutschland.

In unseren Projekten haben wir den ersten Security Token Offering in Deutschland begleitet, der just in diesem Moment in den Public Sale geht. Dabei haben wir gute Erfahrungen mit der Anwendung des Rechts gemacht. Wir hätten natürlich auch eine Wunschliste von Themen, die geändert werden sollten. Die Anpassung der Gesetze und des Rechts reicht nicht. Auch das Ökosystem muss angepasst werden. Wir brauchen Verwahrlösungen und funktionierende Zweitmärkte. Hier ist es wichtig, dass das Parlament und der Gesetzgeber entsprechende Initiativen auf den Weg bringen.

Vorsitzende **Bettina Stark-Watzinger**: Für den Blockchain Bundesverband, Herr Resas.

Sv **Daniel Resas** (Blockchain Bundesverband e. V.): Wir sehen das im Wesentlichen auch so. In unserer Stellungnahme haben wir ausgeführt, dass das Finanzmarktaufsichtsrecht, welches im Wesentlichen europäisch geprägt ist, schon heute technikneutral ausgestaltet ist. Im Zivilrecht sehen wir die gleichen Hindernisse. Wir können uns momentan dem materiellen Wertpapierrecht durch kautelarjuristische Lösungen annähern, was aber nur zu 98 Prozent reicht. Das Security Token Offering ist dafür ein sehr schönes Beispiel. Um funktionierende Kapitalmärkte zu haben, braucht man Anpassungen im Zivilrecht. Auch vor dem Hintergrund, dass institutionelle Marktteilnehmer sich dort engagieren können sollen.

Zum gerade schon angesprochenen Thema des vermeintlichen Wegzugs aus Deutschland: Auch wir haben in der Beratungspraxis Unternehmen nach Liechtenstein, in die Niederlande oder in die Schweiz begleitet. Die Gründe dafür sind vielfältig, allerdings geht es vor allem um die Rechtssicherheit. Dort besteht ein enormes Bedürfnis, welches nicht nur die Finanzaufsicht betrifft. Auch wir arbeiten eng mit der BaFin zusammen und pflegen einen regen Austausch. Es bestehen insbesondere in steuerlicher Hinsicht für viele Emittenten von Token, die zu Finanzierungszwecken verkauft werden, erhebliche Probleme. Es besteht Unklarheit, was auf steuerlicher Seite passiert. Insofern gibt es mehrere Gründe für den Wegzug.

In dem Kontext ist mir eine saubere Abschichtung wichtig: Blockchain-Unternehmen ist nicht gleich Blockchain-Unternehmen. Jedes Blockchain-Unternehmen emittiert einen Token zu bestimmten Zwecken. Token können zu Finanzierungszwecken emittiert werden, müssen es aber nicht. Token können wie im Security Token Offering klassischen Wertpapieren angenähert sein, können aber auch gänzlich andere Rechte verbriefen. Ich glaube, es ist gut, wenn das ein bisschen differenzierter betrachtet wird.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion die LINKE., Herr De Masi.

Abg. **Fabio De Masi** (DIE LINKE.): Ich richte meine erste Frage an Frau Rechtsanwältin Claudia Otto von COT Legal. In Ihrer Stellungnahme zum Antrag kommen Sie zu dem Ergebnis, dass es keine spezifischen Blockchain-Gesetze geben soll, weil die Gesetzgebung technologieneutral ausgestaltet sein sollte. Wie lässt sich das mit dem allgemeinen Ruf nach einem stärkeren Rechtsrahmen vereinbaren, wie er auch im Antrag gefordert wird? Inwiefern ist der bestehende Rechtsrahmen besonders im Hinblick auf den Verbraucherschutz ausreichend?

Eine weitere Frage geht an Frau Dr. Zoppei von „mafia-nein-danke“. Wo sehen Sie den drängendsten Regulierungsbedarf im Hinblick auf geldwäscherechtliche Risiken der Blockchain? Es existieren ja Pseudonyme, zwar in einer öffentlich einsehbaren Transaktionskette, jedoch mit einer Anonymität der personenbezogenen Daten.

Vorsitzende **Bettina Stark-Watzinger**: Frau Otto für COT Legal.

Sve **Claudia Otto** (COT Legel): Der Ruf nach Blockchain-Gesetzen baut auf einer idealen Vorstellung auf. Diese ideale Blockchain-Welt, die besonderer Rahmenbedingungen bedarf, gibt es jedoch nicht. Vielmehr sollte dem aktuellen Rechtsrahmen mehr Achtung geschenkt werden. Dieser aktuelle Rechtsrahmen enthält zahlreiche notwendige Schutzgesetze, die unbeachtet bleiben und gar aktiv umgangen werden. Zu nennen ist hier unter anderem die Flucht in die englische Sprache, die Unstimmigkeiten und juristische Mängel schwerer erkennbar macht. Dem gegenüber steht das verletzte Verbraucherrecht, das umfassende und klar verständliche Informationen verlangt.

Zu nennen ist außerdem, dass durch Unwissenheit und mangelnde Erfahrung Missverhältnisse zwischen Leistung und Gegenleistung schwerer erkennbar sind, was in einem verbotenen Wuchergeschäft münden kann. Darüber hinaus wird das Gesetz gegen den unlauteren Wettbewerb mit seinen Verboten der irreführenden und druckausübenden geschäftlichen Handlungen vergessen.

Der bestehende Rechtsrahmen ist stark. Er soll zu Gunsten weniger Marktakteure aufgeweicht werden, denen der Rechtsrahmen nicht gefällt. Das ist insbesondere an dem Wunsch zu erkennen, die allgemeine zivilrechtliche Prospekthaftung zu Gunsten einer in Sachen Blockchain-Produkte zahnlosen, praktisch haftungsausschließenden spezialgesetzlichen Prospekthaftung zu streichen. Schutzgesetze, ob zu Gunsten von Verbrauchern oder auch von unternehmerischen Geschäftspartnern, dürfen

nicht zu Gunsten einer bestimmten Technologie beschnitten oder abgeschafft werden. Darauf liefe es hinaus, und darin dürfte im Übrigen eine verbotene Beschränkung der europäischen Grundfreiheiten und Grundrechte liegen.

Die Schutzgesetze müssen jedoch auf ihre Wirksamkeit und Umsetzung überprüft werden. So rege ich insbesondere an, das elektronische Wertpapier an die Voraussetzungen des besonderen Schutzes vor Vervielfältigung und Veränderung zu knüpfen. Dabei ist es völlig gleich, unter Anwendung welcher Technologie es geschaffen und aufbewahrt wird. Der Schutz von Anlegern muss stets von gleicher Qualität und Intensität sein. Fakt ist, dass die Blockchain-Technologie diesen Schutz nicht bietet. Verlust, Verwässerung und sonstige Schädigung durch Dritte sind ein technologieimmanentes Risiko.

Vorsitzende **Bettina Stark-Watzinger**: Frau Dr. Zoppei für mafianeindanke.

Sve **Dr. Verena Zoppei** (mafianeindanke e. V.): Es gibt mehrere Gründe, warum User ihre Identität oder die Eigenschaften der Finanztransaktionen versteckt halten möchten. Viele davon sind legitim. Diese Anonymität kann aber gleichzeitig auch für illegale Zwecke ausgenutzt werden. Nach einer Recherche der Technischen Universität in Sydney haben ein Viertel der Bitcoin-Nutzer Verbindungen zu illegalen Geschäften. Am letzten Freitag hat die australische Finanzaufsicht die Registrierung von zwei Krypto-Währungsbörsen wegen Drogenhandels ausgesetzt. Europol betrachtete den Trend seit Jahren und hat festgestellt, dass Bitcoin immer noch die am meisten genutzte digitale Währung im Darknet ist, um mit Waffen und Drogen illegal zu handeln.

Auch andere Währungen, die eine komplette Anonymität bieten, wie zum Beispiel Zcash, Ethereum und Monero, werden von kriminellen Netzwerken immer mehr bevorzugt; allen voran durch die italienische Camorra und 'Ndrangheta. Wer dieses Risiko nicht erkennt, wird sich nicht dagegen schützen können. Die Forderung in Punkt 4 des Antrags nach einer koordinierten Zusammenarbeit der Aufsichtsbehörden mit den anderen zuständigen Behörden reicht nicht aus. Konkrete Rahmenbedingungen für eine einheitlich laufende Solvenz- und Geldwäscheaufsicht über Kryptowährungen bei den Schnittstellen zu den offiziellen Währungen, wie zum Beispiel Tauschbörsen, Handelsplattformen und elektronische Geldbörsen, müssen im Zusammenhang mit der nationalen Umsetzung der 5. Geldwäscherichtlinie gesetzlich normiert werden.

Im Zusammenhang mit der unter Punkt 9 des Antrags genannten Forderung der Schaffung eines eigenen Tatbestandes im Kreditwesengesetz (KWG), um die Verwahrung von Private- und Public-Keys durch Depotbanken zu regulieren, ist es aus meiner Sicht wichtig, dass das Anbieten des Handels mit Kryptowährungen nach § 1 Absatz 11 Nr. 7 KWG ausdrücklich als Anbieten von Finanzinstrumenten klassifiziert wird.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion BÜNDNIS 90/DIE GRÜNEN, Herr Dr. Bayaz.

Abg. **Dr. Danyal Bayaz** (B 90/GR): Ich stelle drei Fragen an Frau Dr. Siedler.

Es gibt ein aktuelles Eckpunktepapier des Bundesministeriums der Finanzen (BMF). Ich weiß nicht, inwiefern Ihnen das geläufig ist. Können Sie Stellung beziehen, ob wir uns ausreichend mit der Technologie auseinandergesetzt haben? Herr Hauer hat im Hinblick auf die für den Sommer angekündigte Strategie der Bundesregierung seine Erwartungshaltung formuliert: Welche Kriterien sollten wir an diese Strategie anlegen, damit es auch wirklich eine Strategie ist, die die Bundesregierung uns vorlegt?

Welche wirtschafts- und gesellschaftspolitischen Anreize erwarten Sie von der Politik, um diese Technologie weiterzuentwickeln? Vielleicht können Sie in diesem Kontext auf Non-Profit-Aspekte eingehen.

Was halten Sie von der Schaffung einer Opt-in-Option für Utility Token – gerade bei Prospektrichtlinien, damit wir bei der Emission von Token das Vertrauen der Verbraucher erhöhen können.

Vorsitzende **Bettina Stark-Watzinger**: Frau Dr. Siedler für die DWF Rechtsanwaltsgesellschaft.

Sve **Dr. Nina-Luisa Siedler** (DWF Germany Rechtsanwaltsgesellschaft mbH): Das Eckpunktepapier des Bundesministeriums der Finanzen (BMF) und des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) greift die aktuelle Diskus-

sion um die Security Token auf, also die Entmaterialisierung des Wertpapiers. Das ist dringend notwendig. Diese Diskussion führen wir seit mehr als zehn Jahren in Deutschland. Wir begrüßen sehr, dass das jetzt in Angriff genommen wird. Allerdings hat das nur bedingt Bezüge zur Blockchain-Technologie. Das gilt sicherlich auch für die Nutzung anderer Technologien, was in dem Papier auch deutlich wird.

Ich habe in dem Papier die Auseinandersetzung mit den Grundlagen der Blockchain-Technologie und den neuen Möglichkeiten, die sie schafft, vermisst. Bislang liegt in den Verlautbarungen der öffentlichen Hand und der Politik der Schwerpunkt enorm auf der Distributed Ledger Technologie (DLT). Das kann ich verstehen, da sich DLT als schlichte Datenbank-Technologie sehr leicht in das bisherige System einordnen lässt.

Allerdings fände ich es sehr begrüßenswert, wenn wir uns mehr mit den Potentialen der originären Blockchain-Technologie auseinanderzusetzen würden, um der Abwanderung der Blockchain-Ur-Community nicht weiter zuzuschauen und der Technologie einen Schub zu verleihen. Das bezieht sich vor allem auf den Public-Bereich und auf den Mischbereich der Public Permissioned Ledger, die in vielfältigen Formen denkbar ist. Beispielsweise kann über eine Blockchain nachgedacht werden, die nur von lizensierten Banken betrieben werden kann. Die Europäische Kommission wiederum konstruiert zurzeit eine europäische Blockchain-Partnership, welche eine von den Staaten betriebene Blockchain zur Verfügung stellen möchte. Es sind auch Mischformen denkbar, mit denen man sich langsam an das Thema herantastet.

Wir sollten auf keinen Fall bei den rein private permissioned DLT-Lösungen stehenbleiben, weil ansonsten die Potentiale der Technologie nicht gehoben werden können. Es ist schön, dass wir weitere Dinge elektronisieren, mit Blockchain hat dies aber im Kern nichts zu tun. Bei der Analyse der Möglichkeiten der Blockchain-Technologie sollten wir schauen, wie wir sie besser verstehen und sie fördern können. Wir sollten schauen, wie wir uns den Governance-Modellen im öffentlichen Bereich zuwenden können. Wir sollten Kriterien aufstellen, wie wir den Aufbau einer solchen digitalen Infrastruktur aus Deutschland heraus fördern können.

Der deutsche Verein Interplanetary Database Foundation mit Sitz in Berlin versucht, eine permissioned Blockchain zu bauen. Diese läuft nur durch die Mitglieder, ist jedoch öffentlich. Das ist also eine öffentliche Infrastruktur, die dort gebaut werden soll. Für solche Unternehmungen fehlen uns Kriterien zur Gemeinnützigkeit. Wir brauchen dringend eine neue Kategorie der Gemeinnützigkeit für genau diesen nicht-kommerziellen Bau öffentlicher, digitaler Infrastruktur.

Zum Token Opt-in: Ich begrüße diesen Vorschlag aus Frankreich sehr. Ich bin der Meinung, dass Deutschland und Frankreich bei diesem Thema einen Schulterschluss üben sollten. Parallel sollten vergleichbare Regelungen erarbeitet und wechselseitig anerkannt werden. Auf europäischer Ebene wird ein solcher Vorschlag lange brauchen, während Deutschland und Frankreich ein starkes Tandem wären, dem sich schnell weitere Länder anschließen würden.

Vorsitzende **Bettina Stark-Watzinger**: Die nächste Frage kommt von der Fraktion der SPD, Herr Hakverdi.

Abg. **Metin Hakverdi** (SPD): Meine Frage geht an die Bundesbank, an Herrn Dr. Diehl. Wo stehen wir mit der Technologie der Blockchain-Anwendungen im Finanzmarkt insgesamt?

Die Deutsche Bundesbank hat 2018 ein Blockchain-Projekt zusammen mit der Deutschen Börse zu Prototypen gemacht. Welche Ergebnisse gibt es?

Ich habe außerdem eine Frage an Herrn Fußwinkel von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Können Sie etwas zum Vorschlag des Bundesministeriums der Finanzen (BMF) und des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) zur Behandlung von elektronischen Wertpapieren sagen?

Vorsitzende **Bettina Stark-Watzinger**: Herr Fußwinkel von der BaFin.

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)): Die BaFin begrüßt das jetzt veröffentliche Eckpunktepapier ausdrücklich. Es bietet die Möglichkeit, sich zwei wesentliche Aspekte technologieneutral anzuschauen. Zum einen die Möglichkeit, Schuldverschreibungen oder Wertpapiere im Allgemeinen digital herauszu-

geben. Zum anderen die Prüfung, welche Regulierungsmöglichkeiten im Bereich von Krypto-Token bestehen, speziell bei Utility Token.

Das Papier ist so aufgebaut, dass wir eine marktnahe Konsultation sehen. Es ist relativ wichtig, dass zunächst die Meinung des Marktes eingeholt wird, um nicht an den Bedürfnissen des Marktes vorbei zu regulieren. Ziel ist, dabei technologieneutral zu bleiben und nicht mit der europäischen Regulierung in einen Konflikt zu geraten. Da die DLT von Natur aus grenzüberschreitend ist, stehen alle nationalen Ansätze vor dem Problem, dass sie zu einer Zersplitterung der Landschaft führen und einer solchen Technologie von ihrem Konzept her nicht gerecht werden. Im Eckpunktepapier wird das aus unserer Sicht hinreichend adressiert.

Vorsitzende **Bettina Stark-Watzinger**: Herr Dr. Diehl für die Deutsche Bundesbank.

Sv **Dr. Martin Diehl** (Deutsche Bundesbank): Wir haben dieses Projekt gemeinsam mit der Deutschen Börse betrieben, weil wir schon lange zusammenarbeiten, beide Infrastrukturanbieter im Finanzsektor sind und dadurch ähnliche Interessen haben. Bis 2016, als wir das Projekt gestartet haben, haben wir uns primär theoretisch mit dem Thema beschäftigt. Wir haben den Austausch zu Experten, Praktikern und Wissenschaftlern gesucht und einschlägige Konferenzen besucht. Allerdings ist das so, als ob jemand versucht, Klavierspielen zu lernen, indem er Konzerte besucht oder mit Musikern spricht. Er muss natürlich selber spielen. Daher haben wir uns für ein praktisches Projekt entschieden, mit einem Partner, der auch sehr technologieaffin ist und Interesse daran hat.

Zu den Erkenntnissen aus unserem Projekt: Uns ging es um das Verständnis, wie die DLT praktisch funktioniert. Wir haben uns gefragt, ob wir das Programmieren mit unseren Leuten und unserer IT hinbekommen; ob wir verschiedene Blockchain-Typen aufsetzen können. Wir haben uns mit einem Projekt beschäftigt, welches Wertpapiere mittels einer Blockchain abwickeln sollte. Das nannten wir zunächst Digital Coin oder Digital Securities.

Als wir gesehen haben, wie es funktioniert, wollten wir wissen, wie schnell es funktioniert und wie sicher es ist. Die Erkenntnisse kurz zusammengefasst: Wir wissen, dass die einzelne Transaktion langsamer ist als in den herkömmlichen Systemen und mehr Ressourcen kostet. Das hängt an dem Konsensmechanismus, der in der Blockchain immer vorhanden ist. Der Konsens muss immer hergestellt werden, was Ressourcen kostet. Wir haben aber auch gesehen, dass die gängigen Blockchain-Varianten grundsätzlich in der Lage sind, die Volumina abwickeln zu können, die wir für die Finanzmarkt-Infrastruktur brauchen. Wir haben damals mit den Anbietern Hyperledger Fabric und Digital Asset gearbeitet, die sich mittlerweile weiterentwickelt haben und sicherlich noch besser geworden sind.

Ob das jetzt vorteilhaft ist, ergibt sich erst aus einer Gesamtschau. Auch die Nachabwicklung von Folgeprozessen muss betrachtet werden. Zunächst ist die Technik viel teurer, ist langsamer und benötigt mehr Ressourcen. Sie kann jedoch vorteilhaft sein, wenn sie Folgeprozesse erleichtert. Beispielsweise durch eine Erleichterung von komplexen Abwicklungsprozessen und gemeinsamen Datenbanken. Je einfacher die Prozesse sind, beispielsweise der Zahlungsverkehr, desto weniger wird die DLT als relevant erachtet. Bei relativ komplexen Abwicklungsverfahren mit mehreren Partnern, beispielsweise bei der Wertpapierabwicklung, sehen wir hingegen eine größere Relevanz.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der CDU/CSU, Herr Dr. Tebroke.

Abg. **Dr. Hermann-Josef Tebroke** (CDU/CSU): Ich habe zwei Fragen an Herrn Prof. Prinz von der Fraunhofer-Gesellschaft. Zum einen zum Thema Datenschutz, zum anderen zum Thema Forschungsförderung.

Zum Ersten: Immer wieder ist von großen Bedenken bzw. von Aussagen zu hören, dass es eine Herausforderung ist, eine mit der Datenschutzgrundverordnung (DSGVO) konforme Blockchain-Technologie zu entwickeln. Wie ist da der Stand der Forschung? Gibt es schon eine mit der DSGVO-konforme Technologie?

Zum Zweiten: Herr Rübe sprach eben davon, dass er mehr Grundlagenforschung fordere und erwarte, dass die Player zusammengebracht werden. Wie würden Sie Forschungsförderung organisieren? Gibt es genügend anerkannte Forscherinnen und Forscher, um den notwendigen Schub zu erreichen?

Vorsitzende **Bettina Stark-Watzinger**: Herr Prof. Prinz für die Fraunhofer-Gesellschaft.

Sv **Prof. Wolfgang Prinz** (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.): Die Datenschutzgrundverordnung (DSGVO) ist ein viel diskutiertes Thema. Woran liegt das? Wenn Sie einmal Daten in die Blockchain geschrieben haben, können Sie diese zwar für ungültig erklären, aber nicht löschen. Die Daten sind in dem Ledger vertreten.

Es gibt zwei Möglichkeiten, das zu umgehen. Die eine Möglichkeit ist, dass Sie keine Klartextdaten reinschreiben, sondern einen sogenannten Hash eines Wertes. Das ist sicher, soweit dieser Hash nicht zurückgerechnet werden kann. Er muss so konstruiert sein, dass eine Zurückrechnung nicht möglich ist. Die andere Möglichkeit ist, dass Daten verschlüsselt in die Blockchain geschrieben werden. Dieser Schlüssel wird nicht bekanntgegeben oder vernichtet. Auf diese Vernichtung muss dann vertraut werden. Es gibt Juristen, die behaupten, dass auch ein Hash ein identifizierendes Mittel ist. Darüber existiert ein Streit unter Juristen. Wenn wir irgendwann in der Lage sind, Schlüssel zu knacken, die zur Verschlüsselung von privaten Informationen auf der Blockchain genutzt wurden, ist die Blockchain im Prinzip voll auslesbar. In öffentlichen Blockchains können Daten nicht nachträglich verschlüsselt werden, weil sonst die Geschichte auf der Blockchain geändert würde. Das sind die Probleme, mit denen momentan gekämpft wird. Ich denke, dass die Forschung dazu einiges entwickeln kann. Im Moment bestehen diese zwei Muster, um eine mit der DSGVO-konforme Blockchain zu entwickeln.

Zur Forschungsförderung: Wir sollten bedenken, dass die Blockchain-Technologie eine tolle Kombination schon existierender Technologien ist. Netzwerk-, Kryptographie- und Softwareengineering sind sehr interessant zusammengefasst. Dafür gibt es in Deutschland sehr gute Forscher. Trotzdem gibt es im Moment noch keine Blockchain-Professur. Erste werden in verschiedenen Bundesländern angedacht. In NRW versuchen wir gerade, dieses Thema in Form eines Zentrums besser voranzubringen. Ich glaube, dass wir in die Grundlagen investieren sollten. Das, was wir im Moment als Blockchain kennen, ist eine sehr einfache Technologie. Sie beruht auf einer sehr einfachen Datenstruktur, die im ersten Semester gelehrt wird. Im Bereich der Forschung kann hier noch sehr viel getan werden.

Ich glaube, dass wir in drei, vier Jahren nicht mehr über die Blockchain reden. Wir sehen jetzt schon bei IOTA und anderen, dass ganz andere Datenstrukturen genutzt werden. Hier kann bei den Grundlagen mehr getan werden. Grundlagen sollten unterstützt werden, aber auch die Anwendung. Die Forschungsförderung kann in den verschiedenen Branchen einiges unternehmen. Dabei sollte von Projekten Abstand genommen werden, die drei, vier oder fünf Jahre laufen. Es sollten Kurzläufer gestartet werden. Diese sollten versuchen, ein Thema relativ schnell aufzugreifen und dynamisch anzugehen, eventuell mit Start-Ups und Universitäten zusammen. Das ist besser als die übliche Forschungsförderung, für deren Projekte schon ein Jahr für die Beantragung gebraucht wird. Beantragen Sie jetzt ein Blockchain-Projekt, welches erst in einem Jahr gefördert wird, ist das Projektthema in einem Jahr obsolet. Hier müssen wir agiler werden, um schneller und kurzfristiger etwas starten zu können.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der CDU/CSU, Herr Hauer.

Abg. **Matthias Hauer** (CDU/CSU): Meine erste Frage richtet sich an Frau Gehra von Immutable Insight GmbH. Ihr Unternehmen hat untersucht, dass viele Krypto-Token faktisch tot sind und nur noch ein rudimentäres Marktgeschehen beobachtet werden kann. Können Sie das näher erläutern?

Welches Potential sehen Sie bei ICOs als Investitionsobjekt für Anleger und zur Mittelstandsfinanzierung?

Eine weitere Frage richte ich an den Blockchain Bundesverband. Können Sie ebenfalls eine Einschätzung dazu abgeben? Herr Resas hat gerade etwas zum dringenden gesetzgeberischen Handlungsbedarf im Zivilrecht gesagt. Sie sagten, dass 98 Prozent kautelarjuristisch gelöst werden können und bei den restlichen 2 Prozent etwas getan werden müsse. Können sie konkret etwas zu diesen zwei Prozent sagen?

Vorsitzende **Bettina Stark-Watzinger**: Frau Gehra für Immutable Insight.

Sve **Katharina Gehra** (Immutable Insight GmbH): Zunächst zur Analyse, die wir zu Token gemacht haben, bei denen es tatsächlich noch Wachstum gibt. Ich möchte betonen, dass wir nicht die Aussage treffen, dass diese Technologie kein Potential

hat. Zwar hat nicht jeder Onlineshop, der 1997 eröffnet wurde, überlebt. Allerdings gibt es heute Amazon, über das wir uns einig sind, dass es zu einem neuen Wirtschaftsplayer geworden ist.

Was haben wir uns angeschaut? Was passiert mit der Technologie, obwohl der Preis eingestürzt ist? Wir konnten zwei Dinge feststellen. Erstens: Die Nutzerzahlen wachsen weiterhin exponentiell. Ähnlich wie beim Smartphone können wir davon ausgehen, dass die massenhafte Adaption kommt. Wenn die Userzahlen weiter wachsen, ist es nicht die Frage, ob es kommt, sondern nur noch wie schnell. Ich rege an, dass wir einen Standortvorteil schaffen und nutzen. So kann verhindert werden, dass wir in zehn Jahren auf die gleiche Entwicklung wie beim iPhone von Apple zurückblicken. Es besteht nur jetzt die Chance, diesem exponentiellen Wachstum gerecht zu werden und eine Grundlage zu schaffen, um einen effektiven Start zu ermöglichen.

Das Zweite ist, dass die Finanzierungsmöglichkeiten deutlich besser sind. Entgegen der Aussage von Frau Dr. Zoppei können wir Geldwäsche auf der Blockchain effektiv verhindern und bekämpfen. Es wird mit den Analysen unmöglich, auf der Blockchain effektiv Geld zu waschen. Wir suchen nicht mehr die Nadel im Heuhaufen, wie es die heutige Regulierung auch im Zahlungsverkehr versucht. Wir sieben den Heuhaufen durchgehend und finden Nadeln, von deren Existenz wir heute im Zahlungsverkehr nichts wissen. Unser großer Appell an die Bundesregierung und an das Parlament ist, diese neue Generation der Compliance der aktiven Geldwäschebekämpfung in Echtzeit zu nutzen.

Vorsitzende **Bettina Stark-Watzinger**: Für den Blockchain Bundesverband, Herr Resas.

Sv **Daniel Resas** (Blockchain Bundesverband e. V.): Zu den kommerziellen Realitäten momentan im Markt: Der ICO-Hype und die Utility Token Sales sind merklich abgekühlt. Das ist kein Geheimnis und lässt sich der Tagespresse entnehmen. Gleichwohl sehen wir noch Potential. Es ist nicht so, dass Utility Token gänzlich vom Markt verschwunden sind. Sie werden nur nicht mehr zu Finanzierungszwecken öffentlich verkauft. Das hat auch damit zu tun, dass klassisches Venture Capital den Markt noch stärker für sich entdeckt hat. Die meisten Projekte, die wir derzeit begleiten, sind von den üblichen Verdächtigen vorfinanziert. Diese Projekte sind in den ersten zwei Jahren nicht auf Public Sales angewiesen.

Um die Frage nach den rechtlichen Verbesserungen oder dem Anpassungspotential kurz anzureißen: Ausgangspunkt muss die Technologieneutralität sein. Das sehen wir auch so. Bei der Finanzmarktaufsicht gehen wir davon aus, dass wir mit den bisherigen Regeln im Wesentlichen gut leben können. Eine Ausnahme sind die Anpassungen im Prospektrecht. Dort besteht Verbesserungspotential bei der Verwendung bestimmter Anhänge.

Aus unserer Sicht ist das Wichtigste, dass wir im Zivilrecht vorankommen. Insbesondere muss das Urkundserfordernis für Wertpapiere mit Blick auf die Security Token aus dem Weg geräumt werden. Gerade vor dem Hintergrund eines funktionierenden Kapitalmarkts macht es keinen Unterschied, ob es sich um einen Retail-Investor oder um einen institutionellen Investor handelt. Ein gutgläubiger Investor muss davon ausgehen können, ein Finanzinstrument wirksam erworben zu haben, wenn er auf dem Kapitalmarkt investiert. Zurzeit kann ein Investor das nur zu 98 Prozent.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der AfD, Herr König.

Abg. **Jörn König** (AfD): Eine Frage an Herrn Bärligea von BearingPoint. Frau Dr. Siedler hat den Unterschied zwischen Public und Private-DLT bzw. Blockchain angesprochen. Es wird oft unterstellt, dass Public Blockchains für den privaten Marktteilnehmer unkontrollierbar seien. Ist das wirklich so? Wie sehen Möglichkeiten aus, eine gewisse Kontrolle auszuüben?

Können Sie Ihre Möglichkeiten oder Varianten einer Löschung in der Blockchain skizzieren, die mit der Datenschutzgrundverordnung (DSGVO) konform sind?

Vorsitzende **Bettina Stark-Watzinger**: Herr Bärligea für BearingPoint.

Sv **Ralph Bärligea** (BearingPoint GmbH): Frau Dr. Siedler hat das richtig ausgeführt. Die Chancen, die sich aus Public Blockchains ergeben, sollten unbedingt genutzt werden. Ich vergleiche das mit dem Internet. Es hat sich ein allgemein gültiges, öffentlich genutztes Internetprotokoll durchgesetzt. Diese Daten werden auch öffentlich über das Internet übertragen. Selbst der Deutsche Bundestag über-

trägt seine Daten über das Internet. Die Abgeordneten können von überall mittels ihrer Laptops auf die Bundestagsserver zugreifen. Das geschieht jedoch über verschlüsselte VPN-Verbindungen, also über Tunnel. Genau so können Daten auf der Blockchain verschlüsselt werden, wie es schon Herr Prof. Prinz ansprach. Diese Schlüssel haben eine Länge von mindestens 60 Stellen und bestehen aus Buchstaben und Zahlen, die rein zufällig entstehen. Dabei entstehen unendliche Kombinationsmöglichkeiten, die nur gehackt werden können, wenn - wie bei einem Zahlenschloss - alle ausprobiert werden. Die Diskussion, ob das gehackt werden könnte, ist interessant, aber eher hypothetisch.

Wir vertrauen der gleichen Technologie bereits beim Übertragen von Daten über das Internet. Der Unterschied dazu ist, dass die Daten auf der Blockchain dauerhaft gespeichert werden. Zwar gibt es beim Internet eine Vorratsdatenspeicherung, aber die Daten werden nur durchgeleitet. Die DIN-Norm 66398, die sich auf das Löschen und auch auf das mit der Datenschutzgrundverordnung (DSGVO) konforme Löschen bezieht, spricht in diesem Zusammenhang von Transportsystemen.

Es wurde nach den verschiedenen Varianten des Löschens gefragt. Die eine Variante ist das Verschlüsseln mit Vernichtung des Schlüssels. Das ist bei ICOs (Initial Coin Offerings) gängige Praxis. Wenn Tokens nicht zum Ausgabeemissionskurs veräußert werden können, werden die Schlüssel zu solchen Tokens vernichtet, damit sie im Nachhinein nicht veräußert werden können. So wird der Marktpreis stabilisiert. Eine weitere Variante ist das bloße Referenzieren von Daten auf der Blockchain. Die Daten liegen dabei nicht tatsächlich auf der Blockchain, sondern werden als Fingerabdrücke, als perfektes Pendant, gesichert. Die Daten auf der herkömmlichen Datenbank können so nachträglich nicht mehr geändert werden, da sie nicht mehr zu dem Eintrag auf der Blockchain passen würden. Über dieses Verfahren können Daten glaubwürdig referenziert werden.

Die DSGVO sagt ganz klar, dass Daten dann nicht personenbezogen sind, wenn sie sich nicht auf eine natürliche Person zurückführen lassen. Aus meiner Sicht ist eine Referenzierung auf der Blockchain ohne Personenbezug, wenn die Originaldaten der Person gelöscht werden. Das sollte den Marktteilnehmern seitens der Datenschutzbehörden vermittelt werden, damit der Markt sicherer wird und mehr Menschen sich trauen, dieses Verfahren anzuwenden.

Ich sehe noch eine dritte Variante der Löschung, das Zeitscheibenverfahren. Stellen Sie sich zwei Geschäftspartner vor, die Geschäfte machen, welche schon heute in ihren Datenbanken gespeichert sind. Jeder hat einen Knotenpunkt. Die Daten der Geschäfte müssen nach Handelsgesetzbuch und Abgabenordnung zehn Jahre lange aufbewahrt werden. Die Geschäftspartner könnten jedes Jahr eine neue Blockchain beginnen und diese nach Ablauf des Jahres in das Archiv legen und nach zehn Jahren löschen.

Bestimmt werden uns Technik und Innovation damit überraschen, was alles möglich wird. Es kommt am Ende auf die Ausgestaltung der Technik an.

Vorsitzende **Bettina Stark-Watzinger**: Die nächste Frage kommt von der Fraktion der SPD, Herr Dr. Zimmermann.

Abg. **Dr. Jens Zimmermann** (SPD): Ich stelle meine Frage an Herrn Uhde von SAP. Wir haben über viele Details diskutiert. Für mich ist ein fundamentales Thema, wie weit wir technologisch bei der Blockchain sind. Wie sind dazu Ihre Erfahrungen, und wie ist Ihre Einschätzung? Was befindet sich konkret im Realbetrieb? Was sind am Ende nur Konzepte? Welche Knackpunkte sehen Sie momentan?

Wie ist Ihr Eindruck zum Anteil der Blockchain-Technologie – bzw. Abwandlungen im DLT- Bereich – an Ideen und Geschäftsmodellen, von denen Sie sagen, dass sich ein echter Mehrwert gegenüber anderen technischen Alternativen ergibt?

Vorsitzende **Bettina Stark-Watzinger**: Herr Uhde von SAP.

Sv **Thomas Uhde** (SAP SE & Co. KG): Zunächst würde ich unterschreiben, dass ein Unterschied zwischen den Public Blockchains und den private permissioned Blockchains gemacht werden muss. In Public Blockchains ist es fast schon unausweichlich, dass auch anonym teilgenommen werden kann. Daher liegt für viele unserer Unternehmen und viele unserer Kunden der Fokus auf den private permissioned Blockchains, wenn es um eine produktive Anwendung geht. In diesem Bereich ist die Technologie heute schon sehr weit.

Es gibt Fälle, die schon im produktiven Einsatz sind, auch bei unseren Kunden. Zudem gibt es eine Vielzahl von Projekten, die sich in einem sehr seriösen Testbetrieb befinden. Daher erwarte ich, dass es in den nächsten ein, zwei Jahren eine Vielzahl von Fällen geben wird, die zumindest im private permissioned Sektor in einem sehr breiten Feld Anwendung finden werden.

Ich stimme zu, dass es bei den private permissioned Blockchains eher um Prozessoptimierungen im Konsortialkontext zwischen verschiedenen Unternehmen und zwischen verschiedenen Akteuren geht. Gerade, wenn man ein bisschen auf die Finanzmarkthemen, die wir heute beleuchten, schaut, ist es auch aktuell eher eine Dokumentation, bzw. eine Abrechnungshilfe oder ein Austausch von Informationen über Finanzmarktgeschäfte die über andere Kanäle wirklich stattfinden.

Bei den Public Blockchains fällt es mir sehr schwer, eine allgemeingültige Aussage zu treffen, wie weit die Technologie ist. Die eine Technologie gibt es dort eben nicht. Es gibt eine Vielzahl von Blockchain-Technologien im public space. Ich würde meine Einschätzung auf die bekannten und heute diskutierten Beispiele beziehen. Sie sind technologisch in der Lage, die Themen, die wir besprochen haben, abzudecken und abzubilden.

Gleichzeitig sehen wir im Kundendialog, dass es gerade bei größeren Unternehmen noch eine gewisse Zurückhaltung gibt, weil der Rechtsrahmen doch noch relativ unklar ist. Dies gar nicht nur bezogen auf die steuerliche Betrachtung, sondern auch bei Themen wie der DSGVO und den Umgang mit personenbezogenen Daten. Public Blockchains haben durchaus ein sehr hohes Potential, zu Themen wie der Digitalisierung einen essenziellen Beitrag zu liefern und auch ein Katalysator zu sein.

Die zweite Frage betraf den Prozentsatz der Innovationsprojekte in diesem Bereich, der wirklich an den Features der Blockchain-Technologie hängt. Das ist ein sehr hoher Prozentsatz. Ich stimme nicht ganz überein, dass die private permissioned Blockchains einfach nur Datenbanken sind. Ich sehe es eher komplementär dazu, weil es ganz eindeutige Aspekte gibt, wo wir die Funktionalitäten einer Blockchain mit Datenbanken nicht abbilden können. Wir hatten es mehrfach versucht, weil wir aus dem Datenbankgeschäft kommen. Für uns wäre es schön gewesen, wenn es so gewesen wäre, es ist aber leider nicht so. Es ist ein hoher Prozentsatz, der tatsächlich seriös auf der Blockchain-Technologie basiert.

Vorsitzende **Bettina Stark-Watzinger**: Vielen Dank. Die nächste Frage kommt von der CDU/CSU Fraktion, Herr Steiniger, bitte.

Abg. **Johannes Steiniger** (CDU/CSU): Meine Frage geht an die BaFin. Immer wieder wird gefordert, dass man zu einer Kategorisierung der Token kommt. Auch die FDP schlägt dies in ihrem Antrag vor. Können Sie dazu Stellung nehmen, wie Sie das sehen?

Ich würde zweitens Herrn Rübe bitten, dies auch einmal aus der Praxis zu bewerten. Braucht man eine solche Kategorisierung zur Vereinfachung?

Vorsitzende **Bettina Stark-Watzinger**: Wir starten mit Herrn Fußwinkel, BaFin.

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht): Die BaFin ist eine rechtsanwendende Behörde. Das heißt, was für uns und auch für die Adressaten entscheidend ist, sind die gesetzlichen Tatbestände der verschiedenen Aufsichtsgesetze und deren Anwendung durch die BaFin. Bekanntermaßen finden sich die drei Token-Kategorien nicht in den Gesetzen. Was auch sinnvoll ist, da es sich dabei um Hilfsfallgruppen handelt, die den Markt etwas überschaubarer machen. Daher ist das für uns zunächst ein Kommunikationsmittel. Das gilt auch für die Schweizer Kollegen, die gerne angeführt werden, dass sie nach diesen drei Kategorien agieren würden. Sie wenden, genau wie wir, ihre Aufsichtsgesetze an.

Was wir nicht können, ist einen Sachverhalt unter einen nicht bestehenden Tatbestand zu subsumieren – das schafft dann auch keine Rechtssicherheit. Token-Kategorien, die sich in der rechtlichen Beurteilung nicht niederschlagen, zu sehr in den Vordergrund zu stellen, schafft keine Rechtssicherheit, sondern eine Scheinsicherheit. Es hilf allerdings, diese drei Kategorien bei der Orientierung zu benutzen. So haben wir es auch getan und kommuniziert. Es ist ebenso festzuhalten, dass die Sachverhalte sich diesen drei Kategorien nicht eindeutig zuordnen lassen. Würden wir dazu kommen, rein hypothetisch, solche Kategorien zu formalisieren, würde das Innovationen einengen, weil man faktisch Standardisierungen schafft. Wenn die BaFin

auf Grundlage dieser drei Kategorien Entscheidungen treffen könnte, wären diese entweder sehr pauschal und würden dem Einzelnen nicht helfen, oder man schafft faktisch eine Standardisierung, weil hybride Gestaltungsformen so nicht mehr möglich wären. Aus diesem Grund trifft die BaFin viele Einzelfallentscheidungen, um dem Einzelnen die Rechtssicherheit, die er braucht, individuell zu geben.

Abg. **Johannes Steiniger** (CDU/CSU): Wenn ich das richtig sehe, macht es die Aufsicht in der Schweiz so. Können Sie auf das Beispiel ein bisschen näher eingehen? Ist das von der Schweiz eher Marketing, um zu sagen, bei ihnen sei es einfacher? Oder was steckt dahinter? Wäre es dann nicht sinnvoll, so etwas auch bei uns zu machen?

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht): Die Schweiz macht dies nur in der Kommunikation, genau wie wir. Es gibt dieses eine Papier, dessen Verfasser ich kenne, weil wir im behördlichen Austausch stehen. Was die Schweiz definitiv nicht macht, ist in ihrem Aufsichtsrecht de lege lata Kategorien zu bestimmen, die diesen drei Token-Kategorien entsprechen. Zum Teil braucht man sie auch nicht. Ein Security-Token ist ein Wertpapier. Ein Utility-Token ist sehr schwer definierbar, es hat meistens auch Charakteristika der andern beiden Klassen. Das gilt übrigens auch für die meisten Currency-Token. Die Schweizer haben die Kategorisierung also tatsächlich als Hilfsmaßnahme genutzt, um ihre Praxis bei der ganz normalen rechtlichen Beurteilung ein wenig zu strukturieren. So ist auch das Papier der Schweizer zu verstehen, auf das Sie anspielen.

Die BaFin hat das Gleiche mit Hilfe eines Aufsatzes gemacht. Wir haben zwei größere Veröffentlichungen zu diesem Bereich. Das eine ist die stark juristisch orientierte Darstellung zu ICO's vom Februar 2018. Das andere ist ein Artikel in den BaFinPerspektiven, der die drei Token-Kategorien verwendet. Wir haben das bewusst getrennt, um keine Verwirrung zu stiften, dass die Kategorien juristisch formalisiert wären. Sie dienen lediglich zur Strukturierung.

Vorsitzende **Bettina Stark-Watzinger**: Herr Rübe, BOTLabs.

Sv **Ingo Rübe (BOTLabs GmbH):** Wie zuvor vom Blockchain Bundesverband gehört, ist es aus der Praxis heraus für uns als Unternehmen sicherlich das Wichtigste, Rechtssicherheit zu haben.

Wir beginnen oft mit Venture Capital und verwalten das Geld anderer. Wir versuchen, daraus ein gutes Geschäft zu machen. Das bedeutet, dass wir Rechtssicherheit für das brauchen, was wir produzieren. So produzieren wir zum Beispiel einen Utility Token. Der Utility Token ist immer noch relativ unklar gefasst. Der Security Token hingegen ist davon wunderbar abgegrenzt. Bei dem einen braucht man einen Prospekt, bei dem anderen nicht. Der Vorschlag, den wir hier gehört haben, dass man eine freiwillige Prospektpflicht, ein Prospekt-Opt-in für Utility Token schafft, wäre für Firmen, die wohlmeinend sind und Wert schaffen wollen, sicherlich eine gute Möglichkeit, auch um mehr Vertrauen zu schaffen. Denn hierdurch entstünde mehr Rechtssicherheit. Ich sehe eigentlich nur die Unterscheidung zwischen Utility Tokens und Security Tokens, denn Crypto Currencies sind eine Mischform.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der FDP, Herr Schäffler.

Abg. **Frank Schäffler** (FDP): Meine Frage geht an den Blockchain Bundesverband und Herrn Bärligea von BearingPoint: Wie schätzen Sie die steuerlichen Rahmenbedingungen für die Kryptowährungs-Token ein? Was müsste man tun, um mehr Rechtssicherheit in Deutschland zu schaffen?

Vorsitzende **Bettina Stark-Watzinger**: Blockchain Bundesverband, Herr Himmer.

Sv **Klaus Himmer** (Blockchain Bundesverband e. V.): Ich denke, die Frage ist aus mehreren Blickwinkeln zu betrachten und auch zu beantworten. Zum einen aus Investorensicht, zum anderen aus Sicht des Emittenten und nicht zuletzt aus Finanzdienstleistungsperspektive. Ich denke, aus allen drei Blickwinkeln sollten Lösungsansätze gefunden werden, um die größten Unsicherheiten für alle Beteiligten zu klären. Meiner Auffassung nach bestehen aktuell die größten Rechtsunsicherheiten vor allem bei den Privatinvestoren. Im steuerlichen Bereich sind wir leider noch nicht so weit wie im Aufsichtsrecht. Diesbezüglich kann ich der BaFin ein Lob aussprechen.

Es gibt zur steuerlichen Behandlung noch keine Leitlinien. In der Literatur der Verwaltungsanweisungen ist derzeit nur eine Subsumtion der Token

unter die privaten Wirtschaftsgüter zu finden. Wie bereits gehört, haben Token sehr verschiedene rechtliche und auch technische Ausgestaltungen. Deshalb kann diese pauschale Einordnung der Komplexität der Realität nicht gerecht werden. Das mag vielleicht daher kommen, dass zunächst nur über den Bitcoin geredet wurde, einen sogenannten Currency Token. Es sollte auf jeden Fall ein technologieneutraler Ansatz gewählt werden. Es kommt nicht darauf an, dass diese Werte auf der Blockchain als Technologie verwahrt oder transferiert werden, sondern auf die zu Grunde liegenden Werte.

Dieselben Fragen stellen sich letztlich auch bei den institutionellen Investoren, also wenn Token dem steuerlichen Betriebsvermögen zuzurechnen sind. Hier geht es darum, zum Beispiel die Steuerbefreiung, die wir bei Schachtelbeteiligungen, bei der Körperschaftsteuer und im Gewerbesteuerrecht kennen, auch auf Token-basierte Geschäftsmodelle anzuwenden.

Aus Sicht der Emittenten sollte auch der Rechtsfolge bei der Ausgabe unterschiedlicher Token Rechnung getragen und zwischen verschiedenen Konzeptionen differenziert werden. Das kann bei Token, die keine Rechtsansprüche verbriefen, wie zum Beispiel den Currency Token, recht einfach sein. Auch Security Token sind steuerrechtlich einfach zu handhaben. Dabei muss zwischen Eigenkapital und Fremdkapital unterschieden werden. Dazu gibt es den sogenannten Genussrechtstest, der auf keiner Legaldefinition beruht, sondern aus der Rechtsprechung und aus der Rechtspraxis Möglichkeiten vorsieht, um eine Einordnung vorzunehmen.

Bei den Utility Token, die einen Rechtsanspruch gegenüber den Emittenten verbriefen, aber keine Wertpapiere sind, verbleiben wichtige Fragen, die noch ungeklärt sind. Letztlich geht es darum, ob der gesamte Finanzierungserlös sofort mit Ertragsbesteuerung belastet wird oder ganz im Gegenteil überhaupt nicht. Um mehr Sicherheit zu schaffen, muss diese Frage geklärt werden. Die steuerliche Behandlung von Token sollte technologieneutral erfolgen. Wir haben einen solchen Ansatz in unserer Stellungnahme vorgeschlagen.

Vorsitzende **Bettina Stark-Watzinger**: Herr Bärligea, für BearingPoint.

Sv **Ralph Bärligea** (BearingPoint GmbH): Herr Fußwinkel von der BaFin hat vorhin schon richtig ausgeführt, dass diese Klassifizierung in Utility und Security Token eine Hilfskonstruktion ist. Das heißt, es gibt immer auch hybride Formen. Von der Klassifizierung hängt natürlich auch die Besteuerung ab. Zum Beispiel sind Payment Token nach einem Jahr Haltefrist steuerfrei. Gewinnausschüttende oder zinsaus-schüttende Token nach zehn Jahren. Das ist teilweise noch unklar. Ich habe Ihnen in meiner schriftlichen Stellungnahme ein Fallbeispiel genannt, auch wenn ich kein Steuerexperte bin. Wenn also zum Beispiel eine Firma, die Rechenleistung beziehen will, dafür einen bestimmten Token kauft, der sich dazu eignet und ihn dauerhaft hält, wäre dieser dem Anlagevermögen zuzurechnen. Der Token könnte dann mit der entsprechenden steuerlichen Maßgeblichkeit in der Bilanz zum Anschaffungswert geführt werden. Nutzt die Firma aber den Token nur als Zahlungsmittel, als Payment Token, dann würde er nach dem Niederstwertprinzip dem kurzfristigen Umlaufvermögen zugerechnet. Ich pflichte Herrn Fußwinkel bei, dass die Aussage für den Einzelfall getroffen werden muss, man aber durchaus diese Hilfskategorien nutzen kann.

Vorsitzende **Bettina Stark-Watzinger**: Vielen Dank. Für die Fraktion DIE LINKE., Herr De Masi.

Abg. **Fabio De Masi** (DIE LINKE.): Meine Frage richtet sich an Frau Dr. Zoppei. Frau Gehra hat ausgeführt, dass es auch bei der Geldwäschebekämpfung Potentiale gibt, die sich aus der Blockchain-Technologie ergeben. Beispielsweise die Nachvollziehbarkeit der Transaktionshistorien, die öffentliche Einsehbarkeit der Blockchain und anderes. Wie bewerten Sie das? Halten Sie bei den Aufsichtsinstitutionen in Deutschland oder in der EU dieses Potential für ausgeschöpft?

Vorsitzende **Bettina Stark-Watzinger**: Frau Dr. Zoppei, mafianeindanke.

Sve **Dr. Verena Zoppei** (mafianeindanke e. V.): FinTech-, RegTech-Firmen und Startups, die Risikomanagementdienstleistungen für Finanzinstitute anbieten, wenden schon heute die DL-Technologie an, um Big Data zu analysieren. Die Technologie eignet sich für die Verwaltung, für die sichere Aufbewahrung und den Austausch von Big Data. Damit Deutschland von dem Potential dieser Technologie für die Geldwäscheprävention profitieren kann,

sollten zukünftige Rahmenbedingungen geschaffen werden. Ich werde drei konkrete Anwendungen nennen: Im Hinblick auf Geldwäscheprävention im Finanzsektor können die DL-Technologien für neue Kundenanwendungen eingesetzt werden, um zum Beispiel einen schnellen Austausch von Informationen über die wirtschaftlich Berechtigten oder die Transaktionsgeschichte zwischen verschiedenen Finanzinstituten zu erlauben. Immer wieder sind große europäische und deutsche Banken in Geldwäscheskandale verwickelt, bei denen sich Schwierigkeiten ergeben, eine fiktive Kontrolle über die Beziehungen zwischen den Banken zum Zweck der Geldwäscheprävention zu erlangen. Besonders im Hinblick auf solche Hindernisse sind DL-Technologien dafür geeignet, einen besseren Informationsaustausch zwischen respondent und correspondent zu ermöglichen. Zweitens, verdächtige Transaktionen müssen unter dem Geldwäschegesetz verpflichtend an die Zentralstelle für Finanztransaktionsuntersuchungen gemeldet werden. Derzeit verwenden viele Finanzinstitute eine automatisiertes Verfahren für die Meldung solcher verdächtiger Transaktionen, wie zum Beispiel häufige Überweisungen knapp unter der Meldepflicht. Diese Praxis könnte zum Beispiel mit Smart Contracts ergänzt werden. Dafür muss die Bundesregierung Rahmenbedingungen schaffen. Drittens, die Zentralität des Ledgers hätte das Potential, den Zugang zu den relevanten Informationen für Strafverfolgungsbehörden zu ermöglichen, ohne dass die Daten aus den verschiedenen Finanzinstituten gesammelt werden müssten. Als Ergebnis einer Meldung kann dann ein Ermittlungsverfahren wegen Geldwäsche eingeleitet werden. In Bezug auf diese Verwendung von Beweisen in digitaler Form, eignen sich DL-Technologien durch die sogenannte ASH-Funktion für die Wahrung der Integrität.

Schließlich ist die Notwendigkeit zu unterstreichen – wie dies auch Punkt 4 des Antrages hervorhebt –, Daten zur Blockchaintechnologie zu erheben. Nicht nur für allgemeine Zwecke, sondern auch um eine objektive Risikobewertung mit Bezug auf Geldwäsche, Terrorismusfinanzierung und die Prävention solcher Delikte zu ermöglichen.

Vorsitzende **Bettina Stark-Watzinger**: Herr De Masi, bitte.

Abg. **Fabio De Masi** (DIE LINKE.): Frage an Frau Otto: Wie bewerten Sie die im Antrag geforderte Abschaffung der Urkundserfordernisse zur Einführung eines qualifizierten digitalen Registers? Gibt es Ihrer Meinung nach verbraucherschutzrechtliche Bedenken? Wäre dies mit dem BSchuWG für öffentliche Schuldtitel vereinbar?

Vorsitzende **Bettina Stark-Watzinger**: Frau Otto, COT Legal.

Sve **Claudia Otto** (COT Legal): In jedem Fall kann man das Bedürfnis für das elektronische Wertpapier bestätigen. Doch die Papierform bietet mit Stand heute noch immer den besten Schutz. Das rein elektronische Wertpapier ist ohne weiteres unbegrenzt vervielfältigbar und veränderbar – ein PDF-Dokument und ein Papier mit Originalsiegel und Unterschriften in einem Banktresor sind das hingegen nicht. Risiken und Chancen müssen umfassend gegeneinander abgewogen werden. Kann ein gleichwertiger Schutz beim elektronischen Wertpapier hergestellt werden, kann es dem Wertpapier gleichgestellt werden.

Das BSchuWG enthält Regelungen, die Parallelen zur Blockchain-Technologie aufweisen. Von daher ist es nachvollziehbar, dass man über entsprechende Lösungen nachdenkt. Wobei ich aber darauf hinweisen möchte, dass öffentlicher Glaube, wie etwa im Bundesschuldbuch, nicht durch Gläubigereingaben entstehen kann. Eine inhaltliche sowie rechtliche Prüfung muss jedem Eintrag vorangehen, und wenn Gläubiger keine direkten Einträge vornehmen, braucht man auch keine Blockchain. Eine Dokumentation von öffentlichem Glauben darf nicht von technischen Rahmenbedingungen der einzelnen Gläubiger abhängen. Wenn auf deren Rechnern eine kompromittierte Blockchain-Kopie vorhanden wäre, dann könnte dies beim nächsten Synchronisierungsvorgang auch das ganze Netzwerk kompromittieren.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der CDU/CSU, Herr Hauer.

Abg. **Matthias Hauer** (CDU/CSU): Meine Fragen richten sich an die Deutsche Börse AG. Ich würde gern aus Ihrer Sicht wissen, welche Relevanz, Vor- und Nachteile sich aus der Blockchain-Technologie für den Kapitalmarkt ergeben. Bitte unterschieden Sie nach öffentlicher und privater Blockchain. Bitte gehen Sie kurz auf den vom BMF im Eckpunktepapier gemachten Vorschlag ein.

Wie ist die Position der Deutschen Börse dazu? Welche Art von Blockchain-Instrumenten, Utility Token oder Security Token sehen Sie als geeignetes Finanzierungsinstrument für den Mittelstand?

Vorsitzende **Bettina Stark-Watzinger**: Herr Hachmeister, Deutsche Börse.

Sv **Jens Hachmeister** (Deutsche Börse AG): Bezogen auf die Nutzung der DL-Technologie ist bereits eine Menge ausgeführt worden. Wie Herr Fußwinkel sagte, sind eine Verringerung der Transaktionskosten sowie auch der Einsatz als Basistechnologie für den Kapitalmarkt und als Refinanzierungsinstrument wichtige Themen. Für uns als Marktplatzbetreiber tritt ein weiterer Aspekt in den Vordergrund: Inwiefern können Token dazu dienen, Finanzinstrumente mit Intelligenz aufzuladen, wenn man sie weiter entmaterialisiert? Das heißt, das asset servicing von Finanzinstrumenten könnte potentiell automatisch in das Instrument selbst eingefügt werden. Das wäre ein weiterer Effizienzgewinn.

Auf der anderen Seite könnte die Abbildung von Vermögensgegenständen in Token – dabei rede ich nicht nur von Wertpapieren – es ermöglichen, das Spektrum zugänglicher Vermögenswerte für Investoren deutlich zu verbreitern. Das heißt, die Entmaterialisierung bietet bezogen auf Wertpapiere noch weitere und größere Möglichkeiten, als wir sie heute in der Nutzung sehen.

Zum zweiten Punkt der öffentlichen und privaten Blockchains: Die Deutschen Börse baut, betreibt und belädt in ihrem Geschäftsmodell Kapitalmarktinfrastruktur in einem regulierten und definierten Rahmen. Natürlich tut sie das mit Hilfe von Technologie. Nur dann können wir transparente und integre Märkte sicherstellen sowie abbilden, die dann einen entsprechenden Investorenschutz und eine gute Rechtssicherheit für alle Marktakteure garantieren. Aus unserer Sicht ist das Thema einer vertrauenswürdigen Marktinfrastruktur das Zentrum aller Überlegungen. In ihrem Aufbau beginnt die vertrauenswürdige Marktinfrastruktur häufig ganz unten mit den Netzwerken, die wir betreiben wollen und müssen. Diese Netzwerke sind kontrolliert, also der Zugang zu ihnen ist reglementiert. Für Börsen- oder Kapitalmarktinfrastrukturanbieter spielt nicht nur eine Rolle, Märkte und Marktstruktur zu definieren sondern auch Zugänge und Regelwerke. Außerdem ist zu definieren, wie auf Märkten agiert wird und was auf den Märkten gehandelt wird. Schließlich muss man dies auch begleiten und überwachen.

Vor diesem Hintergrund bieten vor allem private und permissoned Blockchains Anwendungspotentiale für die Deutsche Börse. Herr Uhde hat es gesagt: Wir reden über industrielle Anwendungen in der Finanzindustrie –einem Industriezweig, der hoch reguliert ist.

Zum Eckpunktepapier: Die Entmaterialisierung der Wertpapiere und der Rahmen, der darum geschaffen werden soll, gehen als nächste Schritte aus unserer Sicht in die richtige Richtung.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion BÜNDNIS 90/DIE GRÜNEN, Herr Dr. Bayaz.

Abg. **Dr. Danyal Bayaz** (BÜNDNIS 90/DIE GRÜNEN): Ich würde gerne Herrn Fries drei Fragen stellen. Zunächst mit Ihrem Blick von außen: Bitte bewerten Sie die Finanzaufsicht der Bundesrepublik Deutschland bezüglich der Kompetenzen zu diesem Thema in qualitativer und quantitativer Hinsicht. Können Sie ganz gezielt auf die Prüfkompetenzen eingehen und darüber hinaus auf das Thema Datenschutz und DSGVO? Inwieweit sehen Sie Anpassungsbedarf, wenn wir über eine Rechtsdefinition personenbezogener Daten sprechen, für die keine Lockerung der DSGVO notwendig ist, die aber trotzdem eine Zentralisierung der Verwaltung einer Blockchain ermöglicht?

Vorsitzende **Bettina Stark-Watzinger**: Herr Dr. Fries für die Ludwig-Maximilians-Universität München.

Sv **Dr. Martin Fries** (Ludwig-Maximilians-Universität München): Zur Qualifikation der BaFin: Ich höre nur Lob und eine hohe Meinung von der BaFin. Auch im Bereich der Blockchain. Worüber wir sehr dankbar sein dürfen. DLT ist eine junge Technologie. Damit ist es ganz natürlich, dass zu diesem Zeitpunkt noch nicht die halbe BaFin an diesem Thema sitzt. Mit Blick darauf, dass wir heute mit sehr unterschiedlichen Auffassungen über diese Technologie diskutieren, glaube ich, dass es nicht schadet, wenn die qualitativ schon gute Befassung der BaFin mit diesem Thema quantitativ noch aufgestockt wird.

Wenn es um die Standortfaktoren in der Zukunft geht – niemand kann die Zukunft ganz sicher voraus sehen –, tun wir gut daran, die BaFin im

Bereich DLT entsprechend auszustatten. Das sage ich auch mit Blick auf diejenigen, die individuell mit guten Gründen der Blockchain-Technologie kritisch gegenüber stehen. Es gibt ja schon einen Rechtsrahmen, der vielleicht nicht an allen Ecken und Enden ausreichend ist, der aber doch an vielen Stellen die Blockchain-Technologie erfasst. Wenn man dieses Recht anwenden möchte, dann ist die BaFin eine der ersten, die zu dieser Rechtsanwendung berufen ist. Man sollte die BaFin entsprechend ausstatten, um das bestehende Recht durchzusetzen.

Ihre zweite Frage bezog sich auf den Datenschutz. Auch da haben wir schon einiges gehört, dem ich insgesamt eigentlich beipflichten möchte. Ich glaube, dass wir im Bereich des Datenschutzrechtes Unsicherheit von zwei Seiten erkennen können. Zum einen von Seiten der Technologie. Wir sprechen hier insbesondere über Artikel 17 DSGVO. Darin geht es um das Recht, vergessen zu werden. Man muss das Recht des Individuums sicherstellen, personenbezogene Daten von sich löschen zu lassen. Es ist die Frage, was die Blockchain leisten kann; wie viele Löschungen sie vornehmen kann. Manche sagen, die Blockchain kann entsprechende Löschungen nicht sicherstellen. Sie sei quasi das ultimative Gedächtnis. Andere sagen, dass man die kritischen Daten auf eine Art vorgelagerten Account auslagern könnte. Wenn man diesen löschen würde, wären auch die personenbezogenen Daten entfernt. Es besteht in dieser Frage Unsicherheit in Bezug auf die DL-Technologie. Diese müssen wir erst einmal klären. Wenn bestimmte Daten bisher noch nicht löschbar sind, dann ist es aber vielleicht möglich, diese Technologie datenschutzkonform weiter zu entwickeln.

Zum anderen sehe ich auch eine gewisse Rechtsunsicherheit im Bereich der DSGVO. Im Grundsatz finde ich es gut, dass wir jetzt einen noch wirksameren Datenschutz haben als zuvor. Gleichzeitig erfährt man aus der Praxis, dass es noch viel Rechtsunsicherheit gibt. Was sind personenbezogene Daten? Was ist, wenn der Personenbezug weg ist, man ihn aber irgendwann in der Zukunft wieder herstellen kann? Sind das dann trotzdem personenbezogene Daten? Im Idealfall würde der europäische Gesetzgeber versuchen, die DSGVO weiter zu konkretisieren. Was man auch an vielen anderen Stellen tun muss und was ein paar Jahre in Anspruch nimmt. Ob man dann tatsächlich für die Blockchain-Technologie den Datenschutz ein Stück zurück nimmt, das ist dann eine rechtspolitische Frage, der ich mich hier enthalte.

Vorsitzende **Bettina Stark-Watzinger**: Die Fraktion der SPD, Herr Hakverdi.

Abg. **Metin Hakverdi** (SPD): Zunächst eine Frage an die Bundesbank, Herr Dr. Diehl. Eine Frage zur Regulierung und zur Aufsicht. Welche Herausforderungen sehen Sie generell bei der Blockchain-Technologie? Welche Rolle spielt eventuell Ihr Haus bei der Regulierung?

Danach eine Frage an SAP, Herrn Uhde: Es wird oft gesagt, dass die Blockchain-Technologie Intermediäre ersetzen oder zumindest ergänzen kann. Erstens, geht das überhaupt? Muss ich mir das als Ergänzung oder als Alternativmodell vorstellen? Zweitens, was sind die Vor- und Nachteile aus Ihrer heutigen Sicht? Wie weit ist man zu diesem Zeitpunkt?

Vorsitzende **Bettina Stark-Watzinger**: Dr. Diehl, Deutsche Bundesbank.

Sv **Dr. Martin Diehl** (Deutsche Bundesbank): Die große Herausforderung für die Zukunft ist, die Technologieneutralität da herzustellen, wo sie möglicherweise nicht gegeben ist. Ich sage möglicherweise, weil vieles, was dort an Meinungen kursiert, meines Erachtens nicht durch die Realität gedeckt ist. Zum Beispiel, wenn Token emittiert werden. Eine allgemeine Entscheidung dafür zu fordern, trifft nicht den Kern. Denn diese Token werden sehr individuell und sehr spezifisch emittiert – unter ganz individuellen Bedingungen. Logischerweise muss man als Regulierer dann eine Einzelfallentscheidung treffen. Ob das durch die BaFin oder durch die Bewertung in der aufsichtsrechtlichen Praxis durch die Bundesbank, die die operative Aufsicht bei den Banken innehat, stattfindet, spielt dabei keine Rolle.

Die Weiterentwicklung der Aufsicht wird noch auf vielen Feldern betrieben werden. Wir sind als Bundesbank bei der Institutsaufsicht tätig, sowohl was die Unterlegung von Risiken durch Kapital betrifft als auch was das Risikomanagement der Institute betrifft. Das ist bisher immer noch ein Nischenphänomen – sowohl die Investition in Token, die Hinterlegung von Token als Sicherheit für Kredite als auch die Nutzung der Blockchain durch Institute. Es ist noch ein sehr kleines Thema. Wir haben alle

Mitarbeiter mit dem Verständnis geschult, das wir bisher aufgebaut haben. Andere Gremien – internationale Gremien – werden das weiter entwickeln müssen. Wie viel Kapital müssen wir hinterlegen, wie volatil sind die Märkte wirklich? Daran arbeiten wir zum Beispiel zusammen mit unseren Partnern im Baseler Ausschuss.

Dem Vorschlag zur Technologieneutralität kann ich mich nur anschließen. Auch dem Vorschlag von Herrn Hachmeister von der Deutschen Börse, im Bereich der Anleihen einen Token zu schaffen, der rechtssicher übertragen werden kann. Das gleiche gilt für die Forderung, dass das Wertpapier nicht mehr an die Papierform gebunden sein soll. Das ist sicher der richtige Weg. Im Aktienrecht fehlt noch, dass Token als Katalysator für die Digitalisierung insgesamt dienen und nicht nur für die DLT. Das soll anschließend kommen und wird etwas komplizierter werden, aber wir müssen es ermöglichen. Wenn wir dabei technologieneutral wären, wären wir ein großes Stück weiter.

Vorsitzende **Bettina Stark-Watzinger**: Herr Uhde, SAP.

Sv **Thomas Uhde** (SAP SE & Co. KG): Intermediäre zu ersetzen, ist für mich kein technologisches, sondern eher ein organisatorisches Thema. Rein technologisch gesehen, ist es im Kern der Blockchain bzw. der DLT enthalten, dass man niemanden benötigt, der eine solche Plattform betreibt. Das ist eines der Grundversprechen dieser Technologie. Viel spannender wird es, wenn man die organisatorischen Ebenen ansieht und sich fragt, wozu man bisher Intermediäre gebraucht hat, nämlich um verschiedenste Akteure an einen Tisch zu bekommen. Beispielsweise bei einem einfachen Wertetransfer, bei dem ich jemandem Geld sende, welches dann nicht mehr mir gehört, sondern dem Anderen, ist es relativ einfach, sich auf Regularien zu einigen. Wenn man aber komplexere Prozesse wie beispielsweise Smart Contracts betrachtet, ist das viel schwieriger.

Spannenderweise sehen wir das bei allen Blockchains, gerade aber auch bei private permissioned Blockchains. Wobei diesbezüglich kein Unterschied zwischen public und private permissioned Blockchains besteht. Wie treffen sich denn die Akteure einer private permissioned-Blockchain? Treffen sie sich auf der Straße und unterhalten sich darüber, jetzt etwas zusammen zu machen? Es gibt niemanden, der sie an einen Tisch bringt, wenn es keinen Intermediär gibt. Daher gibt es aktuell organisatorisch häufig noch Intermediäre, technologisch aber nicht mehr.

Vorsitzende **Bettina Stark-Watzinger**: Die Fraktion der CDU/CSU, Herr Steiniger.

Abg. **Johannes Steiniger** (CDU/CSU): Heute geht es uns darum, noch mehr darüber zu erfahren, was später in einer Blockchain-Strategie stehen soll. Wir haben einiges zum Thema Rechtssicherheit, aber auch zur Durchsetzung des Rechtsrahmens gehört. Spannend fand ich das Thema Forschungsexzellenz. Lassen Sie uns doch symbolisch einige Lehrstühle schaffen, um ein Zeichen in Richtung Szene zu setzen. Eine weitere interessante Frage wäre, welche konkreten Projekte die Bundesregierung, jeweils in den eigenen Ministerien, umsetzen könnte. Ich möchte Herrn Rübe von BOTLabs als Vertreter aus der Praxis fragen, in welchen Ministerien oder in welchen Bereichen man sich konkrete Projekte vorstellen könnte? In welchen Bereichen könnte die Politik hier voran gehen?

Vorsitzende **Bettina Stark-Watzinger**: Herr Rübe von BOTLabs.

Sv **Ingo Rübe** (BOTLabs GmbH): Wir haben in den letzten Jahren diverse Ministerien von innen kennen gelernt und haben dort über Pilotprojekte gesprochen. Wir haben auch mit dem Landwirtschaftsministerium über eine dezentralisierte Lebensmittelinhaltsstoffe-Datenbank nachgedacht, die man auf einer Public-Blockchain gut realisieren könnte. Wir haben auch mit dem Wirtschaftsministerium geredet. Wir sehen viele potentielle Projekte, auch im Finanzministerium.

Wir haben kurz mit dem Ministerium für Entwicklung geredet, wo es auch einige Punkte gibt. Das betrifft zumeist das Thema der Intermediäre. Ich möchte ein bisschen widersprechen. Ich glaube, die Technologie hat durchaus Potential, Intermediäre überflüssig zu machen. Wir sehen insbesondere im Internet zurzeit eine sehr starke Verklumpung von Intermediären und eine Monopolisierung, die nicht nur für das Internet, sondern zum Beispiel auch für die europäische Wirtschaft sehr unerfreulich sind. Wir haben kaum eine Möglichkeit, gegen Facebook oder Google anzugehen. Wir versuchen es mit rechtlichen Mitteln, das Problem ist aber ein technologisches Problem. Als Beispiel: Die Firma Uber

stellt eine Plattform bereit. Wenn auf dieser Plattform viele Fahrer sind, wird das auch attraktiver für die Fahrgäste. Gibt es viele Fahrgäste, ist es umso attraktiver für die Fahrer. Auf diese Weise bildet sich ein Monopol. Das ist ein Problem, das wir zurzeit im Internet haben.

Das Problem kann wie folgt angegangen werden: Der Intermediär, als Datensammler, stellt kein amerikanisches Unternehmen mehr dar, die Datensammlung wird veröffentlicht und anschließend in eine Blockchain oder eine andere DLT-Technologie überführt. Was den großen Vorteil hat, dass man ein Level-Playing-Field produziert. Die Daten stehen dann allen potentiellen Marktteilnehmern zur Verfügung, und jemand anderes könnte ein besseres Uber bereitstellen. Das ist ein großer Vorteil, den die Blockchain, insbesondere die permissioned Blockchain, bietet. Das nennen wir Web 3.0, also die nächste Iterationsstufe des Internets.

Ich wünsche mir Anstöße aus den Bereichen der Ministerien, der Regierung und der Politik, die das weiter nach vorne bringen. Das würde die deutsche bzw. die europäische Wirtschaft massiv stärken. Man sollte hierzu Projekte anstoßen. Ich denke die gesamte Blockchain-Szene steht bereit, um solche Dinge zu diskutieren. Wir würden in diesem Bereich eine wirklich große Wirkung erzielen. Es ist schön, über kleine Projekte wie Lebensmittelinhaltsstoffe-Datenbanken zu reden. Dass Deutschland und Europa sich den großen Herausforderungen in dieser Frage stellen, sehe ich ehrlicher Weise noch nicht. Vielleicht ist es an mir vorbei gegangen, aber ich wünsche mir in diesem Bereich mehr.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der AfD, Herr König.

Abg. **Jörn König** (AfD): Meine Frage geht an den Blockchain Bundesverband, Herrn Klaus Himmer. Wie ist Ihre Meinung zur Besteuerung? Wie sollte man die Besteuerung eventuell gestalten? Nach dem First In, First Out (FIFO) oder dem Last In, Last Out. Wie sollte man aus Ihrer Sicht forks behandeln, so dass es für den Privatnutzer praktikabel ist?

Vorsitzende **Bettina Stark-Watzinger**: Bundesverband Blockchain, Herr Himmer.

Sv **Klaus Himmer** (Blockchain Bundesverband e. V.): Ich habe versucht, das bereits darzustellen: Alle Blockchain-basierten Vermögenswerte werden zumindest gedanklich in einen Topf geworfen. Deshalb entsteht die Frage überhaupt: FIFO oder etwas anderes? Wir haben hier einen Bezug auf § 23 EStG, der die privaten Wirtschaftsgüter zum Gegenstand hat. Man muss bei dieser Fragestellung doppelt differenzieren. Nämlich einmal zwischen privaten und institutionellen Anlegern, aber auch wieder aus Sicht der Token-Klassifizierung. Wenn es sich tatsächlich um Security Token im steuerlichen Sinne handelt, also um Finanzinstrumente im steuerlichen Sinne, dann gilt das Abgeltungssteuerregime und nicht mehr § 23 EStG. Entsprechend kommen wir über § 20 EStG in Verbindung mit dem Abgeltungssteuererlass an dieser Stelle schon obligatorisch in das FIFO-Verfahren. Dieses ist nach dem Abgeltungssteuererlass depotgetrennt vorzunehmen. Also für jedes Depot einzeln. So haben zum Beispiel die Token, die ich bei der Commerzbank halte, eine eigene FIFO-Kette und diejenigen, die ich bei der Deutschen Bank halte, auch.

Liegt kein steuerlicher Security-Token vor, aber ein Token, der steuerlich als Fremdwährung klassifiziert wird, so sind wir dem Gesetz nach ebenfalls beim FIFO-Verfahren. Fremdwährung ist dabei so definiert, dass irgendein Staat der Welt diesen Token als gesetzliches Zahlungsmittel anerkannt haben muss. Wenn auch nicht leicht zu finden, gibt es aber zum Beispiel den venezolanischen Petro. Dieser ist bedauerlicherweise nach der Gesetzesbegründung wiederum depotübergreifend anzuwenden. Das stand damals in der Gesetzesbegründung der Unternehmenssteuerreform 2008. Wenn ich also Petro bei der Deutschen Bank und bei der Commerzbank halte, müsste ich sie zusammen in einen Topf werfen und eine FIFO-Kette bilden.

Meines Erachtens nach ist aber eine depotgetrennte Anwendung von FIFO die einzige gesetzessystematische und sinnvolle Gangart, da diese das einzige Verbrauchsfolgeverfahren ist, das das deutsche Steuerrecht bei gleichartigen Sachverhalten kennt. Dann käme es zu keiner unterschiedlichen Behandlung vergleichbarer Einkunftsarten. Dieser Auffassung folgen auch erste Stimmen aus der Finanzverwaltung, wie man dem Erlass des Finanzsenators von Hamburg entnehmen kann. Die Depottrennung ist meines Erachtens auch aus dogmatischer, teleologischer und praktischer Sicht die einzig zutref-

fende Behandlung. Denn dieses Bewertungsvereinfachungsverfahren ist wie der Name schon sagt, eine Bewertungsvereinfachung.

Es gibt in § 23 EStG das overriding principle des Einzelbewertungsgrundsatzes wie im Handelsrecht. Wenn ich einen Token aus einem Depot verkaufe, zum Beispiel bei der Commerzbank, dann kann ich ganz genau sagen, dass ich einen Token verkaufe, der von der Commerzbank kommt. Das Bewertungsregime sorgt also nicht für zusätzliche Komplexität. Dementsprechend ist hier dem overriding principle des Einzelbewertungsgrundsatzes Vorrang einzuräumen.

Zusammenzufassend ist zu sagen, dass für die Token, die keine Fremdwährung und auch keine Securities im steuerlichen Sinne sind, die Frage der steuerlichen Behandlung gesetzlich nicht geregelt ist. Ich habe ausgeführt, dass ich hier empfehlen würde, ein depotgetrenntes FIFO anzuwenden.

Abschließend kurz noch etwas zu den forks: Hier würde ich mich der herrschenden Literaturmeinungen anschließen. Hard forks sind demnach nach der „Fußstapfentheorie“ zu behandeln. Sie stellen also zunächst einen ertragssteuerneutralen Vorgang dar, wie eine Art Wertaufspaltung. Die historischen Anschaffungskosten sind auf die zwei danach bestehenden Assets aufzuteilen. Hierfür ist die Gesamtwertmethode anzuwenden, wie das auch in der Literatur aktuell die herrschende Meinung ist. Aus ökonomischer und gesetzessystematischer Sicht ist das am zutreffendsten und sorgt auch in der Praxis für eine gangbare Lösung. Viele hard forks bekommt der Rechtsanwender gar nicht mit. Wenn man also nach dem gerade dargestellten Prinzip vorgeht, könnte man diese auch gesetzessystematisch richtig erfassen.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der SPD, Herr Binding.

Abg. **Lothar Binding (Heidelberg)** (SPD): Ich habe eine Frage an Herrn Fußwinkel und an Herrn Dr. Diehl bezüglich der Bemerkung von Herrn Hachmeister, der vorhin gesagt hat, dass das Spektrum an Vermögenswerten durch die derzeit diskutierte Technologie verbreitert werden könnte. Das kann einen hoffen oder fürchten lassen. Die BaFin hat 2017 vor der Nutzung von Initial Coin Offerings (ICOs) gewarnt. Auch Bitcoins oder Kryptowährungen dienen, so ist jedenfalls das Klischee, im Wesentlichen der Spekulation. Mich würde interessieren, was wir unter diesen Gesichtspunkten besonders bei der Förderung von Blockchain-Technologien beachten müssen?

Vorsitzende **Bettina Stark-Watzinger**: Herr Fußwinkel für die BaFin.

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)): Das ist eine interessante Frage. Es ist wichtig, einen angemessenen Ausgleich zwischen den Risiken, vor denen wir schon gewarnt haben, und dem hohen Potential, das es durchaus für verschiedene technologische Anwendungen gibt, zu finden. Damit man nicht in eine Art „Innovation Bias“ verfällt und aufgrund der technologischen Eigenschaften einer bestimmten Technologie Vorteile gewährt, die den Risiken aber nicht gerecht wird.

Die Warnung der BaFin erfolgte zwei Tage vor der Abmahnung der europäischen Aufsichtsbehörden. Wir bringen uns im Hinblick auf die adressierten Risiken auch im internationalen Kontext ein. Die BaFin ist der Ansicht, dass Alleingänge hier wenig hilfreich sind, da es nur wieder das Prinzip des Level-Playing-Fields gefährdet. Man sollte einen überlegten Ansatz machen und sich ansehen, was von der Regulierung heute schon erfasst wird und was durch die Umsetzung der Geldwäscherichtlinie, durch das Eckpunktepapier und die geplanten Regulierungsmaßnahmen zusätzlich erfasst wird. Dann kann man sich fragen, was möglicherweise noch an Regulierungsbedarf übrig bleibt.

Vorsitzende **Bettina Stark-Watzinger**: Herr Dr. Diehl, Deutsche Bundesbank.

Sv **Dr. Martin Diehl** (Deutsche Bundesbank): Ich komme direkt zum zweiten Teil. Auch die Bundesbank hat wiederholt vor ICOs und vor Investitionen in Bitcoins gewarnt. Diesbezüglich deckt sich unsere Meinung. Wir tauschen uns eng aus. Aufgrund der extrem schwankenden Werte und der fehlenden Basis gibt es so viele Spekulationen. Üblicherweise haben die meisten Krypto-Assets, wie Bitcoin usw. keinen intrinsischen Nutzen. Anders ist es bei den echten Utility Coins, die das Recht verbriefen, eine Softwareleistung, eine Speichermöglichkeit etc. kaufen zu können. Diese haben einen kleinen Nutzen. Das ist ähnlich einem Chip, wie man ihn auf dem Jahrmarkt kaufen kann, um damit Autoscooter fahren zu können. Hier können Sie nun etwas Digitales nutzen und haben

einen kleinen intrinsischen Nutzen. Die meisten Coins oder Token haben das nicht, deswegen schwankt der Wert extrem. Deshalb setzt auch die Branche, zumindest aus unserer Beobachtung, zunehmend auf sogenannte Stable Coins, da sie erkannt hat, dass etwas, was als Wertaustauschmedium und vor allen Dingen auch als Wertaufbewahrungsmedium genutzt werden soll, stabil sein muss. Die Stable Coins, bei denen es verschiedene Varianten gibt, sind in der gängigsten Variante mit einer echten Währung hinterlegt, meistens mit dem US-Dollar oder dem Euro. Bei einer anderen Variante wird versucht, die Angebotsmenge so zu steuern, dass der Wert des Coins stabil ist. Dort gibt es aus unserer Sicht bisher kein gangbares Verfahren. Die dominante Form ist diejenige, die den Coin mit einer Währung hinterlegt. Dann ist es allerdings nur ein „Abziehbild“ einer echten Währung, die Stabilität verspricht.

Wir finden die ganze Debatte etwas überhöht. Wir würden uns gerne viel stärker auf die Technologie konzentrieren. Wir wissen, dass wir zum Bezahlen in der Technologie Coins brauchen. Deswegen habe ich eben auch für Token plädiert. Wir brauchen Token, um die Digitalisierung in der Wirtschaft zu befeuern. Wir glauben, dass es in aller Regel auch ausreicht, wenn man zum Beispiel den digitalen Euro, ich spreche von Geschäftsbankengeld, auf Blockchains bringt, und zwar auf geschlossene Blockchains aus den Gründen, die einige schon ausgeführt haben. Insbesondere in den Bereichen, die mit Governance zu tun haben, werden nur geschlossene Blockchains tragfähig sein.

Vorsitzende **Bettina Stark-Watzinger**: Für die CDU/CSU-Fraktion, Herr Hauer.

Abg. **Matthias Hauer** (CDU/CSU): Ich würde den Blockchain-Bundesverband zu dem gerade genannten Thema bitten, Stellung zu nehmen, da ich ein Kopfschütteln bei Ihnen wahrgenommen habe. Vielleicht können Sie noch etwas aus Ihrer Sicht hinzusteuern?

Vielleicht können Sie uns aus ihrer Sicht beantworten, welche Anwendungsbereiche bei der Blockchain-Technologie Sinn machen und welche nicht?

Vorsitzende **Bettina Stark-Watzinger**: Blockchain-Bundesverband, Herr Resas.

Sv **Daniel Resas** (Blockchain Bundesverband e. V.): Bezüglich des Kopfschüttelns ist sicherlich der falsche Eindruck entstanden. Herr Diehl wird mir sicher die schnippische Bemerkung nachsehen, dass es interessant ist, wenn der Zentralbanker einem Tauschmittel den intrinsischen Wert abspricht.

Ungeachtet dessen sehen wir das natürlich auch so. Die Technologie und insbesondere die Feldversuche der LBBW und der Commerzbank aus den letzten Wochen lassen auf ein sehr großes Potential schließen, wenn es darum geht, Settlementsysteme auf Basis von Blockchains abzubilden. Das ist im Rahmen bestehender E-Geld-Lizenzen erfolgt. Das ist für uns aber nur der eine Teil der Wahrheit.

Wir, als Blockchain-Bundesverband, erhoffen uns natürlich nicht nur im Bereich der Industrieanwendungen große Potentiale, sondern auch darüber hinaus. Insofern schließen wir uns gerne Herrn Rübe an. Unser Eindruck ist, dass wir dort ehrlicherweise noch ganz am Anfang stehen. Die sogenannten ICOs, die heute schon verschiedentlich Gegenstand der Diskussion waren, sind eigentlich ein wunderbares Beispiel dafür. In der Theorie geht es darum, dezentrale Geschäftsmodelle, die auf einem Open-Source-Gedanken beruhen, finanzierbar und monetarisierbar zu machen, und zwar im gesamten Netzwerk als solchem. Das darf natürlich nicht darüber hinweg täuschen, dass auch Open-Source-Netzwerke bzw. dezentral betriebene Netzwerke auch marktwirtschaftlichen Regeln folgen. Die Initiatoren solcher Modelle profitieren im Idealfall natürlich von der Wertsteigerung entsprechend der zurückbehaltenen Token. Das ist an sich auch nicht falsch. Es ist lediglich eine andere Art, ein Open-Source-Modell bzw. dezentrales Netzwerk zu finanzieren, bei der es nicht mehr darum geht, konventionelle Cashflows über eine zentrale Entität zu aggregieren. So erschließen sich auch zum Beispiel Preissprünge oder schwer erklärbare Bewertungen an Sekundärmärkten. Bekannte Bewertungsmethoden, wie das Discounted-Cashflow-Verfahren oder andere Ertragswertmethoden, greifen dort ins Leere. Wir sind dort noch komplett am Anfang.

Die größten Potentiale liegen meiner Meinung nach in einem ersten Schritt in der Finanzwirtschaft. Wenn es darum geht, Daten sicher auszutauschen und dezentral zu verwalten, drängt sich der Gedanke des Handels auf. Damit sind wir im

Wesentlichen heute bei der Finanzwirtschaft. Wir sehen noch weitere Anwendungsfälle, insbesondere wenn es darum geht, digitales Identitätsmanagement auf die Blockchain zu holen. Das ist einer der wesentlichen Punkte, die uns in den nächsten Jahren beschäftigen werden, und stellt zugleich eine Schlüsseltechnologie für die in der Finanzwirtschaft dann hoffentlich platzgreifenden Anwendungsfälle dar. Ohne ein vernünftiges Identitätsmanagement ist diese Aufgabe nur schwer zu leisten.

Wir sehen auch das Bedürfnis nach Stabilität. Stable Coins finden sich nicht nur unter unseren Mandanten, wir sehen auch im internationalen Kontext eine verstärkte Nachfrage. Wir sehen auch die Zweiteilung, auf der einen Seite klassisch mit Fiatgeld unterlegte Währungen und auf der anderen Seite algorithmisch erzeugte Stable Coins. Unserer Auffassung nach kann es durchaus einen parallelen Weg geben. Warum sprechen wir denn hier über Stable Coins? Das, was wir brauchen und was uns im Rahmen dezentraler Netzwerke fehlt, ist das sogenannte „Computable Money“. Wenn es elektronisches Zentralbankgeld gäbe, würden wir uns diese Frage in vielerlei Hinsicht nicht stellen. Das ist unser Standpunkt. Vielleicht wollen meine Kollegen noch etwas ergänzen.

Sv **Dr. Sebastian Keding** (Blockchain Bundesverband e. V.): ICOs haben einen relativ schlechten Ruf, was auch teilweise gerechtfertigt ist. Es gab in diesem Bereich viel Betrug. Wir sind auch nicht dafür, ICOs um jeden Preis zu machen. Für Leute, die das machen wollen und Hilfe bei der Rechtsanwendung brauchen, sollte es vom Gesetzgeber an dieser Stelle noch Hilfestellungen geben.

Vorsitzende **Bettina Stark-Watzinger**: Für die Fraktion der FDP, Herr Schäffler.

Abg. **Frank Schäffler** (FDP): Ich habe eine Frage an Herrn Fußwinkel von der BaFin und an Herrn Romba von lindenpartners. Wir haben auf eine Kleine Anfrage an die Bundesregierung die Antwort erhalten, dass sich derzeit eine Person bei der BaFin in Vollzeit um das Thema kümmert. Halten Sie das für ausreichend, auch unter dem Gesichtspunkt, dass wir bei ICOs Betrugsfälle in Millionenhöhe erlebt haben? Können Sie ausschließen, dass das in diesem Jahr in ähnlicher Weise passiert?

Die zweite Frage an Herrn Romba: Sie haben vorgeschlagen, einen One-Stop-Shop einzurichten. Können Sie beschreiben, was dahinter steckt und weshalb das notwendig ist? Wie schätzen Sie diesbezüglich die Arbeit der BaFin ein?

Vorsitzende **Bettina Stark-Watzinger**: Wir beginnen mit Herrn Fußwinkel, BaFin.

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Diese eine Person ist ein Vollzeitäquivalent. Es sind nämlich tatsächlich sechs Personen, was wir auch auf die Kleine Anfrage geantwortet haben. Bei der Anfrage geht es allerdings darum, wer sich mit dem technologischen Hintergrund der Technologie beschäftigt. Die BaFin hat einen klaren Aufgabenkatalog, nämlich die Sicherstellung der Marktintegrität, die Prospektprüfungen, die Banken- und die Wertpapieraufsicht. In diese Bereiche spielt das Netzwerk herein, das wir intern aufgebaut haben, um diese Technologie zu verstehen. Wir wollen, dass diese Technologie im Rahmen der Regulierung behandelt wird. Deswegen sind es in der Summe sechs Vollzeitäquivalente, die sich mit dem Thema beschäftigen. Das haben wir ausgerechnet. Das entspricht dem Aufwand, der durch Prospektanfragen und ähnliches anfällt.

Über diverse Untersagungsmaßnahmen, die wir auch veröffentlichen, und Kommunikationsmittel auf verschiedenen Kanälen sorgen wir für die Aufrechterhaltung der Marktintegrität in diesem Bereich. Eine Garantie kann man natürlich nicht geben. Das ist völlig klar. Zumal es eine grenzüberschreitende Tätigkeit ist. Wir schauen uns die Anbieter aus dem Ausland an, decken solche Geschäfte auf und verfolgen diese gegebenenfalls oder unterbinden sie. Gleichzeitig sorgen wir dafür, dass nachhaltige Angebote die entsprechenden Prüfverfahren bestehen, wie es zum Beispiel beim Security Token geschehen ist. Daher bin ich trotz der vermeintlich gering klingenden Zahl sehr zuversichtlich.

Vorsitzende **Bettina Stark-Watzinger**: Herr Romba von lindenpartners.

Sv **Eric Romba** (lindenpartners (Partnerschaft von Rechtsanwälten mbH)): Wir versuchen uns einmal in die Perspektive eines Gründers oder eines Unternehmers zu versetzen, der ein Security-Token-Offering zum Beispiel in Europa plant. Was macht er? Er recherchiert. Da wäre es sehr wünschenswert,

wenn man eine Anlaufstelle hätte, wo man das findet, was man sucht. Es gibt einen Wettbewerb zwischen den Jurisdiktionen, die schon vielfach genannt wurden: Liechtenstein, Malta, Gibraltar. Denn Regulierungsarbitrage ist dort vermeintlich einfacher, obschon auch dort Europarecht gilt. Daher wäre es wünschenswert, wenn die BaFin ein Anlaufpunkt sein könnte. Es gibt schon sehr viele Informationen, die zur Verfügung gestellt werden. Herr Fußwinkel hat hierzu das Hinweisschreiben genannt. Das kann man noch über Checklisten ausbauen. Wir werden oft gefragt, ob es keine Checklisten gäbe, an denen die Anforderungen an einen Security Token abgearbeitet werden könnten. Beispielsfälle könnten anonymisiert veröffentlicht werden. Die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Bankenaufsichtsbehörde (EBA) haben sich in ihren Veröffentlichungen auch bestimmte Coins und Tokens anonymisiert angesehen und bewertet. Solche Bewertungen könnte man auf eine Webseite stellen. Wir reden gar nicht davon, dass man eventuell auch mit Chatbots arbeitet. Denn diejenigen, die im Krypto-Segment unterwegs sind, sind digital sehr affin. Mit einem Chatbot kann ich durchprüfen lassen, was ich plane und ob ich mich eher im Securitiy-Token- oder im Utility-Token-Bereich befinde. Das wäre sicherlich hilfreich. Wir betreiben auch ein bisschen Standortmarketing und Wettbewerbspolitik. Das ist sicherlich nicht die primäre Aufgabe der BaFin, weil sie eine Kontrollbehörde und Rechtsanwenderin ist. Aber wir sehen aus unserer Beratungspraxis, dass Interessenten zumindest auf der Website der BaFin waren. Deswegen sollte man dort auch mehr Informationen zur Verfügung stellen.

Vorsitzende **Bettina Stark-Watzinger**: Die Fraktion der CDU/CSU, Herr Steiniger.

Abg. **Johannes Steiniger** (CDU/CSU): Meine Frage geht an Frau Dr. Siedler, da Sie sich mit der rechtlichen Seite des Themas Blockchain beschäftigen. Wenn Sie drei Wünsche an die Politik hätten, in welchen Bereichen müsste man rechtlich etwas ändern?

Vorsitzende **Bettina Stark-Watzinger**: Frau Dr. Siedler, DWF Rechtsanwaltsgesellschaft.

Sve **Dr. Nina Luisa Siedler** (DWF Germany Rechtsanwaltsgesellschaft mbH): Ich würde verschiedene Themen sehen. Es ist sehr wichtig, dass wir jetzt die Entmaterialisierung des Wertpapiers angehen. Dann würde ich mir wünschen, dass wir bei der Blockchain-Technologie und den Fragen der Anwendungsmöglichkeiten nicht einfach ein „Weiter so“ praktizieren. So klingt es im Eckpunktepapier zumindest an, wenn in diesen Bereichen ausschließlich lizensierte Finanzintermediäre oder akkreditierte Investoren eine Rolle spielen sollen. Stattdessen sollte man überlegen, zunächst inhaltliche Anforderungen an die Technologie zu definieren und einen lizensierten Finanzintermediär für ein Audit und die Kontrolle zu nutzen. Der beaufsichtigte Finanzintermediär könnte dann feststellen, welches Register bestimmte Voraussetzungen technologischer Art, aber auch im Hinblick auf die Governance-Struktur für diese Technologie erfüllt. Das wäre eine Weiterentwicklung gegenüber der Festschreibung von zentralen Intermediären in der aktuellen Form.

Drittens würde ich mir eine neue Klasse der Gemeinnützigkeit für solche nicht renditeorientierten Unternehmen wünschen, die versuchen, öffentliche Infrastrukturen zu schaffen. Das wäre ein deutlicher Schritt, um gesellschaftspolitisch die Potentiale der Blockchain-Technologie für Deutschland zu fördern und nutzbar zu machen. Das sind ganz wichtige Punkte.

Insgesamt wünsche ich mir, dass wir uns mehr mit den Grundlagen der Technologie auseinandersetzen, statt sie nur wie jede andere Datenbank zu behandeln, in unsere Schubkästen einzusortieren und dort ruhen zu lassen. Denn damit werden wir die Potenziale sicherlich nicht nutzen können und auch nicht dafür sorgen, dass die Blockchain-Industrie oder die Community sich weiter in Deutschland verfestigt. Das sind genau die Bereiche, in denen wir weiter Unterstützung brauchen.

Ganz klassisch ist in diesem Bereich die Aufteilung der Blockchain-Unternehmen. Es gibt den Teil, der öffentliche Infrastruktur baut, typischerweise Open Source und nicht profitorientiert. Wir könnten steuerliche Anreize setzen, damit sich diese Infrastruktur richtig bildet, auch im Hinblick auf die Wahl des On-Chain Governance-Mechanismus. Man hört viel Kritik über den Proof-of-Work bezüglich des hohen Energieverbrauchs. Sie haben es in der Hand zu sagen, dass wir diese Art von Konsensmechanismus nicht fördern, sondern nur die Arten, die keinen hohen Energieverbrauch beinhalten. Zu dieser Non-Profit-Einheit kommt in der

Regel noch ein Unternehmen hinzu, das den Code entwickelt und entsprechend dafür bezahlt wird, damit die eigentlichen Gründer oder Initiatoren ihr Geld verdienen. Diese häufig zu beobachtende Trennung können wir für uns sehr gut nutzen und weiter fördern. Das wäre ein großer Wunsch.

Vorsitzende **Bettina Stark-Watzinger**: Die Fraktion der SPD, Herr Dr. Zimmermann.

Abg. **Dr. Jens Zimmermann** (SPD): Wenn der Blockchain Bundesverband drei Empfehlungen – jenseits des Antrags der Fraktion der FDP – an die Politik hätte, was wären die drei prioritären Maßnahmen?

Von Frau Otto hätte ich gerne drei Empfehlungen, was die Politik auf keinen Fall tun sollte.

Vorsitzende **Bettina Stark-Watzinger**: Wir beginnen mit dem Blockchain Bundesverband. Herr Resas.

Sv **Daniel Resas** (Blockchain Bundesverband e. V.): Neben den schon bereits eingebrachten Anträgen?

Abg. **Dr. Jens Zimmermann** (SPD): Weil Sie das so flapsig sagen, wären Sie der Meinung, der Bundestag sollte dem vorliegenden Antrag zustimmen?

Sv **Daniel Resas** (Blockchain Bundesverband e. V.): Im Wesentlichen deckt sich meine Meinung mit dem, was Frau Siedler gerade schon angedeutet hat. Ich glaube, wir brauchen im Wesentlichen zwei Dinge. Zum einen brauchen wir einen klar kommunizierten politischen Willen. Das macht eine ganze Menge aus. Das darf man nicht unterschätzten. Das Marketing, das bestimmte Jurisdiktionen betrieben haben, lässt sich vielfach darauf zurückführen. Wer bei der Öffnung der Trust Square AG in Zürich, einem Co-Working-Space, dabei war, hat gesehen, dass die Züricher Politprominenz anwesend war und entsprechende Unterstützung signalisiert hat. Das ist das eine. Rechtssicherheit ist das andere. Insofern unterstützen wir den Antrag der Fraktion der FDP entsprechend. Darüber hinaus gibt es neben der zivilrechtlichen und finanzaufsichtsrechtlichen Sicht auch noch die steuerrechtliche Seite, die momentan einen ganz wesentlichen Standortnachteil darstellt. Das in der Gesamtschau würde uns schon ganz erheblich helfen. Damit würde ich schließen und Frau Otto das Wort geben wollen.

Vorsitzende **Bettina Stark-Watzinger**: Frau Otto von COT Legal.

Sve **Claudia Otto** (COT Legal): Drei Empfehlungen, was man auf keinen Fall tun sollte? Ich beginne mit dem Ratschlag, sich nicht zwischen den verschiedenen Angaben zur Technologie und deren Realisierung zu verzetteln, sondern vielmehr darauf zu hören, was die Parteien wollen. Was ist der Parteiwille, der dahinter steht? Es ist oft der Fall, dass gar kein Kaufvertrag zu einem Token vorliegt, sondern gegebenenfalls ein Darlehensvertrag, also ein komplett anderer Vertrag. Das darf man nicht vergessen.

Auch darf man die Verbraucherinteressen nicht vergessen, die sich über die verschiedenen Risiken, aber auch über die Chancen informieren wollen. Herr Romba hatte diesbezüglich für die Blockchain-Produktanbieter schon gute Beispiele genannt, was man tun könnte. Ich halte zum Beispiel die Vorgehensweise des Bundeskartellamts bei der Missbrauchsaufsicht für sinnvoll, eine Entscheidungsdatenbank mit Namen und Sachverhalten zu führen, sodass die Verbraucher im Einzelnen nachvollziehen können, worum es ging, und nicht nur oberflächlich zusammengefasste Informationen erhalten. Obwohl die Verbraucherwarnung der BaFin zu den ICOs sehr gut war, müsste eine Datenbank für Verbraucher aufgebaut werden, die es ermöglicht, leicht und verständlich an Informationen zu kommen. So könnte über eine Suchfunktion die Möglichkeit eröffnet werden, zum Beispiel nach Kryptowährungen oder Ponzi Schemes zu filtern, um zu entscheiden, ob man investiert oder nicht.

Ich würde mit dem Rat schließen wollen, sich noch einmal klar zu machen, was hinter dem sicherlich auch interessanten und spannenden Konstrukt der Blockchain steht. Ganz oft sind es Wege, die wir rechtlich schon durchdacht haben, die jetzt neu gegangen werden und vielleicht ein wenig vernebelt werden. Das darf man nicht vergessen. Es gibt gute und redliche Anbieter, aber es gibt und es wird auch immer unredliche Anbieter geben.

Vorsitzende **Bettina Stark-Watzinger**: Die Fraktion DIE LINKE., Herr De Masi.

Abg. **Fabio De Masi** (DIE LINKE.): Ich möchte Frau Otto fragen, ob Sie glauben, dass die BaFin hinsichtlich des finanziellen Verbraucherschutzes hinreichend aufgestellt ist. Was ist Ihre Erfahrung als Anwältin im Bereich des finanziellen Verbraucherschutzes?

Ich habe auch eine Frage an Herrn Dr. Diehl, was die Bundesbank angeht. Wir hatten die Diskussion um die öffentliche Infrastruktur, was auch die Zahlungsinfrastruktur betrifft. Das Wesen von Geld ist eben nicht der intrinsische Wert, sondern eine vertragliche Beziehung, die öffentlich reguliert ist. Die Kritik am Bitcoin ist, dass es kein Geld und kein effizientes Zahlungsmittel ist. Es gibt eine sehr spannende Diskussion unter den Zentralbanken, der schwedischen Reichsbank und auch in Estland, über den E-Euro. Es gibt aus dem Bereich der Banken die Befürchtungen, dass ein digitaler Bank Run ausgelöst würde, wenn ein E-Euro von den Zentralbanken angeboten würde. Wie nehmen Sie als Bundesbank an diesen Diskussionen teil?

Vorsitzende **Bettina Stark-Watzinger**: Frau Otto, COT Legal.

Sve **Claudia Otto** (COT Legal): Die Erweiterung des Online- und Informationsangebotes für Verbraucher halte ich auf jeden Fall für ausbaufähig. Das beinhaltet schon sehr viele nützliche Informationen. Ich halte eine übersichtliche Datenbank mit ausgiebigen Suchmöglichkeiten zu den besonders attraktiven Stichworten für sehr sinnvoll.

Die BaFin darf konkrete Fragen zu Empfehlungen oder auch Warnungen zu speziellen Unternehmen nicht beantworten. Die Verbraucher müssen schon selbst recherchieren. Das ist richtig so und soll auch so bleiben. Denn man muss aufpassen, dass man den schmalen Grat nicht überschreitet. Der kollektive Verbraucherschutz sollte berücksichtigen, inwieweit die Gefahren in das Zivilrecht hineinreichen, da der Verbraucher diese Gefahren im Allgemeinen nicht überblicken kann. Das sind insbesondere die Fälle des Wuchers, in denen Unwissenheit und Unerfahrenheit der Verbraucher ausgenutzt werden. Das öffentliche Recht im Sinne der Finanzierung ist immer auch vom Zivilrecht flankiert. Dort muss für einen Ausgleich gesorgt werden, damit keine großen Schutzlücken entstehen, wenn wir den Fokus nur auf das Finanzrecht legen.

Vorsitzende **Bettina Stark-Watzinger**: Herr Dr. Diehl, Deutsche Bundesbank.

Sv **Dr. Martin Diehl** (Deutsche Bundesbank): Zum digitalen Euro oder E-Euro: Wir sprechen immer vom digitalen Zentralbankgeld. Hierzu haben wir eine skeptische Meinung. Das ist richtig. Diese unterscheidet sich aber nicht wesentlich von denen anderer Zentralbanken, nicht im Euro-System und auch nicht in den G20. Wir haben im letzten Jahr im Rahmen des Ausschusses der Bank für Internationalen Zahlungsausgleich (BIZ) gemeinsam ein Papier erstellt. Insofern gibt es keine Divergenzen.

Zwei Punkte sind bei digitalem Zentralbankgeld zu unterscheiden. Erstens, digitales Zentralbankgeld, das nur für Wholesale, also von Banken etwa für die Wertpapierabwicklungen genutzt wird. Dann bliebe es in einem geschlossenen Rahmen. Das kann man sich für eine effizientere Abwicklung vorstellen.

Das Zweite ist digitales Zentralbankgeld praktisch für jedermann. Dann hätten wir etwas geschaffen, bei dem jeder direkt Zugang zum Zentralbankgeld hätte. Das könnte möglicherweise starke Substitutionseffekte von den bisherigen Intermediären auslösen, was wiederum Effekte auf die Stabilität, auf das bisherige Geschäftsmodell der Banken, auf die geldpolitische Neutralität und auch auf die Stabilität unserer Bilanz haben könnte. Denn wir müssten dann vermutlich mehr Basisgeld bereitstellen. Der Kreditmultiplikator wäre ein anderer. Das hat sehr weitreichende Implikationen ökonomischer Art.

Wir sind uns daher einig, was auch im BIZ-Papier des CPMI-Ausschusses (Committee on Payments and Market Infrastructures) nachzulesen ist, dass wir auf absehbare Zeit davon abraten würden, digitales Zentralbankgeld für die breite Öffentlichkeit bereitzustellen. Auch die Schwedische Reichsbank, die eine E-Krone erschaffen hat, macht das nur, um einen Ersatz für das Bargeld zu haben. Sie sagt klar, dass das nichts mit Blockchain zu tun hat und auch nicht auf Blockchain oder DLT-basiert laufen wird. Da steht ein ganz anderes Ziel dahinter.

Vorsitzende **Bettina Stark-Watzinger**: Die letzte Frage in dieser öffentlichen Anhörung kommt von BÜNDNIS 90/DIE GRÜNEN, Herr Dr. Bayaz.

Abg. **Dr. Danyal Bayaz** (BÜNDNIS 90/DIE GRÜNEN): Zum Abschluss würde ich gern der BaFin die Möglichkeit geben, zu einigen Punkten Stellung zu beziehen. Mich würde interessieren, inwiefern Regulierungsvorhaben auch auf europäischer Ebene diskutiert werden? In welchen Gremien besprechen Sie das? Inwiefern sind Sie diesbezüglich in einem internationalen Austausch?

Sie haben letztes Jahr mit einer Studie zu Big Data und künstlicher Intelligenz auf sich aufmerksam

gemacht. In dieser Studie wurde das Thema Kryptoassets nicht berücksichtigt. Ist etwas Ähnliches zu erwarten? In dem Kontext hatte ich Herrn Hufeld so verstanden, dass er Sandbox-Lösungen beim Thema FinTechs immer kritisch gegenüber stand. Inwiefern ist das im Krypto-Bereich ein Thema? Haben Sie sich damit auseinandergesetzt?

Können Sie uns einmal einen Einblick geben, wie viele Anträge Sie für ICOs im Quartal bekommen und wie lange die Bearbeitungszeit dauert? Können Sie uns eine Zahl nennen?

Vorsitzende **Bettina Stark-Watzinger**: Herr Fußwinkel, BaFin.

Sv **Oliver Fußwinkel** (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)): Ich fange mit der letzten Frage zu den Zahlen an. Die Anfragen zu den ICOs spielen sich grundsätzlich im niedrigen Bereich ab. Im letzten Jahr waren sie im niedrigen dreistelligen Bereich. Das ist allerdings viel, wenn man bedenkt, dass dahinter eine neue Technologie und ein neues Konzept stehen.

Die Frage nach der Bearbeitungszeit ist schwieriger zu beantworten, als man denkt. Wir, wie auch die Antragssteller und deren Berater, hatten sehr oft die Situation, dass wir mit einem „lebenden Konstrukt“ zu tun haben. Anders als bei den klassischen Kapitalmarktprodukten bekamen wir keinen fertigen Prospekt zu einem fertigen Produkt. Sowohl die Programmierung als auch die Konzeptionierung ändert sich ständig. Das heißt, wir haben normalerweise eine Reaktionszeit innerhalb eines Verwaltungsverfahrens, die zwischen zwei und vier Wochen liegt. Die Gesamtverfahrensdauer hängt in hohem Maße davon ab, wie weit das Vorhaben zu dem Zeitpunkt, wo es zu uns kommt, schon ausgearbeitet ist. Wir müssen teilweise immer wieder neu prüfen. Die Rechtslage gibt das zwingend vor, da am Ende ein verbindlicher Rechtsakt oder eben nur eine Auskunft vorliegen muss. Um dem Bedürfnis nach Informationen, was insbesondere auch im Prospektbereich zunehmend gefordert wird, gerecht zu werden, geben wir Zwischenauskünfte im Rahmen des ganz normalen Verwaltungsverfahrensrechts. Diese Zwischenauskünfte gestalten wir so aus, dass sie oft einem Rechtsgutachten gleichkommen. Wir geben dabei sehr ausgiebige, rechtliche Stellungnahmen ab. In aller Regel enthalten die Zwischenauskünfte auch Begründungen, wenn es um die Erlaubnispflicht geht, weil dabei auch die Strafbarkeit für die Adressaten eine Rolle spielt, sodass diese sich ein Bild machen können. Dahinter steckt ein völlig anderer Aufwand, als wenn man nur einen Dreizeiler abgibt, wie dies viele andere im Ausland machen.

Bei den Regulierungsvorhaben fasse ich mich kürzer. Dort setze ich die Standardisierung voran. Im gesamten DLT-Bereich ist die Schaffung von Standards, die einheitlich gelten, die Grundlage. Wir sind involviert in die gesamten Verfahren bei ESMA, EBA, IOSCO (International Organization of Securities Commissions) und FSB (Financial Stability Board)). In all diesen Gremien sind wir beteiligt. Die Empfehlungen der beiden europäischen Aufsichtsbehörden entstehen nicht im luftleeren Raum, sondern unter Beteiligung der nationalen Aufsichtsbehörden. Daran beteiligt sich auch die BaFin. Die Empfehlungen sind bekannt. In diesem Rahmen habe ich meine Stellungnahme abgegeben. Die BaFin denkt, dass Sandboxes kein vernünftiger Weg sind, zumindest keine regulatorische Entity Based Sandbox, bei der wir uns aussuchen, wer regulatorische Vorteile genießt. Das heißt aber nicht, dass wir nicht innovationsoffen agieren können. Es sollte nur nicht in dem Rahmen passieren, dass wir jenseits der Ermessensausübung, der Proportionalität und der Verhältnismäßigkeit Erleichterungen gewähren, weil das wiederum das Level Playing Field gefährdet.

Vorsitzende **Bettina Stark-Watzinger**: Wir sind am Ende unserer öffentlichen Anhörung angekommen. Vielen Dank an die Experten für die Übermittlung der Stellungnahmen zur Frage der zukunftsfähigen Rahmenbedingungen für die Distributed-Ledger-Technologie, welche wir nun zur Beratung in die Fraktionen mitnehmen. Herzlichen Dank für Ihre Zeit und die intensive Diskussion. Ich wünsche Ihnen eine gute und erfolgreiche Woche.

Schluss der Sitzung: 15:49 Uhr

B. Stark-Watzinger

Bettina Stark-Watzinger, MdB

**Vorsitzende**

**- Anlagenverzeichnis -**

**Anlage 1:** Stellungnahme von Herrn Ralph Bärlingea, BearingPoint GmbH

**Anlage 2:** Stellungnahme des Blockchain Bundesverbandes e. V.

**Anlage 3:** Stellungnahme der BOTLabs GmbH

**Anlage 4:** Stellungnahme von Herrn Dr. Martin Fries, Ludwig-Maximilians-Universität München

**Anlage 5:** Stellungnahme der Immutable Insight GmbH

**Anlage 6:** Stellungnahme von Frau Claudia Otto, COT Legel (Rechtsanwältin)

**Anlage 7:** Stellungnahme von Herrn Eric Romba, lindenpartners (Partnerschaft von Rechtsanwälten mbH)

**Anlage 8:** Stellungnahme von Frau Dr. Nina-Luisa Siedler, DWF Germany Rechtsanwaltsgesellschaft mbH

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:**<br><br>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:**<br><br>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** | |
|---|---|---|---|
| | | **beim Anwender selbst (on-premise)** | **bei Drittanbieter (off-premise)** |
| **Nutzergruppe** | **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**

BLOCKCHAIN BUNDESVERBAND

BLOCKCHAIN
BUNDESVERBAND E.V.
VR 36105 B
27 / 661 / 52176

ADDRESS
c/o Jolocom
Waldemarstrasse 37a
10999 Berlin, Germany

info@bundesblock.de
www.bundesblock.de

Commerzbank Berlin
IBAN DE29 1004 0000
0228 8900 00
BIC COBADEFFXXX

8. März 2019

**Schriftliche Stellungnahme im Rahmen der öffentlichen Anhörung zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ (BT-Drucksache 19/4217)**

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

wir danken für die Gelegenheit zur Stellungnahme im Rahmen der öffentlichen Anhörung zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ (BT-Drucksache 19/4217). Gerne ergreifen wir die Gelegenheit zur Stellungnahme:

Zu den Punkten im Einzelnen:

## 1. Kompetenzausstattung der BaFin

Wir konnten einen deutlichen Kompetenzaufbau bei der Bundesanstalt für Finanzdienstleistungsaufsicht („**BaFin**") ab der zweiten Jahreshälfte 2017 beobachten. Das fachliche Wissen bei den auf diese Themen spezialisierten Mitarbeitern ist inzwischen sehr gut.

Allerdings halten wir die personelle Ausstattung der mit den Blockchain/DLT beschäftigten Abteilungen noch für zu gering. Die BaFin ist aktuell nicht nur mit einer Vielzahl von Anfragen durch Unternehmen beschäftigt, sondern auch mit der Koordination und Vorbereitung der korrespondierenden Arbeiten im BMF, der Abstimmung der Fragen auf europäischer Ebene im Rahmen der ESMA und vielfältigen weiteren Aufgabenstellungen. Für eine zeitnahe Bearbeitung der Unternehmens-Anfragen fehlen daher die erforderlichen personellen Kapazitäten. Dabei ist zu berücksichtigen, dass Unternehmen im Hochtechnologiebereich eine sehr hohe Geschwindigkeit bei der Entscheidungsfindung erfordern. Eine Verfahrensdauer von Monaten (statt Wochen) führt sehr häufig dazu, dass die Unternehmen in Jurisdiktionen mit einer agileren Finanzaufsicht ziehen.

## 2. Transparenz der BaFin in Bezug auf die Blockchain Technologie

Wir unterstützen die Forderung nach größtmöglicher Transparenz bei der behördlichen Entscheidungsfindung über Blockchain-/DLT-bezogene Fragestellungen. Dies gilt in der Tat in besonderem Maße für die BaFin, der die Aufsicht über die Einhaltung von finanzaufsichtsrechtlichen Erlaubnisanforderungen sowie Prospektanforderungen obliegt.

Die BaFin hat in ihrem Hinweisschreiben vom 20.02.2018 (GZ: WA 11-QB 4100-2017/0010) kommuniziert, nur Einzelfallentscheidungen in diesem Bereich treffen zu wollen. Dies schafft jedoch keine hinreichende Transparenz über die gerade entstehende Verwaltungspraxis der BaFin. In ihrer Veröffentlichung vom August 2018 (BaFin Perspektiven) hat die BaFin dann erstmals öffentlich konkretere Hinweise zu der Frage der Token-Klassifizierung gegeben. Die Ausführungen stehen ausdrücklich weiterhin unter dem Vorbehalt der Einzelfallentscheidung.

Die (grundsätzlich verständliche) Eigenerwartung der BaFin, nur langfristig aufrecht zu erhaltende Kriterien zu veröffentlichen, behindert eine rechtssichere und sinnvoll gesteuerte Entwicklung der schnelllebigen Technologiebranche. Daher begrüßen wir den Beginn der öffentlichen Kommunikation über die aktuell angelegten Abgrenzungskriterien im August 2018 und regen eine Fortschreibung dieser Linie durch Veröffentlichung eines formalen Hinweisschreibens zu dem Thema an.

Ebenfalls für sinnvoll hielten wir die Flankierung eines solchen Hinweisschreibens durch eine Veröffentlichung von Einzelfallentscheidungen, auf anonymisierter Basis. Diesem Wunsch werden regelmäßig datenschutzrechtliche Bedenken sowie die Vertraulichkeitsverpflichtung der BaFin entgegengehalten. Ein Weg, diesen Bedenken zu begegnen, ist eine rein typisierende Darstellung. Die englische Finanzmarktaufsicht FCA hat (Guidance to Crypto Assets, Consultation Paper (CP 19/3)) ebenso wie die MAS aus Singapur (A Guide to Digital Token Offerings) damit begonnen, Musterbeispiele zu bilden,

um Abgrenzungen deutlicher werden zu lassen. Ferner würde eine Einwilligung in eine Veröffentlichung durch die betroffenen Unternehmen von datenschutzrechtlichen sowie Vertraulichkeitsbedenken befreien. Viele Unternehmen haben ausdrücklich Interesse, über das Ergebnis ihrer Abstimmung mit der BaFin zu informieren. Dies wird ihnen jedoch aktuell von der BaFin ausdrücklich untersagt unter Hinweis darauf, dass mit der Auskunft der BaFin, wie der Fall von ihr beurteilt wird, keine Werbung gemacht werden darf.

Die Forderung nach einer mehrsprachigen Veröffentlichung der Informationen der BaFin in diesem Bereich begrüßen wir ausdrücklich. Der Sektor ist durch Internationalität geprägt aufgrund der grundsätzlich grenzüberschreitend genutzten Technologie.

## 3. Prospekterstellung und Prospekthaftung

Token-Emittenten sollten unabhängig von der Klassifizierung der Token die Möglichkeit haben, sich an die EU-Prospektvorschriften für Wertpapierprospekte zu halten und einen durch die nationale Aufsichtsbehörde gebilligten Prospekt zu veröffentlichen. In der EU ist die Veröffentlichung eines gebilligten Prospekts der "Goldstandard" für das Angebot von Wertpapieren an die Öffentlichkeit und damit insbesondere an Privatanleger, da der Prospekt einer Kohärenzprüfung durch die zuständige Aufsichtsbehörde unterfällt. Wir unterstützen das aus Frankreich bekannte „ICO-Gesetzesmodell" zur Förderung von Transparenz am Kapitalmarkt, indem ein freiwilliges Opt-in für wertpapierfremde-Token (also alle Token, die nicht als Security-Token zu qualifizieren sind) geschaffen wird. Die Aufsichtsbehörde fungiert dann nicht nur als Prüf- sondern auch als Hinterlegungsstelle. Hierdurch würde nicht nur mehr Transparenz im noch jungen und stetig wachsenden ICO Markt entstehen, sondern auch Sicherheit bei den Investoren, welche ein auf Inhalt und Plausibilität gebilligtes Dokument der BaFin als Grundlage für fundierte Investitionsentscheidungen nutzen könnten, zudem würde ein zivilrechtlich relevantes Haftungsdokument geschaffen werden. Das Opt-in und somit die Billigung des Prospekts durch die BaFin würde für die Token-Emittenten die „eingeschränkte" Prospekthaftung ermöglichen und damit die zivilrechtliche Prospekthaftung im weiteren Sinne nach Maßgabe der BGH-Rechtsprechung ausschließen.

Eine verbindliche Auskunft der BaFin zur Prospektfreiheit nach dem Vorbild von § 4 KWG bzw. § 5 Abs. 3 Satz 1 KAGB wäre sehr zu begrüßen. Die BaFin sollte – ähnlich wie sie dies für sonstige Anfragen derzeit durch ihr Kontaktformular für FinTechs anbietet – Anfragen zur Prospektpflicht bei jungen Unternehmen, auch verbindlich ohne die Einreichung eines kompletten und kostenintensiven Prospekts ermöglichen. Die Anbieter von Token hätten somit einen bestandskräftigen feststellenden Verwaltungsakt zur Verfügung, was die Rechtssicherheit im Vergleich zu den bisher bekannten Auskünften, die in ihrer konkreten Ausgestaltung derzeit leider unterschiedlich und von ihrer Rechtsnatur her mitunter unklar sind, zur Verfügung.

Wie bereits die ESMA in ihrer diesjährigen Veröffentlichung zu Crypto-Assets darstellt, gibt es einige europäische Aufsichtsbehörden, die einen Token-spezifischen Prospektanhang unterstützen. Auch wir befürworten dies. Es sollten neue Anhänge zur Prospekt-

verordnung erstellt werden, um Mindestdarstellungsanforderungen speziell für ein Angebot von Wertpapier-Token an die Öffentlichkeit aufzunehmen. Diese Offenlegungspflichten sollten angemessen angepasst werden, um der Tatsache Rechnung zu tragen, dass die meisten Token in der Vorbereitungsphase von Start-ups ohne nennenswerte finanzielle Historie ausgegeben werden. Ein Vorbild kann der EU-Wachstumsprospekt nach Art. 15 EU-ProspektVO sein. Um im Rahmen der EU-Harmonisierung europaweite einheitliche Standards zu setzen, sollte dieser Vorschlag durch die Bundesregierung auf EU-Ebene diskutiert werden. Eine nationale Lösung wäre in Anbetracht des internationalen Umfelds der Token-Geschäfte nicht zielführend. Dies wird insbesondere dann praxisrelevant, wenn Token auf Grundlage von gebilligten Prospekten grenzüberschreitend in der EU vertrieben werden sollen.

Auch für wertpapierfremde Token sollten neue Anhänge zur Prospektverordnung erstellt werden. Die Token-spezifischen Besonderheiten gelten nicht nur für Security-Token, sondern gerade auch bei sonstigen Token (so in etwa bei den Utility Token, welche in den vergangenen 18 Monaten vermehrt von Start-ups zur Unternehmensfinanzierung ausgegeben wurden).

## 4. Behörden

(a) Entwicklung interner Überprüfungsmechanismen und -werkzeuge für Transaktionen auf DLT-Netzwerken im Rahmen des Veranlagungsverfahrens

Die Blockchain bietet grundsätzlich das Potential sämtliche im Netzwerk vorgenommenen Transaktionen nachzuvollziehen und zu analysieren. Die Netzwerkteilnehmer bleiben nur anonym, insoweit die Identität hinter den von ihnen verwendeten kryptografischen Schlüsselpaaren unbekannt ist. Konnte zu einem Zeitpunkt ein Schlüsselpaar einer Identität zugeordnet werden, gilt gleiches für die Transaktionshistorie und zukünftige Transaktionen. Die Identifizierung des Schlüsselinhabers kann dabei durch ihn selbst bzw. einen Schnittstellenanbieter erfolgen, der dem Geldwäschegesetz unterliegt. Insbesondere im Hinblick auf die Überprüfung der in der Steuerveranlagung durch den Steuerpflichtigen offengelegten Einkünfte sowie bei der Bekämpfung von Steuerhinterziehung und Geldwäsche, sollten die Steuer- und Aufsichtsbehörden entweder eigene Softwarelösungen schaffen oder Kooperationen mit privaten Unternehmen anstreben, welche derartige Dienstleistungen erbringen können.

(b) Etablierung eines Analyseinstruments für Blockchain-bezogene Daten ausländischer Finanzdienstleister, welche der deutschen Finanzverwaltung über den AEOI gemeldet werden

Werden Token von Investmentunternehmen verwahrt, die gemäß den Common Reporting Standards (CRS) verpflichtet sind Finanzinformationen zu melden, werden diese im Rahmen des Automatischen Informationsaustausches (AEOI) u.a. an Deutschland geliefert. Insofern sollte sichergestellt werden, dass die in Deutschland zuständigen Behörden diese Informationen interpretieren und analysieren, sowie einen Abgleich mit den in der Steuerveranlagung deklarierten Einkünften vornehmen können.

(c) Informationsaustausch zwischen Aufsichts- und Steuerbehörden zur sachgerechten steuerlichen Einordnung neuer Token

Insofern neue Token emittiert werden, welche in Deutschland mit einer Prospektpflicht einhergehen, beinhaltet der Prospekt regelmäßig Ausführungen zu zivilrechtlichen Grundlagen sowie steuerrechtlichen Rechtsfolgen. Es ist anzuraten eine interne Datenbank zur Verwaltung und zum Informationsaustausch dieser Informationen zwischen den Aufsichts- und Steuerbehörden einzurichten.

## 5. Klärung der regulatorischen und gesetzlichen Rahmenbedingungen

Hinsichtlich der Kompatibilität ist zwischen verschiedenen Aspekten zu unterscheiden. Soweit Rechte wirksam an Token geknüpft werden können (dazu sogleich) werden diese zum Teil bereits jetzt von europarechtlichen Regelungen erfasst. So ist beispielsweise ein Gewinnbeteiligungsrecht, das mit einem Token verbunden ist, bereits jetzt von der europarechtlichen Kapitalmarktregulierung (MiFiD und ProspektVO) erfasst. Aus speziell deutsch-zivilrechtlicher Perspektive existieren insoweit allerdings einige dogmatische Herausforderungen, um diese Verbindung von Token und Rechtsposition zu erreichen (dazu sogleich). Weitere zivilrechtliche Herausforderungen betreffen unter anderem die Frage, ob und wer bei derart (unterstellt) dezentralisierten Registern für Fehler innerhalb des Netzwerks haftet.

Ebenfalls noch nicht endgültig geklärt ist die Frage der rechtlichen Einordnung von Token und – darauf aufbauend – wie die Rechtsposition des Token"inhabers" zu schützen ist. Die überwiegende Ansicht qualifiziert Token mangels Verkörperung nicht als „Sache" im Sinne des § 90 BGB, sondern als „sonstigen Vermögengegenstand". Das sind individualisierbare, vermögenswerte Objekte und Güter, über die Rechtsmacht im Sinne von Herrschafts- oder Nutzungsrechten ausgeübt werden kann. Wer den private key besitzt, der hat zugleich die Herrschaftsmacht über den Token. Diese Rechtsposition muss geschützt werden. Ob und inwieweit zB §§ 823, 1006 BGB etc ggf analog zu Gunsten des Schlüsselinhabers anwendbar sind, ist gegenwärtig Stand verschiedener Diskussionen. Eine gesetzgeberische Klarstellungen wäre dringend wünschenswert.

Nicht endgültig geklärt ist ebenfalls die Anwendbarkeit des deutschen und europäischen Verbraucherschutzrechts, speziell im Hinblick auf das Erfordernis und die Ausgestaltung von Widerrufsrechten. Token werden im Internet verkauft, so dass die Regelungen über Fernabsatzverträge grds. Anwendung finden dürften. Wünschenswert wäre eine Klarstellung des Gesetzgebers, ob und wann der Verkauf von Token unter den Ausnahmetatbestand des § 312g Abs.2 Nr. 8 BGB fällt, ein Widerrufsrecht mithin ausgeschlossen ist. Weiterhin wäre wünschenswert, dass die in Anhang I zu Art. 246a § 1 EGBGB vorgesehene Musterwiderrufsbelehrung so angepasst wird, dass sie mit der erforderlichen Rechtssicherheit auf den Verkauf von Token angewendet werden kann. Eine Klarstellung sollte zudem erfolgen im Hinblick auf die Frage, ob Token als digitale Inhalte im Sinne der europäischen Vorgaben anzusehen sind, da hiervon u.a. abhängt, ob Erwerber auf etwaig bestehende Widerrufsrechte verzichten können.

## 6. Klärung des Urkundenerfordernisses

Die Bundesregierung sollte die Abschaffung des Urkundenerfordernisses (soweit ein solches besteht) für u.a. Aktien und Schuldverschreibungen prüfen und die Begebung entmaterialisierter digitaler Wertpapiere auf Grundlage eines „qualifizierten digitalen Register" (im Folgenden auch „**QDR**") (analog den Regelungen im Bundesschuldwesengesetz für öffentliche Schuldtitel) ermöglichen. Dementsprechend begrüßen wir grundsätzlich den am 7. März 2019 veröffentlichten gemeinsamen Vorstoß des Bundesministeriums der Finanzen und des Bundesministeriums der Justiz und Verbraucherschutz zur Einführung sog. elektronischer Wertpapiere.

Auch wenn heute schon die Möglichkeit besteht, bestimmte Rechtspositionen rechtlich so mit einem Token zu verknüpfen, dass man bei wirtschaftlicher Betrachtungsweise von einer digitalen Verbriefung (sog. Tokenisierung) sprechen kann, bedarf es insbesondere im Hinblick auf die Schaffung kapitalmarktähnlicher Sekundärmärkte für wertpapierähnliche Token diverser Anpassungen im deutschen Zivil- und Aufsichtsrecht, um die für Marktteilnehmer erforderliche Rechtssicherheit zu gewährleisten. Nur mit funktionierenden Sekundärmärkten lässt sich das wirtschaftliche Potenzial der Tokenisierung von Rechtspositionen vollständig heben. Rechtstechnisch geht es dabei um die Entmaterialisierung von Wertpapieren, also die Möglichkeit der Begebung entmaterialisierter Wertrechte, die nur noch digital verwaltet werden. Die DLT ist dabei eine mögliche Technologie, um ein QDR zu betreiben.

Insbesondere das zivilrechtliche Erfordernis einer Urkunde (im Sinne einer physischen Verbriefung) nach dem zivilrechtlichen Wertpapierbegriff stellt ein Hindernis bei der Tokenisierung (d.h. digitalen Verbriefung) von Vermögenswerten dar. Dies gilt sowohl für Eigen- als auch Fremdkapitalinstrumente.

Im Kapitalmarktrecht ist mittlerweile anerkannt, dass tokenisierte Vermögensrechte bei entsprechender Umlauffähigkeit übertragbare Wertpapiere im Sinne der MiFID II darstellen können (vgl. die Definition der "Transferable Securities" nach Art. 4 Abs. 1 Nr. 44 der Richtlinie 2014/65/EU). Das Erfordernis einer urkundlichen Verbriefung kennt das europäisch geprägte Kapitalmarktecht nicht. Das hat zur Folge, dass solche Token, die als Wertpapier im kapitalmarktrechtlichen Sinn qualifizieren, u.a. in den Anwendungsbereich des Wertpapierprospektregimes (WpPG und ab dem 21. Juli 2019 die Wertpapierprospekt-VO), der MAR, der MIFIR und des WpHG fallen. Dies entspricht auch der aufsichtsrechtlichen Verwaltungspraxis der BaFin und anderer nationaler Aufsichtsbehörden bei Anwendung der genannten Vorschriften, die jüngst entsprechende Wertpapierprospekte für sog. Security Token Offerings genehmigt haben.

Davon zu unterscheiden ist jedoch der Wertpapierbegriff des deutschen Zivilrechts, der für die zivilrechtliche Begebung, Übertragung, Belastung und Verwaltung von Wertpapieren (und damit mittelbar auch der darin verkörperten Rechte) maßgeblich ist (sog. zivilrechtlicher Wertpapierbegriff):

Zwar ist auch die deutsche Kapitalmarktpraxis seit Einführung des stückelosen Effektengiroverkehr weitgehend entmaterialisiert und vom gesetzlichen Leitbild gelöst in dem

Sinn, dass die Berechtigten, also die Anleger, keine (einzel-)verbrieften Urkunden mehr erhalten. Die Wertpapiere werden in der Kapitalmarktpraxis nur noch globalverbrieft, bei einem Zentralverwahrer hinterlegt und in den entmaterialisierten Effektengiroverkehr eingebucht. Die Berechtigung eines Anlegers an einem Wertpapierbestand wird in einem pyramidenförmigen Verwahrungssystem zwischen Zentralverwahrer und Depotbanken nur durch Depotgutschriften repräsentiert und die (wirtschaftliche) Übertragung erfolgt durch entsprechende Depotumbuchungen.

Dies darf aber nicht darüber hinwegtäuschen, dass sich die zivilrechtliche Übertragung nach deutschem Recht begebener girosammelverwahrter Wertpapiere weiterhin nach dem sachenrechtlich geprägten deutschen Wertpapierrecht richtet. Nach der für die Praxis maßgeblichen ganz herrschender Meinung im deutschen Zivilrecht handelt es sich bei einem Wertpapier um ein urkundlich verbrieftes Vermögensrecht, zu dessen Ausübung der Besitz der (physischen) Urkunde nötig ist. Der Eigentumsübergang erfolgt, wenn der Buchungsvorgang bei der Wertpapiersammelbank abgeschlossen ist. Die Umschreibung im Depotbuch dokumentiert dabei nach außen die Änderung des (Fremd-)Besitzwillens der Depotbanken im Rahmen des mehrstufigen Besitzmittlungsverhältnisses und führt zum Verlust des Eigentums des Veräußerers nach § 929 S. 1 BGB.

Wegen des Urkundenerfordernisses erfasst der zivilrechtliche Wertpapierbegriff nach dem für die Praxis maßgeblichen herrschenden Verständnis keine rein digitalen Vermögenswerte. Anders als die Rechtsordnungen in beispielsweise Frankreich, Spanien, Italien, Luxemburg oder der Schweiz kennt das deutsche Zivilrecht grundsätzlich keine entmaterialisierten Wertrechte (zur Ausnahme der entmaterialisierten Anleihen der öffentlichen Hand sogleich). Folglich können (digitale) Token mangels physischer Urkunde derzeit zivilrechtlich nicht als Wertpapier qualifizieren.

Dies hat eine Reihe von Konsequenzen für die Kapitalmarktfähigkeit von Token. Nur wenn eine vergleichbare Rechtssicherheit (insbesondere bezogen auf die Übertragung und Verwahrung) wie im konventionellen Kapitalmarkt gewährleistet ist, werden auch institutionelle Marktteilnehmer sich in signifikantem Maße engagieren können. Dazu gehört insbesondere die Möglichkeit eines gesetzlich gesicherten gutgläubigen Erwerbs. Derjenige Anleger, der gutgläubig eine digital verbriefte Rechtsposition erwirbt, muss davon ausgehen können, diese Rechtsposition auch wirksam erworben zu haben. Umgekehrt muss sich der Emittent darauf verlassen können, schuldbefreiend an den formell Legitimierten, also den Tokeninhaber, leisten zu können. Jeder Zweifel daran hindert letztlich die Etablierung vertrauenswürdiger Kapitalmärkte, von der alle Investorenklassen gleichermaßen profitieren.

Da es für die Tokenisierung, d.h. für die rein digitale Verbriefung von Rechtspositionen in Form von entmaterialisierten Wertrechten, an vergleichbaren gesetzlichen Instrumenten fehlt, versucht sich die Praxis derzeit mit kautelarjuristischen Lösungen zu behelfen. Dazu wird auf Grundlage der jeweiligen Token-Bedingungen eine Beziehung zwischen Token und tokenisiertem Recht konstruiert, die derjenigen zwischen einer Inhaberschuldverschreibung und verbrieften Recht funktional weitgehend angenähert ist. Dies geschieht u.a. dadurch, dass die entsprechenden Bedingungen regelmäßig vorsehen, dass die Geltendmachung des tokenisierten Rechts gegenüber dem Emittenten nur

durch den Tokeninhaber möglich ist und die wirksame Übertragung des tokenisierten Rechts die technische Übertragung des Tokens voraussetzt. Dadurch soll verhindert werden, dass technische Zugriffsmöglichkeit auf den Token und materiell-rechtliche Berechtigung an der digital verbrieften Rechtsposition auseinanderfallen.

Die Schwäche dieser Hilfskonstruktion ist, dass diese weitgehende Annäherung lediglich schuldvertraglicher Natur ist, also nur zwischen den Parteien Wirkung entfaltet. Im Gegensatz z.B. zur Inhaberschuldverschreibung, bei der das „Recht aus dem Papier" dem „Recht am Papier" folgt, genügt eben nicht nur die technische Übertragung des Tokens zur wirksamen Übertragung der darin digital verbrieften Rechtsposition. Mangels gesetzlich gesicherten Gutglaubensschutzes kann der Erwerber einer digital verbrieften Rechtsposition derzeit nicht mit der – jedenfalls für institutionelle Marktteilnehmer – notwendigen Sicherheit davon ausgehen, dass er diese Rechtsposition auch wirksam erworben hat. Deshalb bedarf es der zivilrechtlichen Gleichstellung von Wertpapieren und digital verbrieften Rechtspositionen:

Bund und Länder können bereits heute vollständig entmaterialisierte Anleihen emittieren, die durch Eintrag in das Bundes- oder Landesschuldbuch begründet werden. Auf diese privatrechtlichen Verbindlichkeiten der öffentlichen Hand finden die gleichen sachenrechtlichen Vorschriften Anwendung wie auf verbriefte Schuldverschreibungen. Mit dem Bundesschuldenwesengesetz (BSchuWG) hat der Gesetzgeber über § 6 BSchuWG eine Gleichbehandlung der Forderungen des Bundes mit verbrieften Forderungen realisiert, indem er die Sammelschuldbuchforderungen als Wertpapiersammelbestand fingiert (§ 6 Abs. 2 S. 1 BSchuWG) und die Vorschriften des Depotgesetzes als entsprechend anwendbar erklärt (§ 6 Abs. 2 S. 6 BSchuWG).

Der Gesetzgeber könnte in entsprechender Weise die Fiktion auf bestimmte digitale Rechtspositionen erstrecken, die in einem dezentralen Register, das als QDR qualifiziert, verwaltet werden. Anstelle des Vertrauens des öffentlich geführten Registers des BSchuWG steht das Vertrauen in das kryptographisch gesicherte dezentrale Register. Der aus Register eindeutig zuzuordnende Token würde den notwendigen Rechtsschein für die Inhaberschaft des digital verbrieften Rechts begründen.

Wegen des fragmentarisch geregelten deutschen Wertpapierrechts erfordert die Einführung von kapitalmarktfähigen Wertrechten eine Reihe von Anpassungen in unterschiedlichen Gesetzen und Rechtsnormen. Dazu zählen u.a. das BGB, das DepotG, das SchuldVG, das AktG, die ZPO und die InsO. In Anbetracht des Umstandes, dass die DLT nur eine mögliche Technologie zur Schaffung und Übertragung von entmaterialisierten Wertrechten ist und sich diese Technologie noch in einem sehr frühen Entwicklungsstadium befindet, ist es unerlässlich, die Einführung von Wertrechten möglichst technologieneutral auszugestalten. Die Schaffung eines DLT-Sonderrechts ist daher weder erforderlich noch zweckmäßig. Gleichwohl dürfte es sich anbieten, die für die Begebung, Übertragung und Verwaltung von Wertrechen wesentlichen Regelungen in einer Art Wertrechtegesetz zentral zu erfassen.

Damit ist noch nicht die Frage beantwortet, welche Anforderungen an ein QDR zu stellen sind. In Anbetracht der Rechtsfolgen, die an die hier vorgeschlagene Gleichstellung von

digitalem Wertrecht und konventionellem Wertpapier geknüpft sind, wird man sich in diesem Zusammenhang mit einer Reihe von möglichen Themen beschäftigen müssen, die sich nicht nur auf technische (z.B. IT-Sicherheit und Datenschutz, Standardisierungsbemühungen), sondern vor allem auch konzeptionelle Fragestellungen (Betrieb des Registers und mögliche regulatorische Anforderungen an die beteiligten Parteien, Konsensbildung, Finalität der Buchungen, Beweisfähigkeit, Risikomanagement und Compliance) beziehen.

Darüber hinaus muss die Einführung von entmaterialisierten Wertrechten mit unterschiedlichen aufsichtsrechtlichen Regelungen synchronisiert werden. Dies betrifft nicht nur unterschiedliche nationale Vorschriften des KWG, des WpHG und des KAGB, sondern auch europäische Vorschriften wie die Verordnung über Wertpapierfinanzierungsgeschäfte (SFTR) sowie die Verordnung über Wertpapierzentralverwahrer (CSDR). Letztere verlangt beispielsweise, dass Wertpapieren, die an Sekundärmärkten gehandelt werden, im Effektengiro bei einem Zentralverwahrer eingebucht werden.

Vor dem Hintergrund der sich eröffnenden neuen technologischen Möglichkeiten sollte geprüft werden, ob technische Mindeststandards definiert werden können, unter denen ein dezentrales Verwaltungssystem neben dem monopolisierten Zentralverwahrungssystem anerkannt werden kann.

## 7. Banken

Im Rahmen der am Markt bestehenden Geschäftsmodelle mit Kryptowährungen und anderen Token übernehmen Banken verschiedene Funktionen. Sofern das Geschäftsmodell den Erwerb von Token gegen Zahlung von FIAT-Währungen umfassen, übernehmen Banken die Abwicklung der Geldzahlungen und führen hierbei Konten für Kunden und/oder Anbieter, auf die die Geldzahlungen verbucht werden. Für diese Tätigkeiten gelten die gleichen Regeln wie für entsprechenden Tätigkeiten, die nicht im Zusammenhang mit Geschäftsmodellen mit kryptographischen Token erbracht werden.

Banken übernehmen dahingegen nur selten die Funktion als Verwahrer von Token. Üblicherweise wird diese Dienstleistung von Unternehmen angeboten, die aus dem Blockchain-Bereich kommen und gegebenenfalls bei ihrem Geschäftsmodell mit Banken oder Finanzdienstleistungsinstituten kooperieren.

Angebote für die Verwahrung von Token können verschiedene Ausgestaltungen haben. Diese reichen von Software oder Online-Angeboten, bei denen nur der Nutzer Zugriff auf die Private Keys des Wallet hat und somit jederzeit ohne Mitwirkung des Anbieters über die dem Wallet zugeordneten Token verfügen kann, bis zu Online-Angeboten bei denen Token für einzelne oder mehrere Nutzer einen oder mehreren Online-Wallets zugeordnet werden, für die nur der Anbieter über den Private Key verfügt. Der Nutzer kann hier somit ohne Mithilfe des Anbieters nicht über die Token verfügen.

Insbesondere das letztere Angebot geht mit Risiken für den Kunden einher, da der Kunde darauf vertrauen muss, dass der Anbieter über eine angemessene Organisation und Sicherheitsmechanismen verfügt, um einen Verlust der Token zu vermeiden, und

darüber hinaus jederzeit in der Lage ist, über die dem Online-Wallet zugeordneten Token zu verfügen bzw. dem Nutzer verfügbar zu machen (vgl. EBA, Report with advice for the European Commission on crypto assets, Rn. 31 mit einer Übersicht von Risiken für Verbraucher im Zusammenhang mit Anbietern von Online-Wallets).

Dementsprechend stellen bestehende Definitionen, wann eine Verwahrung von Token vorliegt, darauf ab, dass der Anbieter den Private Key des Wallets für den betreffenden Nutzer hält. So definiert Art. 3 Nr. 19 der Richtlinie (EU) 2018/843 (5. Geldwäscherichtlinie) Anbieter von elektronischen Geldbörsen als einen Anbieter, der Dienste zur Sicherung privater kryptografischer Schlüssel im Namen seiner Kunden anbietet, um virtuelle Währungen zu halten, zu speichern und zu übertragen. Diese Definition deckt sich auch mit der von der European Securities Markest Authority in ihrem „Advice Initial Coin Offerings and Crypto-Assets" (ESMA50-157-1391) dargelegten Einschätzung, welche Tätigkeiten als Verwahrung von Kryptowährungen qualifizieren könnte (ESMA50-157-1391, Rn. 164).

Diese Tätigkeit (auch wenn sie von Banken erbracht werden), ist weder mit der Tätigkeit einer Kontoführung noch der einer Wertaufbewahrung vergleichbar. Anders als bei der Kontoführung nimmt der Anbieter der Verwahrung von Token gerade keine Buchungen auf dem Konto vor. Die dem Wallet zugeordneten Token werden diesem vielmehr durch Validierung der Transaktion in dem (dezentralen) Netzwerk zugebucht. Der Anbieter der Online-Wallet ist lediglich in der Lage mittels des Private Keys (im Auftrag des Kunden) Transaktionen in Bezug auf das Online-Wallet auszulösen. Auch erfolgt wie bei der Wertaufbewahrung keine Verwahrung von beweglichen Sachen, sondern eine Speicherung des Private Key für den Nutzer und somit eine Speicherung von Daten. Wegen diesen Unterschieden ist eine entsprechende Einordnung als Kontoführung oder Wertaufbewahrung zur Zeit nicht angebracht.

Anbieter von Online-Wallets, die auch die Private Keys für deren Nutzer verwahren, unterliegen in Bezug auf diese Tätigkeit keiner Erlaubnispflicht nach dem Kreditwesengesetz. Dies gilt auch, wenn die entsprechende Tätigkeit von unter dem Kreditwesengesetz regulierten Instituten erbracht wird. Als nach dem Kreditwesengesetz regulierte Tätigkeit käme grundsätzlich das Depotgeschäft (§ 1 Abs. 1 Satz 2 Nr. 5 KWG) in Betracht. Das Depotgeschäft ist die Verwahrung und Verwaltung von Wertpapieren für Dritte. Bei den Wertpapieren handelt es sich in diesem Zusammenhang nur um Wertpapiere im Sinne von § 1 Abs. 1 des DepotG. Diese umfassen Urkunden, die ein Recht in einer Weise verbriefen, dass nur der Inhaber der Urkunde dieses Recht ausüben kann. Die durch Token repräsentierten Rechte sind nicht in einer Urkunde verbrieft. Token qualifizieren daher zur Zeit nicht als Wertpapiere im Sinne des DepotG. Dies gilt auch für die Verwahrung von Token, die als Wertpapiere im Sinne des Kreditwesengesetz / Wertpapierhandelsgesetz qualifizieren, da auch diese nicht in Urkunden verbrieft sind.

Sofern Wertpapierdienstleistungsunternehmen die Verwahrung von Token mittels Online-Wallets anbieten, ist zu beachten, dass das Depotgeschäft ebenfalls als Wertpapiernebendienstleistung nach § 2 Abs. 9 Nr. 1 WpHG qualifiziert. Die Definition des Depotgeschäfts nach dem Wertpapierhandelsgesetz weicht jedoch von der Definition des Kre-

ditwesengesetzes ab. Das Depotgeschäft im Sinne des Wertpapierhandelsgesetzes umfasst die Verwahrung und Verwaltung von Finanzinstrumenten (im Sinne des WpHG) für andere einschließlich der damit verbundenen Dienstleistungen. Dementsprechend könnte in Bezug auf Token, die als Wertpapiere und damit als Finanzinstrumente im Sinne des Wertpapierhandelsgesetzes qualifizieren, der Tatbestand des Depotgeschäfts erfüllt sein, wenn man annimmt, dass der Verwahrer des Private Keys letztendlich auch die dem betreffenden Online-Wallet zugeordnete Token, die als Wertpapier qualifiziert, verwahrt.

Diesbezüglich ist zu beachten, dass nach § 84 WpHG ein Wertpapierdienstleistungsunternehmen Maßnahmen zum Schutz der Eigentumsrechte seiner Kunden an Finanzinstrumenten treffen muss, die sich im Besitz des Wertpapierdienstleistungsunternehmens befinden. Ein solches Wertpapierdienstleistungsunternehmen ist verpflichtet, Wertpapiere, die es bei der Erbringung von Wertpapierdienstleistungen von Kunden erhält, an ein Kreditinstitut weiterzuleiten, das nach dem Kreditwesengesetz zum Betreiben des Depotgeschäfts zugelassen ist. Diese Regelung erscheint in Bezug auf Token, die als Wertpapiere qualifizieren, problematisch, da zum einen Kreditinstitute regelmäßig die Verwahrung von Private Keys / Token in Form von Wallets nicht anbieten und zum anderen sich das Depotgeschäft im Sinne des Kreditwesengesetz signifikant von der Verwahrung von Private Keys / Token unterscheidet. Daher wäre eine gesetzgeberische Klarstellung (idealerweise auf europäischer Ebene) wünschenswert, dass das betreffende Wertpapierdienstleistungsunternehmen Maßnahmen zu treffen hat, die sicherstellen, dass die wirtschaftliche Verfügungsgewalt über die Token beim jeweiligen Kunden verbleibt.

Sofern aufgrund den mit der Nutzung von Online-Wallets, bei denen der Private Key vom Anbieter verwahrt wird, verbundenen Risiken eine Regulierung der Tätigkeit erfolgt, wäre eine einheitliche europäische Regulierung wünschenswert, die es erlaubt, die entsprechende Dienstleistung in allen Mitgliedsstaaten der EU zu erbringen.

Im Rahmen einer etwaigen Regulierung sind die Blockchain-spezifischen Besonderheiten zu berücksichtigen. Eine pauschale Übertragung der Erlaubnisanforderungen und Organisationspflichten von Kreditinstituten und Finanzdienstleistungsinstituten erschiene hierbei als überzogen. Für die Sicherung der rein digital verwahrten Private Keys ist vielmehr die Nutzung zuverlässiger IT Systeme und Vorhaltung entsprechender Backup-Lösungen erforderlich.

## 8. Steuern

### (a) Steuerrechtliche Tokenklassifizierung

Auch im Steuerrecht spiegelt sich die Innovationskraft der Blockchain insoweit wider, dass bis dato nur ausgewählte Äußerungen der Finanzverwaltung und des Gesetzgebers zur ertragsteuerlichen Klassifizierung Blockchain-basierter Token identifizierbar sind. Neben vereinzelten Anfragen des FDP-Bundestagsabgeordneten Frank Schäffler aus 2013 (vgl. BT-Drs. 17/14530, S. 40.), die sich ausschließlich auf Bitcoin beschränkten, sorgte insbesondere das Antwortschreiben des Parlamentarischen Staatssekretärs Dr.

Michael Meister vom 29.12.2017 (vgl. BT-Drs. 19/370, S. 21) – in welchem sich die Aussagen erstmals auf den generellen Terminus „Kryptowährungen" bezogen – für die derzeit ganz h.M., dass Geschäfte mit Blockchain-basierten Vermögenswerten im Privatvermögen pauschal unter § 23 EStG als private Veräußerungsgeschäfte subsumiert werden können (vgl. Stellungnahmen der Finanzverwaltung: OFD NRW vom 20.04.2018, Kurzinformation ESt, Nr. 04/2018; FinMin Hamburg vom 11.12.2017, DB 2018, S. 159; Literaturmeinungen: Behrendt, P./Janken, S., DStZ 2018, S. 345; Heuel, I./Matthey, I., EStB 2018, S. 265; Hornung, C./Westermann, B., DStZ 2018, S. 303; Kanders, T./Thonemann-Micker, S./Gräfen, M., ErbStB 2018, S. 149; Reiter, C./Nolte, D., BB 2018, S. 1180f.; Richter, L./Augel, C., FR 2017, S. 948f.; Pinkernell, R., Ubg 2015, S. 25; Eckert, K.P., DB 2013, S. 2109.). Diese undifferenzierte Klassifizierung von Kryptoassets als private Wirtschaftsgüter sollte insbesondere unter Berücksichtigung der verschiedenen funktionalen und rechtlichen Ausgestaltungsformen von Token sowie der daraus resultierenden Rechtsbeziehungen zwischen Tokeninhabern und Emittenten nicht in allen Fällen zu einer rechtskonformen Besteuerung führen. Vielmehr beschränkt sich diese steuerliche Würdigung wohl ausschließlich auf Token, die in brancheninternen Abgrenzungsversuchen als Currency- oder Utility-Token bezeichnet werden. U.E. bedarf es hier einer steuerspezifischen Differenzierung von verschiedenen Tokenmodellen, welche mit unterschiedlichen Rechtsfolgen einhergehen. Auf dieses Differenzierungserfordernis sollte in zukünftigen Verlautbarungen der Bundesregierung und Finanzbehörden insbesondere hingewiesen werden. U.E. könnte ein Differenzierungsschema wie folgt, die am Markt zu beobachtenden Erscheinungsformen sowie systemimmanente Rechtsfolgen widerspiegeln:

| Kategorie | Rechtliche Grundlage | Steuerrecht (Emittent) | Steuerrecht (Investor - laufend) | Steuerrecht (Investor - Exit) |
|---|---|---|---|---|
| Currency Token | Keine Rechtsansprüche | KSt, GewSt | - | PV: ESt (PVG)<br>BV: BE |
| Utility Token | Rechtsbeziehung zwischen Tokeninhaber und Emittent | USt, KSt, GewSt (bei Einlösung) | - | PV: ESt (PVG)<br>BV: BE |
| Mezzanin-Kapital (FK-ähnlich) und Derivate | i.d.R. schuldrechtliche Vertragsbeziehung | FK | PV: ESt (AbgSt)<br>BV: BE | PV: ESt (AbgSt)<br>BV: BE |
| Genussrecht (EK-ähnlich) | Schuldrechtliche Vertragsbeziehung | EK | PV: ESt (AbgSt)<br>BV: BE (ggf. § 8b KStG / § 9 Nr. 2a GewStG) | PV: ESt (AbgSt – ggf. § 17 EStG)<br>BV: BE (i.d.R. § 8b KStG) |

Je nach Ausgestaltung, bestimmt sich neben den ertragsteuerlichen Implikationen auch die verfahrensrechtliche Vorgehensweise. So unterliegen Erträge aus hier als Mezzanine-Kapital, Genussrecht oder Derivate dargestellte Tokenmodelle grundsätzlich nach den §§ 20, 43a ff. EStG dem Kapitalertragsteuerabzug, insofern es sich um einen inländischen Emittenten handelt oder die Verwahrung durch ein inländisches Kreditinstitut erfolgt.

(b) FIFO-Verbrauchsfolgeverfahren bei Veräußerungen von Currency und Utility Token

Nach § 20 Abs. 4 S. 7 EStG i.V.m. Rz. 97 ff. des BMF-Schreibens vom 18. Januar 2016 (Abgeltungsteuererlass) ist das First In First Out (FIFO) Verbrauchsfolgeverfahren bei der Ermittlung von Veräußerungsgewinnen aus Wertpapieren zu Grunde zu legen. Nach Rz. 97 f. des Abgeltungsteuererlasses ist diese ferner für jedes Depot einzeln vorzunehmen. Demnach gilt dies auch für Tokenmodelle, die vorstehend als Mezzanine-Kapital, Genussrecht oder Derivate dargestellt wurden. Fraglich ist die Behandlung von Currency und Utility Token, welche als private Wirtschaftsgüter dem Besteuerungsregime des § 23 EStG unterliegen. Nach ganz h.M. soll auch hier FIFO zur Anwendung kommen (vgl. FinMin Hamburg, DB 2018, S. 159; Behrendt, P./Janken, S., DStZ 2018, S. 345; Reiter, C./Nolte, D., BB 2018, S. 1182; Heuel, I./Matthey, I., EStB 2018, S. 267; Pinkernell, R., Ubg 2015, S. 25). Jedoch fehlt es bisher – mit Ausnahme des Erlasses des FinMin Hamburgs vom 11.12.2017 – einer gesetzlichen Grundlage oder Verwaltungsanweisung. In Frage kommt insbesondere in Hinblick auf das BFH-Urteil vom 24.11.1993 auch die Anwendung eines gewichteten Durchschnitt-Verfahrens, da § 23 Abs. 1 S. 1 Nr. 2 S. 3 EStG FIFO ausschließlich für Fremdwährungen normiert, welche als gesetzliche Zahlungsmittel eines ausländischen Staats definiert sind. Bis auf wenige Ausnahmen wie den venezolanischen Petro sollte dies wohl regelmäßig bei Blockchain-basierten Token nicht der Fall sein.

U.E. sollte aus gesetzessystematischen Erwägungen das FIFO-Verfahren auch für Currency und Utility Token gesetzlich oder durch Verwaltungsanweisung normiert werden, um eine Ungleichbehandlung ggü. anderen Anlageklassen zu vermeiden, für welche das deutsche Einkommensteuergesetz stringent das FIFO-Verfahren im Privatvermögen vorsieht. Ebenso sollte, wie im Abgeltungsteuererlass vorgesehen, die Anwendung des FIFO-Verfahrens depotgetrennt vorzunehmen sein, um dem Einzelbewertungsgrundsatz des § 23 EStG als „overriding principle" gerecht zu werden. Die Anwendung eines Bewertungsvereinfachungsverfahrens wie FIFO ist ein praxisnotwendiges Mittel, um der Marktkomplexität gerecht zu werden, sollte jedoch im Zweifelsfall nicht dem normierten Willen des Gesetzgebers vorgehen. Wenn ein Token in einem Depot veräußert wird, lässt sich dieser Veräußerungsvorgang regelmäßig diesem Depot zuordnen, ohne, dass dies den Komplexitätsgrad der Berechnung steigert. Demnach entspricht eine depotgetrennte, also eine nach Walletanbietern und Börsen differenzierte Anwendung von FIFO, dem teleologischen Sinn des § 23 EStG und gewährleistet trotzdem eine praxisnotwendige Vereinfachung.

(c) Rechtssystematische und praxistaugliche steuerliche Erfassung von Hard Forks durch die sog. Fußstapfentheorie

Fraglich ist, wie sog. Hard Forks, d.h. Aufspaltungen öffentlicher Blockchains ertragsteuerlich zu würdigen sind. U.E. sollte hier die herrschende Literaturmeinung zutreffend und Forks als ertragsneutraler Vorgang im Wege der Fußstapfentheorie zu behandeln sein. Die Aufteilung der historischen Anschaffungskosten sollte dabei nach der Gesamtwertmethode erfolgen (vgl. Hakert, A./Kirschbaum, B., DStR 2018, S. 882; Himmer, K./Berchtold, M. et al., Forks, 29.01.2018, http://www.explore-ip.com/2018_Implikationen-Soft-und-Hard-Forks.pdf, 23.02.2019).

(d) Etablierung einer praxistauglichen Regelung für den Einsatz von Token als Zahlungsmittel für Waren und Dienstleistungen

Die steuerliche Klassifikation von Fremdwährungen, Currency und Utility Token als private Wirtschaftsgüter bzw. Finanzinstrumente führt zu einer potentiellen Steuerpflicht von Transaktionen mit diesen. Die hieraus resultierenden Dokumentationserfordernisse stellen ein bedeutendes Hindernis für die Verwendung von Blockchain-basierten Token als alternatives Zahlungsmittel dar, da alltägliche Kaufvorgänge nur schwer mit dem rechtlichen Erfordernis der Veräußerungsgewinnermittlung vereinbar sind. Dies ist insbesondere kritisch in Bezug auf micro-payments, welche voraussichtlich im Rahmen von Internet of Things (IoT) Anwendungen eine entscheidende Rolle einnehmen werden (vgl. Sixt, E./Himmer, K. et al., Positionspapier Tax & Accounting, Bundesverband Blockchain e.V.). U.E. sollte die bestehende Freigrenze des § 23 EStG – zumindest für diese Zwecke – signifikant erhöht oder lex specialis Regelungen für diesen Anwendungsfall gefunden werden, um eine Steuerfreiheit resp. Vereinfachung der Dokumentationserfordernisse in diesem Zusammenhang sicherzustellen. Eine weitere denkbare Vorgehensweise wäre, Zahlungsvorgänge im Rahmen der persönlichen Lebensführung des Steuerpflichtigen von der Besteuerung auszuschließen.

(e) Überprüfung marktgängiger Dokumentationstools und Entwicklung von Empfehlungen für Steuerpflichtige

Durch die mediale Aufmerksamkeit, welche sich insbesondere im Jahr 2017 auf Blockchain-basierte Vermögenswerte richtete, kam es zum Markteintritt von Privatinvestoren, die regelmäßig im Unklaren über marktübliche Compliance-Anforderungen im Finanz- und Asset-Management-Umfeld sind. Dies führte zu einer nicht unbeträchtlichen Anzahl an Anlegern, die potenziell ohne Kenntnis über die steuerlichen Rechtsfolgen signifikante steuerpflichtige Einkünfte durch Tauschvorgänge zwischen verschiedenen Kryptoassets realisierten, ohne, dass ihnen Steuerliquidität in Euro zur Verfügung steht. Vor diesem Hintergrund, laufen betroffene Steuerpflichtige Gefahr Steuerhinterziehung zu begehen, wenn sie sich nicht aktiv um die Steuercompliance bemühen, d.h. ihre Anlagetätigkeit gegenüber dem Finanzamt offenlegen. Dieses Risiko wird zusätzlich durch offene Rechtsfragen, Fehlinformationen und der mangelnden Fähigkeit vieler Steuerberater große Datenmengen aufzubereiten verstärkt.

Da herkömmliche Finanzanlagen im Rahmen des Abgeltungsteuerregimes einer Quellenbesteuerung unterliegen, verlassen sich Anleger und Berater zumeist auf den Steuerabzug durch das Finanzinstitut oder den Emittenten bzw. auf offizielle Dokumente dieser. Da Currency und Utility Token jedoch keiner Quellenbesteuerung unterliegen und die branchenüblichen Finanzdienstleister i.d.R. keine Steuerreporting-Dienstleistungen erbringen, liegt die Berechnung und Erklärung der Einkünfte bei den Steuerpflichtigen und / oder ihren steuerlichen Beratern. Dies führt oftmals zu Eigenberechnungen oder den Rückgriff auf ausländische Serviceanbieter, welche nicht mit länderspezifischen Gesetzesvorgaben vereinbar sind. Bis eine funktionierende Infrastruktur im Markt vorhanden ist, kommen daher Softwarelösungen, welche Anlegern und Beratern ermöglichen rechtskonform Einkünfte in einer Form zu ermitteln und offenzulegen, dass sie von den Finanzämtern überprüft und akzeptiert werden können, eine wichtige Bedeutung zu.

Derzeit gibt es wenige Softwarelösungen für den deutschen Markt. Da es dem durchschnittlichen Rechtsanwender nicht möglich ist, Anbieter hinsichtlich einer zutreffenden Anwendung gesetzlicher Regelungen zu differenzieren, ist eine Analyse der Softwarelösungen durch die Steuerbehörden, sowie eine daraus resultierende Handlungsempfehlung für Rechtsanwender dringend zu empfehlen.

(f) Auslegung des § 23 Abs. 2 Nr. 2 S. 4 EStG in Bezug auf Blockchain-basierte Token

Oft diskutiert wird eine etwaige Verlängerung der Spekulationsfrist, wenn z.B. durch Teilnahme an Konsensfindungsalgorithmen neue Coins generiert werden. Gemäß § 23 EStG stellen Verkäufe von privaten Wirtschaftsgütern nur private Veräußerungsgeschäfte dar, wenn zwischen Anschaffung und Veräußerung nicht mehr als ein Jahr liegt. Falls durch das Wirtschaftsgut in zumindest einem Kalenderjahr Einkünfte erzielt werden, erhöht sich die Haltefrist gemäß § 23 Abs. 1 Nr. 2 S. 4 EStG auf 10 Jahre. Eine Verzehnfachung der Haltefrist hätte enorme Auswirkungen auf das Verhalten der Marktteilnehmer, denn steuerfreie Gewinne in einem derzeit noch sehr neuen und volatilen Markt wären nicht planbar. Zukunftstechnologien wie das Proof of Stake-Verfahren würden somit zumindest weniger Interesse erfahren, was potentiell mit einer negativen Auswirkung auf die Attraktivität des Innovationsstandorts Deutschlands einhergeht.

Die Einführung der Haltefristverlängerung lässt sich auf das Unternehmensteuerreformgesetz 2008 zurückführen. Die Verlängerung wurde aufgrund von Steuersparmodellen – sog. Containerleasingmodellen – eingeführt, um einen Steuerspareffekt, der sich aus einem Auseinanderfallen zwischen pauschaler Abschreibung (nach AfA-Tabelle) und tatsächlichem Wertverzehr ergab einzudämmen (vgl. BT-Drs. 16/4841, S. 58). U.E. erfordert die Gesetzesnorm demnach eine teleologische Reduktion auf ihre Zweckbestimmung als Steuervermeidungsbekämpfungsvorschrift. Die grammatikalische Umsetzung im Gesetzestext ist folglich zu breit und undifferenziert. Da Token, welche als private Wirtschaftsgüter qualifizieren, regelmäßig keinem natürlichen Wertverzehr und entsprechend keiner Abschreibung unterliegen, ist durch diese ein Steuersparmodell i.S.d. Containerleasings undenkbar. Eine Klarstellung des Gesetzgebers oder eine differenzierte Eingrenzung auf Steuersparmodelle durch Verwaltungsanweisung wäre daher erstrebenswert.

Wir bedanken uns bei den Mitgliedern der Working Group Finance, die an dieser Stellungnahme mitgewirkt haben (in alphabetischer Reihenfolge):

Dr. Christoph Gringel (Heuking Kühn Lüer Wojtek)
Dr. Sebastian Keding (McDermott Will & Emery)
Klaus Himmer (CryptoTax)
Daniel Resas (Schnittker Möllmann Partners)
Alireza Siadat (Simmons & Simmons)
Dr. Nina-Luisa Sieder (DWF Germany)

Mit freundlichen Grüßen

Florian Glatz
Präsident

Daniel Resas
Working Group Finance

BOTLabs GmbH | Keithstraße 2-4 | 10787 Berlin

**Schriftliche Stellungnahme zur öffentlichen Anhörung zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt zu schaffen" (BT-Drucksache 19/4217)**

Ingo Rübe, Geschäftsführer der BOTLabs GmbH, wurde die Gelegenheit gegeben, zu den Fragen der Anhörung schriftlich Stellung zu nehmen. Von dieser Option wird bezüglich des Punktes 7

> *„Transaktionen in der Blockchain werden häufig mithilfe sogenannter Smart Contracts abgewickelt. Derzeit bestehen jedoch Bedenken bezüglich der Rechtsgültigkeit sowie möglicher technologischer Sicherheitslücken von Smart Contracts. Die Bundesregierung muss in diesem Zusammenhang die Rechtsgültigkeit von Smart Contracts prüfen und Vorschläge erarbeiten, um für mehr Rechtssicherheit bei Smart Contracts zu sorgen."*

wie folgt Gebrauch gemacht. Wir erachten diesen Punkt als besonders wichtig, da er die Grundlage eines völlig neuen Wirtschaftszweiges darstellt und den Gesetzgeber und die Verwaltung vor große Herausforderungen stellt.

## Smart Contracts und die deutsche Rechtsordnung

1. Smart Contracts erfüllen nur teilweise die Funktionalität von Verträgen und gehen in ihren Funktionalitäten weit über klassische Verträge hinaus.

    a. Was sind Smart Contracts?

Smart Contracts können in der Vertragserstellung und im Vertragsabschluss anstelle von mündlichen oder schriftlichen Verträgen treten und sehr stark standardisierte und technisch-abwickelbare Abläufe – ähnlich wie eine mechanischer Automat – durchführen.
Der Werteaustausch funktioniert hier mit Kryptowährungen und anderen technisch überprüfbaren Leistungen (z. B. gefahrene Kilometer eines Fahrzeugs).

Auch wenn der Name „Smart Contracts" den Eindruck erweckt, dass diese anstelle von Verträgen treten, diese vollständig automatisch vollziehen und damit traditionelle Verträge obsolet machen, kann die Technologie diese Hoffnung nicht erfüllen. Es handelt sich eben nicht um Verträge, die in einen Rechtsrahmen eingebunden sind, sondern um einfache Software-Automaten, die binäre Entscheidungen treffen und niemals Umstände außerhalb ihrer beschränkten Programmierung in die Entscheidungsfindung einbeziehen.

    b. Ergänzung durch geltendes Recht

In jenen Bereichen, in denen Verträge zwingendem Recht zuwiderlaufen oder ergänzende Ansprüche, die auch dann geltend gemacht werden können, wenn diese nicht explizit im Vertrag geregelt sind (wie etwa das Gewährleistungsrecht) zustehen, können Vertragspartner ihre Transaktionen nicht ohne die üblichen staatlichen Justiz- und Vollzugsorgane durchsetzen,



BOTLABS GmbH | Keithstraße 2-4 | 10787 Berlin | Geschäftsführer Ingo Rübe | +49 151 16t8 149 49 | ingo.ruebe@botlabs.org | botlabs.org
AG Charlottenburg HRB 193450 B | USt-ID DE316284270 | Bankverbindung Deutsche Bank AG DE46 7007 0010 0249 097[illegible]

sodass der automatische Vollzug in diesen Bereichen obsolet wird bzw. zu rechtswidrigen Ergebnissen führt.

c. Höhere Funktionalität von Smart Contracts

Darüber hinaus haben höher entwickelte Smart Contracts auch die Funktionalität, dass sie Vermögen – ähnliche einem Treuhänder, aber in automatisierter Form – aufbewahren und verwalten können. So kann ein Smart Contract einen Vermögenswert erhalten haben, der als Gegenleistung des Vertrages bezahlt werden soll. Solange die Gegenleistung nicht erbracht ist, hält der Smart Contract den Wert zurück.

2. Smart Contracts eröffnen großes technisches Potenzial

Die daraus entstehenden Möglichkeiten sind sehr vielfältig, gleichzeitig stecken ihre Entwicklungen noch so in den Kinderschuhen, dass ihr volles Potential kaum überblickt werden kann. Einige Beispiele:

- Ganze Unternehmen können über Smart Contracts virtualisiert werden (Distributed Autonomous Organisations - DAOs)
- Token Curated Registries (TCRs) können als Basis von Investitionen in Unternehmen oder Projekte verwendet werden
- Im Zusammenhang mit TCRs wird eine Verbindung zwischen Blockchains und Künstlicher Intelligenz (KI) dergestalt geschaffen, dass die Kuratoren der Registries mittelfristig durch KI ersetzt werden.
- Self Owned Devices werden möglich. Ein Gerät (beispielsweise ein Auto) kann eine solitäre rechtliche Einheit bilden, sich selbst beim Hersteller leasen und sich dem Markt für Fahrten anbieten, die Fahrer automatisch bezahlen lassen und die Einnahmen für die Leasinggebühren, Treibstoff und Wartung ausgeben. Überschüsse könnten mit 100% besteuert werden, da das Auto ja keine Verwendung für Gewinne hat.

3. Divergenzen zwischen zivilrechtlicher Zuordnung und Smart Contracts

Im Zusammenhang mit Smart Contracts im Allgemeinen sowie mit TCRs und DAOs im Speziellen wird davon gesprochen, dass diese Vermögen „halten“ können – also über die einbezahlten oder darin generierten Vermögenswerte verfügen, diese dem ursprünglichen Eigentümer entziehen oder dem zukünftigen Eigentümer, der unter Umständen noch gar nicht ermittelt ist, den Zugriff noch verweigern.

Dieses Halten von Vermögen und das autonome Zuteilen an neue Eigentümer durch Software ist in der deutschen Rechtsordnung nicht vorgesehen. Vielmehr ist es vorgesehen, dass Sachen generell nur entweder jemandem gehören und damit fix zugeordnet oder derilinquiert wurden, der Besitz also aufgegeben wurde und die Sache nun niemandem mehr zuzuordnen ist. Die rechtliche Vermögenszuordnung und die Zuordnung durch die Software klaffen somit auseinander, weil zivilrechtlich auch dann, wenn der Smart Contract die Verfügung über das Vermögen entzieht, das Eigentum an dem Vermögen durch eine Person rechtlich fingiert wird.

So wird ein Vermögen, das in einem Smart Contract gelockt ist, bis die Gegenleistung erfüllt ist, weiterhin dem Vermögen des Einzahlers zuzuordnen sein und in dem Moment übergehen, in dem die Bedingung für den Transfer an die andere Partei erfüllt ist, unabhängig davon, wann der Transfer tatsächlich stattfindet.

4. Smart Contracts als Gesellschaften bürgerlichen Rechts

a. Auf Dauer agierende Smart Contracts

Dadurch, dass Smart Contracts Werte halten können, entstehen auch Smart Contracts, die auf Dauer eingerichtet sind und bei denen diese Funktionalität im Mittelpunkt steht oder zumindest eine zentrale Rolle spielt. Diese Smart Contracts halten Vermögenswerte nicht nur in Hinblick auf eine bestimmte Transaktion, sondern in Hinblick auf eine Vielzahl von Transaktionen oder als Investment in den jeweiligen Smart Contract.

b. Mögliche gesellschaftsrechtliche Einordnung

In diesen Fällen müsste nach der derzeitigen Nomenklatur des Gesellschaftsrechts eine Gesellschaft bürgerlichen Rechts entstehen. Die Personen, die Vermögen in einen Smart Contract fließen ließen müssten also als Personengesellschaft miteinander verbunden sein. Die Verfügungen über die im Smart Contract gehaltenen Werte werden zwischen den Personen und der Software getätigt, sodass die Software rein technisch, die Personen aber rechtlich als die Halter der Werte angesehen werden.

c. Rechtsunklarheit für alle Beteiligten

Dies führt zu allerlei unliebsamen Konsequenzen, weil plötzlich Personen, die in keiner Weise dauerhaft miteinander verbunden sein wollten, als Gesellschaft anzusehen wären. Auch die Themenbereiche Haftung, Eigentum an dem Smart Contract sowie die handels- und steuerrechtliche Einordnung von Leistungen und Umsätzen könnten hier zu massiven Problemen führen. Nicht zuletzt, da die rechtliche Einordnung dieser technischen Konstrukte in die dafür nicht gemachte Rechtsordnung so unklar ist, dass sowohl Personen, die in diesem Bereich technisch und/oder unternehmerisch agieren wollen als auch jene, die Smart Contracts nur für die jeweiligen Zwecke benutzen wollen, nicht abschätzen können, wie sie sich rechtskonform verhalten sollen.

d. Vorschlag zur Einbettung der Technologie in die bestehende Rechtsordnung

Wichtig wäre es einen Rechtsrahmen zu schaffen – sei es in Form eines Gesetzes für Distributed-Ledger-Technologien, sei es in Form von Ergänzungen und Konkretisierungen der Auslegung in den bestehenden Regelungen – der allen Beteiligten Klarheit über ihrer jeweiligen Eigentums- und Besitzverhältnisse sowie die rechtliche Qualifikation ihrer Interaktionen gibt.

5. Was müsste getan werden?

Notwendig wären die folgenden Maßnahmen:

a. Rechts- und Handlungsfähigkeit autonomer Smart Contracts

Smart Contracts brauchen Rechts- und Handlungsfähigkeit um die oben dargestellten Handlungen auch rechtlich vornehmen zu können.

b. Anmelde- und Prüfwesen

Zu diesem Zweck könnte der Smart Contract angemeldet werden und eine Prüfung stattfinden.

c. Steuerrechtliche Konsequenzen

Mit der Etablierung eines angemeldeten Smart Contracts ist auch der steuerrechtliche Anknüpfungspunkt geklärt, sodass erzielte Gewinne besteuert werden können.

d. Anmelder

Die Anmeldung würde offenlegen, wer den Smart Contract initiiert hat und auf Basis welcher Algorithmen Vermögensverfügungen gemacht werden. Im Falle zivilrechtlicher oder strafrechtlicher Haftungen wären konkrete natürliche oder juristische Personen greifbar. Dies könnte ebenfalls durch Blockchainmechanismen sichergestellt werden.

e. Rechtssicherheit durch Anmeldung

Durch ein Anmeldeverfahren würde die Anwendbarkeit deutschen Rechts festgehalten werden.

f. Commitment durch Kompetenz und Personalaufbau

Um eine solche Lösung umzusetzen, müsste die für die Anmeldung zuständigen Stellen z.B. die BaFin oder die Amtsgerichte, allerdings auch entsprechende Kompetenzen und Personal aufbauen. Die Anmeldung sollte ja mit einer qualitativ hochwertigen und zeitnahen Prüfung verbunden sein. Langfristig könnte dann über eine weitgehende Automatisierung nachgedacht werden.

6. Eine verbindliche Rechtsgrundlage bietet Staaten große Chancen

Mit den vorgeschlagenen Adaptionen der deutschen Rechtsordnung könnte die Bundesrepublik Deutschland der internationalen Blockchain-Szene einen rechtlichen Rahmen bieten, der weit über jenen anderer Rechtsordnungen hinausgeht. Mit diesem Standortvorteil ließen sich insbesondere jene Unternehmen und Projekte langfristig binden, die auf eine nachhaltige Geschäftsgebarung und eine rechtssichere Implementierung Wert legen. Damit würde ihre Wertschöpfung dem deutschen Staat zugänglich gemacht werden.

Zudem könnte diese rechtlich innovative und umfassende Berücksichtigung von Smart Contracts in der deutschen Rechtsordnung dafür sorgen, dass Unternehmen sich in Deutschland ansiedeln, deren Wertschöpfung und Arbeitsplätze sich hier sonst nicht verwirklicht hätten.

7. Zusammenfassung

Aktuell ist die deutsche Rechtsordnung zivil-, handels- und steuerrechtlich nicht in der Lage, innovative Smart Contracts in ihr Rechtssystem einzubetten. Die daraus entstehende Rechtsunsicherheit lässt für Unternehmer, Kunden, Verbraucher sowie den staatlichen Vollzug der Regelungen breite Nachteile entstehen, die sich auch negativ auf den Innovationsstandort Deutschland auswirken.

Demgegenüber steht das riesiges Potenzial ein völlig neuen Wirtschaftszweiges und damit verbunden die Ansiedlung und langfristige Bindung neuer Unternehmen im deutschen Wirtschaftsraum .

Der Gesetzgeber sollte hier aktiv werden.

MARTIN FRIES

Finanzausschuss des Deutschen Bundestages

An die Vorsitzende
Frau Bettina Stark-Watzinger MdB
Platz der Republik 1
11011 Berlin

# Stellungnahme

zu Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt

Zum Antrag der FDP-Fraktion im Deutschen Bundestag und ihrer Abgeordneten vom 11. September 2018 (BT-Drucks. 19/4217) möchte ich einige Überlegungen beisteuern, die sich vorrangig auf die im Antrag unter Ziffer III. 7. und 8. geforderten Maßnahmen beziehen.

## 1. Rechtsgültigkeit von Smart Contracts

Die rechtswissenschaftliche Literatur ist sich weitgehend einig darüber, dass es sich bei den in jüngster Zeit vieldiskutierten *smart contracts* nicht um Verträge im klassischen Sinne, sondern um Programmcode handelt, der dazu dient, vertragliche Pflichten automatisiert zu erfüllen oder Gütertransaktionen automatisch zu vollziehen.

> *Kaulartz/Heckmann*, CR 2016, 618 (621)
> *Finck*, in: Fries/Paal (Hrsg.), Smart Contracts, 2019, S. 1 (4 ff.)

Wer sich in ein solches Transaktionsprogramm einklinkt, kann damit zwar in den Grenzen des Vertragsrechts und namentlich des AGB-Rechts einen Vertrag schließen. Ein solcher Vertragsschluss ist aber im Kern nichts Anderes als ein Online-Kauf mit Einzugsermächtigung für den Kaufpreis oder ein eBay-Gebot mit einem bedingten Handlungsauftrag für den automatischen Bietagenten. Regelungsbedarf für das deutsche Recht sehe ich an dieser Stelle nicht. Selbst diejenigen ausländischen Rechtsordnungen, die in den vergangenen Jahren Blockchain-Gesetze erlassen haben – siehe etwa die Arizona Revised Statutes, § 44-7061 (E) No. 2) sowie die

MARTIN.FRIES@JURA.UNI-MUENCHEN.DE

Tennessee Senate Bill 1662, § 47-10-201(2) – beschränken sich mit Blick auf *smart contracts* im Wesentlichen auf deskriptive Definitionen, die das bisher geltende Recht nicht entscheidend verändern.

*Finck*, Blockchain Regulation and Governance in Europe, 2019, S. 161 ff.
*Fries*, in: Brägelmann/Kaulartz (Hrsg.), Rechtshandbuch Smart Contracts, 2019, im Erscheinen

**2. Sicherheitslücken bei Smart Contracts**

Weil der Programmcode eines *smart contract* nicht notwendig mit dem vertraglichen Pflichtenprogramm übereinstimmt, kann es dazu kommen, dass der Code eine im Vertrag nicht vorgesehene Transaktion ausführt oder aber eine Transaktion nicht ausführt, die nach dem Vertrag eigentlich statthaft wäre. Ebenso können Dritte Lücken im Code zum unrechtmäßigen Zugriff auf Token oder andere Vermögenswerte nutzen. Solche Transaktionen geschehen im Sinne des § 812 Abs. 1 S. 1 BGB ohne Rechtsgrund und lassen sich daher auf dem Rechtsweg wieder rückgängig machen. Gleichwohl trägt natürlich der Betroffene, dessen Vermögenswert unrechtmäßig verschoben wurde, die Anspruchs- und Beweislast für seinen Bereicherungsanspruch wie auch das Risiko, dass die bereicherte Person unauffindbar oder insolvent ist.

*Fries*, AnwBl 2018, 86 (88 f.)
*Heckelmann*, NJW 2018, 504 (506)

Nun werden sich Fehler im vertragsausführenden Code nie ganz verhindern lassen. Umso mehr lohnt sich allerdings eine Investition in die Programmqualität von *smart contracts*. Nach meiner Wahrnehmung ist die Blockchain-Community für dieses Thema seit dem Hack der Investmentplattform *The DAO* 2016 durchaus sensibilisiert. Im Bereich des Finanzmarkts könnten gleichwohl Prüfkompetenzen der BaFin für weiter gesteigerte Sorgfalt auf Seiten der Programmgestalter sorgen. Die BaFin müsste hierfür ihre bereits bestehenden Kompetenzen im Bereich der Distributed-Ledger-Technologie ausbauen, was allerdings mit Blick auf die prognostizierte Bedeutung der Blockchain-Technologie ohnehin sinnvoll erscheint. Auch bei einer aktiveren Rolle der BaFin müsste freilich die Letztverantwortung für den Code und seine Fehler beim Emittenten bleiben.

*Hoppen*, „TheDAO-Hack" und der letzte Flug Otto Lilienthals am 09.08.1896, CR-online-Blog v. 21. Juni 2016
*Möslein*, ZBB 2018, 208 (209 ff.)

### 3. Einführung einer Blockchain-Form

Die meisten Rechtsordnungen kennen für rechtserhebliche Erklärungen und Verträge inzwischen neben der klassischen Schriftform auch eine elektronische Form. In Deutschland knüpft § 126a BGB diese Form an eine qualifizierte elektronische Signatur. Nun haben mehrere US-amerikanische Bundesstaaten vor kurzem eine Blockchain-Form geschaffen und der elektronischen Form gleichgestellt, vgl. Arizona Revised Statutes § 44-7061(A) und (B), Tennessee Senate Bill 1662, § 47-10-202(a) und (b), Vermont Statutes, Title 12, § 1913.

Der Erlass einer ähnlichen Vorschrift in Deutschland wäre im Moment allerdings nicht sinnvoll, weil die heute verbreiteten Distributed-Ledger-Technologien im Unterschied zur qualifizierten elektronischen Signatur nicht unbedingt eine Aussage zur Identität der Netzwerkteilnehmer einfordern. Demgegenüber erscheint es durchaus erwägenswert, eine Verbriefung von Wertpapieren nicht nur auf Papier, sondern auch in einem *distributed ledger* zu ermöglichen.

*Kaulartz/Matzke*, NJW 2018, 3278 (3281 ff.)

### 4. Blockchain und Datenschutzrecht

Ohne Frage gibt es erhebliche Spannungen zwischen dem in Europa soeben erst weitgehend harmonisierten Datenschutzrecht und der Blockchain-Technologie. Im Kern geht es darum, dass die europäische Datenschutz-Grundverordnung (DSGVO) in Art. 17 Abs. 1 ein Recht auf Vergessenwerden statuiert, während Distributed-Ledger-Technologien im Grundsatz ein lückenloses Gedächtnis haben. Die DSGVO gilt zwar wie auch das Bundesdatenschutzgesetz nur für *personenbezogene* Daten, ein solcher Personenbezug ist allerdings bei Finanztransaktionen regelmäßig herstellbar. Das Dilemma lässt sich nur auflösen, wenn man entweder das geltende Datenschutzrecht lockert oder die Blockchain-Technologie entsprechend anpasst.

Bei Art. 17 DSGVO handelt es sich um eine junge Norm mit durchaus rationalem Telos, die eine ewige Datenspeicherung gegen den Willen der Betroffenen ganz bewusst verhindern möchte. Insofern sind Lösungsansätze für das Dilemma weniger in einer DSGVO-Novelle, sondern eher bei einer Anpassung der Blockchain-Technologie zu suchen. Am ehesten möglich erscheint dabei eine Entkopplung des Personenbezugs von den im *distributed ledger* gespeicherten Daten, alternativ ggf. auch eine Zentralisierung der Blockchain-Verwaltung mit zusätzlichen Kompetenzen der verantwortlichen Stelle.

*Schrey/Thalhofer*, NJW 2017, 1431 (1433 ff.)
*Martini/Weinzierl*, NVwZ 2017, 1251 (1252 ff.)
*Pesch*, in: Fries/Paal (Hrsg.) Smart Contracts, 2019, S. 13 (18 ff.)

Es erscheint gegenwärtig offen, ob es gelingen wird, die Distributed-Ledger-Technologie datenschutzkonform weiterzuentwickeln, ohne dass sie ihre wesentlichen Vorteile, namentlich den Verzicht auf Intermediäre und die hohe Fälschungssicherheit, einbüßt. Sollte dieser Versuch scheitern, wäre immerhin nicht jegliche Nutzung von Blockchain-Anwendungen ausgeschlossen, denn außerhalb des Finanzmarkts gibt es im B2B-Bereich eine Vielzahl von Projekten, die vorrangig nicht mit personenbezogenen, sondern mit objektbezogenen Daten arbeiten und daher dem Anwendungsbereich von DSGVO und BDSG von vornherein nicht unterfallen.

*Martin Fries ist Privatdozent an der Juristischen Fakultät der Ludwig-Maximilians-Universität München. https://twitter.com/mrtnfrs, https://www.youtube.com/jurapodcast/.*

IMMUTABLE ▪
▪ INSIGHT

Immutable Insight GmbH Am Schloßberg 16A 82547 Eurasburg

Deutscher Bundestag
Finanzausschuss
Die Vorsitzende
Bettina-Stark Watzinger, MdB
Platz der Republik 1
11011 Berlin

*- per E-Mail an finanzauschuss@bundestag.de -*

Katharina Gehra
Geschäftsführerin

+49 160 979 365 20
k@immutableinsight.com

07.03.2019

**Öffentliche Anhörung zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ (BT-Drucksache 19/4217)**

**Hier: Stellungnahme der Immutable Insight GmbH**

Sehr geehrte Frau Stark-Watzinger,

vielen Dank für die Benennung als Sachverständige in der öffentlichen Anhörung im Finanzausschuss zum Thema Blockchain.

Gerne nehmen wir die Gelegenheit zur schriftlichen Stellungnahme wahr, um die Abgeordneten vorab darüber aufzuklären, welchen besonderen Beitrag wir mit den Erkenntnissen aus innovativen Analysen für Sie als Gesetzgeber leisten können.

Bisher wurde die Blockchain-Technologie in der öffentlichen Wahrnehmung mehrfach mit Geldwäsche, Spekulation und Betrug bei so genannten Initial Coin Offerings (ICOs), eine neue Vorgehensweise um Kapital einzusammeln, in Verbindung gebracht. Auch das augenscheinliche Maß an Anonymität hat gemeinhin zu einem Image beigetragen, das Misstrauen nährt.

Diese Bedenken konnten sich jedoch nur deswegen so lange halten, weil verlässliche Daten, wissenschaftliche Auswertungen und die daraus entstehende Transparenz und Kenntnis gefehlt haben. Dieses Problem lösen wir. Durch proprietäre Algorithmen auf Basis der Physik komplexer Systeme und Statistik hat ein Wissenschaftler der Universität Freiburg mit einem Team aus erfahrenen Bankenspezialisten und professionellen Investoren eine Methodik entwickelt, die gerade auch Ihnen als Gesetzgeber eine Transparenz ermöglicht, die weit über das Maß hinausgeht, das in den bestehenden Aktien- oder Anleihenmärkten möglich ist. Anders als in diesen traditionellen Märkten liegen in der Blockchain per Definition immer 100% aller Transaktionen vor – da es die Natur der Blockchain ist, eine ewige, unveränderbare

Datenkette zu sein. Deshalb ist die statische Validität aller Berechnungsergebnisse signifikant höher und Aussagen wesentlich verlässlicher. Regelungen für einen Markt werden dadurch einfacher, zielgerichteter und deutlich effektiver.

Für den Gesetzgeber ergibt sich ein ganz neuer Ansatz. Missbrauchsfälle und Marktanomalien können präzise identifiziert und nachgewiesen werden. Geldwäsche, Betrug und Manipulation folgen Schemata, die wir auf Basis schon einiger weniger Parameter identifizieren können. Was bedeutet das? Wir suchen nicht die Nadel im Heuhaufen, sondern wir sieben den Heuhaufen kontinuierlich und finden Nadeln von denen Sie nicht wussten, dass es sie gibt. Zudem analysieren wir die Blockchains in Echtzeit und können dadurch auch präventiv eingesetzt werden. Eine neue Generation Compliance ist nun möglich, mit der nicht nur auf Basis des Einzelfalls hinterher einer Verdachtsmeldung *ex post* nachgegangen wird, sondern *ex ante* bzw. währenddessen kontrolliert werden kann. Diese Chance für einen neuen normativen Ansatz sollten Sie sich als Gesetzgeber vor Augen führen, wenn Sie über Regelungen in diesem Bereich nachdenken. Beispielsweise könnte sogar Geldwäsche in Echtzeit verhindert werden.

Damit können staatliche Regelungen und Kontrolle die Anwendung der Technologie für die Bürger und die Wirtschaft so sicher machen, wie die Technologie selbst.

Wie relevant diese Frage ist, zeigt sich bei der Betrachtung der zunehmenden Verbreitung der Technologie. Heute zeigt sich bereits, dass unabhängig von den volatilen und mitunter sinkenden Preisen von einzelnen Kryptowährungen das Wachstum der Konten und der Transaktionen weiterhin exponentiell und unabhängig vom Preis anhält. Das bedeutet, dass die Nutzung sich ähnlich schnell verbreitet wie zu Beginn des Internets und der Smartphones. Die Vorstellungskraft am Anfang einer solchen Entwicklung über das Maß der Ausbreitung ist meist gering, aber angesichts der Erfahrungen mit dem iPhone seit 2007 wird heute eine exponentielle Entwicklung von einer vermeintlichen Nische zu einem weiteren Massenphänomen leichter verständlich. Ähnlich wie beim Internet ist in den Anfängen auch noch manche Verbesserungsmöglichkeit gegeben, aber die Technologie als solche wird durch die breite Adaption weiterentwickelt werden. Die Chance zu handeln und einen normativen Rahmen vorzugeben ist jetzt, bevor sich erneut große Akteure mit monopolähnlicher Stellung entwickeln und eine Regelung dann ungleich schwerer.

Das Potential der Technologie liegt demnach in unserem Fokus. Beispiele aus der Praxis zu Manipulationen zeigen wie unsere Methodik diese verhindern können:

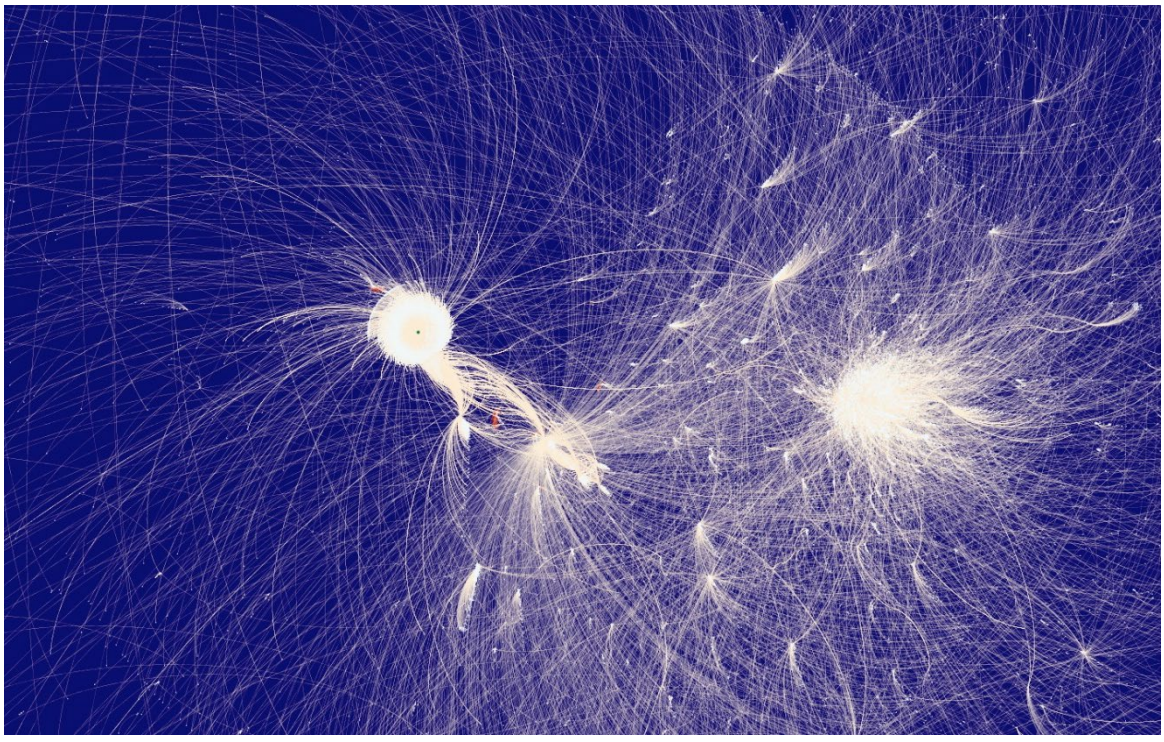
1. Preismanipulationen: Nutzer versuchen mit abgestimmtem Verhalten einen Preis künstlich in die Höhe zu bringen, um dann alles auf einmal zu verkaufen. Da das Verhalten aller Nutzer gleichermaßen betrachtet wird, fällt auf, wenn ungewöhnlich hohe Stückzahlen ungewöhnlich oft mit denselben oder einem kleinen Kreis an Nutzern gehandelt werden. Dieses Verhalten kann mit anderen, früheren oder parallel stattfindenden Mustern abgeglichen und bewertet werden. Bevor es jetzt zu dem kompletten Verkauf, also vollständigem Abstoßen des Bestands kommt, kann der Vorgang beobachtet und bei konkretem Verdacht direkt gehandelt werden. Das ist ein großer Fortschritt zu bestehenden Systemen, wird aber derzeit leider noch nicht genutzt. Wenn es implementiert ist, sind Blockchain-Nutzer vor Preismanipulationen sicher.
2. Geldwäsche: Nutzer versuchen Fiatwährungen, das heißt beispielsweise Euro oder US Dollar, über eine Reihe von Transaktionen mit unterschiedlichen Beträgen und unterschiedlichen Konten über Blockchains hinweg, das heißt beispielsweise Bitcoin, Ethereum, Omni und durch verschiedene Kryptowährungen wie Bitcoin, Ether oder den sog. „stable coin“ Tether, der an den US Dollar gekoppelt ist, den Verlauf der

Ströme zu verschleiern und somit Geld zu waschen. Das ist aber aufgrund der vollständigen Datenketten jederzeit nachweisbar – in Echtzeit, aber auch noch zu jedem Zeitpunkt danach. Mustererkennung wie unsere verhindert die vermeintliche Verschleierung von Transaktionen und sucht ähnliche Muster mit angepassten Parametern, so dass auch andere Fälle zurückschauend und auch wieder in Echtzeit gefunden werden. In bestehenden Systemen sind solche institutsübergreifenden und fragmentierten Einzelhandlungen jeweils unterhalb der kritischen Meldepflicht und daher eine Taktik, um Geld zu waschen. Das ist durch traversale Algorithmen und anderen Metriken mit unseren Methoden erkennbar, so dass präventiv reagiert werden kann.

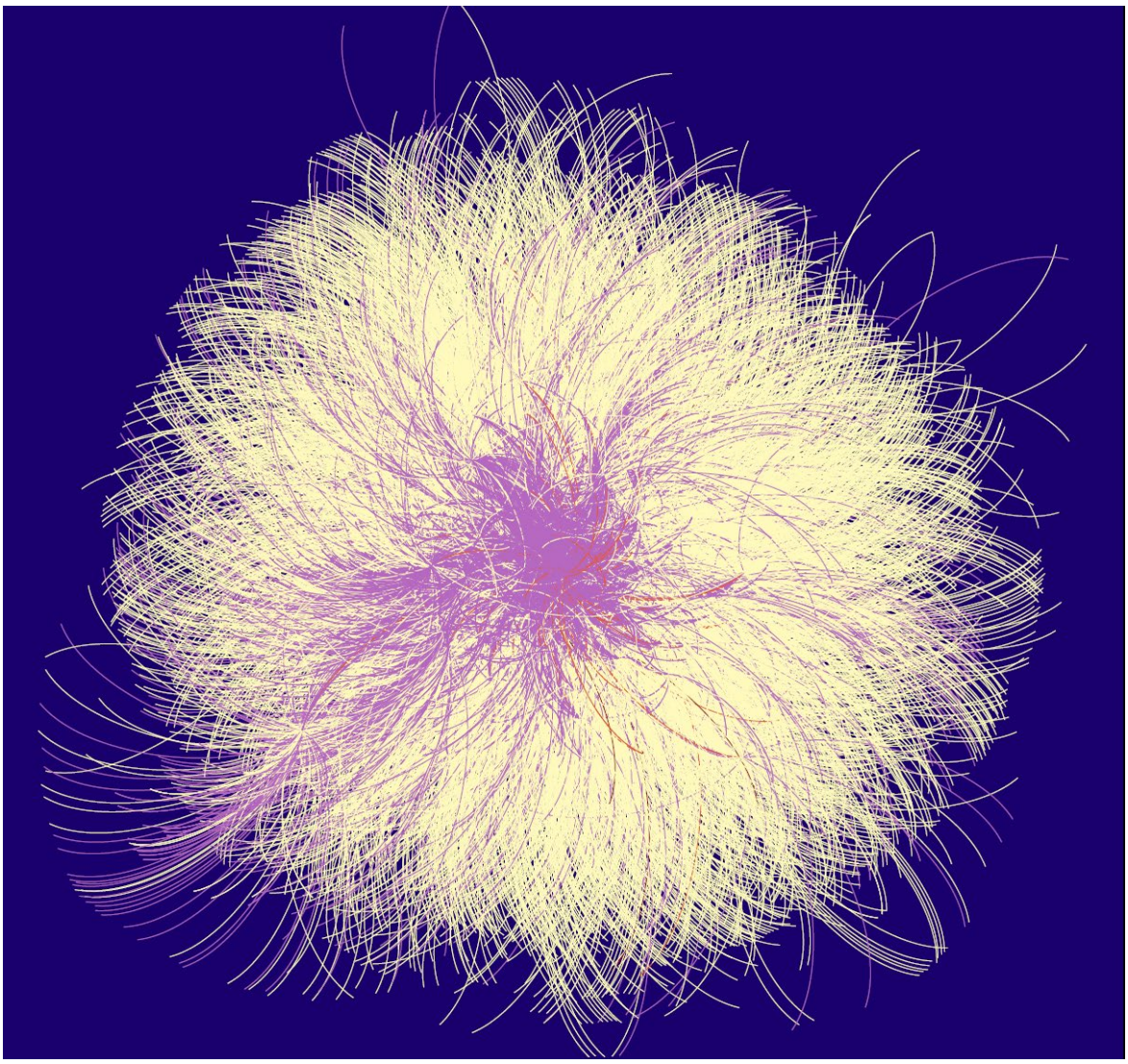
3. **Steuerbetrug**: Die Feststellung von Käufen und Verkäufen kann standardisiert pro Konto („Wallet“) erfasst werden. Angaben von Steuerschuldnern können über Muster verifiziert werden. Die Identifizierung von Personen erfolgt niemals durch uns. Dies ist eine Aufgabe der Schnittstellen zwischen Krypto- und Fiatwährungen und kann gegebenenfalls von entsprechenden Behörden erfolgen. Die dafür erforderliche durchgängige Beweiskette an Bewegungen auf der Blockchain erstellen wir lückenlos.
4. **Verhinderung von Cum-Ex Geschäften:** Durch die eindeutige Verortung eines Wertgegenstands auf der Blockchain mit der exakten Zeitangabe eines Wertübertrags ist eindeutig, wer welchen Wertgegenstand wann genau besessen hat. Die Grundlage von Cum-Ex Geschäften entfällt auf diese Weise. Auch hier ergibt sich eine bessere Ausgangssituation, um die staatliche Rahmenordnung in der Praxis durchzusetzen.

Zur Erläuterung, wie unsere Analysen diese Erkenntnisse hervorbringen, und um ohne technische Vorkenntnis die Ergebnisse verstehen zu können, arbeiten wir mit Bildern. Wir visualisieren die komplexen Datensätze, die den Vorgang statisch oder dynamisch erklären. In diesem Brief ist natürlich nur eine statische Darstellung an einem Beispiel möglich:

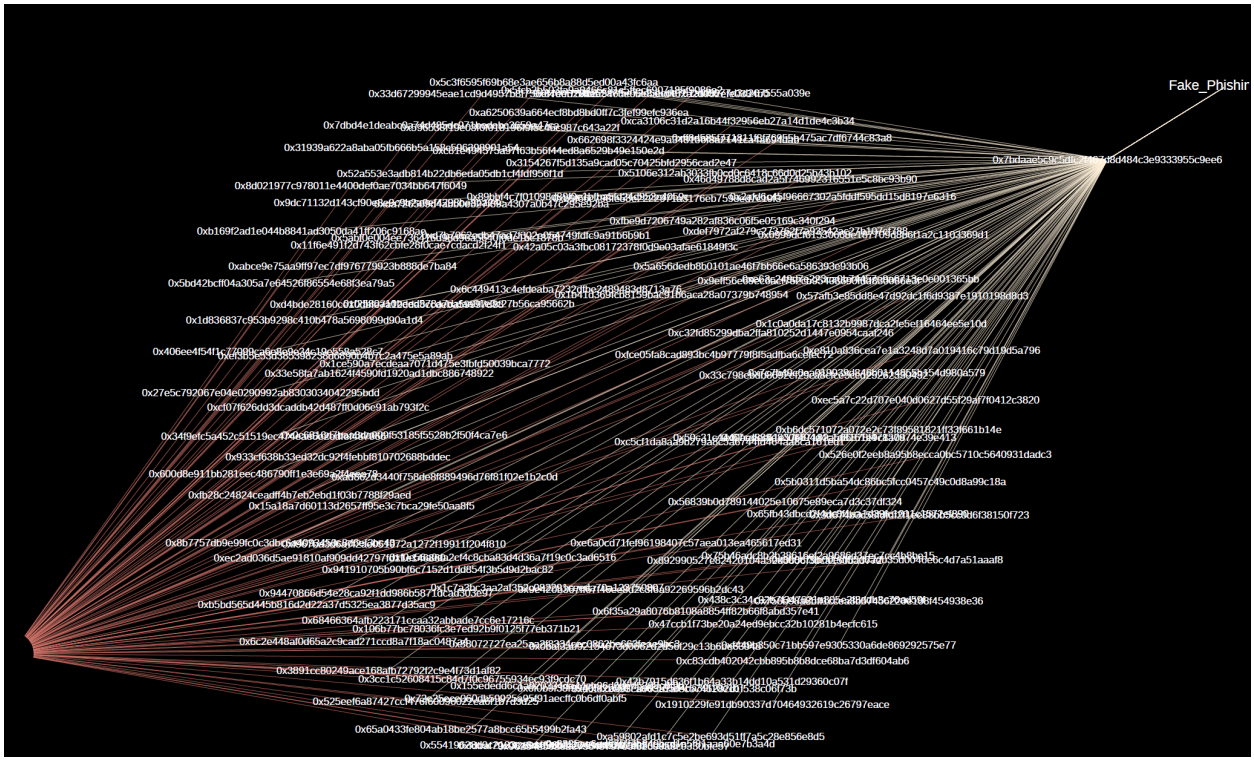
1. **Verbindungen 1. Grades**: Wir starten mit einer Darstellung am Beispiel der Ethereum Blockchain. Dort gibt es Stand heute 46.621.472 Konten, davon sind öffentlich abrufbar 1.389 Betrugskonten, das heißt 0,03% der Konten sind sogenannte „Scams“. Hier haben wir eine Visualisierung der Verbindungen 1. Grades von insgesamt 22.738 Knoten mit 118.796 Transaktionen hin zu Betrugskonten von einer Gesamtzahl von 402.376.199 Transaktionen auf der Ethereum Blockchain.



2. **Verbindungen 2. Grades**: Interessanter wird es mit jeder weiteren Analyse darüber, wie diese bekannten Knoten im weiteren Netzwerk integriert sind und wie dort 8.672 andere Nutzer mit insgesamt 152.860 Transaktionen betroffen sind. In der Graphik ist der Betrugsknoten rot markiert und alle anderen betroffenen Nutzer mit direkter Verbindung abgebildet. Das zeigt das Ausmaß der Verbreitung schon im 2. Grad.



3. **Verbindungen 3. Grades:** Aufgrund der exponentiellen Zunahme der Verbindungen haben wir nun die Darstellung wieder nur auf einen Knoten begrenzt und zeigen, wie mit Verbindungen 3. Grades über Zwischenknoten, die alle einem bestimmten Muster unterliegen und nur von den Betrugsknoten genutzt werden, eine Exchange wahrscheinlich unwissentlich mit dem Betrugskonto in Zusammenhang steht.

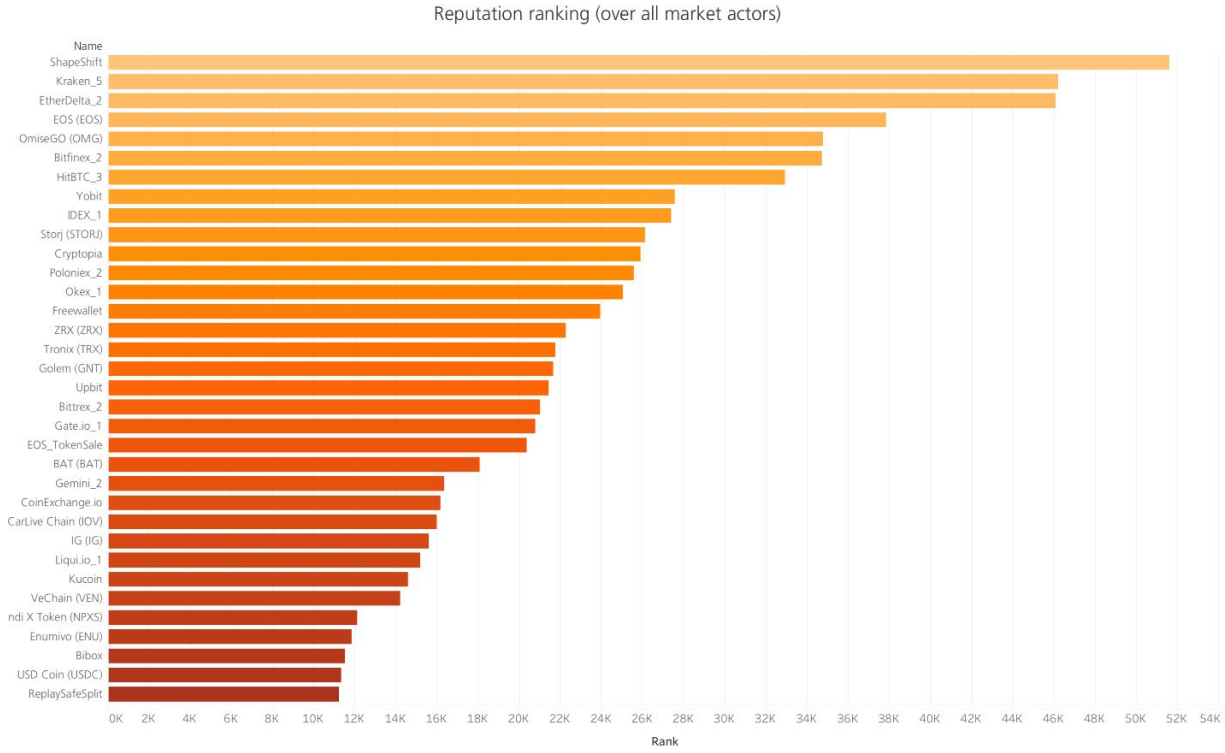



Diese Art von Transparenz macht den Unterschied. Sie ist nur auf Basis der vollständigen Daten der Blockchain in dieser Form möglich. Wenn diese Analysen eingesetzt werden, ist das Handeln und Agieren auf der Blockchain sicherer und besser regelbar als in anderen Bereichen.

Für die Legislative ergeben sich daraus eine Reihe von neuen Chancen, mit Blockchain umzugehen:

1. **Moderner, effektiver Staat – Vertrauen für die Bürger und die Wirtschaft**
   Ziel dieses Ansatzes ist es, BaFin, sowie Steuer- und Strafverfolgungsbehörden zu befähigen, in Echtzeit zu analysieren und zu reagieren, damit Deutschland der attraktivste und zugleich sicherste Standort für die entstehende Industrie basierend auf der Distributed-Ledger-Technologie wird. Diese technologische Überwachung ist nicht nur effektiver, sie ist vor allem auch viel kostengünstiger. Die Einrichtung solcher Systeme erlaubt eine automatisierte Kontrolle 24 Stunden am Tag, sieben Tage die Woche und bedarf vergleichsweise wenig personelle Ressourcen für einen deutlich besseren Effekt. Da keine personenbezogenen Daten verwendet werden, wird auch der Datenschutz auf dieser Ebene vollständig gewährt und dort, wo sich der konkrete Verdachtsfall in eine personenbezogene Untersuchung umwandelt, kann der Staat diese Daten entsprechend vertraulich behandeln und die Identität des Einzelnen schützen. Ein Staat, der durch moderne Methoden eine Vorreiterrolle einnimmt, kann das Vertrauen seiner Bürger und der Wirtschaft in seine Verlässlichkeit und das funktionierende Gemeinwesen beweisen. Jeder kann teilhaben an der neuen Technologie und wird dabei vor Betrug geschützt.

2. **Sicherheit durch Standortattraktivität**
   Standortattraktivität führt auch zu einer wachsenden Anzahl von Teilnehmern in den verschiedenen Netzwerken, das heißt „Nodes“, also Knotenpunkten in einer Blockchain. So kann sich Deutschland vor Konzentrationsrisiken in anderen Ländern schützen und die Dezentralität als ein bestimmendes Element in der Sicherheitsarchitektur einer Blockchain erhalten. Derzeit variiert die Anzahl der Nodes teilweise stark. Generell sind 50% der Anzahl an Nodes eine kritische Schwelle für die Sicherheit des Netzwerks. Kurzfristig kann man Nodes im Markt kaufen, ein gewisser Puffer ist daher empfehlenswert. Als Beispiel: Bei Ethereum dominieren derzeit die Vereinigten Staaten von Amerika mit ca. 34% der Knoten, gefolgt von Deutschland mit ca. 12% und der Volksrepublik China mit 7,5%. Eine weitere internationale Diversifizierung und vor allem die Stabilisierung der Anzahl der deutschen Knoten sollte Teil einer Sicherheitsinfrastruktur sein, die auch von der Attraktivität des Standorts abhängt.
   Neben den Nodes betrifft das heute schon die wichtigsten Anbieter auf der Ethereum Blockchain, keiner davon ist jedoch in Deutschland ansässig:




3. **Wirtschaftspolitik für die Industrie 4.0 und das Internet der Dinge**
   Für den Industriestandort Deutschland ist neben der Finanzplatzattraktivität vor allem aber auch die Bedeutung von Distributed-Ledger-Technologien für die produzierende Industrie zu betonen. Industrie 4.0 und das Internet der Dinge ziehen sich als Zukunftsthemen durch die Automobilwirtschaft, die Energiewirtschaft, Logistik und dem Gesundheitswesen und alle diese brauchen ebenso effektive und moderne, effiziente Regelungssysteme, die mithilfe der neuen Analysemethoden andauernd geprüft, gewartet und vor Missbrauch geschützt werden können. Auch kritische Infrastruktur kann dadurch besser abgesichert werden und Attacken abgeschreckt werden. Die Analysemethodik kann nämlich grundsätzlich auf allen privaten wie auch öffentlich zugänglichen Blockchains angewandt werden. Damit ist auch Maschine an Maschine-Kommunikation als Basis des Internets der Dinge deutlich besser handhabbar und Algorithmen können auf diesen speziellen Anwendungsfall ausgerichtet werden.

4. **Echte Prävention von Geldwäsche und eine neue Compliance**
   In den bestehenden Systemen ist Geldwäsche oft einzelfallbasiert und reaktiv. Die Systematik von Geldwäsche und Betrugsaktivitäten wird dadurch nicht erfasst. Wenn man als Gesetzgeber den Anspruch hat, diese kriminellen Aktivitäten nicht nur hinterher aufzudecken, sondern sie systematisch zu bekämpfen, kann man dies durch die Anwendung der Analysemethoden auf den Blockchains nun in Echtzeit realisieren. Eine Verpflichtung der Anbieter von Tokens, E-Geldinstituten und Händler zur Nutzung der neuen, technologisch möglichen Monitoring-Methoden in Echtzeit ist dafür die Grundlage.

5. **Harmonisierung der Rechtsgrundlagen und Schließung von Regelungslücken**
   Anpassung der Gesetzgebung, so dass die rechtlichen Tatbestände mit den bestehenden Analysemöglichkeiten auch abgedeckt sind und Regelungslücken, beispielsweise zwischen EU oder EWR Staaten geschlossen werden

Wenn nun in Deutschland eine Diskussion über die zukünftige Rolle der Distributed-Ledger-Technologie und ein effektives Regelwerk gesprochen wird, kann unsere „Made in Germany"-Expertise Grundlage für eine international führende Rolle Deutschlands begründen. Sie haben es jetzt allein in der Hand, der Technologie den Schrecken zu nehmen und faires und wohlstandsförderndes Wachstum durch eine Zukunftstechnologie zu ermöglichen.

COT LEGAL

Rechtsanwältin Claudia Otto
OpernTurm
Bockenheimer Landstraße 2-4
60306 Frankfurt am Main
Telefon: +49 69 667 748 360
Telefax: +49 69 667 748 450
Mail: claudia.otto@cot.legal
Web: https://cot.legal

# Schriftliche Stellungnahme

der geladenen Sachverständigen Rechtsanwältin Claudia Otto

im Rahmen der

## Öffentlichen Anhörung zu dem Antrag der Fraktion der FDP „Zukunftsfähige Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt schaffen“ (BT-Drucksache 19/4217)

im Finanzausschuss des Deutschen Bundestages am 11. März 2019

Inhaltsverzeichnis

Zum Antrag

I. Zum Beschlussantrag I 3
II. Zum Beschlussantrag II 3
III. Zu den Maßnahmenforderungen 4
1. Aufbau von „Kompetenzen" innerhalb der BaFin 4
2. Mehr Transparenz und Einblick in die Praxis der BaFin 5
3. Beschneiden von Verbraucherrechten und Enthaftung durch „freiwillige Prospekte" 5
4. Zur technischen Möglichkeit der Blockchain-Recherche 10
5. (Verbraucher-)Schutzvorschriften dürfen nicht angetastet werden 10
6. Das Urkundserfordernis nicht abschaffen, sondern ergänzen 15
7. Smart Contracts mit Bedacht verwenden, Verbraucher und Wirtschaft stärken 15
8. Die Datenschutzgrundverordnung (DSGVO) ist nicht das Problem, sondern die „Use Cases" 16
9. „Wallet"-Verwaltung durch die Banken? 16
10. Besteuerung 17

Anlage

Die andere Seite der Krypto-Münze

I. Blockchain-Technologie 1
1. Überblick 1
2. Mythen und Realität 1
3. Reale Gefahren, über die Blockchain-Produkteanbieter schweigen 4
II. Smart Contracts 5
1. Was ist ein Smart Contract? 5
2. Verwendung und Probleme 5
III. Token 6

## I. Zum Beschlussantrag I

Die Blockchain ist eine interessante Technologie, deren primärer Zweck im direkten Teilen von Nutzerwissen besteht. Die Nutzer bestimmen, welches Wissen sie mit anderen teilen möchten. Und sie bestimmen gemeinsam, welches Wissen teilenswert ist. „Wissen" ist hier weit zu verstehen.

Weil die Abstimmung zum regelmäßigen Aufstauen neuer Einträge führen würde, wird der Abstimmungsprozess durch einen Konsensmechanismus ersetzt. Das bedeutet, auch eine inhaltliche Prüfung der Einträge findet nicht statt. Aus diesem Grund gelangen ungehindert falsche Daten und Behauptungen, strafbare Inhalte und sonstig rechtlich problematische Materialien in die gemeinsame Datensammlung. Auch die vermeintliche Unabhängigkeit von den „Großen" ist vielmehr eine andere Form der Abhängigkeit, mit anderen Risiken. Diese werden in der Anlage „Die andere Seite der Krypto-Münze" erläutert.

Die Blockchain-Technologie ist nicht mehr neu. Sie ist mittlerweile, geht man vom Peer-to-Peer Electronic Cash System nach *Satoshi Nakamoto* (i.e. *Bitcoin*) aus, über zehn Jahre alt. Ihre Entwicklungsfortschritte im Vergleich zu anderen Technologien sind eher klein. Sie ist nicht ökonomisch, was u.a. aus dem nicht vorgesehenen Löschen von Alt-Daten folgt. Die Risiken der Nutzung sind dazu enorm hoch, wie sich aus der Anlage ergibt. Die beworbenen „Use Cases" befinden sich fast ausschließlich in der Experimentierphase – dementsprechend gibt es wenig belastbare Erfahrung mit Anwendungsmöglichkeiten dieser Technologie. Grundsätzlich können bewährte Technologien eine bessere, verlässlichere und sicherer Umsetzung gewährleisten. Dabei ist jedoch nicht ausgeschlossen, dass es nicht-prominente, nützliche Anwendungen gibt oder geben kann.

Gesetze müssen technologieneutral sein. Zum einen, um die Innovationskraft der Wirtschaft zu fördern statt zu bremsen. Zum anderen, um ihre Umgehung unter Anwendung anderer Technologien zu verhindern. Die Gesetze geben einen Rahmen vor, der mit juristischem Handwerkszeug zu bestimmen und auszufüllen ist. Insofern wird kein Bedarf für Blockchain-Gesetze gesehen. Das Geschäft mit den „Token" stellt jedoch eine Gefahr für die Rechtsordnung, vor allem die Verbraucher, dar. Hier muss der Schutz verbessert werden.

## II. Zum Beschlussantrag II

Das Potential der Blockchain-Technologie, im Vergleich zu anderen Technologien, ist auch nach über zehn Jahren ungewiss. Insbesondere ist ungewiss, ob eine geradezu exponentiell an Datenvolumen zunehmende Datensammlung in 10 Jahren überhaupt noch nutzbar ist. Niemand weiß, was mit den ausschließlich hierin konzentrierten Daten passieren wird. Der Grund für ein Tätigwerden des Gesetzgebers sollte es daher vielmehr sein, den Wirtschaftsstandort Deutschland sowie seine Bürger (i.e. Verbraucher) zu stärken und Innovation mit einem technologieneutralen Ansatz zu fördern, wie vor.

Dem Antrag ist insoweit beizupflichten, dass Rechtsunsicherheit besteht, die beseitigt werden muss. Diese Rechtsunsicherheit gründet sich aber vor allem auf dem Umstand, dass wesentliche Informationen vonseiten der Blockchain-Produkteanbieter nicht zur Kenntnis gebracht werden. Die Rechtsunsicherheit kann durch mehr Offenheit auf Anbieterseite und Aufklärung vonseiten der Aufsicht beseitigt werden.

## III. Zu den Maßnahmenforderungen

### 1. Aufbau von „Kompetenzen" innerhalb der BaFin

Es ist nicht klar, was der Antrag mit „Kompetenz" meint:

#### a) Fachliche Kompetenz?

Ein Mangel an fachlicher Kompetenz bei der BaFin ist nicht ersichtlich. Eine solche Forderung wäre nicht nur unangemessen, sondern auch widersprüchlich: So wird die Einzelfallprüfungspraxis der BaFin unter II. Abs. 2 verurteilt, weil sie

> *„nötige Innovationen im Markt hemmt"*.

Die Einzelfallprüfung verlangt fachliche Kompetenz, doch die Einzelfallprüfung will der Antrag offenbar abgeschafft wissen. Die Einzelfallprüfung wäre vielleicht obsolet, würde eine Sach- und Rechtslage aufgezeigt, die leicht zu klären wäre. Das ist jedoch nicht der Fall. Im Übrigen hat die offene, kompetente und verständliche Information der Verbraucher bisher die BaFin übernommen.

#### b) Kompetenz im Sinne von Zuständigkeit?

Die BaFin ist eine Aufsichtsbehörde. Die Forderung einer weiteren Kompetenz im Sinne der Zuständigkeit,

> *„Die BaFin sollte insbesondere bei Fragen zur Blockchain-Technologie eine aktivere Rolle bei der Förderung des Finanzplatzes Deutschland im Sinne der Wettbewerbspolitik einnehmen"*

ist problematisch. Eine zugunsten der Blockchain-Technologie aktive*re*, und damit einseitige wettbewerbspolitische Förderung geht über die Aufsichtsfunktion hinaus und dürfte eine Markteingriffsposition begründen. Darin kann eine Benachteiligung anderer Anbieter gleicher Produkte, aufbauend auf anderen – weniger riskanten – Technologien, liegen. Die BaFin darf darüber hinaus gegenüber Verbrauchern keine Empfehlungen aussprechen und viele Fragen nicht beantworten, etwa zur Sicherheit einer Geldanlage oder Vertrauenswürdigkeit eines Unternehmens.[1] Erst recht darf die BaFin kein Absatzgeschäft, womöglich noch zum Nachteil von Verbrauchern, wider ihre Aufgabe des kollektiven Verbraucherschutzes aktiv fördern. Etwa, indem sie ihren Verbraucherwarnungen widerspricht. Das Risiko des Totalverlustes besteht weiterhin, wie sich aus der **Anlage** ergibt.

#### c) Kompetenz im Sinne von Personalstärke?

Dem Antrag ist zuzustimmen, soweit er mehr Kompetenz im Sinne der Personalstärke fordert, um die jeweils notwendige Einzelfallprüfung in kürzerer Zeit vornehmen zu können.

Kryptowährungen, „Token", ICO und Verwandte wie „STO" (Security Token Offering), „ITO" (Initial Token Offering) und „TGE" (Token Generation Event), stellen die BaFin vor große Herausforderungen. Die größte Herausforderung von allen ist jedoch, die besonders kreativ ummantelten Vorhaben vieler Blockchain-Produkteanbieter auf ihren Kern hin zu untersuchen und diesen der rechtlichen Prüfung zu unterziehen. Zu oft geht es schlichtweg um die Umgehung von bestehendem Recht. Hier ist die BaFin ein ganz entscheidender, unverzichtbarer Garant für Verbraucherschutz.

---

[1] https://www.bafin.de/DE/Verbraucher/BaFinVerbraucherschutz/Grenzen/was_macht_die_bafin_nicht_node.html (zuletzt abgerufen am 3. März 2019).

Darüber hinaus ist das für Aufsichtszwecke aus einer öffentlichen Blockchain zu extrahierende Wissen derart zahlreich, dass es nur mit einem großen, professionell breit aufgestellten Team erfasst, in Beziehung gesetzt und bewertet werden kann.

### 2. Mehr Transparenz und Einblick in die Praxis der BaFin

Dem Antrag ist insoweit zuzustimmen, dass die BaFin mehr Einblick in ihre Arbeit geben sollte. Die Transparenzforderungen sind jedoch (erneut) einseitig zugunsten der Blockchain-Produkteanbieter:

Die Blockchain-Produkteanbieter (in spe) sollen sich über die konkreten Anforderungen an sie informieren können. Das ist eine legitime Forderung. Abzulehnen ist jedoch ihre Forderung, nur in anonymisierter Form Gegenstand der verlangten Informationsplattform werden zu können, wenn sie gegen geltendes Recht verstoßen haben. Es ist ein längst überfälliger und notwendiger Schritt, eine Plattform vergleichbar der Entscheidungsdatenbank der Missbrauchsaufsicht des Bundeskartellamts[2] einzurichten, bei der (auch) Verbraucher sich schnell, unkompliziert und umfassend informieren können.

Die belgische *Financial Services and Markets Authority* (*FSMA*) führt beispielsweise ein übersichtliches, leicht erfassbares und durchsuchbares Informationsportal über rechtswidrig agierende Unternehmen im Finanzbereich.[3] Dabei kann die Suche u.a. direkt nach hochrelevanten Sachverhalten wie „Cryptocurrency" oder „Ponzi Schemes" gefiltert werden. Insbesondere für Verbraucher ist eine solche leichte Verfügbarkeit von Informationen – ausweislich der allgemeinen Verbraucherwarnungen von ESMA, BaFin u.a. – existentiell wichtig. Die Website der BaFin ist leider unübersichtlich, schwer zu bedienen und nicht verbraucherfreundlich.

Allerdings kann die Forderung nach mehr Transparenz nicht so weit gehen, dass die BaFin die Verpflichtung notwendiger Verbraucherinformation vor bzw. bei Vertragsschluss den Blockchain-Produkteanbietern abnimmt.

Für die Schaffung und den Betrieb eines solchen Informationsportals bedarf es des Personalaufbaus, siehe oben.

### 3. Beschneiden von Verbraucherrechten und Enthaftung durch „freiwillige Prospekte"

Ziffer 3 des Antrags zielt offenbar darauf ab, Verbraucherrechte empfindlich zu beschneiden und gleichzeitig die Blockchain-Produkteanbieter von jeder Haftung zu befreien.

#### a) Streichung des Nebeneinanders von spezialgesetzlichen und zivilrechtlichen Ansprüchen

Den Verdacht löst folgender Satz aus:

> *„Für diese soll dann anstatt des allgemeinen zivilrechtlichen Rahmens die gesetzliche Prospekthaftung gelten."*

Die geltenden § 306 Abs. 6 S. 2 Kapitalanlagegesetzbuch (KAGB) und § 20 Abs. 6 S. 2 Vermögensanlagegesetz (VermAnlG) stellen gleichlautend klar, dass zivilrechtliche Ansprüche *neben* den Ansprüchen aus der spezialgesetzlichen Prospekthaftung stehen:

---

[2] https://www.bundeskartellamt.de/SiteGlobals/Forms/Suche/Entscheidungssuche_Formular.html?nn=3590026&cl2Categories_Format=Entscheidungen&cl2Categories_Arbeitsbereich=Missbrauchsaufsicht&docId=3590026 (zuletzt abgerufen am 27. Februar 2019).

[3] https://www.fsma.be/en/warnings/companies-operating-unlawfully-in-belgium (zuletzt abgerufen am 27. Februar 2019).

> *„Weiter gehende Ansprüche, die nach den Vorschriften des bürgerlichen Rechts auf Grund von Verträgen oder unerlaubten Handlungen erhoben werden können, bleiben unberührt."*

Wenn hier im Antrag von „anstatt" die Rede ist, bedeutet dies im Ergebnis die Forderung einer Streichung des Nebeneinanders von (Verbraucher-)Ansprüchen.

b) Entrechtung der Verbraucher „made in Germany"

Die geforderte Beschränkung der Haftung auf die spezialgesetzliche Prospekthaftung würde bedeuten, dass die zu „freiwilliger Prospekterstellung optierenden" Anbieter von Blockchain-Produkten sich von Anfang an von der Haftung frei machen könnten:

aa) Haftungsfreiheit als Anreiz zur Anlegermanipulation

So regelt vorgenannter § 20 Abs. 4 Nr. 1 VermAnlG den Ausschluss des Anspruchs aus Prospekthaftung, wenn

- *die Vermögensanlagen nicht auf Grund des Verkaufsprospekts erworben wurden,*

und § 306 Abs. 3 S. 2 Nr. 2 KAGB jenen Ausschluss, wenn

- *die Anteile oder Aktien nicht auf Grund des Verkaufsprospekts oder der wesentlichen Anlegerinformationen erworben wurden.*

Eine entsprechende Ausschlussregelung findet sich in § 23 Abs. 2 Nr. 1 Wertpapierprospektgesetz (WpPG). Hiernach besteht der Anspruch nach den §§ 21 oder 22 WpPG nicht, wenn

- *die Wertpapiere nicht auf Grund des Prospekts erworben wurden.*

Die Erfahrung der letzten Jahre hat gezeigt, dass Investitionsentscheidungen im „Krypto-Bereich" zu oft auf beeinflussten[4] Emotionen[5], vor allem auf Angst (FOMO, Fear Of Missing Out),[6] und nicht etwa Sachinformationen wie in einem Verkaufsprospekt beruhten. Ein bekanntes Beispiel ist der sog. Fake Exit Scam, ein PR-Stunt des Vorstandsvorsitzenden der *Savedroid AG* im April 2018.[7] Er gab in den sozialen Medien vor, sich mit dem Geld der Investoren abgesetzt zu haben, während auf der Firmen-Website „And it's gone!" stand. Der Firmensitz war geräumt. Es brach Panik aus. Auf der ganzen Welt wurde vom *Savedroid* ICO berichtet. Hier wurden vorhersehbare, da menschliche Denk- und Verhaltensweisen zielgerichtet ausgelöst und ganz bewusst zu Marketingzwecken ausgenutzt. Es gibt keinen Grund zur Annahme, dass diese Art der Absatzförderung der Vergangenheit angehört.

Wird die zivilrechtliche Prospekthaftung gestrichen, gibt es sogar einen Anreiz, Anleger zu manipulieren. Denn dann kommt es auf fehlerhafte Angaben im Prospekt nicht mehr an.

bb) Haftungsausschluss dank manipulierbarer Technologien

Des Weiteren regelt § 20 Abs. 4 Nr. 2 VermAnlG, dass ein Anspruch aus spezialgesetzlicher Prospekthaftung nicht besteht, wenn der Sachverhalt, über den unrichtige oder unvollständige

---

[4] *Penke*, „Es war wie bei Wolf of Wall Street", „Peniswitze auf Kosten der Kunden", 21. August 2018, https://www.gruenderszene.de/allgemein/savedroid-mitarbeiter-ico (zuletzt abgerufen am 6. März 2019).
[5] Im Internet finden sich etwa Anleitungen wie „Verdiene Millionen! 5 Schritte zum eigene Shitcoin" – Geldhelden, finanzielle Bildung (auf die Angabe des Link wurde bewusst verzichtet).
[6] *Dörner*,„ICO-Fieber: Wer bleibt als Amazon der Blockchain-Blase über?", t3n vom 24. Juli 2017, Seite 2, „Das FOMO-Phänomen: Fear of missing out": https://t3n.de/news/ico-blockchain-eos-840805/2/ (zuletzt abgerufen am 6. März 2019).
[7] „DRPR spricht Rüge gegen Savedroid aus", 29. Oktober 2018, PRReport, https://www.prreport.de/singlenews/uid-885886/drpr-spricht-ruege-gegen-savedroid-aus/ (zuletzt abgerufen am 6. März 2019).

Angaben im Verkaufsprospekt enthalten sind, nicht zu einer Minderung des Erwerbspreises der Vermögensanlagen beigetragen hat.

§ 23 Abs. 2 Nr. 2 WpPG lautet ähnlich, dahingehend, dass ein Anspruch nach den §§ 21 oder 22 WpPG nicht besteht, sofern der Sachverhalt, über den unrichtige oder unvollständige Angaben im Prospekt enthalten sind, nicht zu einer Minderung des Erwerbspreises der Wertpapiere beigetragen hat.

In einem öffentlichen Blockchain-Netzwerk besteht ausweislich der Anlage jederzeit die Gefahr, dass jemand die Kontrolle über das Netzwerk erlangt und ausnutzt.[8] „Preise" von „Token" können dann „von innen" manipuliert werden. Darüber hinaus können die „Kurse" sog. Kryptowährungen und „Token" von außerhalb des Netzwerks,[9] etwa durch Trading Bots,[10] beeinflusst werden. Es genügt zudem ein Programmierfehler, der bei einer Technologie mit wenig Erfahrungswerten an der Tagesordnung ist.

Selten, womöglich nie, wird eine Minderung des Erwerbspreises auf einen fehlerhaften Verkaufsprospekt zurückzuführen sein. Auch hier würde die Haftung der Anbieter quasi ausgeschlossen. Sie könnte sogar aktiv beseitigt werden.

### cc) Haftungsausschluss wegen offenkundiger Unrichtigkeit

Vorstehendes bedeutet im Ergebnis, unrichtige Informationen in freiwillig erstellten Prospekten zu „Blockchain"-Produkten blieben weitgehend ohne Konsequenzen. Die Verbrauchertäuschung würde (l)egal. Verbraucherschutz darf jedoch nicht zum glücklichen Einzelfall werden.

Es besteht ebenfalls kein Anspruch aus spezialgesetzlicher Prospekthaftung, wenn der Erwerber die Unrichtigkeit oder Unvollständigkeit der Angaben des Verkaufsprospekts beim Erwerb kannte (§ 20 Abs. 4 Nr. 3 VermAnlG, § 306 Abs. 3 S. 2 Nr. 1 KAGB, § 23 Abs. 2 Nr. 3 WpPG). Wie in der Anlage aufgezeigt, sind die regelmäßig behaupteten, wesentlichen Eigenschaften der Blockchain-Technologie unrichtig. Im Hinblick auf die immensen Risiken sind die Angaben regelmäßig unvollständig. Da korrekte Informationen jedoch frei zugänglich im Internet verfügbar sind,[11] wären anderslautende Prospekte für Blockchain-Produkte sogar offenkundig unrichtig.

Kein Geschädigter könnte auf Vorlage widerlegen, dass er öffentlich zugängliche Informationen zu Blockchain, Smart Contracts und Token gesehen haben soll. Er könnte, würde es nach dem Willen der Blockchain-Produkteanbieter gehen, ihnen nicht einmal mehr eine unerlaubte Handlung vorwerfen.

### dd) Das Zivilrecht darf nicht ausgeschaltet werden

Es wäre fatal, würde die zivilrechtliche Haftung antragsgemäß ausgeschaltet. Denn das Zivilrecht ist gleichzeitig sowohl die Grundlage für die Existenz von „Blockchain-Produkten" als auch Grund für ihre (schützende) Nichtexistenz:

---

[8] Siehe außerdem zur Macht von sog. Whales, *Cuthbertson*, „Bitcoin Price Crash: „Manipulative Whales' Cause Cryptocurrency Market Meltdown", 6. September 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-crash-whales-cryptocurrency-market-explained-analysis-a8525761.html; *alexth*, „What Are Crypto Whales And Why You Should Fear Them, https://steemit.com/cryptocurrency/@alexth/what-are-crypto-whales-and-why-you-should-fear-them (zuletzt abgerufen am 6. März 2019).

[9] *Gandal* u.a., „Price manipulation in the Bitcoin ecosystem", Journal of Monetary Economics, Vol. 95, Mai 2018, . 86 ff., https://www.sciencedirect.com/science/article/abs/pii/S0304393217301666 (zuletzt abgerufen am 6. März 2019).

[10] *Coleman*, „Bitcoin Price Manipulated by Cryptocurrency Trading Bots: WSJ", 2. Oktober 2018, https://www.ccn.com/bitcoin-price-manipulated-by-cryptocurrency-trading-bots-wsj (zuletzt abgerufen am 6. März 2019).

[11] Vgl. *Ethereum* Legal Agreement: https://www.ethereum.org/agreement (zuletzt abgerufen am 6. März 2019).

(1) Grund für Existenz: Privatautonomie

Wenn von „Token" gesprochen wird, meint man Informationen, also Daten, die in einer elektronischen Datenbank verarbeitet und in ihrer Gesamtheit auf zahlreiche Rechner kopiert werden. Im Rahmen der Privatautonomie kann man grundsätzlich auch Daten zum Gegenstand eines Vertrags, also Verpflichtungsgeschäfts, machen. Forderungen gegen einen anderen können, so wie Buchgeld, ganz unterschiedliche Manifestierung erfahren. Die Blockchain ist nur ein (anderes) Instrument der Dokumentation.

(2) Grund für Nichtexistenz: Mangelnde Eigentumsfähigkeit

Dateneigentum gibt es nicht. Eigentum kann allenfalls an den auf einer körperlichen sog. Hard(ware) Wallet gespeicherten „Token"-Daten bestehen oder der gesamten, abgespeicherten Datenbank-Kopie (vergleichbar einer käuflich erwerb- und downloadbaren Software).[12] Im letzteren Falle ist ein Kaufvertrag über die Kopie als ein „sonstiger Gegenstand" im Sinne des § 453 Abs. 1 Alt. 2 Bürgerliches Gesetzbuch (BGB) denkbar.

Doch die „Token" als Daten sind aus der gesamten, untrennbaren Datensammlung der Blockchain nicht herauslös- und übertragbar. Eigentum im Sinne des § 903 BGB kann an „Token" daher nicht entstehen. Der hierfür charakteristische Ausschluss „jedermanns" von der Einwirkung ist in einem Blockchain-Netzwerk nicht möglich, was sich schon aus der fehlenden eigenen Kontrolle über das Netzwerk, seine Rechner und seine gemeinsam geteilte Datensammlung ergibt. Erlangt jemand die Kontrolle über das Netzwerk wie in der Anlage beschrieben, kann er jeden „Token-Kontostand" zu seinen Gunsten ändern und die veränderte Datensammlung mit mindestens 51 % der Netzwerk-Rechner synchronisieren. Der zuvor als „Berechtigter" Ausgewiesene kann als Teil der Minderheit nichts hiergegen unternehmen. Er konnte schon den die Kontrolle erlangenden Angreifer nicht von der Änderung abhalten. D.h. er konnte ihn – wie jedermann – nicht von seiner „Rechtsposition" ausschließen, die „seine Token" angeblich „verkörpern".

c) Keine verbindlichen Auskünfte durch die BaFin zu ungeprüften Fragen

Die Forderung, dass die BaFin verbindliche Auskünfte auf unzureichend geklärter Sach- und Rechtslage treffen soll, ist abzulehnen. Die „Token" der Blockchain-Produkteanbieter bergen zu viele Risiken und Nachteile für Verbraucher sowie die Finanzwirtschaft als Ganzes. Redlichen Unternehmen würde infolge einer Benachteiligung im Wettbewerb der Anreiz genommen, sich redlich zu verhalten.

aa) Weitere ungeklärte Fragen: LeerverkaufsVO

Unter Hinweis auf den Schaffungsprozess von „Token" in der Anlage muss zusätzlich geklärt werden, grundsätzlich und stets im Einzelfall *vor* Auskunft, ob es sich bei „Verkäufen" von „Token" dieser Art und Herkunft um verbotene ungedeckte Leerverkäufe im Sinne der Verordnung (EU) Nr. 236/2012 (EU-LeerverkaufsVO)[13] vom 14. März 2012 handelt.

Hier kann, in Entsprechung mit den Artt. 12 ff. LeerverkaufsVO, grundsätzlich nicht erkannt werden,

- dass „Token" geliehen oder alternative Vorkehrungen getroffen werden, die zu gleichen rechtlichen Ergebnissen führen,

[12] Siehe hierzu z.B. EuGH in der Rechtssache UsedSoft GmbH ./. Oracle International Corp., Urteil vom 3. Juli 2012 – C-128/11, abrufbar unter http://curia.europa.eu/juris/document/document.jsf?docid=124564&doclang=DE (zuletzt abgerufen am 27. Februar 2019).
[13] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012R0236&from=DE (zuletzt abgerufen am 28. Februar 2018).

- dass bezüglich des „Token" eine Leihvereinbarung getroffen wird oder ein vertrags- oder eigentumsrechtlich unbedingt durchsetzbarer Anspruch auf Übertragung des Eigentums an einer entsprechenden Anzahl von Wertpapieren derselben Gattung besteht, so dass das Geschäft bei Fälligkeit abgewickelt werden kann,
- dass „Verkäufer" von einem Dritten die Zusage erhalten, dass der „Token" lokalisiert wurde, und dass dieser Dritte die Maßnahmen gegenüber Dritten ergriffen hat, die dafür notwendig sind, dass er das Geschäft bei Fälligkeit abwickeln kann.

Wenn jedermann „Token", i.e. in unendlicher Zahl Erschaffbares, selbst schreiben kann, dann sind diese bei „Verkauf" nicht gedeckt. Erst wenn zusätzlich, nach Erschaffung unter und in Entsprechung mit Umständen der Außenwelt, „Token" als „Stellvertreter" generiert werden, kann ernsthaft über eine Wertpapiereigenschaft und den Handel von Wertpapieren gesprochen werden.

Unter Verweis auf die Durchführungsverordnung (EU) Nr. 827/2012 vom 29. Juni 2012[14] und die hierin enthaltene Offenlegung durch die zuständige Behörde auf der von ihr verwalteten oder beaufsichtigten Website, wird hier ein weiteres Argument für die auf Seite 5 ausgeführte Notwendigkeit eines umfassenden, übersichtlichen Informationsportals gesehen.

### bb) Investorenschutz im Falle der Kontrollerlangung

Das Wertpapiererwerbs- und Übernahmegesetz (WpÜG) hat die Aufgabe, einen verlässlichen Rechtsrahmen für öffentliche Angebote zum Erwerb von Wertpapieren und von Unternehmensübernahmen zu schaffen. Ziel ist es insbesondere, Übernahmevorgänge im Interesse aller Beteiligten transparent und rechtssicher zu gestalten und zugleich einen angemessenen Schutz der Minderheitsaktionäre zu gewährleisten.[15]

Wenn Unternehmen Unternehmensanteile ausschließlich in „Token"-Form auf der Basis einer öffentlichen Blockchain ausgeben könnten, so wäre die in der Anlage beschriebene Kontrollerlangung über das Blockchain-Netzwerk durch einen Dritten, der kein Erwerber im Sinne des Gesetzes ist, nicht von diesem Schutzgesetz umfasst. Eine zusätzliche Dokumentation in der Blockchain-Datenbank wäre hingegen, ungeachtet offener Datenschutzfragen, unschädlich. Sie schafft keine neuen Risiken und Bedürfnisse nach neuen Schutzgesetzen.

### cc) Wir brauchen ein „elektronisches Wertpapier"

Ausweislich § 2 Wertpapierhandelsgesetz (WpHG) ist ein Wertpapier nicht von der Ausstellung einer (Papier-)Urkunde abhängig. Doch ausweislich § 151 Strafgesetzbuch ist es erforderlich, dass Wertpapiere gegen Nachahmung und damit Vervielfältigung besonders gesichert sind.

Eine besondere Sicherung gegen Vervielfältigung stellt die Blockchain-Technologie ausweislich der Ausführungen in der Anlage gerade nicht dar. Es braucht nur die Kontrolle, um die Existenz des „Wertpapiers" zu beseitigen, es zu verändern oder eben seinen Wert zu verwässern.[16]

Ein „elektronisches Wertpapier" muss von vornherein seine grundsätzliche Gefahr der unendlichen Vervielfältigung durch hohe Anforderungen an die Datensicherung berücksichtigen. Man kann vertreten, dieses Erfordernis ergäbe sich durch Auslegung, etwa durch eine Analogie zu § 151 StGB. Doch hinreichend klar, so notwendig für eine Strafbarkeit nach den §§ 151, 152, 146 ff. Strafgesetzbuch (StGB), ist dies nicht. Eine gesetzgeberische Regelung zum Schutze redlicher,

[14] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1440661438180&uri=CELEX:32012R0827 (zuletzt abgerufen am 28. Februar 2018).
[15] Begründung zum Entwurf eines Gesetzes zur Änderung des Wertpapiererwerbs- und Übernahmegesetzes, Drs. 17/3481 vom 27. Oktober 2010, S. 3, http://dip21.bundestag.de/dip21/btd/17/034/1703481.pdf (zuletzt abgerufen am 28. Februar 2018).
[16] Detaillierter *Otto*, „Haste mal nen Token?", Ri 2018, 143 (146 f.).

ausgebender Unternehmen und Investoren sollte aufgrund der realen Gefahren wenigstens geprüft werden.

### 4. Zur technischen Möglichkeit der Blockchain-Recherche

Öffentliche Blockchain-Datenbanken können von jedem handelsüblichen Rechner mit Internetzugang und von jedermann eingesehen werden. Z.B. kann die *Ethereum*-Blockchain mithilfe von *https://etherscan.io* durchsucht werden, die *Bitcoin*-Blockchain unter Zuhilfenahme des Blockexplorers *https://explorer.bitcoin.com/btc*. Diese aufzurufen ist auch den Steuerbehördenmitarbeitern grundsätzlich problemlos technisch möglich.

Die Herausforderung ist jedoch, die Mitarbeiter so zu schulen, dass sie wissen, wie die Einträge in den Blockchain-Datenbanken zu lesen sind. Insbesondere ist zu berücksichtigen, dass Massen von Transaktionen (= Einträgen) herausgesucht, ausgewertet, in Beziehung gesetzt und bewertet werden müssen. Hierfür bedarf es einer erheblichen (Fach-)Personalaufstockung.

Versierte Programmierfachleute sind in der Lage, Computerprogramme zu entwickeln, welche die Blockchain-Datenbanken nach vorgegebenen Kriterien durchsuchen, auswerten und für die Steuerbehördenmitarbeiter so aufbereiten, dass sie aus dem Datenkonglomerat ein steuerlich relevantes Ergebnis ablesen können. Doch auch solche effizienten Lösungsansätze bedürfen des Fachpersonals oder erheblicher Geldmittel für die Beauftragung geeigneter Dienstleister.

### 5. (Verbraucher-)Schutzvorschriften dürfen nicht angetastet werden

Wie bereits ausgeführt wurde, sprechen wir bei „Token-Übertragungen" „über die Blockchain" tatsächlich von Datenveränderungen in einer mit an einem Vertrag unbeteiligten Dritten gemeinsam geführten Datenbank bzw. Datensammlung. Vergleichbar dem Buchgeld werden hier allenfalls Forderungen dokumentiert und saldiert. Dass im Rahmen der Privatautonomie und infolge einer rechtslaienhaften Bewertung von Kaufvertrag und einer zu verschaffenden besonderen Rechtsposition gleich dem Eigentum gesprochen wird, ändert hieran nichts. Die Erklärungen der Parteien sind nicht nach ihrer Wortwahl, sondern nach ihrem wirklichen Willen (§ 133 BGB) und dem Maßstab von Treu und Glauben mit Rücksicht auf die Verkehrssitte (§ 157 BGB) auszulegen.

Daher ergibt sich aus neumodischen, unklaren Wortschöpfungen wie „Token" kein Grund zur Gesetzesänderung. Auch gibt es keine zu behebende grundlegende Rechtslücke, die nicht mit dem juristischen Handwerkszeug „Auslegung" gefüllt werden kann:

#### a) Zur Frage des Vertragsschlusses unter pseudonym agierenden Parteien

Das geltende Zivilrecht verlangt nicht, dass die Parteien eines Vertrages (des sog. Verpflichtungsgeschäfts) einander persönlich kennen. Das wird insbesondere im Rahmen der sog. Stellvertretung deutlich:

#### aa) Stellvertretung bei Ungewissheit über die Person des Vertretenen

Nach herrschender Meinung genügt es, wenn der Stellvertreter der einen Vertragspartei der anderen Vertragspartei deutlich macht, dass er für einen anderen handelt. Er muss ihn nicht namentlich bezeichnen. Der Bundesgerichtshof führte hierzu in seiner Entscheidung vom 17. Dezember 1987 unter dem Aktenzeichen VII ZR 299/86 aus:

> *„Nach § 164 Abs. 1 Satz 2 BGB wirkt eine von einem Vertreter im Rahmen seiner Vertretungsmacht abgegebene Willenserklärung auch dann für und gegen den Vertretenen, wenn sie der Vertreter zwar nicht ausdrücklich in dessen Namen abgibt, die Umstände jedoch ergeben, daß sie im Namen des Vertretenen erfolgen soll. Als Auslegungsregel*

> *beantwortet die Vorschrift nicht nur die Frage, ob der Vertreter im Namen eines anderen gehandelt hat. Sie ist vielmehr auch dann maßgebend, wenn ungewiß ist, in welchem Namen der Vertreter einen Vertrag abschließt (vgl. BGHZ 62, 216, 220/221 m.w.N.; 64, 11, 15; BGH NJW 1983, 1844; 1984, 1347, 1348; Urteil vom 17. November 1975 - II ZR 120/74 = WM 1976, 15, 16 = BB 1976, 154; Beschluß vom 28. Februar 1985 - III ZR 183/83 = WM 1985, 751). In einem solchen Fall ist die Willenserklärung des Vertreters ebenfalls gemäß §§ 133, 157 BGB unter Berücksichtigung aller Umstände auszulegen. Von Bedeutung ist also, wie sich die Erklärung nach Treu und Glauben mit Rücksicht auf die Verkehrssitte für einen objektiven Betrachter in der Lage des Erklärungsgegners darstellt. Dabei sind die gesamten Umstände des Einzelfalles zu berücksichtigen, insbesondere die dem Rechtsverhältnis zugrundeliegenden Lebensverhältnisse, die Interessenlage, der Geschäftsbereich, dem der Erklärungsgegenstand zugehört und die typischen Verhaltensweisen (BGH WM 1976, 15, 16)."*

An den Ausführungen wird auch wieder deutlich, dass die Partei-Willenserklärungen, die im Rahmen eines Vertrages inhaltlich übereinstimmend und mit Bezug aufeinander abgegeben werden, maßgeblich sind. Nicht etwa die Dokumentation am Vertragsschluss unbeteiligter Dritter. Wenn in der Blockchain-Datenbank rechtslaienhaft ein „Kaufvertrag" dokumentiert ist, kann es sich unter Berücksichtigung der gesamten Umstände des Einzelfalles, insbesondere der dem Rechtsverhältnis zugrundeliegenden Lebensverhältnisse, der Interessenlage, des Geschäftsbereichs, zu dem der Erklärungsgegenstand zugehört und der typischen Verhaltensweisen, auch um einen Darlehensvertrag handeln.

#### bb) „Das Geschäft für den, den es angeht"

Darüber hinaus gibt es das sog. (verdeckte) Geschäft, für den, den es angeht. Der Bundesgerichtshof beschrieb es in seinem Urteil vom 16. Oktober 2015 unter dem Aktenzeichen V ZR 240/14 wie folgt:

> *„Ein solches Geschäft ist dadurch gekennzeichnet, dass der handelnde Bevollmächtigte nicht zu erkennen gibt, ob er für sich oder einen anderen handelt, aber für einen anderen aufgrund einer erteilten Vollmacht handeln will und es dem Geschäftsgegner gleichgültig ist, mit wem das Geschäft zustande kommt".*

Im Falle von *Bitcoin* etwa dürfte den hinter den Pseudonymen „Adresse" stehenden Parteien häufig egal sein, mit wem sie interagieren – solange die gewünschte Datenveränderung an der Blockchain-Datenbank, die Zuweisung eines „Wertes", erfolgt. Nicht egal ist es unter Umständen den Strafverfolgungs-, Steuer- und Aufsichtsbehörden. Doch das berührt die zivilrechtliche Wertung nicht.

### b) Eigentum darf nicht ausschließlich auf einer jederzeit änderbaren elektronischen Information beruhen

Ein sehr prominenter Rechtsirrtum taucht immer wieder im Zusammenhang mit der Blockchain-Technologie auf: Eigentum wird angeblich leichter übertragbar. Besonders gern ist von der Grundstücksübertragung über das Blockchain-Grundbuch die Rede.[17]

Den Befürwortern ist jedoch nicht klar, welche Schutzziele die bestehenden Eigentumsvorschriften verfolgen. Besonders deutlich wird eines hiervon an § 935 Abs. 1 S. 1 BGB:

> *„Der Erwerb des Eigentums auf Grund der §§ 932 bis 934 tritt nicht ein, wenn die Sache dem Eigentümer gestohlen worden, verloren gegangen oder sonst abhanden gekommen war."*

[17] Hierzu ausführlich *Otto*, „Die Vermessung des Blocksbergs", Ri 2018, 16 ff.

Ein gutgläubiger Eigentumserwerb, etwa weil in einer öffentlichen Datensammlung das „Eigentum" des Verkäufers dokumentiert ist, kann nach bestehendem Recht nicht erfolgen, wenn der Gegenstand, an dem Eigentum bestehen soll, tatsächlich einem anderen gestohlen wurde. Vorgänge der realen Welt sind in einer Blockchain nicht dokumentiert. Die hier dokumentierten „Zustände" werden nicht auf ihre inhaltliche Richtigkeit überprüft. Jedermann kann sich in einer öffentlichen Datenbank rühmen, Eigentümer fremden Eigentums oder gar Herrscher über ein Königreich Deutschland zu sein.

Ein Eintrag in einer solchen Datenbank hat geringe oder keine Beweiskraft. Selbst wenn Parteien in übereinstimmendem Willen einen Zustand der Außenwelt in der Blockchain dokumentieren, kann dieser, wie in der Anlage ausgeführt, von einem die Kontrolle über das Blockchain-Netzwerk erlangenden Dritten jederzeit verändert werden.

Würde nun auf Wunsch der Blockchain-Produkteanbieter die bestehende Rechtslage dahingehend geändert, dass Eigentum durch Dokumentation in der Blockchain übertragen werden kann, würde großes Unheil folgen: Jedermann könnte von heute auf morgen entrechtet und enteignet werden.

### c) Privatautonomie und ihre wichtigen, schutzzweckorientierten Grenzen

Wenn Parteien die Dokumentation von Eigentum in elektronischer Form wie etwa der Blockchain wünschen, so können sie dies grundsätzlich tun. Dabei müssen sie jedoch Folgendes berücksichtigen:

#### aa) Zustände der realen Welt sind „wahrer"

Die Eigentumsvermutung des § 1006 Abs. 1 S. 1 BGB ist stärker als jede irgendwie dokumentierte Behauptung der Rechtsposition Eigentum: Wer eine bewegliche Sache in Besitz hat, zu dessen Gunsten wird vermutet, dass er Eigentümer ist. Das gilt natürlich nicht, siehe oben, für gestohlene, verloren gegangene oder sonst abhanden gekommene Sachen, § 1006 Abs. 1 S. 2 Hs. 1 BGB.

#### bb) Zusätzliche Dokumentation der Rechtsposition außerhalb der Blockchain

Auf die Angaben in einer Blockchain, vor allem in einer öffentlichen Blockchain, darf man sich nicht verlassen. Wo keine inhaltliche Prüfung stattfindet und jederzeit jemand Drittes (sogar unbemerkt) die Kontrolle über die Dokumentation erlangen kann, kann keine verbindliche Rechtsposition abgeleitet werden.

Es sollte bei einer rein elektronischen Dokumentation von Rechtspositionen sichergestellt sein, dass eine Änderung durch Einwirkungen Dritter bestmöglich ausgeschlossen ist. Dabei muss nicht auf Papier im Tresor zurückgegriffen werden, wenn ein besonderer Schutz vor Änderung oder Verlust anders realisiert werden kann. Doch mehr als eine zusätzliche Dokumentation, die bei der Ermittlung des Parteiwillens berücksichtigt werden kann, kann auch diese Lösung nicht darstellen.

#### cc) Viele „Token"-Geschäfte sind potentiell verboten

Parteien können grundsätzlich vereinbaren, was sie möchten, solange insbesondere gesetzliche Verbote nicht entgegenstehen. Wenn „Token" an Verbraucher „verkauft" werden, gibt es ganz wesentliche rechtliche Vorgaben und Verbote zu berücksichtigen, die Verbraucherverträge (mindestens teilweise oder in Gänze) unwirksam oder anfechtbar machen. Nur weil eine konkrete Einordnung bisher nicht vorgenommen worden ist, heißt es nicht, dass die „Token"-Geschäfte rechtlich in Ordnung sind.

(1) Allgemeine Geschäftsbedingungen: § 307 Abs. 1 BGB

Im Hinblick auf „Token"-Verträge gibt es eine wesentlich zu berücksichtigende Vorschrift in dem Abschnitt der Allgemeinen Geschäftsbedingungen. § 307 Abs. 1 BGB konstatiert:

> *„Bestimmungen in Allgemeinen Geschäftsbedingungen sind unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist."*

Regelmäßig ist es bei Blockchain-Produkten der Fall, dass die Anbieter in ihren – oft bewusst ausschließlich in englischer Sprache bereitgestellten Vertragsdokumentationen – nicht klar und verständlich kommunizieren, was der Verbraucher eigentlich „kaufen" soll. Der Begriff „Token" verschleiert, dass hier kein eigentumsfähiger Gegenstand erworben wird, sondern nur eine Dokumentation einer vermeintlichen Rechtsposition in der Blockchain erfolgt, deren Bestand – entgegen oft begleitender Darstellungen – ausweislich der Anlage nicht sicher ist.

Darüber hinaus ist im Falle der in der Anlage näher erklärten Smart Contracts nicht zu erwarten, dass der Verbraucher der zur Anwendung kommenden Programmiersprache mächtig ist. Wenn ein Computerprogramm gleichzeitig Vertragstext sein soll, dürfte eine unangemessene Benachteiligung nach vorstehender Vorschrift gegeben sein.

(2) Fehlende äquivalente Gegenleistung: Wucher gemäß § 138 Abs. 2 BGB

§ 138 Abs. 2 BGB regelt die Nichtigkeit eines Rechtsgeschäfts, dessen Charakter ein auffälliges Missverhältnis von Leistung und Gegenleistung zeigt:

> *„Nichtig ist insbesondere ein Rechtsgeschäft, durch das jemand unter Ausbeutung der Zwangslage, der Unerfahrenheit, des Mangels an Urteilsvermögen oder der erheblichen Willensschwäche eines anderen sich oder einem Dritten für eine Leistung Vermögensvorteile versprechen oder gewähren lässt, die in einem auffälligen Missverhältnis zu der Leistung stehen."*

Wenn sich ein Blockchain-Produkteanbieter von einer mit dieser Technologie und hierauf basierenden Produkten unerfahrenen Vertragspartei, echtes Vermögen, etwa in Form von gesetzlichen Zahlungsmitteln, gegen wertlose „Token" und/oder die bloße Dokumentation einer vermeintlichen und unsicheren Rechtsposition, versprechen oder gewähren lässt, so kann dieser Vertrag wegen Wuchers nichtig sein.

Die Unerfahrenheit kann nicht nur bei Verbrauchern, sondern auch bei Unternehmern und ihren Vertretern vorliegen. Eine Zwangslage wie etwa Angst und gar (Geld-)Not, die ein umfassendes Prüfen der Sach- und Rechtslage faktisch ausschließt, kann darüber hinaus ausgenutzt werden.

Die Nichtigkeit eines Vertrages über ein „Blockchain-Produkt" ist natürlich eine Frage des Einzelfalls. Dennoch muss die BaFin solche Umstände im Rahmen ihrer einer Freigabe vorgeschalteten Einzelfallprüfung berücksichtigen; der kollektive Verbraucherschutz ist eine ihrer Aufgaben.

(3) Unlautere geschäftliche Handlungen

Gemäß § 3 Abs. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) sind

> *„Geschäftliche Handlungen, die sich an Verbraucher richten oder diese erreichen, unlauter, wenn sie nicht der unternehmerischen Sorgfalt entsprechen und dazu geeignet sind, das wirtschaftliche Verhalten des Verbrauchers wesentlich zu beeinflussen."*

Unvollständige und falsche Produkt-Informationen (vgl. „irreführende geschäftliche Handlungen, § 5 UWG) in einer Fremdsprache, versehen mit vertrauenserweckenden Zusätzen wie „Made in Germany", sowie das Auslösen von Zeitdruck entsprechen nicht der unternehmerischen Sorgfalt. Diese Praktiken sind geeignet, das wirtschaftliche Verhalten der Verbraucher wesentlich zu beeinflussen. § 3 Abs. 3 UWG unterstützt diese im Einzelfall zu bestätigende, allgemeine Bewertung der unzulässigen geschäftlichen Handlung:

Nach Ziffer 8 der Anlage zu § 3 Abs. 3 UWG, ist eine stets unzulässige geschäftliche Handlung

> *„Kundendienstleistungen in einer anderen Sprache als derjenigen, in der die Verhandlungen vor dem Abschluss des Geschäfts geführt worden sind, wenn die ursprünglich verwendete Sprache nicht Amtssprache des Mitgliedstaats ist, in dem der Unternehmer niedergelassen ist; (...)"*

Nach Ziffer 2 der Anlage zu § 3 Abs. 3 UWG, ist eine stets unzulässige geschäftliche Handlung

> *„die Verwendung von Gütezeichen, Qualitätskennzeichen oder Ähnlichem ohne die erforderliche Genehmigung;"*

Nach Ziffer 7 der Anlage zu § 3 Abs. 3 UWG, ist eine stets unzulässige geschäftliche Handlung

> *„die unwahre Angabe, bestimmte Waren oder Dienstleistungen seien allgemein oder zu bestimmten Bedingungen nur für einen sehr begrenzten Zeitraum verfügbar, um den Verbraucher zu einer sofortigen geschäftlichen Entscheidung zu veranlassen, ohne dass dieser Zeit und Gelegenheit hat, sich auf Grund von Informationen zu entscheiden;"*

Das Geschäft mit den „Token" sollte dringend mehr Aufmerksamkeit von lauterkeitsrechtlicher Seite erfahren:

An „Token" kann kein Eigentum zwecks Ausschluss Dritter von der Einwirkung erworben werden, siehe Seite 8. „Token" sind als Daten lediglich Teil einer Dokumentation, wobei die Dokumentationsdauer und Unveränderthеit des dokumentierten Zustands entsprechend der Ausführungen in der Anlage ungewiss ist. Andere Zusicherungen sind unwahre Werbeversprechen. Daher dürfte im Falle eines „Verkaufs" von „Token" fast in der Regel eine irreführende geschäftliche Handlung im Sinne des § 5 Abs. 1 S. 2 Nr. 1 UWG vorliegen.

> *„Unlauter handelt, wer eine irreführende geschäftliche Handlung vornimmt, die geeignet ist, den Verbraucher oder sonstigen Marktteilnehmer zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Eine geschäftliche Handlung ist irreführend, wenn sie unwahre Angaben enthält oder sonstige zur Täuschung geeignete Angaben über folgende Umstände enthält:*
>
> *1. die wesentlichen Merkmale der Ware oder Dienstleistung wie Verfügbarkeit, Art, Ausführung, Vorteile, Risiken, Zusammensetzung, Zubehör, Verfahren oder Zeitpunkt der Herstellung, Lieferung oder Erbringung, Zwecktauglichkeit, Verwendungsmöglichkeit, Menge, Beschaffenheit, Kundendienst und Beschwerdeverfahren, geographische oder betriebliche Herkunft, von der Verwendung zu erwartende Ergebnisse oder die Ergebnisse oder wesentlichen Bestandteile von Tests der Waren oder Dienstleistungen;"*

## 6. Das Urkundserfordernis nicht abschaffen, sondern ergänzen

Das Papier ist in der Tat nicht mehr zeitgemäß. Es ist jedoch weiterhin das (rechts-)sicherste Mittel der Vertragsdokumentation. Das auf Seite 9 f. angeregte „elektronische Wertpapier" bedarf der (zusätzlichen) Anforderung des besonderen Schutzes vor Nachahmung, i.e. Vervielfältigung.

Die Blockchain ist kein geeignetes, „qualifiziertes digitales Register". Es handelt sich hierbei einfach nur um eine strukturierte Datensammlung, i.e. Datenbank, lediglich mit anderen Anfälligkeiten als etwa eine *Excel*-Datei. Die Vervielfältigung und Änderung von Daten ist in beiden Fällen durch denjenigen möglich, der die Kontrolle hierüber hat. Wenn die Blockchain ein qualifiziertes digitales Register gesetzlicher Anerkennung werden soll, darf die *Excel*-Datei mit ihren *Excel*-Blättern nicht anders behandelt werden, nur weil sie des zusätzlichen Teilens via E-Mail oder etwa *SharePoint* bedarf.

Zusammenfassend ist zu sagen: Eine *zusätzliche* Dokumentation in einer Blockchain ist, vorbehaltlich datenschutzrechtlicher Fragestellungen, unproblematisch.

## 7. Smart Contracts mit Bedacht verwenden, Verbraucher und Wirtschaft stärken

Eine kurze Darstellung zu Smart Contracts findet sich in der Anlage. Es handelt sich hierbei *nicht* um Verträge.

Es gibt darüber hinaus eine Bewegung, auch unter Juristen, die Verträge unabhängig von der Blockchain-Technologie (voll)automatisieren und diese als „Smart Contract" bezeichnen will. Sie bezieht sich hierbei oft auf Ideen des *Nick Szabo* aus den Neunzigern des letzten Jahrhunderts, die, vereinfacht gesprochen, den *Amazon Dash Button* beschreiben. Das Oberlandesgericht München hat diese WLAN-Bestellknöpfe mit Urteil vom 10. Januar 2019 (Az. 29 U 1091/18) verboten, weil sie die Verbraucher zum Zeitpunkt der Bestellung nicht ausreichend informieren.

Oft wird von den Verfechtern dieser „Smart Contracts" der Verbraucherschutz als Grund für den Ruf nach gesetzlichen Anpassungen angeführt: Verbraucher sollen nicht nur automatisiert Verträge schließen können, sondern auch automatisch Rückerstattungen erhalten, sobald der unternehmerische Vertragspartner einen vermeintlichen Rückerstattungsanspruch auslöst.

Was die Befürworter aus den Augen verlieren, ist zunächst der Umstand, dass ein Vertrag ein komplexes Lebensverhältnis zwischen menschlichen oder menschlich vertretenen Parteien regelt. Nicht alles ist automatisierbar, erst recht nicht die Unwägbarkeiten des Lebens. Computerprogramme können, ausweislich der Anlage, in ihrer Beschränkung auf klare Anweisungen diese Komplexität und Vielfältigkeit der Möglichkeiten nicht abdecken. Abstrakte Formulierungen, unbestimmte Rechtsbegriffe, umfassende Produktinformationen und Haftungsregelungen sind in Textform schlichtweg wirtschaftlich, sinnvoll und zweckmäßig. Gegebenenfalls handschriftliche Streichungen und Ergänzungen sind zudem auch ohne spezielle Ausbildung schneller und günstiger gemacht als ein Computerprogramm geändert werden kann.

Darüber hinaus krankt diese Idee an einem fehlenden Verständnis für eine funktionierende Wirtschaft:

Würden Unternehmen gesetzlich verpflichtet, auf jeden Fall nicht optimaler Vertragsabwicklung mit einer Preisrückerstattung zu reagieren, würden sie geschwächt und mit ihnen die gesamte Wirtschaft Deutschlands. Unternehmen müssten ihre Einnahmen mindestens für die gesamte Vertragslaufzeit als Rückstellungen buchen und wären gehindert, sie wiederum in Arbeitnehmer, in die Verbesserung und Weiterentwicklung von Produkten sowie Innovationen zu investieren. All diese fehlenden Investitionen gingen wieder zulasten der Verbraucher und würden sich durch die Reduzierung ihrer Arbeitsplätze, die Abkehr vom Verbrauchermarkt und damit weniger

Produktauswahl, oder steigende Preise zwecks Reduzierung der Verpflichtungen bemerkbar machen.

Es ist für eine florierende, funktionierende und verbraucherfreundliche Wirtschaft wesentlich besser, die Verbraucherseite bei der Verfolgung etwaiger Ansprüche zu unterstützen. Das kann z.B. geschehen, indem Rechtsdienstleistern nach dem Rechtsdienstleistungsgesetz (RDG) der Weg geebnet wird, der aufgrund seiner Nähe zum Berufsrecht der Rechtsanwälte noch einem Gang durch den Dornenstrauch am Wegesrand gleicht. Gesamtwirtschaftlich betrachtet bewirkt eine durch die Rechtsdienstleister gestärkte Verbrauchermarktseite wiederum die Stärkung der Wirtschaft durch die Schaffung neuer Arbeitsplätze und einen starken Anreiz auf der Anbieterseite, gute Produkte verbraucherfreundlich anzubieten.

„Smart Contracts" in der propagierten Form schaden Verbrauchern und Wirtschaft im Ergebnis mehr als sie nützen. Die praktische, gemeinsame elektronische Vertragsverwaltung mit Informations-, Bezahl- und Kündigungsfunktion ist hingegen längst eine Realität für viele Unternehmen. Sie kommt gänzlich ohne diesen überschätzten Begriff aus.

## 8. Die Datenschutzgrundverordnung (DSGVO) ist nicht das Problem, sondern die „Use Cases"

Die Blockchain kann, wenn sie nicht schon als Mittel ganz oder teilweise automatisierter Verarbeitung personenbezogener Daten angesehen wird, ein Dateisystem im Sinne der DSGVO sein, i.e. eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird (Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 6 DSGVO).

Die Adresse in einem öffentlichen Blockchain-Netzwerk wird hier als ein personenbezogenes Datum angesehen, da von ihr aus, in Verbindung mit den einsehbaren Transaktionen, der Bezug zur natürlichen Person „hinter" der Adresse hergestellt werden kann.[18] Die natürliche Person ist damit grundsätzlich identifizierbar im Sinne von Art. 4 Nr. 1 DSGVO ist. Daher kann in einem Blockchain-Netzwerk nur von Pseudonymität gesprochen werden.

Die Vorgaben der DSGVO können praktisch nicht erfüllt werden, wenn personenbezogene Daten von *am Netzwerk nicht beteiligten natürlichen Personen* in eine öffentliche Blockchain-Datenbank eingepflegt werden. Der Grund liegt u.a. in dem in der Anlage beschriebenen mangelnden Schutz vor unbefugter sowie unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, der jedoch nach Art. 5 Abs. 1 lit. f DSGVO zu gewährleisten ist. Anderes kann nur gelten, wenn die natürliche Person sich, in Kenntnis aller Vor- und Nachteile des Teilens ihrer Daten mit einer unbegrenzten und unbekannten Personenzahl, selbst in dieses risikobehaftete Netzwerk begibt.

## 9. „Wallet"-Verwaltung durch die Banken?

Die Erfahrung lehrt, dass derjenige, der sich am öffentlichen Blockchain-Netzwerk beteiligt, ein hohes Risiko trägt, das mit der üblichen Sicherheitsschulung nicht in den Griff bekommen werden kann:

Das Risiko beginnt bereits beim Generieren des geheim zu haltenden sog. Private Keys und des aus ihm generierten preisgebaren Public Keys, die wiederum beide zusammen in der Signatur einer Transaktion den Ersteller als Berechtigten ausweisen. Je weniger zufällig, desto größer ist das Risiko des Rückschlusses vom Public Key auf den Private Key: Auch die Elliptische-Kurven-Kryptografie ist nicht unfehlbar. Darüber hinaus gibt es falsche Generatoren, die erst gar kein Generieren eines geheimen Private Keys zulassen, sondern schlichtweg dem Skimming, dem Auslesen der erstellten Keys, dienen.

[18] *Otto*, „Wo man mehr weiß, argwöhnt man weniger.", Ri 2018, 164 (171 f.).

Darüber hinaus bergen die sog. „Wallets", also die technischen Anwendungen zur Interaktion mit der Blockchain-Datenbank, oft entwickelt und angeboten von (unbekannten) Dritten, ein erhebliches Datenverlustrisiko. Ganz gleich ob „Soft" oder „Hard(ware) Wallet", wer die Entscheidung für die Datenzugriffslösung trifft, trägt auch das Risiko des totalen Datenverlustes.

Wird „on top of the blockchain" eine „Krypto-Börse" samt „hauseigenen Wallets" errichtet, wird ein weiteres Tor für potentielle Schäden, v.a. durch Hackerangriffe und Malware geöffnet. Hier kann auf die öffentliche Berichterstattung verwiesen werden.

Die Risiken und damit auch Haftungsfallen sind vielfältig und immens. Sie werden immer eine Frage des Einzelfalls und der vereinbarten Risikoverteilung bleiben. Dieses bestimmt schlussendlich das konkrete Rechtsverhältnis zwischen Bank und Kunde. Eine Bank, die angesichts der in der Anlage aufgezeigten Mängel der Blockchain-Technologie sämtliche Risiken auf sich nimmt, ist nicht vorstellbar. Kunden, die sich der Risiken bewusst sind und über technische Kenntnisse verfügen, werden eher die Reduzierung und Kontrolle der Risikoquellen anstreben und selbst aktiv an einem Blockchain-Netzwerk mitwirken. Gerade diese werden niemals Private und Public Key Dritten gegenüber mitteilen.

Dort wo die uninformierten Verbraucher auf findige Blockchain-Geschäftemacher mit ihren freiwilligen Prospekten treffen, greifen oben genannte Schutzvorschriften, vor allem des Zivilrechts. Auch für die „Token" verwaltenden Banken, ob als Kontoführer oder Wertaufbewahrer, wäre es im Ergebnis höchst fatal, würde die zivilrechtliche Haftung zugunsten einer zahnlosen spezialgesetzlichen Prospekthaftung ausgeschlossen. Denn die spezialgesetzlich geregelten Umstände, die die Blockchain-Produkteanbieter um ihre Haftung entlasten, belasten die verwaltenden Banken mit Schadensersatzansprüchen der Kunden.

## 10. Besteuerung

Die steuerlichen Fragen sollten obige Ausführungen sowie die Anlage berücksichtigen.

Anlage zur Stellungnahme von RA'in Claudia Otto, COT Legal (BT-Drs. 19/4217)

# Die andere Seite der Krypto-Münze

## I. Blockchain-Technologie

### 1. Überblick

Die Blockchain-Technologie ist ein Unterfall der Distributed-Ledger-Technologie. Die „Blockchain", oft synonym verwendet, beschreibt zum einen eine besondere Art der Datensammlung und Datenbankstruktur, i.e. Datenpakete genannt Blöcke, die chronologisch miteinander verkettet werden. Zum anderen steht die Blockchain-Technologie für eine Art und Weise der gemeinsamen Datenbankverwaltung und damit Kommunikation in einem Netzwerk, bestehend aus einer veränderlichen teilnehmenden Rechnerzahl. Der Begriff umfasst sowohl „Konstrukt" als auch „Verfahren", verschiedene sogar. Denn eine gemeinsame Datenbankverwaltung umfasst auch klare Regeln dazu, wie die Datenbank aktualisiert, die Block-Kette also um einen weiteren Block ergänzt wird. Weil demokratische Abstimmverfahren zeitaufwändig sind und eine zeitnahe Aktualisierung der gemeinsamen Datensammlung unmöglich wäre, ersetzen sog. Konsensalgorithmen den Abstimmungsprozess im Rahmen der gemeinsamen Datenbankverwaltung. Konsensalgorithmen dienen, bei Gewährleistung einer gewissen Zufälligkeit, der Auswahl „geeigneter" Entscheider aus dem Kreise der Stimmberechtigten. Diese Auswahlverfahren werden im jeweiligen Netzwerk-Protokoll festgelegt.

Die Datensammlung wird ausschließlich voluminöser, da Löschungen grundsätzlich nicht vorgesehen sind. Die an der gemeinsamen Datenbankverwaltung teilnehmenden Rechner werden, weil sie eine vollständige Kopie der Blockchain-Datensammlung vorhalten, Full Archive Nodes (auch Full Nodes) genannt. Weil nicht jeder Rechner über den nötigen Speicherplatz sowie die nötige Rechenleistung verfügt und verfügen wird, gibt es sog. Light Nodes. Diese speichern nur eine leichtgewichtige Miniatur der Blockchain, nicht aber die vollständige Datensammlung. Light Node-Clients ermöglichen, in Abhängigkeit von den Full Archive Nodes, nur eine beschränkte Teilnahme, v.a. durch datenbankändernde Einträge (sog. Transaktionen). Weil Light Nodes keinen für die Blockchain existenznotwendigen Speicherplatz bereitstellen, sind sie bei der gemeinsamen Datenbankverwaltung nicht stimmberechtigt. Für nachträgliche Änderungen an der Blockchain-Datenbank, so wie auch Löschungen, bedarf es einer Mehrheit der stimmberechtigten Full Archive Nodes. Das heißt, eine Kontrolle ausübende Mehrheit entscheidet über Datenbankbestand, -zustand und -fortbestand. Wie und mit welchem Ergebnis diese ausgeübt wird, ergibt sich grundsätzlich aus dem – ggf. ebenfalls zu ändernden – Netzwerk-Protokoll.

### 2. Mythen und Realität

Um die Blockchain ranken sich zahlreiche Mythen, insbesondere, dass

a) die Blockchain-Datenbank dezentral und ohne zentrale Autorität, dem sog. Single Point of Failure, geführt würde,
b) die Blockchain-Technologie sicher sei,
c) die Transaktionen der Transaktionshistorie namens Blockchain verschlüsselt seien,
d) die Blockchain unveränderlich sei und
e) Vertrauen in Personen durch kryptografische Verfahren obsolet sei.

Entgegen dieser Behauptungen bedeutet der Einsatz der Blockchain-Technologie nach den Vorbildern *Bitcoin* und *Ethereum* allerdings, dass

a) ein Blockchain-Netzwerk tatsächlich starker Zentralisierung unterliegt:

aa) Zentralisierung durch Konzentration von Entscheidungsmacht

Es ist eine simple Rechnung: Je voluminöser eine Blockchain-Datensammlung wird, desto weniger verwaltungsberechtigte, i.e. stimmberechtigte Full Archive Nodes wird es geben. Nach *BitInfoCharts*[1] umfasst die *Bitcoin*-Blockchain aktuell rund 241 Gigabyte, die *Ethereum*-Blockchain 189 Gigabyte[2], wobei Letztere binnen 3,5 Jahren fast die Größe der mehr als 10-jährigen *Bitcoin*-Blockchain erreicht hat:

| | Bitcoin (explorer, top100) | Ethereum |
|---|---|---|
| Total | 17,568,729 BTC | 105,097,625 ETH |
| Top 100 Richest | 2,740,930 BTC<br>($10,437,804,284 USD)<br>15.60% Total | |
| Wealth Distribution<br>Top 10/100/1,000/10,000 addesses | 5.38% / 15.60% / 35.19% / 57.75% Total | |
| Addresses richer than<br>1/100/1,000/10,000 USD | 15,078,882 / 4,527,659 / 1,536,332 / 341,593 | |
| Active Addresses last 24h | 477,760 | 252,488 |
| 100 Largest Transactions | last 24h: 225,150 BTC<br>($857,400,395 USD)<br>18.70% Total | last 24h: 308,065 ETH<br>($40,585,000 USD)<br>24.77% Total |
| First Block | 2009-01-09 | 2015-07-30 |
| Blockchain Size | 241.45 GB | 188.82 GB |
| Reddit subscribers | 1,020,324 | 430,905 |
| Tweets per day | 14,475 | 4,409 |
| Github release | v0.17.1 (2018-12-25) | v1.8.23 (2019-02-20) |
| Github stars | 37303 | 22703 |
| Github last commit | 2019-03-02 | 2019-03-02 |
| | Bitcoin | Ethereum |

Wegen der steigenden Datenvolumina im weiteren Zeitablauf werden irgendwann diejenigen die Entscheidungsmacht und damit Kontrolle über Datensammlung und Netzwerk haben, die sich nicht nur handelsübliche, sondern BigData-Rechner „leisten" können. Dieser Zentralisierungseffekt ist bereits heute erkennbar: Im Rahmen des in *Bitcoin* und *Ethereum* (noch) zur Anwendung kommenden *Proof-of-Work*-Verfahrens entscheiden diejenigen über neu hinzuzufügende Blöcke stellvertretend für das gesamte Netzwerk, welche die größte Rechenpower auf sich vereinen. Das sind v.a. Miningfarmen, die im Ausland mit günstigem Strom betrieben werden.

Die Blockchain als Netzwerktechnologie ist, langfristig gesehen, tatsächlich ein Instrument struktureller Macht. Daran wird auch ein Konsensalgorithmus wie *Proof-of-Stake* nichts ändern, der wegen des hohen Stromverbrauchs des *Proof-of-Work*-Verfahrens anvisiert wird. Auch *Proof-of-Stake* zementiert Autorität – derjenigen mit hoher Beteiligung und somit hoher Wahrscheinlichkeit der Kontrolle über das Netzwerkschicksal. Wie man oben am Beispiel *Bitcoin* sehen kann, halten 100 von 477.760 aktiven Adressen bereits 15,60 % aller im Umlauf befindlichen Bitcoins. Wer über die 10.000 Adressen mit den meisten Bitcoins verfügen kann, hätte sogar 57,75 % Netzwerkanteile und damit die Kontrolle über das Netzwerk.

[1] https://bitinfocharts.com/ (zuletzt abgerufen am 3. März 2019).
[2] Siehe auch hierzu *StopAndDecrypt*, „The Ethereum-blockchain size has exceeded 1TB, and yes, it's an issue", 23. Mai 2018, https://hackernoon.com/the-ethereum-blockchain-size-has-exceeded-1tb-and-yes-its-an-issue-2b650b5f4f62 (zuletzt abgerufen am 3. März 2019).

Wer hier keine gewichtige Beteiligung hat, entscheidet nicht mit: Über ihn wird entschieden.

bb) Die sog. Single Points of Failure verlagern sich lediglich auf andere Ebenen

Unter idealen Bedingungen ist es eine Bereicherung, dass im Falle eines Stromausfalls nur ein Netzwerkrechner mit einer vollständigen, aktuellen Kopie der Blockchain „überleben" muss, um die Datensammlung vor Verlust zu bewahren. Schließlich können sich alle anderen Netzwerkrechner bei Stromverfügbarkeit durch Synchronisierung wieder auf den aktuellsten Stand bringen.
In diesem Szenario sind v.a. die Stromnetzbetreiber die Single Points of Failure. Es ist in einer Gesellschaft steigender Vernetzung nicht unmöglich, die Stromzufuhr bei hinreichend vielen der Full Archive Nodes so lange zu unterbrechen, dass ohne weiteren großen Rechenaufwand die Kontrolle über das Netzwerk ausgeübt werden kann. Im Zustand der Kontrolle kann die Blockchain-Datensammlung nach Lust und Laune aktualisiert, d.h. verändert werden. Für die Rückkehrer heißt es dann: Friss oder stirb.

Gleiches gilt für die starke Zentralisierung auf Netzwerkebene sog. Autonomous Systems (AS) in der Hand von Internet Service Providern (ISP). Kann sich die Mehrheit der friedlichen Full Archive Nodes nicht am Validierungs- und Synchronisierungsprozess beteiligen, weil sie mangels Internetverbindung vom Netzwerk abgeschnitten ist, hat ein potentieller Angreifer die Kontrolle über das Blockchain-Netzwerk. Doch nicht nur ein Ausfall ist möglich; auch die Manipulation des Datenverkehrs zwischen den Full Archive Nodes ist „von oben" denkbar.

Je weniger Ausbreitung und Risikodiversifizierung ein Blockchain-Netzwerk auf Strom- oder Internet-Netzwerkebene erfährt, desto schneller kann man durch Blackouts und Manipulieren von Internet Services ein gesamtes Blockchain-Netzwerk in die Knie zwingen – mit schweren Folgen für hiervon abhängige Menschen.

Kritische Infrastrukturen dürfen daher *niemals* von einer Blockchain abhängig gemacht werden.

b) Keine Technologie ist zu 100% sicher

Die reale Möglichkeit der Kontrollerlangung und -ausübung im eigenen finanziellen Interesse ist die größte Schwachstelle der Blockchain.[3] Darüber hinaus fehlt es an Erfahrung mit der Technologie. Schon deshalb kann ihre Sicherheit nicht behauptet werden. Es ist vielmehr allgemein bekannt, dass es keine unfehlbare Technologie gibt.

c) Transaktionen sind weder verschlüsselt noch sicher

Eine Transaktion im Kontext der Blockchain-Technologie ist zunächst nur eine (erwünschte) Änderung an bzw. ein Eintrag in der Datenbank. Was diese Änderung konkret bedeutet, bestimmt sich nach dem Einzelfall. Einer Datenbankänderung die Bedeutung einer Übertragung von Vermögenswerten zuzuschreiben, ändert nichts daran, dass auch das Ein- und Ausschalten von Licht unter Verwendung eines sog. Smart Contracts „auf" einer Blockchain eine Transaktion wäre.

Der Vorgang der notwendigen Übersetzung von Transaktionsdaten in maschinenlesbare Sprache ist keine Verschlüsselung wie der Begriff suggeriert. Jedermann, der weiß, wie man die Einträge (Transaktionen) in einer öffentlichen Blockchain-Datenbank liest, kann sie voll einsehen.

[3] Beispielhaft: *Orcutt*, „Once hailed as unhackable, blockchains are now getting hacked", MIT Technology Review, 19. Februar 2019, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ (zuletzt abgerufen am 3. März 2019); vgl. ebenfalls diverse Beiträge in der Recht innovativ-Reihe seit Ri 01/2017.

Hilfreich dabei sind im Internet zahlreich und kostenfrei verfügbare sog. Converter. Die Adresse als Pseudonym ändert nichts an der Einsehbarkeit der ihr zugeordneten Transaktionsinhalte.[4]

Wer die Kontrolle über das Netzwerk und seine Datensammlung namens Blockchain erlangt hat, kann diese Transaktionen auch nachträglich verändern und etwaige „Vermögenswerte" mehrfach, etwa zu Zahlungszwecken, einsetzen.

### d) Die Blockchain ist veränderlich

Es braucht lediglich eine (rechenleistungsbasierte) Mehrheit und damit die Kontrolle über das Netzwerk und die zugehörige Datensammlung.

### e) Blockchain: Vertrauen, dass nichts passiert

Keine Technologie verlangt Menschen so viel Vertrauen ab, wie die Blockchain-Technologie. Es muss v.a. immer darauf vertraut werden, dass niemand die Kontrolle über das Netzwerk erlangt und ausnutzt.

## 3. Reale Gefahren, über die Blockchain-Produkteanbieter schweigen

Blockchain-Produkteanbieter, die u.a. „Token" auf Basis von „*Ethereum* Smart Contracts" anbieten, erwähnen Risiken der Nutzung nicht. Die *Ethereum Stiftung* hingegen benennt Risiken der Blockchain-Technologie in ihrem Legal Agreement[5], zum Beispiel:

> *„If your machine is compromised you* ***will*** *lose your ether, access to any contracts and possibly more."*
>
> *„The Ethereum Platform rests on open-source software, and there is a risk that the Ethereum Stiftung or the Ethereum Team, or other third parties not directly affiliated with the Stiftung Ethereum, may introduce weaknesses or bugs into the core infrastructural elements of the Ethereum Platform causing the system to lose ETH stored in one or more User accounts or other accounts or lose sums of other valued tokens issued on the Ethereum Platform."*
>
> *„Cryptography is an art, not a science. And the state of the art can advance over time. Advances in code cracking, or technical advances such as the development of quantum computers, could present risks to cryptocurrencies and the Ethereum Platform, which could result in the theft or loss of ETH."*
>
> *„(...) the entire Ethereum Platform could become destabilized, due to the increased cost of running distributed applications."*
>
> *„Insufficiency of computational resources and an associated rise in the price of ETH could result in businesses being unable to acquire scarce computational resources to run their distributed applications. This would represent revenue losses to businesses or worst case, cause businesses to cease operations because such operations have become uneconomical due to distortions in the crypto-economy."*

Da die genannten Risiken nicht *Ethereum*-spezifisch sind, gilt für andere Plattformen und Blockchain-Produkteanbieter nichts anderes.

---

[4] Weiterführend, insbesondere zu *Zcash* und *Monero* in *Otto*, „Wo man mehr weiß, argwöhnt man weniger.", Ri 2018, 164 (168 ff.).
[5] https://www.ethereum.org/agreement (zuletzt abgerufen am 27. Februar 2019).

## II. Smart Contracts

### 1. Was ist ein Smart Contract?

Ein sog. Smart Contract ist im Kontext der „Blockchain-Technologie", vereinfacht gesprochen, ein kleines Computerprogramm. Genauer gesagt handelt es sich um ein sog. Script. Das ist ein kleines Computerprogramm, das wiederum ein anderes Computerprogramm zum Ausführen benötigt. Ein Computerprogramm ist ein Algorithmus geschrieben in einer Programmiersprache. Ein Algorithmus ist eine Arbeitsanweisung an den Computer, wie er die angewiesene Berechnung (Computation) durchführen soll. Der Smart Contract ist also eine in einer Programmiersprache geschriebene Anweisung an den Computer.

Ein Smart Contract ist kein Vertrag im Wortsinne. Dass der Begriff des Smart Contracts zu großer Verwirrung geführt hat, hat sein Begriffsbegründer *Vitalik Buterin*, der „Erfinder" von *Ethereum*, am 13. Oktober 2018, um 10:21 Uhr, offen auf Twitter bereut:

> *„To be clear, at this point I quite regret adoptig the term „smart contracts". I should have called them something more boring and technical, perhaps something like persistent scripts."*

Damit die „Smart Contracts", die ihre Daten aus der Blockchain-Datenbank beziehen, in diesem Fall *Ethereum*, funktionieren, müssen die Netzwerkrechner mehr tun, als nur eine Datensammlung synchron in Kopie vorhalten und aktualisieren: Sie müssen zusammen arbeiten, ihre Rechenleistung zusammenführen zu einem großen Computer. Das nennt man im Falle *Ethereum* die *Ethereum Virtual Machine* (*EVM*).

### 2. Verwendung und Probleme

Ein Vertrag kann sich im Einzelfall aus den Umständen ergeben. Auch im Falle beliebter Computerspiele wie etwa *Cryptokitties*, bei denen gegen gesetzliche Zahlungsmittel „tauschbarer" Ether verwendet wird.

Das *Ethereum*-basierte Smart Contract-Computerspiel namens „King of the Ether"[6] bietet eine recht leicht verständliche Erklärung zur Funktionsweise von Smart Contracts. Besonders positiv ist anzumerken, dass man transparent mit erkannten Fehlern und Sicherheitsrisiken umgegangen ist. Eine Auswahl wird im Folgenden dargestellt.

#### a) Programmierfehler

Der kleinste Programmierfehler kann zu unerwünschten Folgen und damit auch Schäden führen. Daher sollten Smart Contracts so wenig komplex wie möglich sein und ausgiebig getestet werden.

#### b) Böswillige Smart-Contract-Ersteller

Wenn der Ersteller sich bereichern möchte, kann er den Smart Contract entsprechend programmieren. Es ist ein Computerprogramm, das er frei gestalten kann.

#### c) Sicherheitsrisiken außerhalb der Blockchain

Nur weil Smart Contracts in einer vermeintlich sicheren Umgebung betrieben werden, sind sie nicht vor Außeneinflüssen, der Außenwelt oder Dritten sicher. Je mehr Zugriffsmöglichkeiten und Abhängigkeiten bestehen, desto mehr Schwachstellen hat ein Smart Contract. Eine

[6] https://www.kingoftheether.com/thrones/kingoftheether/index.html (zuletzt abgerufen am 27. Februar 2019).

Schwachstelle ist nicht zuletzt die Abhängigkeit vom Mitwirken des Erstellers oder externer Dienstleister.

### d) Alles muss von Anfang an bedacht werden

Das Beispiel des „King of the Ether" zeigt: Wurde die Beendigung im Zeitpunkt der Erstellung nicht bedacht, läuft der Smart Contract auf unbestimmte Zeit weiter. Unter Umständen gegen den Willen des Erstellers. Dieser muss im Nachhinein also erheblichen Aufwand betreiben, um z.B. auf einer Website vor der Nutzung seines Smart Contracts zu warnen und darum zu bitten, keinen Ether aufzuwenden. Erleidet jemand einen geldwerten Verlust, weil er die Warnungen des Erstellers nicht gesehen hat, so hat er keine erkennbare Möglichkeit, seinen Ether wieder zugewiesen zu bekommen. Es gibt kein Impressum.

Im Falle von Smart Contracts, die Vertragsinhalte aktiv regeln sollen, müsste also jede regelungswesentliche Situation im Voraus erdacht und einprogrammiert werden. Das ist, wenn überhaupt möglich, weder sinnvoll noch wirtschaftlich.

## III. Token

Im Kontext des Programmierens bezeichnet ein „Token" das kleinste Element eines Computerprogramms. Jeder seiner Bestandteile ist ein „Token". Im Wesentlichen werden fünf Typen benannt, die ihre jeweilige Funktion im Rahmen einer Programmiersprache beschreiben: Keywords, Identifiers, Operators, Separators und Literals bzw. Constants. Ohne näher wissen zu müssen, was diese Typen konkret bewirken, genügt es, nachzuvollziehen, dass ein „Token" ganz offensichtlich nicht begrenzt verfügbar ist, sondern vielmehr unbegrenzt erschaffen werden kann.[7]

An einem sog. ERC20-Token wird dies besonders deutlich. Dieser „Standard"-Token wird von einem ERC20-Token (Smart) Contract erschaffen, der festgelegten Programmierregeln folgen muss. Hiernach ist insbesondere frei festlegbar, wie viele „Token" erschaffen werden sollen.[8]

„Token" beschreibt also gleichzeitig etwas unbegrenzt Erschaffbares und begrenzt Verfügbares. Wie hier etwas von wirtschaftlichem Wert entstehen soll, ist fraglich.

[7] Auszug aus *Otto*, „Haste mal ´nen Token?", Ri 2018, 143 (145).
[8] https://www.ethereum.org/token (zuletzt abgerufen am 3. März 2019).

# lindenpartners

**lindenpartners** / FRIEDRICHSTRASSE 95 / 10117 BERLIN

Deutscher Bundestag
Finanzausschuss
Die Vorsitzende
Bettina Stark-Watzinger MdB
Platz der Republik 1
11011 Berlin

**ERIC ROMBA**
PARTNER
TEL +49 (0)30 755 424 44
FAX +49 (0)30 755 424 99
ROMBA@LINDENPARTNERS.EU

**lindenpartners**
FRIEDRICHSTRASSE 95
10117 BERLIN
TEL +49 (0)30 755 424 00
FAX +49 (0)30 755 424 99
INFO@LINDENPARTNERS.EU
WWW.LINDENPARTNERS.EU

**per E-Mail: finanzausschuss@bundestag.de**

BERLIN, 6. MÄRZ 2019

UNSER ZEICHEN
ERO/xme/sba

**Geschäftszeichen: PA 7 - 19/ 4217**
**Öffentliche Anhörung zu dem Antrag der Fraktion der FDP "Zukunftsfähige Rahmenbedingungen der Distributed-Ledger-Technologie im Finanzmarkt schaffen" (BT-Drucksache 19/4217)**
**Stellungnahme**

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für die Einladung zur öffentlichen Anhörung zum Antrag der Fraktion der FDP "Zukunftsfähige Rahmenbedingungen der Distributed-Ledger-Technologie (DLT) im Finanzmarkt schaffen" (BT-Drucksache 19/4217). Gerne nutzen wir das Recht zur Stellungnahme. Wie folgt:

## 1. Blockchain und DLT sind nicht nur Bitcoin, Ether und Co

Die Beschäftigung des Deutschen Bundestages mit dem Thema Blockchain und DLT ist ein wichtiges Signal für den Markt. Die offene Diskussion über die Rahmenbedingungen der DLT für den Finanzmarkt ist unterstützenswert. Richtig ist zudem, wie es in dem Antrag 19/

4217 zutreffend formuliert wird, Blockchain und DLT nicht auf den Anwendungsfall von Krypto-Währungen zu reduzieren. Bitcoin war im Jahr 2009 ein erster Anwendungsfall, die Technologie hat sich jedoch in den vergangenen Jahren massiv weiterentwickelt.

Krypto-Währungen und die Finanzierung von Unternehmen über sog. Tokensales auf Blockchains sind daher nur ein Anwendungsfall für die Distributed-Ledger-Technologie (DLT). Es ergeben sich mannigfaltige Anwendungsfälle. Neben der Finanzindustrie spielt das Thema im Bereich Mobility, Infrastruktur, Energie und Immobilien eine Rolle.

Im Verhältnis zu anderen technologischen Entwicklungen steht das Thema Blockchain, DLT und Krypto noch am zeitlichen Anfang. Jeder hat die persönliche Erfahrung, wie z.B. Smart-Phones das individuelle Leben verändert haben. Vergessen wird dabei leicht, dass die massentaugliche Entwicklung von Smart-Phones kaum älter als 12 Jahre ist. Salopp gesagt befindet sich die Entwicklung von Blockchain und DLT erst im Stadium der Entwicklung von "iPhone 1, vielleicht iPhone 2."

## 2. Deutschland braucht kein DLT-Gesetz

In der Debatte um die Anwendung von Blockchain und DLT wird oft gefragt, ob Deutschland ein DLT/ Blockchain-Gesetz braucht. Nach unserer Auffassung braucht Deutschland weder ein DLT-Sonderrecht, noch ein DLT-Gesetz.

a) Security-Token-Offerings Made in Germany sind möglich

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat am 31. Januar 2019 den ersten Wertpapierprospekt für ein Security-Token-Offering für Privatanleger gebilligt. Die Billigung war nicht nur die erste in Deutschland, sondern auch europaweit nach Österreich die zweite innerhalb der EU.

Emittent ist die in Berlin ansässige bitbond Finance GmbH, eine Tochter der bitbond GmbH. Die bitbond GmbH ist ein nach dem Kreditwesengesetz (KWG) reguliertes Institut. Sie bieten die Vermittlung von Darlehen auf Basis der Krypto-Währung Bitcoin an. Die bitbond Finance GmbH hat eine tokenisierte Schuldverschreibung herausgegeben. Die Innovation des Produktes liegt darin, dass eine herkömmliche Verbriefung nicht erforderlich ist, sondern die Führung des Schuldverschreibungsregisters über eine Blockchain erfolgt. Eine bisher im Vermögensanlagengesetz verankerte Namensschuldverschreibung wird durch die Nutzung der DLT übertragbar sowie auch handelbar und damit rechtlich zu

einem Wertpapier im Sinne des deutschen und europäischen Wertpapierbegriffs. In der Konsequenz sind weder Zentralverwahrer, Depotbanken noch Zahlstellen erforderlich. Durch die Nutzung von DLT kann die Emission als sog. Security Token Offering in Eigenemission erfolgen, wodurch auf die Einschaltung einer Emissionsbank verzichtet werden kann. Das Produkt ist dabei rechtlich konform mit dem KWG, dem Kapitalanlagegesetzbuch (KAGB), dem Wertpapierhandelsgesetz (WpHG), dem Wertpapierprospektgesetz (WpPG), dem Vermögensanlagengesetz (VermAnlG), dem Gesetz zum Aufspüren von Gewinnen aus schweren Straftaten (GWG) sowie dem Steuerrecht. Mit dem zugrundeliegenden Konzept können in Zukunft alle illiquiden Assets liquide gemacht werden.

b) DLT stößt rechtlich an Grenzen

Gleichwohl stößt die DLT bei der Emission von Token rechtlich an seine Grenzen. Um das volle Potential der Technologie für den Finanzmarkt zu heben, sind Anpassungen des Zivil- und Aufsichtsrechts unerlässlich. Ziel muss sein, ein harmonisiertes Regelwerk zu schaffen.

aa) DLT und Zivilrecht

Gut illustrieren lässt sich dies am Beispiel des Bürgerlichen Gesetzbuchs i.V.m. dem Schuldverschreibungsgesetz (SchuldVG):

Der in §§ 793 Abs. 1 Satz 1, 796 BGB und § 2 SchVG festgeschriebene Skripturakt führt zu einer Koppelung von Anleihe und Urkunde, die Anleiheemissionen über die Blockchain (also unter Nutzung der Distributed Ledger Technology – DLT) de lege lata ausschließt, bei der die Begründung von Forderungen gegenüber dem Emittenten ausschließlich über einen sog. smart contract im Internet mit anschließender dezentraler Speicherung sämtlicher emissionsrelevanter Daten erfolgt . Kurz gesagt: Das gesetzliche Urkundserfordernis steht einem praktikablen Einsatz von Blockchain-Technologie im Wege. Das Erfordernis einer Urkunde findet sich in einer Vielzahl von Rechtsvorschriften des allgemeinen Zivilrechts, des Schuldverschreibungsgesetzes, des Gesellschafts- und Depotrechts.

Das deutsche Zivil- und Schuldverschreibungsrecht erweist sich insoweit als nicht technikneutral. Denn das Erfordernis der Vorgabe einer Urkunde ist - wenn gleich analog und "off-line" - die Vorgabe einer Technik. Die Lösung ist daher, das deutsche Zivilrecht technikneutral auszugestalten.

Dabei lässt sich für eine Reform leicht auf ein Konzept zurückgreifen, dass der Bund für die eigene Refinanzierung bereits nutzt:

Danach ist für die Begebung einer Schuldbuchforderung des Bundes nach dem Bundesschuldenwesengesetz (BSchuWG) keine Urkunde erforderlich. Sie wird durch die Eintragung in das Bundesschuldbuch ersetzt (§ 5 Abs. 1 und 3 BSchuWG). Handelt es sich um eine Sammelschuldbuchforderung, die auf den Namen einer Wertpapiersammelbank in das Bundesschuldbuch eingetragen ist (§ 6 Abs. 1 BSchuWG), wird die Forderung kraft gesetzlicher Fiktion („gilt") einem Wertpapiersammelbestand gleichgestellt (§ 6 Abs. 2 Satz 1 BSchuWG).

Wollte man dieses Konzept auf die Emission von Anleihen in der Blockchain übertragen, würde der Registerfunktion des Bundesschuldbuchs (§ 5 Abs. 3 BSchuWG) die mit der DLT verbundene dezentrale Registrierung sämtlicher das Rechtsverhältnis zwischen Gläubiger und Emittenten betreffenden Daten entsprechen. Eine Urkundenerstellung wäre in diesem Falle entbehrlich.

In § 2 SchuldVG könnte eine ergänzende Regelung aufgenommen werden, wonach sich die Anleihebedingungen bei einer Emission unter Nutzung der DLT nicht aus einer Urkunde, sondern aus dem (insoweit über die Laufzeit der Anleihe aktuell zu haltenden) Emissionsprospekt ergeben.

Am Ende stünde die Dematerialisierung der Urkunde und die Schaffung eines Wertrechts. Diese Wertrechte könnten vergleichbar dem Schuldbüchern des Bundes auf einem qualifizierten digitalen Register, was Kern der Blockchain-Technologie ist, geführt werden.

Im Detail wären zur Umsetzung weitere gesetzliche Anpassungen erforderlich. Dabei u.a. in folgenden Gesetzen:

- Bundesdatenschutzgesetz (BDSG)/ Datenschutzgrundverordnung (DSGVO)
- Zivilprozessordnung (ZPO) mit Blick auf Beweisfähigkeit und Zwangsvollstreckung
- Insolvenzordnung (InsO)

bb). DLT und Aufsichtsrecht

Anders als das Zivilrecht ist das Finanzmarktaufsichtsrecht schon heute überwiegend technikneutral. Elementarer Begriff im Zusammenhang mit Token ist die Frage der Einordnung als Finanzinstrument.

Die BaFin hat mit Bezug auf Bitcoin und andere Krypto-Währungen hierzu klar Stellung bezogen und diese als Finanzinstrumente, dort Unterfall der Rechnungseinheiten, im Sinne des KWG qualifiziert. Dies ist folgerichtig. Die europäischen Aufseher ESMA und EBA haben sich unlängst ebenfalls zum Thema Krypto-Assets geäußert. Für eine einheitliche Anwendung des weitestgehend europarechtlich gestalteten Finanzmarktaufsichtsrechts wäre es wünschenswert, wenn die Auffassung der BaFin einheitlich betrachtet würde. Dabei geht es nicht darum, neuen Technologien regulatorisch eine Erschwernis zu bereiten, sondern ein level-playing field zu schaffen. Aus unserer Beratungspraxis nehmen wir wahr, dass eine belastbare und vergleichbare rechtliche Einordnung von Token und DLT die Akzeptanz und Wahrnehmung z.B. bei Investoren deutlich erhöht.

Die zivilrechtlichen Änderungen müssen verknüpft werden mit dem Aufsichtsrecht. Dazu werden Anpassungen erforderlich sein, u.a. in folgenden Bereichen:

- KWG und Begriff des Depotgeschäfts (Bankgeschäft vs. Finanzdienstleistungsgeschäft)
- KWG i.V.m. BAIT, MaRisk, MaComp
- Depotgesetz, MaDepot
- Kapitalanlagegesetzbuch (KAGB)
- Zentralverwahrerregulierung (EU-VO CSDR)
- GWG

Damit z.B. Krypto-Handelsplätze ihre Pflicht zur Bereitstellung von Referenzdaten nach Art. 27 MiFIR erfüllen können, muss schließlich die Vergabe von International Security Identification Numbers (ISIN) auch für Security Token ermöglicht werden oder Kennnummern wie die International Token Identification Number (ITIN) als gleichwertige Kennnummer zur Meldung von Referenzdaten anerkannt werden.

## 3. Rahmenbedingungen in Deutschland DLT-freundlich gestalten

Neben den Anpassungen auf zivilrechtlicher sowie aufsichtsrechtlicher Seite ist es erforderlich, die Rahmenbedingungen für Akteure im Bereich DLT freundlich zu gestalten.

DLT ist eine grenzenlose Technologie. Die Marktakteure suchen sich zur Umsetzung die Standorte mit den besten Rahmenbedingungen.

Deutschland, insbesondere voran Berlin, Frankfurt, Hamburg, München und Stuttgart, hat gute Chancen, sich in dem Wettbewerb zu behaupten. Erforderlich ist hierzu nach unserer Auffassung u.a.:

- One-Stop-Shop für Blockchain/ DLT-Geschäftsmodelle bei der BaFin einrichten

Im Rahmen des ersten Security-Token Offerings hat sich die BaFin als versierter und zugänglicher Gesprächspartner erwiesen. Die Haltung der involvierten Mitarbeiter war offen und geprägt von einem großen Wissen. Hierauf ist aufzubauen, einerseits durch Ausbau von Ressourcen an der Schnittstelle von Technologie und Aufsichtsrecht. Andererseits durch das Zurverfügungstellen von Informationen zur Zulässigkeit und Umsetzbarkeit von DLT-Geschäftsmodellen in Deutschland wie z.B. Checklisten für Tokensales, Entscheidungsdatenbanken, Best-Practice-Beispielen.

- Steuerrecht und Steuerverwaltung DLT-fähig machen

Fragen zum Steuerrecht im Zusammenhang mit Blockchain-Anwendungen sind weitestgehend unbearbeitet und unerforscht. Ein einheitliches Verständnis zu Fragen der Ertragsbesteuerung, Umsatzsteuer, Kapitalertrags- und Kirchensteuer über das Ob sowie das Wie sind notwendig. Gleichzeitig sind die Steuerbehörden technologisch in die Lage zu versetzen, steuerbare Sachverhalte aus den Bereichen DLT über Schnittstellen erfassen und bewerten zu können.

## 4. Blockchain-Technologie fördern durch staatlichen Einsatz

Die Entwicklung einer Blockchain-Strategie der Bundesregierung und deren Konsultation ist ein erster richtiger Schritt.

Gleichzeitig muss mit der Strategie das Verständnis verbunden sein, die Blockchain-Technologie durch staatliche Einrichtungen auf kommunaler Ebene oder der Ebene der Länder und des Bundes zu fördern, in dem bisherige Verwaltungsprozesse auf ihre Fähigkeit hin überprüft werden, durch Nutzung der Blockchain-Technologie effizienter und vor allem bürger- bzw. nutzerfreundlicher gestaltet werden zu können. Beispielsweise im öffentlichen Personennahverkehr, beim Bezug von staatlichen Leistungen, im Melde- und KFZ-Wesen, im Gesundheitswesen, im Bereich Gesellschaftsgründungen z.B. bezogen auf Formerfordernisse und Handelsregistereintragungen oder Grundbücher.

Die Förderung der Blockchain-Technologie in Deutschland ist Standortpolitik. Am Maß der Förderung wird sich in absehbarer Zeit zeigen, wo Deutschland im Wettbewerb steht. Die Voraussetzungen sind gut, gleichzeitig lässt die technologische Entwicklung kein Zögern zu. Die Anpassung des rechtlichen Rahmens muss noch in dieser Legislaturperiode erfolgen. Denn das Wissen zur Blockchain-Technologie entwickelt sich nicht zyklisch, sondern kumulativ. Wissenskapital ist mobil und bleibt in Deutschland nur erhalten, wenn die Rahmenbedingungen stimmen.

Mit freundlichen Grüßen

Eric Romba
Rechtsanwalt

DWF Germany Rechtsanwaltsgesellschaft mbH
Linkstr. 12 ● 10785 Berlin ● Germany

per E-Mail: finanzauschuss@bundestag.de

Deutscher Bundestag
Finanzausschuss
Vorsitzende Bettina-Stark Watzinger, MdB
Platz der Republik 1
11011 Berlin

Dr. Nina-Luisa Siedler
Rechtsanwältin

T: +49 30 25090110-0
F: +49 30 25090110-40

E: nina.siedler@dwf.law

9. März 2019

**STELLUNGNAHME ZU DEM**
**ANTRAG DER FDP FRAKTION: „ZUKUNFTSFÄHIGE RAHMENBEDINGUNGEN FÜR DIE DISTRIBUTED-LEDGER-TECHNOLOGIE IM FINANZMARKT SCHAFFEN“**
**(BT-DRUCKSACHE 19/4217)**

Sehr geehrte Frau Vorsitzende,

sehr geehrte Damen und Herren Abgeordnete,

ich bedanke mich für die Einladung zu der öffentlichen Anhörung zu dem o.g. Antrag durch den Finanzausschuss des Bundestages. Die Gelegenheit zu einer schriftlichen Stellungnahme nehme ich hiermit gerne wahr.

## 1. Blockchain/Distributed Ledger Technology (“DLT”)

Die Auseinandersetzung des Bundestages mit Blockchain und DLT ist sehr zu begrüßen. Die öffentliche Diskussion in der Tagespresse wird dabei bislang stark von den Themen Geldwäsche und Energieverbrauch dominiert. Daher möchte ich kurz vorab auf diese zwei Themen eingehen, anschließend die meines Erachtens entscheidenderen Themen anreißen, bevor ich zu den konkreten Fragestellungen in dem Antrag der FDP Fraktion Stellung nehme.

a) Das Geldwäschethema hat von Anfang an eine größere mediale Aufmerksamkeit erfahren, als sachlich zu rechtfertigen ist. Meist genutztes Mittel der Geldwäsche ist und bleibt das Bargeld. Ferner hat sich inzwischen bei Blockchain-Unternehmen die Erkenntnis durchgesetzt, dass die anonyme Annahme von Geldern dazu führt, dass die betreffenden Unternehmen keine (Fiat-) Bankkonten erhalten oder aber jedenfalls die Annahme von Euro (oder anderen gesetzlichen Währungen) aus Kryptogeschäften von ihrer Bank verweigert wird. Unabhängig von einer rechtlichen Verpflichtung identifizieren daher jedenfalls deutsche Unternehmen regelmäßig ihre Geldgeber, um in der (Fiat-) Geschäftswelt handlungsfähig zu

bleiben. Verstärkt wird dieses Ergebnis durch die Änderung der 5. Geldwäsche-Richtlinie, die Anbietern von Zugängen in die Kryptowelt (Kryptobörsen und Wallet-Anbieter) zu Geldwäscheverpflichteten erklärt und bis Anfang 2020 in nationales Recht umgesetzt sein muss. Insgesamt dürften damit Kryptowährungen und andere Token faktisch keine besondere Rolle bei Geldwäscheaktivitäten in Deutschland spielen.

Zweiter, gerne zitierter Kritikpunkt an der Technologie ist ihr vermeintlich zu hoher Energieverbrauch. Diese Kritik greift überhaupt nur bei den (öffentlichen) Blockchains, die wie Bitcoin proof-of-work („PoW“) als Konsensmechanismus verwenden. Inzwischen haben sich viele verschiedene Konsensmechanismen entwickelt, die größtenteils nicht mehr auf dem Einsatz von Rechnerleistung (und damit einhergehend Energieverbrauch) basieren. Industrielle Blockchain- oder DLT-Anwendungen werden kein PoW einsetzen, so dass eine zukünftige Massenanwendung von PoW nicht zu erwarten ist.

b) Ich würde mich daher freuen, wenn sich der Bundestag durch diese zwei populären, aber inhaltlich tatsächlich eher nachrangigen Punkte nicht den Blick auf das Wesentliche verstellen ließe: Die Ermöglichung und Förderung einer Daten- und Kryptoökonomie „made in Germany“. Dem laufenden Fortschritt der digitalen Entwicklung kann sich niemand entziehen. Daher ist es wichtig, die Entwicklung aktiv mitzugestalten und nicht nur zuzuschauen, wie diese rund um uns herum – ohne, dass wir unseren Einfluss geltend machen würden - stattfindet.

Dabei ist es wichtig zu verstehen, dass die Blockchain Technologie als ganz bewusste Gegenbewegung zu der Übermacht großer Monopolisten, wie der bekannten Internet-Giganten, entwickelt wurde. Diese bestimmen schon lange und in zunehmend erschreckenderem Ausmaß unser Handeln in der digitalen Welt. Sie zwingen uns – individuell, aber auch unserem Mittelstand - ihre Regeln auf. Sie bauen ihren Wissensvorsprung durch die immense Konzentration von Daten immer weiter aus.

Wie können Daten also selbstbestimmter und gerechter verteilt und nutzbar gemacht werden? Marktrelevante und verhaltensbezogene Daten können mit Hilfe der Bockchain-Technologie unternehmensunabhängig abgelegt und demjenigen zugeordnet werden, der sie kreiert (nämlich uns als Nutzern, statt einseitig den Unternehmen, mit denen wir interagieren). Eine Datenerfassung auf geteilten Systemen, die idealerweise nicht mehr von einzelnen Unternehmen beherrscht werden, schaffte also eine deutlich vorteilhaftere Infrastruktur. Dafür bedarf es aber rechtlich transparenter und verlässlicher Governance Systeme, um das Vertrauen einer breiten Masse in eine solche neue Infrastruktur zu kreieren.

Es liegt an Ihnen, sehr geehrte Damen und Herren Abgeordnete, das Entstehen des neuen Internet mitzugestalten durch klare Anreizsetzung für den Aufbau gesellschaftspolitisch gesunder Strukturen. Ein Instrument hierfür wäre die Schaffung einer neuen Gemeinnützigkeitskategorie für öffentliche Blockchains, zum Beispiel unter der Voraussetzung, dass bestimmte Mindestkriterien an die Governance (inklusive der zum Einsatz kommenden Konsensmechanismen) erfüllt werden. Eigentlich wäre es eine staatliche Aufgabe, für die grundlegende digitale Infrastruktur von morgen zu sorgen. Tatsächlich wird diese Infrastruktur ausschließlich privatwirtschaftlich gebaut, was zu den bekannten Monopolbildungen mit seinen Nachteilen für Verbraucher, aber auch unseren Mittelstand, geführt hat. Die Blockchain-Technologie gibt Anlass, neu nachzudenken, ob es nicht an der Zeit wäre, dem zumindest eine zweite Säule an die Seite zu stellen durch Förderung einer zwar privat organisierten, aber nicht-gewinnorientierten Infrastruktur-Schaffung, wenn der Staat diese schon nicht selbst zur Verfügung stellt. Basierend auf einer solchen, neuen Infrastruktur könnten dann kommerzielle Angebote entstehen, die nicht mehr einseitig die entstehenden Daten abgreifen könnten, sondern in der Hoheit des Einzelnen belassen müssten, der diese Daten kreiert.

d) Anders als in Deutschland ist auf EU-Ebene die Bedeutung der Governance-Themen bereits erkannt. Die Europäische Kommission hat nach und nach eine bemerkenswert gesamtheitliche Blockchain-Strategie entwickelt: Start bildete die Initiierung der European Blockchain Partnership, mit der eine eigene, durch die EU-Staaten betriebene Blockchain-Infrastruktur geschaffen werden soll, die der öffentlichen Hand eine gesicherte Experimentiergrundlage zur Verfügung stellt. Zweiter Schritt war die Einrichtung des EU Blockchain Observatory and Forum, einer offenen Plattform zum Austausch mit der Blockchain Community samt regelmäßigen Veranstaltungen, Reports und der Einrichtung von Working Groups sowie der Zurverfügungstellung einer Kommunikationsplattform. (Vorläufig) letzter Schritt war die massive Unterstützung der Gründung von INATBA letzte Woche, eines Verbandes der privaten Blockchain-Industrie, dem die Kommission neben Standardsetzung und Entwicklung rechtskonformer Smart Contracts auch das Governance-Thema in den Satzungszweck geschrieben hat.

Es ist daher begrüßenswert, dass sich die Bundesregierung nun ebenfalls mit der Entwicklung einer Blockchain-Strategie beschäftigt. Ich vermisse allerdings eine Auseinandersetzung mit den angesprochenen grundlegenden gesellschaftspolitischen Fragestellungen, um das wichtige Zukunftsthema der Ausgestaltung unserer künftigen, digitalen Infrastruktur mitzugestalten.

**2. Antrag der FDP Fraktion**

**a) Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“)**

Die BaFin hat sich bereits seit geraumer Zeit eine hervorragende Fachkompetenz angeeignet, die auch international anerkannt ist. Diese ist jedoch bei einzelnen, noch wenigen Mitarbeitern konzentriert.

Mit Sorge beobachten wir daher die starke Auslastung dieser geschätzten Kollegen in der BaFin und plädieren, ob der stetig ansteigenden Zahl von Anfragen und der vielfältigen weiteren Inanspruchnahme durch Ministerien und internationale Gremien, für eine deutliche personelle Ausweitung der Kapazitäten für dieses Thema innerhalb der BaFin.

Hochtechnologie-Unternehmen können sich aufgrund der Geschwindigkeit der Weiterentwicklung in ihrem Bereich kein monatelanges Warten auf ein Klären ihrer aufsichtsrechtlichen Fragen leisten. Sie benötigen verlässliche, überschaubare Zeitrahmen für die Beantwortung ihrer Fragen, die sie mit den Produkteinführungsabteilungen in Einklang bringen können. Die aktuellen Bearbeitungszeiten sind für diesen Bereich – gerade auch im Vergleich mit anderen Ländern - schlicht zu lang und zu wenig vorhersehbar. Dieser Standortnachteil für Deutschland ließe sich durch eine deutliche Aufstockung der personellen Kapazitäten beseitigen.

Ferner ist der Ansatz, nur vollständige Anfragen mit bereits vollständiger entworfener rechtlicher Dokumentation zu prüfen, für Startups kaum leistbar. Die hiermit verbundenen Kosten der Rechtsberatung „ins Blaue“ hinein sind vielfach zu hoch. Empfehlenswert wäre daher ein abgestufter Ansatz, in dem zunächst die grundsätzlichen Fragen auf abstrakter Ebene geklärt werden könnten und sodann eine Dokumentation nachzureichen ist, die nur der der Überprüfung der tatsächlichen Umsetzung des Besprochenen unterliegt.

Sehr zu begrüßen ist die sich andeutende Änderung der Verwaltungspraxis der BaFin, nun auch zu der Frage der Prospektpflicht schriftliche Auskünfte zu erteilen. Bislang wurde diese Auskunft nur mündlich erteilt, was Missverständnisse provozieren kann und bei dem Anfragenden stets ein Gefühl der Unsicherheit hinterlässt.

Mit Ausnahme der Frage zur rechtlichen Qualität von Kryptowährungen, die die BaFin frühzeitig als Finanzinstrumente im Sinne von Rechnungseinheiten qualifiziert hat, fehlt es bislang noch an verbindlichen Hinweisschreiben zu den vielfältigen Fragen bei dem gewerblichen Umgang mit kryptographischen Token. Das Hinweisschreiben vom 20.02.2018 (GZ: WA 11-QB 4100-2017/0010) fasst im Wesentlichen nur die offenen Fragen zusammen, ohne nennenswerte Antworten zu geben. Erste Leitlinien für eine umfassende Token-Klassifizierung gab erstmals ein Aufsatz in der Ausgabe BaFin Perspektiven aus August 2018. Es wäre hilfreich, diesen Ansatz nun in einem Hinweisschreiben zu formalisieren. Dabei sollte selbstverständlich sein, dass in diesem schnelllebigen Sektor von einer fortlaufenden Weiterentwicklung der kommunizierten Linie ausgegangen werden muss. Der Anspruch auf Äußerung lediglich dauerhaft aufrecht zu erhaltender Kriterien und Anforderungen sollte in diesem Bereich dem vorhandenen Interesse der Mitteilung von auch nur vorläufiger und unter Beobachtung stehender rechtlicher Bewertung weichen. Die Aufsicht muss für sich in Anspruch nehmen, agiler zu kommunizieren und Einschätzungen auch (für die Zukunft) revidieren zu können, wenn neue Entwicklungen dies erforderlich machen. Deutsche Behörden müssen sich insgesamt dem deutlich gestiegenem Tempo der Entwicklungen anpassen und hierbei auch neue, mutigere Wege einschlagen, um den Standort Deutschland attraktiver zu gestalten.

Hierzu gehört im Bereich der BaFin auch die Schaffung größerer Transparenz ihrer aktuell nur im Einzelfall vorgenommenen Entscheidungen. Erforderlich ist zumindest eine abstrahierte Mitteilung über getroffene Beurteilung, so dass der gesamte Markt mitlernen und sich entsprechend entwickeln kann. Statt jeder dieser Entscheidungen mit dem ausdrücklichen Hinweis zu versehen, dass diese nicht öffentlich werblich eingesetzt werden darf und auch rein sachlich mitteilende Äußerungen zu dem Vorhandensein und Inhalt ihrer Entscheidungen zu untersagen, wäre der umgekehrte Ansatz sinnvoll: Die BaFin sollte die Unternehmen jeweils fragen, ob und wieweit ihr die Zustimmung erteilt wird, über die Einzelfallentscheidung zu informieren. Gerne werden pauschal Bedenken aufgrund von Vertraulichkeitsverpflichtungen und dem Schutz von Geschäftsgeheimnissen vorgebracht, wohingegen ich in der Praxis eher ein Mitteilungsbedürfnis der Unternehmen beobachte.

Aufgrund der stets internationalen Ausrichtung von Blockchain/DLT Unternehmungen wäre zumindest eine parallele Veröffentlichung aller Verlautbarungen auf Englisch wünschenswert.

## b) Prospekte

Prospektpflichten greifen auf nationalem Level (für Vermögensanlagen) und auf EU-Level (für Wertpapiere nach MiFID). Erfreulicherweise besteht inzwischen Klarheit darüber, dass „tokenisierte“ Vermögensanlagen weitgehend dem europäischen Prospektrecht unterfallen und damit diese Prospekte EU-weit genutzt werden können.

Unbefriedigend ist allerdings noch das Fehlen von besonderen Anhängen (den Listen für Prospektinhalte für einzelne Finanzinstrumente) für Token-Emissionen. Hier stellen sich in der Praxis etliche Fragen und die aktuellen Anhänge fragen die für Token-Emissionen speziell erforderlichen Informationen nicht ab. So ist in dem Bereich regelmäßig die detailliert zu beschreibende Finanzhistorie weniger relevant, da die Unternehmen oft jung sind und über diese Daten noch nicht verfügen. Informationen über die entscheidenden technischen und Governance-Fragen werden hingegen von den derzeitigen Formularen nicht erfasst. Ferner steht die verlangte Wertpapierkennnummer (WKN/ISIN) tokenisierten Finanzinstrumenten aktuell nicht zur Verfügung.

Ich unterstütze auch die Forderung nach einer freiwilligen (optionalen) Prospektprüfung von Nicht-Finanzinstrumenten, wie bei der Ausgabe der sog. Utility Token, um die Transparenz

der vorhandenen Informationen in diesem Bereich zu fördern. Der Vorschlag eines Opt-in stammt aus Frankreich, so dass hier idealerweise grenzüberschreitend kooperiert werden sollte, um zu einer Lösung zu gelangen, die nicht ausschließlich national in Deutschland gilt, sondern, wenn nicht gleich auf EU-Ebene, so dann doch wenigstens bilateral grenzüberschreitend anerkannt wird.

Gleiches wäre wünschenswert für die jüngste Einführung der Prospektfreiheit von Wertpapieremissionen mit einem Volumen von bis zu Euro 8 Mio. Während Emissionen bis zu Euro 1 Mio. EU-weit prospektfrei sind, war es dem nationalen Gesetzgeber freigestellt, auch den Bereich bis Euro 8 Mio. von der Prospektpflicht auszunehmen. Deutschland hat hiervon erfreulicherweise Gebrauch gemacht, jedoch in § 3c WpPG vorgeschrieben, dass solche Angebote ausschließlich über Wertpapierdienstleistungsunternehmen an qualifizierte (institutionelle) Anleger vermittelt werden dürfen oder an nicht qualifizierte Anleger nur unter Einhaltung niedriger Beteiligungsbeträge (in Abhängigkeit von der persönlichen finanziellen Situation). Diese Übernahme des amerikanischen Konzeptes der Zulassung nur von wohlhabenden Investoren für risikoreichere Anlagen halte ich persönlich für gesellschaftspolitisch problematisch. Die historische Entwicklung in den USA belegt einen Zusammenhang zwischen der Einführung dieses Konzepts und des weiteren Auseinanderdriftens der Schere zwischen Arm und Reich. Meines Erachtens sollte dieses Konzept überprüft werden im Sinne einer Einführung eher inhaltlicher Anforderungen an Hoch-Risiko-Investoren (Schaffung von „Investmentführerscheinen“ zum Nachweis der erforderlichen Kenntnisse zur Beurteilung von Hoch-Risiko-Investitionen), um auch den weniger vermögenden Bürgern eine gleichberechtigte Teilhabe an diesen potentiell deutlich höheren Gewinn bringenden Anlagen (bei selbstverständlich höherem Risiko und daher auch sinnvollerweise zu verlangender, entsprechender Qualifikation) zu ermöglichen.

Ferner sollte stets grundsätzlich überprüft werden, ob die Festschreibung von zentralen Intermediären in der aktuellen Form weiterhin dauerhaft erforderlich ist oder zugunsten von technologischen und Governance-Vorgaben auf diese verzichtet werden und damit der Monopolwirkung vorgebeugt werden kann.

**b) Zivilrechtliche Fragestellungen**

Zivilrechtlich stellt sich vor allem die Frage nach der rechtlichen Qualität von Token. Token sind weder Sachen (physische Gegenstände) noch Rechte und profitieren daher nicht von einem (Eigentums-) Schutz vergleichbar zu den bekannten absoluten Rechte. Sie stellen nach herrschender Meinung lediglich einen „sonstigen Vermögensgegenstand“ dar, dem vergleichbar zu knowhow ein absoluter Schutz vor „unberechtigtem“ Entzug fehlt. Die aufkommende „Token Economy“, bei der alles durch Token repräsentiert können sein soll („digital twins“), verlangt aber genau nach solch einem absoluten Schutz vergleichbar zu dem Schutz von Eigentum an physischen Gegenständen.

Ferner muss das bisherige Verbraucherschutzrecht im digitalen Bereich, das bislang für die klassische Internetökonomie geschrieben ist, technologieneutral ausgestaltet werden. Unklarheiten bestehen bei der Reichweite der aktuellen Verbraucher-Widerrufsrechte, bei der Verwendung der Musterwiderrufsbelehrung und der Frage, ob Token als digitale Inhalte anzusehen sind (mit entsprechenden Konsequenzen für die Verzichtsmöglichkeit auf Widerrufsrechte). Probleme bereitet auch die Anforderung, Bestellbestätigungen zu übersenden.

Die Idee von Smart Contracts, also sich selbst vollziehender Automatismen, und die weitläufig verbreitete Annahme, dass die Aktionen solcher Smart Contracts keiner beteiligten Partei zuzurechnen sind, sondern dieser quasi wie ein Treuhänder neutral agiert, findet keine

Entsprechung im deutschen Recht. Es stellt sich daher die Frage, ob der Erwartungshaltung der Anbieter- und Nutzerkreise von Smart Contracts unter bestimmten Voraussetzungen (Anforderungen an Audits und ggf. zentraler Autorisierung von Smart Contracts) entsprochen werden kann, um die rechtssichere Anwendung solcher Automatismen zu ermöglichen.

Wir sehen uns schon heute (ganz unabhängig von jeder Blockchain-Diskussion) vielfältig digitalisierten Automatismen ausgesetzt, die von wirtschaftlich dominierenden Anbietern oft ohne ausreichende, individuelle Korrekturmöglichkeiten eingesetzt werden und so *de facto* Nutzer den jeweils privatwirtschaftlich gesetzten Spielregeln unterwerfen. Globale Anbieter können hierbei kaum ihre Systeme allen nationalen Besonderheiten anpassen und setzen darauf, dass Nutzern jedenfalls in der Masse keine Wahl bleibt, als ihre Regeln zu akzeptieren. Dies trifft neben den einzelnen Verbrauchern vor allem gewerbliche, mittelständische Nutzer von globalen Handelsplattformen, die einen Ausschluss von der Plattform während eines langwierigen Rechtsstreits finanziell nur schwer überleben können. Dieses Phänomen der faktischen Rechtssetzung durch (insbesondere) internationale Konzerne bedarf unbedingt einer genaueren Analyse und internationaler Aktion, da es das nationales Recht aushöhlt und zunehmend bedeutungslos werden lässt. Wir müssen zu idealerweise globalen, aber zumindest europäischen Standards für den Umgang mit digitalisierten Automatismen gelangen, die gleichermaßen Rechtssicherheit für Anbieter wie faktische (und nicht nur theoretische) Rechtsdurchsetzungsmöglichkeiten für Nutzer schaffen.

**c) Abschaffung des Urkundserfordernisses**

Die Bundesregierung sollte die Abschaffung des deutschen Urkundenerfordernisses für Wertpapiere prüfen und die Begebung digitaler Wertpapiere auf Grundlage eines qualifizierten digitalen Registers ermöglichen. Zwar hat die BaFin mittlerweile für Rechtssicherheit im Hinblick auf die Prospektpflicht öffentlich angebotener Security Token gesorgt, allerdings verbleiben erhebliche Risiken bei der Begebung von Security Token, die im Wesentlichen auf das Urkundenerfordernis des Wertpapierbegriffs nach deutschem Zivilrecht zurückzuführen sind.

Vor diesem Hintergrund ist der nun vom Finanz- und Justizministerium verfolgte Ansatz zur Einführung elektronischer Wertpapiere im Grundsatz richtig (vgl. dazu das von den Ministerien am 7. März 2019 veröffentlichte Papier zu Eckpunkten für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token). Nur durch entsprechende gesetzgeberische Maßnahmen können die aktuell existierenden wertpapierrechtlichen Unsicherheiten bei der Begebung von Security Token dergestalt überwunden werden, dass mittelfristig liquide Sekundärmärkte entstehen können. Anderenfalls dürfte es zumindest institutionellen Marktteilnehmer schwerfallen, sich auf diesen Märkten zu betätigen. Der vielleicht weniger kritische (weil weniger kenntnisreiche) Kleinanleger würde gleichermaßen geschützt werden und von der geschaffenen Rechtssicherheit profitieren.

Der Gesetzgeber sollte dazu die Regelungen des BSchuWG, die Bund und Ländern die Begebung entmaterialisierter Anleihen ermöglichen, auf entmaterialisierte Wertpapiere erstrecken, die auf einem DLT-basierten Register verwaltet werden, das bestimmten Anforderungen an Technik und Governance genügt. Darüber hinaus wären weitere begleitende Anpassungen in einer Reihe von bestehenden Gesetzen erforderlich, um ein kohärentes Regelungsregime für Security Token zu schaffen. Dabei sollte in jedem Fall geprüft werden, ob es tatsächlich noch zwingend des monopolisierten Zentralverwahrungsregimes bedarf oder durch ein DLT-basiertes System nicht ein identisches Sicherheitsniveau auf der Nachhandelsseite gewährleistet werden kann.

**d) Verwahrung von Token**

Banken agieren derzeit selten als Verwahrer von Token. Diese Tätigkeit wird häufig von Unternehmen aus dem Blockchain-Bereich angeboten, die gegebenenfalls mit Banken oder Finanzdienstleister zusammenarbeiten.

Bisherige Begriffsbestimmungen für das Verwahren von Token stellen darauf ab, dass der Dienstleister den Private Key des Wallets für den betreffenden Nutzer verwahrt (vgl. Art. 3 Nr. 19 der Richtlinie (EU) 2018/843 (5. Geldwäscherichtlinie) sowie European Securities Markest Authority „Advice Initial Coin Offerings and Crypto-Assets“ (ESMA50-157-1391)). Bei dieser Ausgestaltung kann der Nutzer nicht ohne den Anbieter über die auf dem Wallet befindlichen Token verfügen. Der Nutzer ist daher darauf angewiesen, dass der Anbieter angemessenen Maßnahmen ergriffen hat, um einen Verlust der Token zu vermeiden, die verwahrten Token dem Nutzer jederzeit verfügbar machen kann.

Auch wenn diese Tätigkeit für den Nutzer mit Risiken verbunden ist, ist sie nicht mit der Kontoführung von Banken oder einer Wertaufbewahrung vergleichbar. Bei der Kontoführung durch Banken werden die Buchungen auf dem Konto durch die Bank vorgenommen. Dagegen werden die dem Wallet zugeordneten Token durch Validierung der Transaktion in dem (dezentralen) Netzwerk dem Wallet zugerechnet. Der Dienstleister des Online-Wallets nimmt keine Buchungen vor, sondern kann nur durch den Private Key Transaktionen auf dem Online-Wallet auszulösen. Der Dienstleister speichert für den Nutzer den Private Key und somit Daten, es findet somit keine Verwahrung von beweglichen Sachen, wie bei der Wertaufbewahrung statt. Dementsprechend wäre eine Qualifizierung dieser Tätigkeit als Kontoführung oder Wertaufbewahrung derzeit nicht zutreffend.

Dienstleister die im Rahmen des Angebots von Online-Wallets auch die Private Keys für die Nutzer verwahren, unterliegen (auch wenn es sich um nach dem KWG regulierte Institute handelt) hinsichtlich dieser Dienstleistung keiner Erlaubnispflicht nach dem Kreditwesengesetz. Die entsprechende Dienstleistung qualifiziert insbesondere nicht als Depotgeschäft nach § 1 Abs. 1 Satz 2 Nr. 5 KWG, da diese nur die Verwahrung von Wertpapieren in Urkundenform umfasst, was auf Token nicht zutrifft.

Eine etwaige Regulierung von Verwahrern von Token, die den Private Key für den Nutzer verwahren, sollte abgestimmt auf europäischer Ebene erfolgen, um es zu ermöglichen, die Dienstleistung in allen Mitgliedsstaaten der EU anzubieten. Eine pauschale Übertragung der Erlaubnisanforderungen und Organisationspflichten von Kreditinstituten und Finanzdienstleistungsinstituten auf diese Dienstleistung erscheint vor dem Hintergrund der technologisch möglichen Sicherungsmechanismen bei DLT-Lösungen nicht angemessen. Für die Erbringung der entsprechenden Dienstleistung ist vielmehr die Nutzung zuverlässiger IT Systeme und Vorhaltung entsprechender Backup-Lösungen essentiell.

**e) Datenschutz**

Das geltende Datenschutzrecht ist seinem Anspruch nach technologieneutral. Dies ergibt sich nicht nur aus Erwägungsgrund 15 zur DS-GVO. In der Verordnung findet sich keinerlei Hinweis darauf, dass nur bestimmte Technologien bei der Regelung bedacht, andere aber bewusst ausgeschlossen wurden.

Der Einsatz von DLT-Lösungen ist nicht per se datenschutzrechtlich bedenklich. Bei einer sog. private permissioned Struktur (Zugangsreguliert durch ihre Betreiber) können die kritischen Fragen des Datenschutzrechtes etwa hinsichtlich der Verantwortlichkeit, der Rechtsgrundlage

der Verarbeitung, der Transparenz und der Durchsetzung der Betroffenenrechte jedenfalls in Ansätzen hinreichend beantwortet werden.

Kritisch ist die Frage der Einhaltung datenschutzrechtlicher Vorgaben stets dann, wenn es keine personell klar definierte Entität gibt, die die DLT beherrscht (also bei den öffentlichen „unpermissioned“ Blockchain-Lösungen). Dann kommt es regelmäßig (stets in Abhängigkeit der konkreten Ausgestaltung der Blockchain-Infrastruktur) zu der Frage, wer für die Datenverarbeitung verantwortlich ist und gegen wen der Betroffene seine Rechte geltend machen kann.

Besonders diskutiert wird die Problematik, dass DLT Transaktionsdaten naturgemäß dauerhaft und grundsätzlich unveränderbar speichern. Daraus resultiert die Frage, ob die Technologie mit dem datenschutzrechtlichen „Recht auf Löschung“ und dem „Recht auf Vergessenwerden“ aus Art. 17 DS-GVO vereinbar ist.

Das Hauptaugenmerk liegt in diesem Zusammenhang auf den Regelungen des Art. 17 Abs. 1 a) DS-GVO. Die Norm schreibt vor, dass personenbezogene Daten nach Erreichung des Zwecks für die sie erhoben wurden, durch den Verantwortlichen zu löschen sind. Die Abwicklung einer Transaktion auf einer Blockchain oder in einem Distributed Ledger System dürfte, soweit sie unter Einbeziehung personenbezogener Daten erfolgt, ein Verarbeitungsvorgang im Sinne der DS-GVO darstellen. Dieser Verarbeitungsvorgang wäre mit dem Zeitpunkt der erfolgreichen Durchführung der Transaktion, beispielsweise der Übertragung eines Tokens, beendet und der Zweck dieser Datenverarbeitung erreicht, sodass die (personenbezogenen) Transaktionsdaten zu löschen wären. Da jedoch die Transaktionsdaten als solche grundsätzlich nicht aus einer Blockchain oder einem Distributed Ledger System gelöscht werden können, entsteht an dieser Stelle scheinbar eine Kollision mit dem geltenden Datenschutzrecht.

In diesem Zusammenhang ist jedoch bislang unbeachtet geblieben, dass der Zweck der Verarbeitung der Transaktionsdaten nicht nur die Abwicklung der eigentlichen Transaktion, im Sinne der Übertragung eines Tokens ist. Vielmehr dient die Erfassung der Transaktionsdaten, ihre Zusammenfassung in Blöcken und deren kryptographische Verknüpfung der Verhinderung missbräuchlicher Transaktionsdurchführungen und Wertezuweisungen, etwa durch sog. „Double Spending“ oder andere nachträgliche Manipulationen. Die Verarbeitung von Transaktionsdaten dient insofern sowohl dem Zweck, Transaktionen (im Sinne der Zuweisung von Tokens von einem Nutzer an den anderen) durchzuführen, als auch dem Zweck, Manipulations- und Fälschungssicherheit innerhalb des Systems zu gewährleisten.

Der Zweck der Erreichung von Manipulations- und Fälschungssicherheit ist eine fortlaufende (perpetuierte) Aufgabe von Blockchain und Distributed Ledger Systemen. Er kann nicht in einem bestimmten, einen Löschungsanspruch im Sinne des Art. 17 Abs. 1 Nr. 1 DS-GVO auslösenden, Zeitpunkt erreicht werden. Es sollte daher Klarheit für perpetuierte Verarbeitungszwecke geschaffen werden, in dem Sinne, dass eine Zweckerreichung bei bestimmten Verarbeitungstatbeständen nicht eintreten kann.

Offen bleibt jedoch, ab wann von einer Anonymisierung personenbezogener Daten ausgegangen werden kann. Bei Annahme einer hinreichenden Anonymität entfällt der Schutz des jeweiligen Datums durch das Datenschutzrecht. Kann sich ein Nutzer also mit einem aus der Perspektive aller anderen Teilnehmer anonymen Datum in einer Infrastruktur bewegen, wäre ein Schutz durch das Datenschutzrecht weder geboten noch erforderlich. Nach Auffassung des EuGHs (EuGH (2. Kammer), Urteil vom 19.10.2016 – C-582/14 - Breyer/Deutschland) sind bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem Verantwortlichen für die

Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Dies führt bei der stetigen Weiterentwicklung der Technologie und insbesondere von künstlicher Intelligenz unvermeidbar dazu, dass bestimmte Daten unter Einsatz heutiger Technologien als anonym anzusehen sind, aber neue Technologien morgen schon eine Identifizierung der betreffenden Person ermöglichen könnten. Dies stellt insbesondere den Einsatz von Technologien für perpetuierende Datenhistorien, die auf zentrale Datenverarbeiter verzichten, vor nahezu unlösbare Aufgaben.

Insgesamt würde ich es sehr begrüßen, wenn Deutschland deutliche Anstrengungen unternähme, den Anschluss an das Entwicklungstempo auf europäischer Ebene sowie den sehr aktiven Ländern wie Frankreich, der Schweiz, Gibraltar, Malta und Liechtenstein zu finden. Ich vermisse die Auseinandersetzung mit den gesellschaftspolitischen Implikationen der (öffentlichen) Blockchains (im Gegensatz zu den privaten DLT-Lösungen), die gänzlich unterschiedliche rechtliche Fragestellungen und spezifische gesellschaftliche sowie wirtschaftliche Chancen und Risiken mit sich bringen.

Mit freundlichen Grüßen

Dr. Nina-Luisa Siedler
Rechtsanwältin