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

Anlage

Die andere Seite der Krypto-Münze

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 ($10,437,804,284 USD) 15.60% Total	
Wealth Distribution Top 10/100/1,000/10,000 addesses	5.38% / 15.60% / 35.19% / 57.75% Total	
Addresses richer than 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 ($857,400,395 USD) 18.70% Total	last 24h: 308,065 ETH ($40,585,000 USD) 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).