71. Deutscher Juristentag

The next big thing: Blockchain – Bitcoin – Smart Contracts

Wie das disruptive Potential der Distributed Ledger Technology (nicht nur) das Recht fordern wird

Prof. Dr. Dr. Walter Blocher, Kassel

Die digitale Wirtschaft ist längst global unterwegs und nimmt auf Rechtsordnungen – erst recht nationale – wenig Rücksicht. „Digitale Wirtschaft – Analoges Recht – Braucht das BGB ein Update?" wird der 71. Deutsche Juristentag in der Abteilung Zivilrecht daher am 14. und 15. September 2016 fragen. Doch wer auf die ersten 50 Jahre ihrer Geschichte zurückblickt, mag erkennen, dass die Evolution der Informationstechnologie noch lange nicht zu Ende ist. Der Autor wirft einen Blick auf die nächste Netz-Revolution, ausgelöst von dezentralen Blockchains. Damit das nicht wie Science Fiction klingt, erläutert er in einer auch für Laien verständlichen Form, auf welchen technischen Lösungen die Revolution beruht – und was heute schon Wirklichkeit ist und wie diese Entwicklung das Recht in besonderer Weise fordern wird.

Auf Tausenden, künftig vielleicht auf Millionen von Computern verteilte dezentralisierte Verzeichnisse (Distributed Ledger Technology, kurz DLT) können die bislang im elektronischen Geschäfts- und Rechtsverkehr erforderlichen Vertrauensintermediäre (wie Banken, Kreditkartenorganisationen, Notariate, staatlich organisierte Verzeichnisse wie Grundbuch, Handelsregister, aber auch derzeit noch so „modern" erscheinende Plattformen wie Airbnb, Uber, Twitter und Dropbox) über weite Strecken ablösen und durch „Smart Contracts" (mit Beteiligung von Schlichtern) auf bestimmten Gebieten sogar die staatliche Rechtsdurchsetzung überflüssig erscheinen lassen. „Trustless trust" auf der Grundlage von DLT wird durch die damit bewirkte Disintermediatisierung, also den Wegfall sogenannter „vertrauenswürdiger Dritter" als Transaktionsmittler, die Art und Weise, wie wir das Internet nutzen und wie wir Geschäfte schließen, erheblich verändern. Die Möglichkeit, dezentrale (unter Umständen sogar autonome) Organisationen von Mitgliedern aufzubauen, die einander weder kennen noch Vertrauen schenken müssen, lässt kaum einen Bereich der Informationsgesellschaft unberührt. Auch das „Internet of Things" (IoT) erhält mit DLT enormen Schwung. Bislang ungelöste Probleme des Datenschutzes, des Verbraucherschutzes, von elektronischen Abstimmungen, der Verfügung über geistiges Eigentum usw. scheinen mit DLT bewältigbar. Selbst eine Stärkung und Modernisierung demokratischer Strukturen wird davon erwartet.

I. IT-Geschichte in der Nussschale

In der bisherigen, etwas mehr als ein halbes Jahrhundert umfassenden Geschichte der Informationsgesellschaft[1] konnten alle zehn bis 15 Jahre durch neue Technologien ausgelöste tiefgreifende Veränderungen beobachtet werden. So war für die Sechziger- und auch noch die Siebzigerjahre des vorigen Jahrhunderts die auf Mainframes (Großrechnern) wie CDC 1600 oder IBM S/360 beruhende EDV kennzeichnend. Etwa in der Mitte der Siebzigerjahre folgten die Mikroprozessoren, die schließlich in den Achtzigerjahren zum Siegeszug des Personal Computings auf IBM PC und Apple Mac führten. Die Neunzigerjahre wurden vom Durchbruch des Internets, insbesondere des Word Wide Webs (WWW), geprägt. Für die Nullerjahre des 21. Jahrhunderts und für die Gegenwart stehen Smartphones und Social Media. In den nächsten zehn Jahren könnte nun die DLT unter anderem monolithische Platzhirsche erschüttern, ungeahnte Freiräume für flexible Startups schaffen und – weit über das Dezennium hinaus – die Informationsgesellschaft nachhaltig modifizieren.

II. Problematik der herkömmlichen Internet-Nutzung

1. Auswahl und Präsentation nicht-rivalisierend konsumierbarer Information

Der herausragende Erfolgsfaktor für den Siegeszug des Internets war zweifellos die mit seiner Nutzung einhergehende Reduktion von Suchkosten. Information als nichtrivalisierend, also ohne gegenseitige Beeinträchtigung durch mehrere gleichzeitig konsumierbares Kommunikationsgut sollte dadurch allen zugänglich werden. Mehr noch: an die Stelle der Abhängigkeit von relativ wenigen Sendern würde die dem Meinungspluralismus zuträgliche Möglichkeit treten, jeden nicht nur empfangen, sondern auch senden zu lassen. Das Wort „Prosumer"[2], das den zugleich als Produzent und als Konsument auftretenden Internet-Nutzer kennzeichnen sollte, wurde geprägt.

Selbst in der ureigenen Domäne des Internets als Instrument des Informationsaustausches wurden aber zu Beginn gehegte sozialromantische Erwartungen rasch enttäuscht. Zur Bewältigung der jeden Empfänger überfordernden Informationsflut etablierten sich Webportale und Suchmaschinen als unverzichtbare Werkzeuge. Vorstellungen aus der Anfangszeit der Kommerzialisierung des Internets, die das Netz als Nebel von Geld sahen, in den man nur Kondensationskerne stellen müsse, um erfolgreich zu sein, platzten bald wie bunte Seifenblasen. Netzwerkeffekte bewirkten nämlich Konzentrationsprozesse, die zu monopolartigen Marktstellungen der erfolgreichsten Diensteanbieter führten. Nur die blauäugigsten Nutzer glauben, dass deren Nutzung für sie kostenlos sei. Tatsächlich zahlen wir mit dem äußerst knappen Gut Zeit, nämlich in Gestalt unserer Aufmerksamkeit, um welche die Online-Werbekunden buhlen und dabei den Plattformbetreibern fette Gewinne bescheren. Mit jedem Suchvorgang, mit jedem Aufruf einer Website, ja mit jedem Mausklick hinterlassen wir überdies eine glitzernde Spur aus Daten, der zweiten „Währung" der Informationsgesellschaft. Analysen der so entstehenden riesigen Datensammlungen („Big Data") verschaffen deren Herren eine an Allwissenheit grenzende Sicht auf das aktuelle Weltgeschehen und auf künftige Trends.[3]

1 Für einen instruktiven Überblick s. *Danyel*, Zeitgeschichte der Informationsgesellschaft, Zeithistorische Forschungen, H. 2 (2012), S. 186, passim, http://kurzelinks.de/AnwBl-2016-8u9-1.

2 *Toffler*, The Third Wave (1980), passim.

3 Vgl. *Schlieter*, Die Herrschaftsformel – Wie Künstliche Intelligenz uns berechnet, steuert und unser Leben verändert (2015), passim.

Des Weiteren werden die zur Reihung und Filterung der Suchergebnisse verwendeten Algorithmen als Geschäftsgeheimnisse gehütet, sodass dem Nutzer verborgen bleibt, nach welchen Kriterien vorgeblicher Relevanz die „allmächtige" Instanz ihm Informationen präsentiert.[4] An die Stelle des erhofften Pluralismus ist ein beklemmendes Manipulationspotential getreten. Längst befinden wir uns in der „Filter Bubble"[5], die daraus entstand, dass Suchmaschinen aber auch Streamingdienste, E-Commerce-Plattformen etc. auf der Grundlage über den jeweiligen Nutzer gesammelter Informationen, etwa seines Standorts, seines Suchverlaufs, seines Klickverhaltens, der bislang gehörten Musik, gesehener Videos, gelesener Nachrichten und gekaufter Waren die anzuzeigende Information auswählen und – in für ihn intransparenter Weise – alles ausblenden, was nicht der vermuteten Haltung des Empfängers entspricht. Dieser brät gewissermaßen „im eigenen Saft" und kann es sich im Extremfall unbehelligt von verstörenden Beiträgen der als „Lügenpresse" verunglimpften Qualitätsmedien in der Hängematte des eigenen Weltbildes bequem machen.

2. Übertragung rivalisierend zu konsumierender Güter

Dass selbst gemeinfreie Information meist nicht P2P (Peer-to-Peer, also direkt von Rechner zu Rechner), sondern datenträchtig über Intermediäre übertragen wird, ist auf deren Kampf um Marktanteile und die verführerische Macht der Bequemlichkeit, der wir alle früher oder später erliegen, zurückzuführen. Dagegen waren bislang Transaktionen im Zusammenhang mit Sachen im Sinne des § 90 BGB im E-Commerce von vornherein nur unter Inanspruchnahme vertrauenswürdiger Dritter denkbar. Solange das „Beamen" nicht erfunden ist, muss zumindest die körperliche Übergabe ohnehin in der realen Welt, also außerhalb des Netzes stattfinden. Die Bezahlung kann zwar als Überweisung im bargeldlosen Zahlungsverkehr und somit auch auf elektronischem Weg erfolgen, beruht dann aber auf einer geschäftsbesorgungsrechtlichen Weisung des Schuldners an sein kontoführendes Kreditinstitut, was bei der Nutzung institutsübergreifender Gironetze entsprechendes Vertrauen in mehrere Geldinstitute voraussetzt. Nicht wesentlich anders verhält es sich beim Einsatz von Kredit-, Debit- oder Prepaid-Karten oder bei der Nutzung eines Online-Bezahldienstes wie Pay Pal. Für Kreditkarten- und Pay-Pal-Transaktionen werden dem empfangenden Geschäftskunden meist 1,5 bis 5 Prozent Disagio zuzüglich einer Transaktionsgebühr in der Höhe von 0,10 bis 0,25 Euro angelastet. Hat der Empfänger kein Bankkonto, sodass er auf Barauszahlung durch einen MTO (Money Transfer Operator) angewiesen ist, wird es unter Umständen richtig teuer, da dann – je nach Ausgangsland – in der Regel 5 bis 10 Euro Transaktionsgebühr und ein vom Bestimmungsland, von der Währung sowie vom Zeitpunkt und der gewählten Dauer der Transaktion abhängiger Prozentsatz des Überweisungsbetrages fällig werden, die gemeinsam mit dem Spread des verrechneten zum marktüblichen Wechselkurs den beim Empfänger eintreffenden Betrag durchaus um 20 Prozent vermindern können[6]. Die durchschnittlichen Kosten für weltweite Überweisungen betrugen im ersten Quartal 2016 stattliche 7,37 Prozent, wobei der internationale Geldtransfer unter Zuhilfenahme von Geschäftsbanken mit durchschnittlich 11,09 Prozent Kosten sogar am teuersten war[7].

Besondere Schwierigkeiten bereitet schließlich der Online-Handel mit immateriellen Gütern. Ihrer „Natur" nach sind diese Informationsgüter, weisen daher die Merkmale öffentlicher Güter auf, sind also nicht-rivalisierend und – wenn sie in digitaler Form vorliegen – ubiquitär konsumierbar.[8] Um ein durch Unterproduktion entstehendes Marktversagen zu vermeiden, ordnet die Rechtsordnung mit den Immaterialgüterrechten bestimmte Informationsgüter exklusiv deren Produzenten – etwa den Urhebern oder Erfindern – zu und schafft auf diese Weise künstliche Knappheit sowie damit handelbare Rechtsobjekte. Dies ändert aber nichts daran, dass digital verfügbare Werke wie Fotos, Videos oder Musik massenhaft über das Netz verbreitet werden *können*. Dass dies außer dem Rechteinhaber bloß jedermann verboten ist, führt zu einer vor allem von jugendlichen „Digital Natives" kaum als gerecht und sinnvoll empfundenen Situation, dass sie in der virtuellen Welt andauernd von anregendem Material umgeben sind, das perfekt für die Verbreitung, für Mashups und Remixes geeignet wäre, für sie aber „tabu" ist.[9]

Doch auch im professionelleren Umfeld fällt der Umgang mit digitalisierten Immaterialgütern nicht leicht. Dass es mangels tatsächlicher Beherrschbarkeit keinen Besitz und daher auch keinen Gutglaubenserwerb an urheberrechtlichen Befugnissen gibt,[10] stellt einen kaum kalkulierbaren Risikofaktor dar. Nach wie vor verwenden sonst recht smarte Software-Hersteller archaisch anmutende Lizenzurkunden mit Hologrammen und ähnlichen Sicherheitsmerkmalen, die Wertpapieren nachempfunden sind. Für echte Effekten ist die anachronistische Verkörperung freilich längst überholt: Bereits Anfang der 1970er-Jahre wurde der Effektengiroverkehr eingeführt, ohne den im Massenverkehr ein ordentlich funktionierendes Effektenwesen gar nicht mehr denkbar wäre. Transaktionen über dematerialisierte Wertrechte erfolgen hier – wie die Giroüberweisung von Geld – durch Umbuchungen unter Einschaltung von als „Zentralverwahrer" bezeichneten Clearing-Stellen. Dass ausgerechnet Hightech-Unternehmen wie Software-Produzenten bislang nichts dergleichen auf den Weg brachten, liegt daran, dass sie kein Interesse an einer Zweitverwertung von Software-Lizenzen haben. Selbst dass die Erschöpfung des Verbreitungsrechts am dadurch entstehenden Werkstück durch den Download von Software ausgelöst wird, wollten sie daher so lange nicht wahrhaben, bis sie der EuGH[11] eines Besseren belehrte.

Die Musikindustrie wiederum hatte zunächst die Zeichen der Zeit einfach übersehen und – mit dem Kopf fest im Sand – der wachsenden Internet-Community keine passenden Online-Angebote unterbreitet. Als die Umsatzzahlen von Tonträgern dramatisch einbrachen, wurde dies den „Raubkopierern" angelastet, um schließlich begehrliche Finger nach den ei-

4 Vgl. *Stark/Dörr/Aufenanger* (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Medienkonvergenz 10 (2014), passim.

5 Grundlegend und diesen Begriff prägend *Pariser*, The Filter Bubble: What the Internet Is Hiding from You (2011), passim.

6 Vgl. den Aufruf „Western Union: Senken Sie die horrenden Gebühren!" von AVAAZ – Die Welt in Aktion, http://kurzelinks.de/AnwBl-2016-8u9-2.

7 *The World Bank*, Remittance Prices Worldwide, Issue n. 17, March 2016, http://kurzelinks.de/AnwBl-2016-8u9-3.

8 Vgl. *Linde*, Ökonomische Besonderheiten von Informationsgütern, in: *Linde/Keuper/Neumann* (Hrsg.), Wissens- und Informationsmanagement (2009) S. 291 (296 ff.).

9 Vgl. *Lessig*, Free Culture – How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity (2004), S. 44 ff., http://kurzelinks.de/AnwBl-2016-8u9-4.

10 Vgl. *Schulze* in: *Dreier/Schulze* (Hrsg.), Urheberrechtsgesetz, 5. Aufl. (2015), § 44 Rn. 6.

11 Urteil vom 3.7.2012, Rs. C-128/11, EU:C:2012:407 (UsedSoft).

gentlich den Kreativen als Ausgleich für die Schrankenbestimmung der Vervielfältigung zum privaten Gebrauch zustehenden Vergütungsansprüchen auszustrecken. Dass schließlich Musik-Streamingdienste wie Napster, Spotify, Deezer, Amazon Prime Music und Apple Music anstelle der Labels die Vermarktung von Musik im Internet übernahmen, änderte freilich wenig an der meist prekären Situation der Komponisten und ausübenden Künstler. Bei gleichzeitigem Wegfall des Tonträgerverkaufs beziehen sie für das Streaming ihrer Werke meist nur minimale Tantiemen, sodass der Live-Sektor gegenwärtig – wie in früheren Jahrhunderten – für viele Musiker der einzige Bereich ist, der ihnen noch nennenswerte Einkünfte ermöglicht.[12]

3. Zwischenergebnis: Zentralistische Struktur des herkömmlichen E-Commerce

Das Internet hat uns zwar eine dramatische Reduktion von Informationssuchkosten beschert, die Erwartungen hinsichtlich seiner pluralismusfördernden Wirkung aber ebenso gründlich enttäuscht, wie es das Versprechen vielfältiger Geschäftsmöglichkeiten für flexible Kleinunternehmer in einer vernetzten Welt nicht einlösen konnte. Sowohl die Informationsvermittlung als auch und erst recht der E-Commerce von Gütern und Dienstleistungen sowie der Transfer von Geld liegen fest in der Hand weniger globaler Player, die als vertrauenswürdige Dritte finanziell kräftig an allen Transaktionen mitnaschen und so die Verteilungsgerechtigkeit weiter erodieren.

Durch die Verarbeitung und Speicherung sowohl der Stammdaten von Kunden als auch der von ihnen durchgeführten Transaktionen wurden sie überdies zu „Datenkraken", welche ihre Kunden nicht nur besser kennen, als diesen lieb sein kann, sondern durch die gefährliche Akkumulation von Benutzerprofilen als „Honeypots" fungieren, welche auf Angreifer[13] eine ebenso verlockende Wirkung entfalten wie Honigseim auf Bären. Beim Cloud Computing schließlich vertrauen wir überdies noch die von uns gespeicherten Dateien und – falls diese nicht verschlüsselt sind – ihre Inhalte Dienstleistern an, deren Vertrauenswürdigkeit wir nicht prüfen können und – zur Wahrung unseres Seelenfriedens – auch gar nicht prüfen wollen.

III. Das „Gottesprotokoll" als theoretischer Lösungsansatz

Zur Lösung der unbefriedigenden Situation, in der wir uns häufig genötigt sehen, fehlbaren Menschen und den von ihnen betriebenen Systemen als „Trusted Third Party" wie einer Gottheit zu vertrauen, schlug der Jurist, Informatiker und Kryptograf *Nick Szabo* bereits 1999 – und damit bemerkenswerterweise noch vor dem Platzen der Dotcom-Blase – das von ihm so bezeichnete „Gottesprotokoll" vor.[14] Dieses sollte es jedermann ermöglichen, einer denkbar vertrauenswürdigen Instanz Input zu übermitteln, den diese „Gottheit" unter Wahrung vollständiger Diskretion auswerten und die Ergebnisse mitteilen würde. Damit wäre sichergestellt, dass niemand über den Input der jeweils anderen Partei mehr erführe, als sich aus dem Output der Transaktion und dem eigenen Input schließen ließe. Unter Berufung auf Arbeiten von Spezialisten für Netzwerk-Sicherheit zeigte *Szabo*, wie dies theoretisch durch den Einsatz „virtueller Maschinen" durch zwei oder beliebig viele Personen möglich sei, und sprach in diesem Zusammenhang von „smart contract negotiations".

Schon ein Jahr zuvor, nämlich 1998, hatte *Szabo* auf einer Mailinglist seine Ideen für „Bit Gold" skizziert,[15] um damit Geld von der Notwendigkeit vertrauenswürdiger Dritter und zugleich von Gefahren durch Fälschung, Diebstahl und insbesondere Inflation zu befreien. Auf der Basis einer „Proof-of-Work"-Funktion sollten als Geld fungierende Bits in einem extrem rechenaufwendigen und damit fälschungssicheren Verfahren generiert werden. Fast zur gleichen Zeit erschien ein Beitrag[16] des Kryptografen und Microsoft-Mitarbeiters *Wei Dai*, in welchem dieser die Existenz von Geld sowie die Möglichkeit, Verträge durchzusetzen, als essentiell für jede Gesellschaft bezeichnete und stark an die Vorschläge von *Szabo* erinnernde Wege beschrieb, wie beides auf der Grundlage kryptografischer Methoden unabhängig von Staaten realisiert und dadurch die von ihm so bezeichnete „Krypto-Anarchie" erreicht werden könnte.

IV. Theoretischer Durchbruch und „Proof of Concept" durch die Bitcoin-Blockchain

1. Die bahnbrechende Publikation 2008

Ein ganzes Jahrzehnt sollte vergehen, bis *Szabos* und namentlich *Dais* Skizzen wieder aufgegriffen wurden. Zum Teil mag dies daran gelegen haben, dass ihre Realisierung vor dem Millennium in technischer Hinsicht schwierig bis kaum lösbar erscheinen musste. Der Hauptgrund dafür dürfte aber darin zu sehen sein, dass damals die Zeit für die damit erreichbaren Ziele noch nicht reif war, sodass die brillanten Überlegungen allenthalben als schlechte Ideen abgetan wurden.[17]

Dann jedoch erschien – in der Wahrnehmung der meisten wie aus dem Nichts – am 31. Oktober 2008 eine geniale Publikation: *Satoshi Nakamoto*[18], „Bitcoin: A Peer-to-Peer Electronic Cash System"[19]. Wohl nicht zufällig zum Höhepunkt der globalen Banken- und Finanzkrise, durch welche das Vertrauen in Finanzinstitutionen gründlich erschüttert worden war, entwarf sie das erste voll funktionstüchtige, weder von Staaten noch von Finanzinstitutionen oder sonstigen „vertrauenswürdigen Dritten" abhängige oder beeinflussbare

12 Vgl. *Hemming*, Ökonomische Analyse: Musikindustrie und Urheberrecht, in: *ders*., Methoden der Erforschung populärer Musik (2016) S. 410.

13 Im Frühjahr 2016 verkaufte ein unter dem Pseudonym „peace_of_mind" auftretender Hacker 800 Millionen Benutzernamen und Passwort-Hashes von Webseiten wie LinkedIn, Tumblr, VKontakte und Twitter und kündigte an, eine weitere Milliarde folgen zu lassen (vgl. *Scherschel*, Peace: Wer ist der Hacker, der 800 Millionen Passwörter veröffentlicht hat?, Heise online vom 11.06.2016, http://kurzelinks.de/AnwBl-2016-8u9-5.

14 *Szabo*, The God Protocols – Trustworthy computations with untrusted parties, ITAudit Vol. 2/1999, http://kurzelinks.de/AnwBl-2016-8u9-6.

15 Heute sind diese Ideen nur mehr in dem Eintrag *Szabo*, Bit gold, December 29, 2005, auf dem Blogspot „Unenumerated", http://kurzelinks.de/AnwBl-2016-8u9-7, nachzulesen.

16 *Wai Dai*, b-money, Nov, 1, 1998, http://kurzelinks.de/AnwBl-2016-8u9-8.

17 Vgl. *Szabo*, Bitcoin, what took ye so long?, May 28, 2011, auf dem Blogspot „Unenumerated", http://kurzelinks.de/AnwBl-2016-8u9-9.

18 Ob der Beitrag tatsächlich von einem Autor dieses Namens stammt, ob es sich dabei um ein Pseudonym einer Person oder eines Autorenkollektivs handelt, oder ob – was dieser stets bestritten hat – *Nick Szabo* direkt hinter Bitcoin steht, ist bislang ungeklärt, zumal das Phantom im Frühjahr 2011 mit dem Ausspruch, es habe sich „anderen Dingen zugewandt", von der digitalen Bühne Abschied nahm und seither nichts mehr von sich hören ließ (vgl. http://kurzelinks.de/AnwBl-2016-8u9-10).

19 Im HTML-„Original": http://kurzelinks.de/AnwBl-2016-8u9-11, als PDF-Version: http://kurzelinks.de/AnwBl-2016-8u9-12.

Währungssystem. Es beruht vollständig auf Methoden der Informatik und vor allem der Kryptografie, die schon Jahre oder Jahrzehnte zuvor entwickelt und veröffentlicht worden waren, verbindet diese aber in beeindruckender Weise zur Lösung der davor einem sicheren digitalen Zahlungsmittel entgegenstehenden Probleme. Auf dem Konzept des „Proof-of-Work" beruhend macht es zentrale Intermediäre für die Verhinderung des „Double Spending" überflüssig und ermöglicht auf einem P2P-Netzwerk direkte Transaktionen pseudonymer Parteien. Als Anreiz dafür, den ressourcenintensiven „Proof-of-Work" zu erbringen, schüttet es in regelmäßigen Abständen an den jeweils erfolgreichen „Miner" einen exakt vorgegebenen Betrag der Währung Bitcoin (BTC) aus und bewirkt damit zugleich die Geldschöpfung. Wer mit etwas technischem Vorverständnis (hinsichtlich asymmetrischer Signaturen, Hash-Verfahren etc.) *Nakamotos* Beitrag liest, dem werden möglicherweise ähnliche Gedanken wie dem Webbrowser-Pionier und Internet-Investor *Marc Andreesen*[20] durch den Kopf gehen:

> „Oh my god, this is it. This is the big breakthrough. This is the thing we've been waiting for. He solved all the problems. Whoever he is should get the Nobel prize – he's a genius. This is the thing! This is the distributed trust network that the Internet always needed and never had."

2. Funktionsweise der Bitcoin-Blockchain

Die Bitcoin-Blockchain beruht auf einem dezentralisierten, sämtliche Transaktionen erfassenden Verzeichnis, das in einem P2P-Netzwerk von allen vollständigen Netzknoten vollumfänglich gespeichert und laufend aktualisiert wird. Zur Lösung des Problems, dass digitales Geld – wie alle digitalen Daten – leicht kopiert und dadurch doppelt oder mehrfach ausgegeben werden könnte, werden die Transaktionen in exakter chronologischer Reihenfolge erfasst. Die wiederholte Ausgabe ein und desselben Geldbetrags durch denselben Verfügungsberechtigten ist ungültig und daher wirkungslos. Eine Transaktion kann man sich als Buchung im verteilten Verzeichnis vorstellen. Der Verfügungsberechtigte versieht den Hash-Wert der aus der vorangehenden (ihn berechtigenden) Transaktion und der Bitcoin-Adresse des Empfängers (ein aus dessen Public Key abgeleiteter 160-Bit-Hash-Wert) bestehenden Daten mit einer unter Verwendung seines Private Keys erzeugten digitalen Signatur. Die Gültigkeit der so gebildeten Transaktionskette kann anhand der Public Keys der jeweiligen Absender überprüft werden.

Herzstück des Systems ist der Ersatz von sozialem Vertrauen oder Systemvertrauen durch ein Protokoll[21], das es unmöglich oder zumindest völlig unvernünftig macht, eine vergangene Transaktion zu korrigieren, um in betrügerischer Weise den transferierten Betrag nochmals auszugeben. Das wird durch eine Art Lotterie bewerkstelligt, an der sich sog. „Miners" beteiligen. Diese erhalten einen bestimmten Betrag (seit dem jüngsten Reward Halving am 9. Juli 2016 sind es 12,5 BTC) als Belohnung, wenn sie als jeweils erster einen „Block" bilden. Ein solcher Block besteht aus dem Hash-Wert aus dem vorangehenden Block (dadurch werden die Blöcke verkettet, wodurch die „Blockchain" entsteht), den inzwischen über das P2P-Netzwerk verlautbarten neuen Transaktionen und einem sog. „Nonce". Dieses Nonce dient als Lückenfüller bei der Lösung der extrem ressourcenaufwändigen Rechenaufgabe, einen Hash-Wert zu bilden, dessen erste n Stellen ausschließlich aus Nullen bestehen.

Dazu muss man wissen, dass eine Hash-Funktion unabhängig von der beliebig großen Eingabe (etwa einer Zahl, einer Textdatei oder eines Videos) stets einen Wert in vorbestimmter Länge, im Fall der Bitcoin-Blockchain und der dafür verwendeten Hash-Funktion SHA 2 sind es 256 Bit, ergibt. Dieser Wert fungiert als digitaler Fingerabdruck der Eingabedaten. Die Hash-Funktion ist eine mathematische „Einbahnfunktion": Für eine gegebene Datei kann mit geringem Rechenaufwand der Hash-Wert ermittelt werden. Dagegen ist es mit aller verfügbaren Rechenkapazität unmöglich, zu einem gegebenen Hash-Wert in absehbarer Zeit eine weitere Datei (insbesondere durch Verfälschen der ursprünglichen Datei) zu finden, für welche die Hash-Funktion denselben Hash-Wert ermittelt. Die Aufgabe, durch Probieren von Milliarden und aber Milliarden Nonces gemeinsam mit den übrigen Blockdaten eine Eingabedatei zu finden, die einen Hash-Wert ergibt, welcher zumindest die geforderte Anzahl von führenden Nullen aufweist, ist zwar extrem rechenintensiv, aber machbar.

Dafür, dass mit zunehmender Rechenkapazität der Miners auf der Blockchain nicht immer rascher neue Blöcke gebildet und damit auch Bitcoins generiert werden, sorgt die sog. „Difficulty". Diese bestimmt die Anzahl der geforderten führenden Nullen des Hash-Werts und wird vom System alle 2016 Blöcke (was rund zwei Wochen entspricht) automatisch so gewählt, dass ungefähr alle zehn Minuten ein Block gefunden wird. Die „Hashing-Power" eines Miners bestimmt seine Aussicht, als Erster den nächsten Block zu finden. Da die Hash-Funktion ein Pseudo-Zufallszahlengenerator ist, dessen Ausgabe sich schon aufgrund des Austausches eines einzigen Zeichens der Eingabedatei in nicht vorhersehbarer Weise völlig verändert, hängt der Erfolg auch vom Zufall ab. Die Chance in der Bitcoin-„Lotterie" steigt aber proportional mit der Zahl der Nonces, die pro Sekunde gemeinsam mit dem „sinnvollen" Inhalt des zu bildenden Blocks gehashed werden können. Während im Jahr 2009 noch mit PCs, vor allem mit deren schnellen Grafikkarten, erfolgreiches Mining möglich war, gelingt dies heute nur mehr hochspezialisierten Unternehmen und sog. Mining-Pools, die mit Abertausenden ASICs (Application-specific Integrated Circuit – Spezialprozessor, der für die Lösung einer bestimmten Klasse von Aufgaben maßgeschneidert und daher hochperformant ist) und enormem Energieaufwand diesem Geschäft nachgehen. Mit knapp 20 Trilliarden FLOPS (Floating Point Operations Per Second) war die gesamte Hashrate auf der Bitcoin-Blockchain im Juni 2016 etwa so gewaltig, dass man dafür mehr als 200.000 Exemplare des stärksten Supercomputers der Welt Sunway TaihuLight benötigt hätte, der immerhin über fast 11 Millionen Prozessorkerne verfügt.

20 In einem Interview, das er der Washington Post gab und das dort am 21.04.2014 unter der Überschrift „Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today" erschien, http://kurzelinks.de/AnwBl-2016-8u9-13.

21 Damit legt man in der Informatik fest, in welcher Reihenfolge und wodurch oder durch wen Vorgänge veranlasst werden.

Diesen enormen Aufwand betreiben die Miners, um in der etwa alle zehn Minuten ausgespielten „Lotterie“ möglichst oft die Belohnung einzuheimsen. Zugleich machen sie damit aber auch die Bitcoin-Blockchain fälschungssicher. Sollte ein Angreifer eine seiner früheren Transaktionen (und nur eine solche kann das Angriffsziel sein, da er die für andere Transaktionen erforderlichen Private Keys nicht kennt) ungeschehen machen wollen, um den Betrag nochmals ausgeben zu können, müsste er nicht nur den betreffenden Block, sondern auch alle folgenden Blöcke, die ja durch die Hash-Werte miteinander verkettet sind, neu bilden und dabei jeweils nochmals mit enormem Aufwand ein passendes Nonce finden. Schließlich hätte er noch alle anderen Miners beim Finden des aktuellen Blocks zu überholen, um diesen an die Blockchain anzufügen, da stets die längste Blockchain, in der alle Hash-Werte korrekt sind, vom P2P-Netzwerk als die „richtige“ akzeptiert wird. Für den äußerst unwahrscheinlichen Fall, dass jemals ein Miner oder ein Mining-Pool über einen derart großen Anteil der gesamten Hashing-Power verfügen sollte, wüsste er damit Besseres zu tun: Er würde sich an der „Lotterie“ beteiligen, also versuchen, möglichst oft die Belohnung von derzeit 12,5 BTC pro gefundenen Block und überdies die „Transaktionsgebühren“ einzunehmen, welche den Transaktionen freiwillig hinzugefügt werden können, damit diese von den Miners mit hoher Priorität in den nächsten Block eingebunden und damit möglichst rasch „bestätigt“ werden.

V. Auswirkungen auf die Wirtschaftspraxis

Die Leserin oder der Leser – vertraut mit der Internetwelt des Jahres 2016 – wird sich vielleicht fragen, welchen praktischen Nutzen der mit beachtlichem Energieverbrauch einhergehende kryptografische Aufwand stiftet. Die lapidare Antwort könnte lauten, dass der Menschheit dadurch zum ersten Mal in ihrer Geschichte ein öffentlich einsehbares Verzeichnis zur Verfügung steht, das absolut fälschungssicher und von einer zentralen, vertrauenswürdigen Instanz unabhängig ist. Derzeit lassen sich die Konsequenzen dieses Umstands nur in ihren Konturen erahnen.

1. Bitcoin als virtuelle Währung

Dabei ist Bitcoin nur eine von unzähligen denkbaren Anwendungen, gewissermaßen bloß der „Proof of Concept“, also der Beweis, dass die Blockchain funktioniert. Dieser wurde aber mit der en passant bewirkten Schöpfung des ersten ohne Staat und ohne Finanzinstitutionen auskommenden Währungssystems beeindruckend geführt. Dass dieses früh von Kriminellen für ihre dunklen Machenschaften entdeckt wurde, bestätigt letztlich seine Wertschätzung als digitales Geld. Freilich hat dieser Umstand Bitcoin zunächst eine ebenso fragwürdige Reputation beschert wie die – vor allem im Jahr 2013 – extreme Volatilität. Spätestens seit 2015 erfreuen sich Bitcoin und das der Kryptowährung zugrundeliegende Protokoll der Blockchain aber eines stetig zunehmenden Interesses bei Finanzinstitutionen, Handelsunternehmen, Startups und nicht gerade risikoaversen Anlegern. Mit einem Kursgewinn von mehr als 50 Prozent im zweiten Quartal 2016 war Bitcoin zweifellos die performanteste Währung der Welt.

Um selbst BTC-Zahlungen entgegennehmen und danach auch durchführen zu können, bedarf es lediglich einer als „Wallet“ bezeichneten Software, die es in vielfältigen Ausführungen für Smartphone- und Tablet-Betriebssysteme sowie für Desktop-PCs gibt. Für jede Bitcoin-Adresse generiert diese „Bitcoin-Geldbörse“ ein Schlüsselpaar. Sie enthält daher nicht wirklich BTC, sondern kryptografische Schlüssel, sodass man sich ein Wallet eher als digitalen Schlüsselbund vorstellen sollte. Die als 160-Bit-Hash-Wert aus einem Public Key abgeleitete Bitcoin-Adresse gibt man jenem (einem Schuldner oder einem Bitcoin-Trader) bekannt, der einem BTC anweisen will oder soll. Über an eine Bitcoin-Adresse „gesandte“ BTC-Beträge kann man mit dem dazugehörigen Private Key verfügen. Dieser muss daher streng geheim gehalten werden. Der Umgang mit den relativ langen Bitcoin-Adressen und Private Keys wird durch deren Darstellung als QR-Codes sehr erleichtert. So zeigt oder sendet man dem Anweisenden einen die Bitcoin-Adresse sowie den geforderten Betrag in BTC enthaltenden QR-Code, der von dessen Wallet-Software gelesen und interpretiert werden kann. Druckt man QR-Codes eines Schlüsselpaars aus, erhält man damit ein „Paper-Wallet“, das insbesondere als Backup oder von vornherein für die sichere Verwahrung eines mit einem größeren Betrag verbundenen Private Keys verwendet werden kann.

Durch die Möglichkeit, kostenlose oder mit minimalen freiwilligen „Gebühren“ verbundene monetäre Transaktionen ohne Zwischenschaltung von Finanzinstitutionen durchzuführen, wird der BYOB-Ansatz (Be Your Own Bank) bereits realisiert. Das ist selbst für die G20-Staaten ein interessanter Ansatz, finanzielle Inklusion und damit nicht zuletzt mehr Stabilität des internationalen Finanzsystems[22] zu erreichen. In den als „underbanked“ geltenden unterentwickelten Regionen der Erde eröffnet sich damit aber der Mehrheit der Bevölkerung nicht weniger als die Möglichkeit der Teilhabe an der globalisierten Wirtschaft.

2. Bitcoin als Verfügungsmittel über Assets aller Art

Das Potenzial der Bitcoin-Blockchain geht jedoch weit über die Bereitstellung einer Infrastruktur für dezentralisierte Zahlungsströme hinaus. Sie ist vielmehr für alle Transaktionen, bei denen bislang die Gefahr des Double Spending nur durch die Inanspruchnahme kostspieliger und datenträchtiger Dienstleistungen zentraler vertrauenswürdiger Dritter gebannt werden konnte, eine attraktive Alternative.

Die Bitcoin-Blockchain stellt nämlich eine einfache Skriptsprache bereit, mit welcher sich – in engen Grenzen – von einem Absender Bedingungen festlegen lassen, unter denen der Empfänger in der Lage sein soll, über die empfangenen Bitcoins zu verfügen. So können statt nur eines Private Keys zwei davon („Vieraugenprinzip“) oder etwa auch drei von fünf Private Keys für eine gültige Transaktion vorgeschrieben werden. Diese Skriptsprache bietet aber auch die Möglichkeit, einer Bitcoin-Adresse eine bestimmte Anzahl an Gütern zuzuweisen („Issuance“). Mit einer dafür ausgelegten Wallet-App lassen sich dann Teilmengen dieser Assets auf andere Bitcoin-Adressen übertragen („Transfer“)[23].

22 Für die Interdependenz der beiden Ziele vgl. *Monnerie*, Finanzielle Inklusion und Finanzstabilität – zwei ähnliche Problematiken?, Die Volkswirtschaft – Plattform für Wirtschaftspolitik, 11.12. 2014, http://kurzelinks.de/AnwBl-2016-8u9-14.

23 Github Colored-Coins-Protocol-Wiki, http://kurzelinks.de/AnwBl-2016-8u9-15.

Ganz ähnlich, wenn auch etwas archaischer, funktionierten sog. „Colored Coins". Dabei wurden Satoshis, das ist die Bezeichnung für ein Hundertmillionstel BTC und derzeit die kleinste BTC-Untereinheit, mit einem Attribut versehen und damit – metaphorisch gesehen – „eingefärbt", was sie vereinbarungsgemäß zu Repräsentanten bestimmter Assets (etwa einer Software-Lizenz, eines Diamanten, eines Autos oder eines Grundstücks samt darauf befindlichem Haus) machte und dieses damit dem jeweils über den gefärbten Satoshi Verfügungsbefugten zuordnete. Aus historischen Gründen wird bei der Verwendung der Bitcoin-Blockchain als Plattform für Verfügungen über andere Assets als BTC immer noch von „Colored Coins" gesprochen, auch wenn die Assets inzwischen nicht mehr mit Satoshis verknüpft sind. Anders als Bitcoins werden Colored Coins nicht durch den Mining-Prozess erzeugt, sondern vom Issuer mit dem Versprechen aufgelegt, sie gegen die dadurch repräsentierten Assets einzulösen. Daher können sich Nachfrager in diesem Fall nicht bloß auf die kryptografisch abgesicherte Blockchain verlassen, sondern müssen dem Issuer vertrauen. Die Bereitstellung vertrauensbildender Informationen wird durch das Colored-Coin-Protokoll unterstützt, das für die „Asset Verification" eine Verlinkung mit einem Twitter-, Facebook- oder Github-Account des Issuers und alternativ einen Link auf eine Datei auf einem SSL-gesicherten Server anbietet.

Colored Coins erweitern das Anwendungsspektrum der Bitcoin-Blockchain ungemein. So eignen sie sich in idealer Weise dafür, Nutzungsrechte an immateriellen Gütern eindeutig einem Befugten zuzuordnen und weitere Verfügungen darüber in der Absatzkette vornehmen zu lassen. Künftig könnte zum Beispiel Software bei jedem Programmstart prüfen, ob der Anwender auf der Blockchain über ein ihn hierzu berechtigendes Token in Gestalt einer Colored Coin verfügt. Aber auch die Übertragung körperlicher Gegenstände, ja selbst die Ausgabe von Berechtigungsnachweisen für Dienstleistungen (vom Zugang zu digitalen Inhalten über den Kinoeintritt bis zur Miete eines Hotelzimmers) lässt sich auf diese Weise durch den Transfer damit verknüpfter Colored Cloins digital und mit der Sicherheit der Blockchain abwickeln. Dies stellt selbst die Notwendigkeit bislang als unverzichtbar erachteter staatlicher Infrastruktur wie jener des Grundbuchs oder des Handelsregisters in Frage und öffnet gemeinsam mit Blockchain-gestützter Vereinfachung der Steuereinhebung Spielraum für eine Verwaltungsreform, die eine Konzentration auf das „Kerngeschäft" des Staates mit der Aussicht auf eine noch bürgernähere Administration gestattet. Selbst anonyme Wahlen, deren exaktes Ergebnis im Augenblick des Wahlschlusses feststeht, sind mit Colored Coins organisierbar.

Durch die Möglichkeit, in die Blockchain – in begrenztem Umfang – auch Daten zu schreiben, lässt sich sogar ein sicheres Identitäts-Management implementieren, bei welchem der Benutzer entscheidet, wer beziehungsweise welcher Dienst auf welchen Teil seiner Identitätsdaten zugreifen kann.[24] Dies erlaubt die Nutzung mehrerer, dem jeweiligen Kontext angepasster „Identitäten", löst damit in datensparsamster Weise Authentifizierungsaufgaben, befreit uns von der gleichermaßen lästigen wie fehleranfälligen Verwaltung Dutzender Benutzerkennungen samt den dazugehörigen Passwörtern und könnte schließlich – unter der Voraussetzung der behördlichen Bestätigung entsprechender Teile der Identitätsdaten – auch die Funktion digitaler amtlicher Lichtbildausweise übernehmen.

3. Smart Contracts

Nicht zuletzt durch die Nutzung seiner Skriptsprache ist die Bitcoin-Blockchain auch für deutlich komplexere Transaktionen als die bedingungslose Übertragung von BTC oder anderer Assets einsetzbar. So lassen sich durch sog. „Multisig"-Transaktionen nicht nur Gesamtvertretungen im Sinne des Vier- oder Mehraugenprinzips, sondern auch Treuhand- und Schlichtungskonstruktionen abbilden. Eine „2-of-3"-Multisig-Transaktion etwa kann die Vertragserfüllung unterstützen: Der Erwerber transferiert den vereinbarten Kaufpreis an eine Bitcoin-Adresse, die wiederum auf der Basis dreier anderer Adressen gebildet wird, wovon die erste ihm, die zweite dem Veräußerer und die dritte einem unabhängigen Streitschlichter zugeordnet ist. Wird die Ware ordnungsgemäß geliefert (oder ein Werk wie vereinbart hergestellt), signieren die beiden Vertragsparteien, um den Betrag der alleinigen Verfügungsbefugnis des Veräußerers zu unterstellen. Tritt dagegen eine Leistungsstörung auf, kann der Vertrag dadurch einhellig aufgehoben und rückabgewickelt werden, dass beide eine Rücküberweisung an den Erwerber unterzeichnen. Gibt es aber Streit, entscheidet der Schlichter mit seiner Signatur, wer den Betrag in seine alleinige Verfügungsmacht bringen kann.

Will man einer Transaktion noch wesentlich komplexere Regeln zugrunde legen, stößt man damit bald an die Grenzen der bewusst schlicht gehaltenen Skriptsprache der Bitcoin-Blockchain, die zum Beispiel keine Programmschleifen kennt. Daher etablierte sich eine Reihe von Projekten, welche die als Schwächen angesehenen Restriktionen (darunter die mangelnde Skalierbarkeit, die bis zu zehn Minuten dauernde Wartezeit bis zur Bestätigung und damit Absicherung einer Transaktion, der energieverzehrende Mining-Prozess und eben die eingeschränkte Programmierbarkeit) der größten und stabilsten existierenden Blockchain überwinden wollen. Das prominenteste unter ihnen ist wohl „Ethereum". Die von dem damals 19-jährigen *Vitalik Buterin* beschriebene Plattform[25] beruht zwar ebenfalls auf dem von *Satoshi Nakamoto* entwickelten Blockchain-Protokoll, erweitert dieses aber um eine Turing-vollständige (also Programme beliebiger Komplexität zulassende) Programmierumgebung und ist damit für Smart Contracts prädestiniert. Mit 18 Mio. US-Dollar aus einer Bitcoin-Crowd-Funding-Kampagne wurde die Plattform von der in Zug in der Schweiz ansässigen Ethereum Foundation entwickelt. Dass die Marktkapitalisierung der auf der Ethereum-Blockchain entstehenden Kryptowährung Ether (ETH), die hauptsächlich als Zahlungsmittel für den Ressourcenverzehr durch Smart Contracts und damit quasi als deren „Treibstoff" dient, im März 2016 und damit kaum eineinhalb Jahre später bereits die Marke von 1 Mrd. USD hinter sich ließ,[26] zeigt, welche Erwartungen in Smart Contracts gesetzt werden.

24 Vgl. *Zyskind/Nathan/Pentland*, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE CS Security and Privacy Workshops, 181 ff., http://kurzelinks.de/AnwBl-2016-8u9-16.

25 *Buterin*, Ethereum White Paper (2013), http://kurzelinks.de/AnwBl-2016-8u9-17.

26 Für Details s. Crypto-Currency Market Capitalizations, http://kurzelinks.de/AnwBl-2016-8u9-18.

Wie von *Nick Szabo*[27] theoretisch beschrieben, wird der Code von Smart Contracts auf einer virtuellen Maschine, im konkreten Fall der EVM (Ethereum Virtual Machine), ausgeführt. Diese wiederum läuft in abgestimmter und damit völlig gleicher Weise mit sämtlichen Smart Contracts auf allen das Ethereum-P2P-Netzwerk bildenden Knoten. Die bisweilen als „Weltcomputer" bezeichnete EVM ist daher die denkbar ineffizienteste Art und Weise, IT zu betreiben. Dafür macht die auf der Blockchain erzielte und durch sie abgesicherte Übereinstimmung über den Zustand der EVM diese fehlertolerant und ausfallsicher sowie die auf ihr gespeicherten Daten unveränderlich und damit zugleich absolut zensurresistent.

Ein Smart Contract ist Programmcode, der auf einer Blockchain läuft und dort Daten auf der Grundlage anderer (externer) Daten verändert. Im Wesentlichen geht es darum, dass digitale Assets oder Repräsentationen körperlicher Gegenstände zwischen zwei oder mehr Parteien in Form von Transaktionen auf der Grundlage von Daten, die zum Zeitpunkt der Programmierung des Codes noch nicht vorlagen, umverteilt werden. Das ist für sich genommen weder „smart" noch ein „contract". Der ebenso unbeeinflussbare wie unaufhaltsame Ablauf des Codes könnte aber im Hinblick auf formelhaft beschreibbare Teile von Vereinbarungen wegen der dadurch entbehrlichen staatlichen Vollstreckung zu einem wahren „Game Changer" der Vertragsgestaltung und selbst für letztwillige Verfügungen werden. Dabei ist zum Beispiel an strukturierte Finanzprodukte ohne Kreditinstitute und Market-Maker zu denken, aber auch an den Wettbewerbsvorteil, den eine Fluglinie dadurch erzielen könnte, dass sie die Fluggäste – anders als so manche Konkurrentin – beim Settlement von Fluggastrechten nicht im Regen stehen lässt, sondern einen Smart Contract anbietet, der die Entschädigung automatisch auszahlt, sobald sich aus der OAG-Flugplandatenbank ein entsprechender Delay ergibt.

Im Ethereum-Whitepaper[28] wird folgendes Anwendungsbeispiel beschrieben: „A kann pro Tag bis zu X Währungseinheiten beheben, B dagegen nur Y; A und B zusammen können beliebige Summen beheben, und A kann die Befugnis von B widerrufen." Bedenkt man, dass Unternehmen außer aus den handelnden Personen lediglich aus Assets und Regeln, wer darüber in welcher Höhe für welche Zwecke verfügen darf, bestehen, erkennt man schemenhaft das schier grenzenlose Potenzial komplexer Smart Contracts: Schon bald werden AAs (Autonomous Agents), DAs (Decentralized Applications), DOs (Decentralized Organizations), DAOs (Decentralized Autonomous Organizations) und DACs (Decentralized Autonomous Corporations) ökonomische Abläufe und damit unseren Alltag prägen.

VI. Herausforderungen für das Recht und die Rechtswissenschaft

In bestechender Klarheit zeigt *Florian Faust*[29], wie gut es der Vertragspraxis und der Rechtsprechung gelungen ist, aktuelle tatsächliche Probleme der digitalen Welt auf der Grundlage des im Kern „analogen" BGB sachgerechten Lösungen zuzuführen. Mehr als zwanzig Jahre nach dem Beginn der Kommerzialisierung des Internets kann der überwiegende Teil der Fragen im Zusammenhang mit Verträgen über digitale Inhalte als beantwortet gelten.

Von ganz anderer Tragweite sind die Herausforderungen, mit denen sich das Recht und die Rechtswissenschaft durch DLT konfrontiert sehen, die aber bislang allenfalls punktuell diskutiert wurden. Hier geht es bei Weitem nicht nur um neue Tatsachen, sondern um grundstürzende Phänomene, welche mit ihrer liberalisierenden und demokratisierenden Kraft sowohl im staatlichen als auch im privatwirtschaftlichen Machtgefüge zu Verwerfungen führen werden. Nicht zuletzt erfordern sie einen neuen Blick auf die Art und Weise, wie wir Verträge schließen, und das auf die staatliche Macht gestützte Rechtsdurchsetzungsmonopol erhält durch „faktische" Durchsetzung auf der Blockchain Konkurrenz.

Zu den vordringlich zu behandelnden Problemstellungen zählen die (zurückhaltende) Regulierung von Kryptowährungen und das Verhältnis von Smart Contracts zum Vertragsrecht, insbesondere zur AGB-Inhaltskontrolle sowie zum Verbraucherschutz, das Lizenzmanagement und „Smart Property" ebenso wie die Haftung für Schäden aus fehlerhaften Protokollen und Programmcodes. Konstruktionen wie DAs und DAOs sind sowohl gesellschaftsrechtlich als auch im Hinblick auf die Verhinderung ihres Missbrauchs für kriminelle Zwecke zu untersuchen. Wegen der dezentralisierenden und desintermediatisierenden Wirkung von DLT stellen sich auch gänzlich neue Fragen im Zusammenhang mit grenzüberschreitenden Sachverhalten. Schließlich geht es im öffentlichen Recht um einen Rahmen für die Entfaltung der effizienzsteigernden Effekte von DLT, um die mögliche Auslagerung bisheriger Staatsaufgaben (öffentliche Register), um das Identitätsmanagement, um Wahlen auf der Blockchain und nicht zuletzt um die Nutzung des die informationelle Selbstbestimmung stärkenden Potenzials.

Die im September 2016 vom 71. Deutschen Juristentag begonnene Diskussion sollte daher – wie der Autor meint – vom 72. Deutschen Juristentag fortgesetzt werden. Die Digitalisierung der Wirtschaftswelt im Allgemeinen und die disruptiven Effekte der DLT im Besonderen werden nicht aufzuhalten sein und Rechtsordnung wie Rechtsanwender nachhaltig fordern.

27 Oben Fn. 14; den Begriff „Smart Contract" prägte *Szabo* bereits in seinem gleichnamigen Beitrag aus dem Jahr 1994, http://kurzelinks.de/AnwBl-2016-8u9-19.

28 Oben Fn. 25, S. 1.

29 *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update? Gutachten A zum 71. Deutschen Juristentag (2016).

Prof. Dr. Dr. Walter Blocher, Kassel
Der Autor leitet das Fachgebiet Bürgerliches Recht, Unternehmensrecht und Informationsrecht am Institut für Wirtschaftsrecht der Universität Kassel, an der sich im Frühjahr 2016 eine mehr als 20 Fachgebiete umfassende interdisziplinäre DLT-Forschungsgruppe konstituierte.

Leserreaktionen an anwaltsblatt@anwaltverein.de.