Cathrin Hein; Wanja Wellbrock; Christoph Hein

Hype oder Horror. Potenziale und Hürden der Blockchain-Technologie anhand rechtlicher Rahmenbedingungen

2019

https://doi.org/10.25969/mediarep/18733

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Hein, Cathrin; Wellbrock, Wanja; Hein, Christoph: Hype oder Horror. Potenziale und Hürden der Blockchain-Technologie anhand rechtlicher Rahmenbedingungen. In: *ZMK Zeitschrift für Medien- und Kulturforschung*. Blockchain, Jg. 10 (2019), Nr. 2, S. 137–154. DOI: https://doi.org/10.25969/mediarep/18733.

Hype oder Horror

Potenziale und Hürden der Blockchain-Technologie anhand rechtlicher Rahmenbedingungen

Cathrin Hein / Wanja Wellbrock / Christoph Hein

1. Einleitung

Die *Blockchain*-Technologie wird oftmals als »biggest opportunity set we can think of over the next decade« beschrieben.[1] Andere sehen das Potenzial darin: »What the internet did for communications, blockchain will do for trusted transactions.«[2] Wieder andere übertreiben etwas, wenn sie *Blockchain* als »eine Technologie die unser ganzes Denken revolutioniert« feiern.[3] Aber was hat es mit dieser angeblich revolutionären Technologie auf sich?

Blockchain ist eine Basistechnologie, auf deren Grundlage neue Plattformen und Geschäftsmodelle geschaffen werden können.[4] Der bekannteste Anwendungsfall der Blockchain-Technologie dürfte die Kryptowährung *Bitcoin* sein. Im Jahre 2008 veröffentlichte eine unbekannte Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto das *Bitcoin* Whitepaper *Bitcoin: A Peer-to-Peer electronic Cash System*[5] als Blaupause für digitale Währung.[6] Dies wird oft als die Reaktion der digitalen Gemeinschaft auf die weltweite Finanzkrise gesehen, in deren Folge vor allem Banken massiv an Vertrauen eingebüßt hatten. Digitale Währungen auf Basis der *Blockchain*-Technologie kommen ohne entsprechende Intermediäre bei den Transaktionen aus.[7]

1 Sweta Jaiswal: Is Blockchain a Game-Changer for Healthcare?, unter: https://www.nasdaq.com/article/is-blockchain-a-game-changer-for-healthcare-cm944721 (06.04.2018).

2 Graham Rapier: From Yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world, unter: https://www.businessinsider.de/ibm-ceo-ginni-rometty-blockchain-transactions-internet-communications-2017-6?r=US&IR=T (21.07.2017).

3 Milosz Matuschek: Blockchain – eine Technologie revolutioniert unser ganzes Denken, unter: https://www.nzz.ch/meinung/kommentare/new-kids-on-the-blockchain-ld.1319020 (02.10.2017).

4 Stephan Breidenbach und Florian Glatz: Rechtshandbuch Legal Tech, München 2018.

5 Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, unter: https://bitcoin.org/bitcoin.pdf (10.06.2008).

6 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).

7 Christian Siedenbiedel: Bitcoins: Aufstieg und Fall einer seltsamen Währung, unter:

Per Definition ist *Blockchain* eine dezentrale Datenbank, die aus einer stetig größer werdenden Liste von Datensätzen besteht, welche verteilt auf unterschiedlichen Computern gesichert werden. Dabei werden die Transaktionen in Blöcken zusammengefasst und die Prüfsumme des Vorgängerblocks stets als Validierungsmerkmal mitgegeben. Diese Technik wird auch als *Distributed Ledger*-Technologie bezeichnet.[8]

Es stellt sich hierbei die Frage, ob das deutsche Rechtssystem grundsätzlich in der Lage ist, die Herausforderungen, die diese dezentrale Technologie mit sich bringt, zu bewältigen. Bisher gibt es hierzulande noch keine konkreten rechtlichen Regelungen in puncto *Blockchain*. Andere Länder sind hier weiter. In Thailand trat am 13. Mai 2018 ein Gesetz für den Umgang mit Kryptowährungen in Kraft.[9] Der US Bundesstaat Michigan hat einen Gesetzesentwurf vorgestellt, nachdem es strafbar ist, Datensätze, die unter der Verwendung von *Distributed Ledger*-Technologie gespeichert werden, zu ändern.[10] Der US Bundesstaat Tennessee definiert *Blockchain*-Technologie gesetzlich wie folgt: »Blockchain technology means *distributed ledger* technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable, and provides an uncensored truth.«[11]

Eine Studie der Rheinisch-Westfälisch Technischen Hochschule Aachen und der Goethe-Universität Frankfurt wirft darüber hinaus die Frage auf, ob Nutzer eines *Blockchain*-Netzwerkes für rechtswidrige Inhalte verantwortlich gemacht werden können. Im Rahmen der Studie wurden die nichtfinanziellen Inhalte der *Bitcoin-Blockchain* analysiert und dabei u. a. Links zu Kinderpornographie entdeckt. Jeder Nutzer der *Bitcoin-Blockchain* hat per Definition eine Kopie sämtlicher Datensätze auf dem genutzten Computer und könnte sich dadurch strafbar machen.[12]

---

http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/bitcoin-aufstieg-und-fall-einer-seltsamen-waehrung-12848847.html (05.03.2014).

8 Alexander Djazayeri: Rechtliche Herausforderungen durch Smart Contracts, in: jurisPR-BKR 12/2016 Anm. 1 (20.12.2016).

9 Roman Maas: Thailands neues Krypto-Gesetz tritt in Kraft, unter: https://www.btc-echo.de/thailands-neues-krypto-gesetz-tritt-in-kraft/ (16.05.2018).

10 Tanja Giese: Michigan – Unveränderlichkeit der Blockchain soll Gesetz werden, unter: https://www.btc-echo.de/michigan-unveraenderlichkeit-der-blockchain-soll-gesetz-werden/ (16.06.2018).

11 Tennessee Generalversammlung: House Bill 1507, Tennessee (USA), unter: http://www.capitol.tn.gov/Bills/110/Bill/HB1507.pdf (26.03.2018).

12 Hendrik Wieduwilt: Problem für Zukunftstechnologie – Kinderpornographie in der Blockchain gefunden, unter: http://www.faz.net/aktuell/wirtschaft/diginomics/kinderpornographie-in-blockchain-gefunden-15507813.html (23.03.2018).

Es ist unstreitig zu erkennen, dass insbesondere rechtliche Aspekte in der Zukunft eine große Rolle im Umfeld *Blockchain*-basierter Applikationen spielen werden. Für eine Auseinandersetzung mit den rechtlichen Herausforderungen für Privatpersonen und Unternehmen ist es daher unvermeidbar, dass Sie sich ein grundlegendes Verständnis der zugrunde liegenden Technologie aneignen und sich den rechtlichen Risiken und Unschärfen einer Nutzung bewusst sind.

2. Blockchain-Technologie

Bitcoin gilt als der Ursprung der *Blockchain*-Technologie. Hiervon leiten sich die technologischen Eckpfeiler des Systems ab. Es handelt sich um ein dezentrales Netzwerk, innerhalb dessen eine künstlich begrenzte Menge an Wertmarken generiert wird. Während diese Wertmarken eindeutig einem Benutzer zugeordnet werden können, bleibt selbiger anonym. Analog den Banken in der realen Welt wurde vor *Bitcoin* stets eine zentrale Instanz benötigt, um die Transaktionen zu kontrollieren und das *Double Spending* zu verhindern. Eine Einheit einer Kryptowährung darf ebenso nur einmal verwendet werden, wie in früheren Zeiten ein Scheck.[13]

Innerhalb einer *Blockchain* werden sämtliche Transaktionsdaten gespeichert und neue Transaktionen fortlaufend mit der bestehenden Transaktionshistorie abgeglichen und so geprüft, ob ein Wert bereits vorher ausgegeben wurde.[14]

Die Basis *blockchain*-basierter Anwendungen ist der dezentrale Aufbau des Netzwerks. Während es bei einem zentralisierten Netzwerk eine entsprechende Instanz gibt, die die getätigten Transaktionen verwaltet und kontrolliert, verzichtet ein dezentrales Netzwerk auf eben jene Kontrollinstanz und ermöglicht eine direkte Kommunikation zwischen den Teilnehmern, bei der jeder Teilnehmer jederzeit über den einheitlichen Datenbestand verfügt. Derartige Netzwerke sind von außen nicht zu kontrollieren (siehe Abb. 1, S. 134).

Blockchain-Netzwerke sind nicht nur auf die Übertragung von Kryptowährungen ausgelegt. Es können beispielsweise auch im Rahmen von *Smart Contracts* Kaufverträge darüber dokumentiert werden, da alle Transaktionen öffentlich nachvollziehbar sind. Man spricht hier auch vom Internet der Werte (*Internet of Value*), in dem jede Übertragung von Gütern abgebildet werden kann.[15]

---

13 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).

14 Joachim Schrey und Thomas Thalhofer: Rechtliche Aspekte der Blockchain, in: NJW – Neue Juristische Wochenschrift 70/20 (2017), S. 1431–1436.

15 Tatiana Gayvoronskaya, Christoph Meinel und Maxim Schnjakin: Blockchain – Hype oder Innovation, Technischer Bericht Nr. 113, unter: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf (20.09.2018).

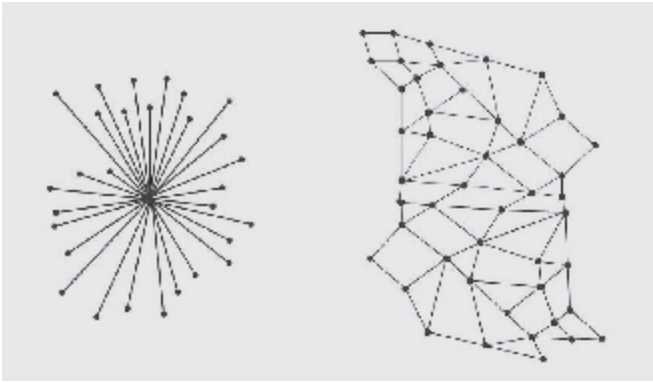

Abb. 1: Zentraler vs. dezentraler Netzwerkaufbau (Stephan Breidenbach und Florian Glatz: Rechtshandbuch Legal Tech, München 2018)

Hierfür werden initial die Vermögenswerte innerhalb des Netzwerks definiert, aufgelistet und den Eigentümern zugeordnet. Für diese Assets erhalten die jeweiligen Eigentümer sogenannte *Tokens*. Diese repräsentieren im weiteren Verlauf das Eigentum am jeweiligen Vermögenswert wodurch so erstmals effektiv das *Double Spending* verhindert werden kann.[16]

Mangels zentraler Instanz verfügen alle Teilnehmer einer *Blockchain* über die gleiche Legitimation innerhalb des Netzwerks. Jeder Teilnehmer hat theoretisch die gesamte Transaktionshistorie gespeichert. Da diese bei *Bitcoin* beispielsweise bereits 147 GB beträgt (Stand Dezember 2017), unterscheidet man inzwischen in sogenannte *Lightweight Nodes* und *Full Nodes*. Erstere speichern lediglich den für sie relevanten Teil der *Blockchain*, letztere dagegen den gesamten Datenbestand.

Ausgangspunkt für die Teilnahme am *Bitcoin*-Netzwerk ist die sogenannte *Wallet*. Diese stellt allerdings keine Geldbörse im eigentlichen Sinne dar, sondern dient lediglich der Verwaltung des *Blockchain*-Kontos. Die Adresse selbiger ist pseudonymisiert und dient der Kontoverwaltung und dem Senden und Empfangen von Transaktionen.[17] Die Transaktionen werden mittels *Public Key*-Verfahren verschlüsselt, wodurch sichergestellt wird, dass nur berechtigte Teilnehmer Transaktionen vornehmen.[18]

16 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).

17 Gayvoronskaya, Meinel und Schnjakin: Blockchain – Hype oder Innovation, (wie Anm. 15).

18 Daniel Burgwinkel: Blockchain Technology – Einführung für Business- und IT Manager, Berlin und Boston 2016; Joachim Schrey und Thomas Thalhofer: Rechtliche Aspekte der Blockchain, in: NJW – Neue Juristische Wochenschrift 70/20 (2017), S. 1431–1436; Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, unter: https://bitcoin.org/bitcoin.pdf (10.06.2008).

Am Beispiel der *Bitcoin-Blockchain* enthalten die Transaktionen primär Informationen über die Herkunft und den Empfänger der *Bitcoins*. Die Besonderheit hierbei ist, dass keine *Bitcoins* in der Quelle übrigbleiben dürfen. Hat man zwanzig *Bitcoins* und möchte nur fünf davon an einen anderen Nutzer überweisen, ist es notwendig, sich die restlichen fünfzehn *Bitcoins* selbst zu überweisen. Ansonsten würde die Differenz als Transaktionsgebühr für den Nutzer verloren gehen. Der vollständige Datensatz wird an die übrigen Teilnehmer des Netzwerks gesendet und zunächst zwischengespeichert, bis er final in einen Block aufgenommen wird.[19]

Alle Transaktionen innerhalb der *Blockchain* werden in Blöcken gespeichert. Sie umfassen bei der *Bitcoin-Blockchain* beispielsweise ungefähr 900 bis 2.500 Transaktionen pro Block. Vor der Aufnahme in einen Block werden die Transaktionen validiert, um zu verhindern, dass bereits ausgegebene *Bitcoins* nicht erneut ausgegeben werden. So entsteht die unveränderbare Transaktionskette, das Markenzeichen der *Blockchain*.[20]

Die sogenannten *Miner* – Computer, die dem Netzwerk Rechenleistung bereitstellen – schließen die Blöcke, errechnen die mathematisch generierte Identifikationszahl und verknüpfen den Block mit dem vorherigen Block in der Kette (siehe Abb. 2, S. 136). Die Ermittlung dieses einmaligen Fingerabdrucks benötigt eine hohe Rechenleistung aufgrund der hohen Anzahl führender Nullen, sogenannter Nonce. Dieser Prozess stellt die Datenintegrität in der *Blockchain* sicher und ermöglicht, dass die Transaktionen nachträglich nicht mehr verändert werden können.[21]

---

19 Gayvoronskaya, Meinel und Schnjakin: Blockchain – Hype oder Innovation, (wie Anm. 15); Stefan Groß und Axel-Michael Wagner: White Paper. Blockchain und Smart Contracts – Moderne IT-Konzepte aus (datenschutz-)rechtlicher Sicht, unter: https://www.psp.eu/media/allgemein/white_paper_blockchain.pdf (10.03.2018).

20 Gayvoronskaya, Meinel und Schnjakin: Blockchain – Hype oder Innovation, (wie Anm. 15); Joachim Schrey und Thomas Thalhofer: Rechtliche Aspekte der Blockchain, in: NJW – Neue Juristische Wochenschrift 70/20 (2017), S. 1431 – 1436; Stephan Breidenbach und Florian Glatz: Rechtshandbuch Legal Tech, München 2018.

21 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4); Stefan Groß und Axel-Michael Wagner: White Paper. Blockchain und Smart Contracts – Moderne IT-Konzepte aus (datenschutz-)rechtlicher Sicht, unter: https://www.psp.eu/media/allgemein/white_paper_blockchain.pdf (10.03.2018); Joachim Schrey und Thomas Thalhofer: Rechtliche Aspekte der Blockchain, in: NJW – Neue Juristische Wochenschrift 70/20 (2017), S. 1431 – 1436; Tatiana Gayvoronskaya, Christoph Meinel und Maxim Schnjakin: Blockchain – Hype oder Innovation, Technischer Bericht Nr. 113, unter: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf (20.09.2018); Daniel Drescher: Blockchain Grundlagen – Eine Einführung in die elementaren Konzepte in 25 Schritten, Frechen 2017; Daniel Burgwinkel: Blockchain Technology – Einführung für Business- und IT Manager, Berlin und Boston 2016.

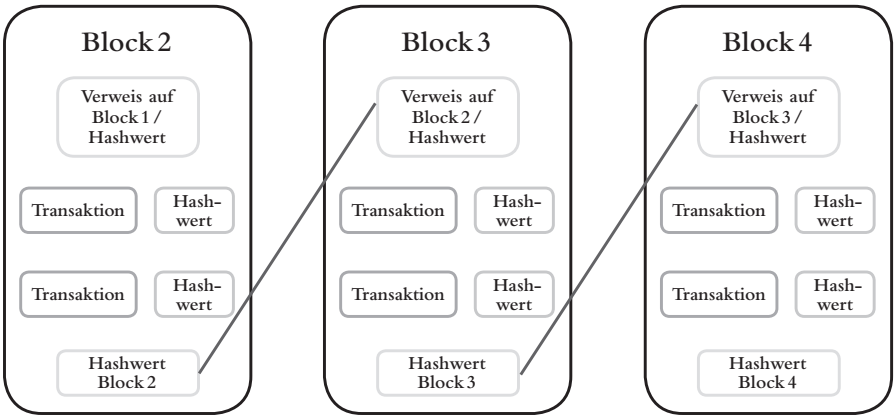

Abb. 2: Prinzip der *Blockchain*-Technologie (Daniel Burgwinkel: Blockchain Technology – Einführung für Business- und IT Manager, Berlin und Boston 2016)

Die Netzwerkteilnehmer sind oft weltweit verteilt, was Unterschiede in der Übertragungsgeschwindigkeit der Daten mit sich bringt. Dadurch kann es zu Ungleichgewichten im Datenbestand kommen, und es ist nicht immer gewährleistet, dass alle Daten zeitgleich bei allen Teilnehmern aktualisiert werden. Um dem entgegenzuwirken, sollte immer nur die längste Kette an Blöcken als valide akzeptiert werden.[22]

Die Bereitstellung der Rechenleistung durch die *Miner* kostet Zeit und Geld und wird innerhalb der *Bitcoin-Blockchain* beispielsweise auf zwei Arten entlohnt. Einerseits wird für die Aufnahme in einen Block eine Transaktionsgebühr von den *Minern* erhoben und andererseits entstehen in jedem neuen Block neue *Bitcoins*, die der jeweilige *Miner* als Entschädigung erhält.[23]

Blockchain ist nicht gleich *Blockchain*. Es gibt unterschiedliche Lösungsansätze auf Basis dieser Technologie. Eine Variante sind private Netzwerke, bei denen ein Beitritt zum geschlossenen Teilnehmerkreis nicht ohne weiteres möglich ist. Beispielhaft sei hier *Hyperledger* genannt, eine Initiative, die *Blockchain*-Anwendungen für Unternehmen entwickelt.[24]

Im Gegensatz dazu ist bei den öffentlichen *Blockchain*-Anwendungen eine Teil-

22 Hans Bechtolf und Niklas Vogt: Datenschutz in der Blockchain – Eine Frage der Technik, in: ZD – Zeitschrift für Datenschutz 8/2 (2018), S. 66–70.

23 Gayvoronskaya, Meinel und Schnjakin: Blockchain – Hype oder Innovation, (wie Anm. 15).

24 Frauenhofer-Gesellschaft: Blockchain und Smart Contracts - Technologien, Forschungsfragen und Anwendungen, unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-

nahme für jedermann möglich und bedarf keiner gesonderten Erlaubnis, beispielsweise das schon erwähne *Bitcoin* oder *Etherum*. Letzteres dient im Übrigen nicht einzig dem Austausch von Kryptowährung, sondern ist gleichzeitig auch eine *Smart Contracts*-Plattform. [25]

Blockchain-Anwendungen setzen eine schnelle Internetverbindung und hohe Rechenleistung voraus. Letztere verursacht insbesondere durch den Stromverbrauch immense Kosten, was auch einer der größten Kritikpunkte an der *Blockchain*-Technologie ist. Gleichzeitig ist es auch der größte Schutz vor Manipulationen. Theoretisch müsste man nur 51% der Rechenkapazität innerhalb einer *Blockchain* kontrollieren und könnte anschließend die Anwendung nach Belieben manipulieren. Allerdings ist es eben aufgrund der hohen Kosten für die Bereitstellung der Rechenkapazität in der Regel lukrativer, diese einfach als *Miner* einzusetzen und dafür *Bitcoins* zu erhalten.[26]

Trotz des geringen Restrisikos des Hackings gewährleistet die *Blockchain*-Technologie einen hohen Sicherheitsstandard, da die Daten dezentral verteilt, für alle Nutzer zugänglich und verschlüsselt sind. Der Verzicht auf Intermediäre, wie beispielsweise Banken, erlaubt eine schnellere Abwicklung und ermöglicht insbesondere in Regionen mit einem weniger stark ausgeprägten Rechtssystem, dass Verträge oder Überweisungen korrekt und sicher ausgeführt werden.[27]

Die zugrunde liegende Technologie ermöglicht eine sichere Transaktionsabwicklung und ein gegenseitiges Vertrauen der Vertragspartner ist nicht notwendig. Es wird die gesamte Transaktionshistorie nachvollziehbar abgebildet und Nutzer können diese jederzeit einsehen. Außerdem arbeiten *Blockchain*-Netzwerke autonom, weshalb sich äußere Einflüsse nicht auf das Netzwerk auswirken [28]

Contracts.pdf?_=1516641660 (10.11.2017); Linux Foundation: Hyperledger Business Blockchain Technologies, unter: https://www.hyperledger.org/projects (20.10.2018).

25 Burgwinkel: Blockchain Technology, (wie Anm. 18).

26 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4); Dennis Streichert: Vorteile und Nachteile der Blockchain-Technologie, unter: https://www.blockchain-infos.de/vorteile-nachteile-blockchain/ (19.10.2018); Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, unter: https://bitcoin.org/bitcoin.pdf (10.06.2008).

27 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4); Dennis Streichert: Vorteile und Nachteile der Blockchain-Technologie, unter: https://www.blockchain-infos.de/vorteile-nachteile-blockchain/ (19.10.2018).

28 Burgwinkel: Blockchain Technology, (wie Anm. 18).

3. Kinderpornographie als Beispiel rechtlichen Handlungsbedarfs

Eingangs wurde bereits auf die gefundenen Links zu kinderpornographischem Material innerhalb des *Bitcoin*-Netzwerks hingewiesen.[29] Dies erfolgt vorwiegend über spezielle Transaktionstypen oder Notizfelder von Standard-Transaktionen.[30] Da innerhalb einer *Blockchain* fortlaufend alle Transaktionsdaten unveränderlich gespeichert und jedem Nutzer zugänglich sind, stellt sich zunächst die Frage, ob das bloße Speichern der Transaktionshistorie, welches Zugangsvorraussetzung für die Teilnahme am Netzwerk ist, mit dem strafbaren *Besitz von Kinderpornographie* nach § 184b Abs. 3 StGB gleichzusetzen ist. Allerdings reicht die Bereitstellung der Daten zum Abruf auf einem Server in der Regel nicht als Straftatbestand aus.[31] Jedoch werden derzeit Änderungen des StGB im Deutschen Bundestag diskutiert, nachdem bereits der Abruf mittels Rundfunk oder Telemedien strafbar wäre.[32] Hier sind also künftig noch Änderungen zu erwarten.

Anders stellt sich der Sachverhalt bei dem Tatbestandsmerkmal des Vorsatzes gem. § 15 StGB dar, werden hier doch Wissen und Wollen der Tatbestandsverwirklichung vorausgesetzt. Ein vorsätzliches Handeln zu unterstellen, wenn der originäre Zweck der Handel mit der Kryptowährung *Bitcoin* ist, scheint fraglich. Gerade weil es die bloße Nutzung des Netzwerks zu einer Straftat erklären würde, da sich irgendwo innerhalb des Netzwerks rechtswidrige Inhalte befinden könnten. Sollte sich eine derartige Lesart allerdings durchsetzen, gäbe es für die Technologie kaum noch praktische Anwendungsfälle.

Es stellt sich noch die Frage, ob die *Miner* aus strafrechtlicher Sicht eine andere Rolle in diesem Prozess einnehmen. Mittäter i. S. v. § 25 Abs. 2 StGB wären sie, wenn sie sich der Verbreitung mitschuldig machen und die Daten einem größeren, nicht mehr kontrollierbaren Personenkreis zugänglich machen.[33] Zwar stellen sie ihre Rechenleistung dem Netzwerk zur Verfügung und tragen durch das Schließen der Blöcke maßgeblich zur Verbreitung der Daten bei, andererseits prüfen sie

29 Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohfeld und Klaus Wehrle: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin unter: https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf (10.03.2018).

30 Blockchain Bundesverband e.V.: Blockchain – Chancen und Herausforderungen einer neuen digitalen Infrastruktur für Deutschland, Version 1.1, unter: https://bundesblock.de/wp-content/uploads/2017/10/bundesblock_positionspapier_v1.1.pdf (16.10.2017).

31 Eric Hilgendorf und Brian Valerius: Computer- und Internetstrafrecht – Ein Grundriss, 2. Auflage, Berlin und Heidelberg 2012.

32 Deutscher Bundestag: Gesetzentwurf der Fraktionen der CDU/CSU und SPD zur Änderung des Strafgesetzbuches vom 23.09.2014, Drucksache 18/2601, unter: http://dipbt.bundestag.de/doc/btd/18/026/1802601.pdf (23.09.2014).

33 Urs Kindhäuser: Strafgesetzbuch Lehr- und Praxiskommentar, 7. Aufl., Baden-Baden 2017.

die Transaktionen nicht inhaltlich und haben somit keine Verantwortung für die Transaktionen der Nutzer und können keinen Einfluss auf selbige nehmen. Eine zentrale Kontrolle des Inhalts würde den eigentlichen Zweck des Netzwerks, beispielsweise den dezentralen Austausch von Kryptowährung, aushebeln. *Vorsatz* nach § 15 StGB kann ebenso wenig unterstellt werden. Zweck des Netzwerks ist der Handel mit Kryptowährung und die Motivation zur Teilnahme für die Miner ist finanzieller Natur.

Rechtswidrige Inhalte innerhalb von *Blockchain*-Transaktionen stellen einen neuen Sachverhalt dar, der rechtlich noch nicht ausreichend analysiert ist. Der Gesetzgeber sollte hier Rahmenbedingungen schaffen, um für den durchschnittlichen Nutzer Rechtsicherheit zu schaffen.

4. Datenschutzrechtliche Aspekte der Blockchain-Technologie

Die seit Mai 2018 für die EU-Mitgliedstaaten geltende Datenschutz-Grundverordnung muss auch in Deutschland für die Verarbeitung personenbezogener Daten angewendet werden. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen« und eine Identifizierung, ohne dass anderweitige Informationsquellen genutzt werden, ermöglichen. Allerdings ist vorab zu klären, ob in einer öffentlichen *Blockchain* überhaupt derartige Daten enthalten sind oder ob es sich vielmehr um anonymisierte Informationen handelt, bei denen betroffene Personen nicht mehr identifiziert werden können.[34]

Innerhalb eines *Blockchain*-Netzwerks werden Pseudonyme anstelle von Klarnamen verwendet, wodurch eine unmittelbare Identifizierung der jeweiligen natürlichen Personen nicht möglich ist. Allerdings würde es sich immer noch um eine identifizierbare Person nach Art. 4 Nr. 1 DS-GVO handeln, wenn durch die Verknüpfung des Pseudonyms mit weiteren Daten ein Rückschluss auf die natürliche Person möglich wäre.[35] Es ist demnach fraglich, ob die Adresse eines Nutzers in einer *Blockchain* als Pseudonym gilt und die DS-GVO anwendbar wäre oder es sich aufgrund der Verschlüsselungsmechanismen bereits um anonyme Daten handelt und demnach das Datenschutzrecht keine Anwendung findet.[36] Die Adresse

34 Benedikt Buchner und Jürgen Kühling: Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

35 Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14); Benedikt Buchner und Jürgen Kühling: Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

36 Benedikt Buchner und Jürgen Kühling: Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

eines Benutzers im *Bitcoin*-Netzwerk wird mittels einer Hash-Funktion generiert und ist prinzipiell als Pseudonymisierung anzusehen, da die Herstellung eines Personenbezugs für die Zukunft nicht ausgeschlossen werden kann.

Der relativen Theorie folgend ist die Identifizierung natürlicher Personen durch Dritte sehr weit gefasst und eine Anonymisierung nahezu ausgeschlossen. Allerdings lässt sich ein *Verantwortlicher* i.S.d. DS-GVO innerhalb eines *Blockchain*-Netzwerks nicht eindeutig identifizieren. So gesehen müsste die absolute Theorie Anwendung finden und demzufolge die Möglichkeiten, die eine dritte Partei zur Identifizierung ergreifen könnte, in Betracht gezogen werden. Fraglich ist demnach, welche Mittel eine andere Person nach allgemeinem Ermessen wahrscheinlich einsetzt, um die Person hinter dem Pseudonym zu identifizieren. Dabei müssen der technologische Fortschritt und die Verhältnismäßigkeit zwischen notwendigem Aufwand und Identifizierungsinteresse berücksichtigt werden.[37] Würden in der *Blockchain* beispielsweise Gesundheitsdaten verschlüsselt gespeichert werden, könnte ein höheres Identifizierungsinteresse unterstellt werden als etwa bei weniger sensiblen Daten.[38]

Über die Verknüpfung von *Bitcoin*-Transaktionen mit der IP-Adresse des Nutzers können Rückschlüsse auf die Vermögensverhältnisse und das Verhalten des Nutzers erfolgen und dadurch eine Deanonymisierung der dahinterstehenden Person herbeigeführt werden.[39] Weiterhin kann die Identität durch die Verknüpfung mit Zusatzinformationen ermittelt werden, wie beispielsweise der Einkauf in einem Online-Shop und die daraus resultierende Lieferadresse.[40] Eine *Blockchain* hat immer auch ein vollständiges Profil aller Nutzer und ihrer Transaktionen. Am Beispiel der *Bitcoin-Blockchain* werden demnach sämtliche finanziellen Vorgänge lückenlos archiviert. Veröffentlicht eine Person ihre *Bitcoin*-Adresse, so ist es möglich, sämtliche Zahlungsvorgänge dieser Person nachzuvollziehen. Beispielsweise

37 Johanna Hofmann und Paul Johannes: DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs – Begriffsklärung der entscheidenden Frage des sachlichen Anwendungsbereichs, in: ZD – Zeitschrift für Datenschutz 7/5 (2017), S. 221–225.

38 Benjamin Talin: Blockchain – Möglichkeiten und Anwendungen der Technologie, unter: https://morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/ (04.07.2018).

39 Mario Martini und Quirin Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ – Neue Zeitschrift für Verwaltungsrecht 26/17 (2017). S. 1251–1270; Alex Biryukov, Dmitry Khovratovich und Ivan Pustogarov: Deanonymisation of clients in Bitcoin P2P network, unter: https://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf (10.05.2019); Tatiana Gayvoronskaya, Christoph Meinel und Maxim Schnjakin: Blockchain – Hype oder Innovation, Technischer Bericht Nr. 113, unter: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf (20.09.2018).

40 Bechtolf und Vogt: Datzenschutz in der Blockchain, (wie Anm. 22).

hat Wikileaks die eigene *Bitcoin*-Adresse veröffentlicht, um Spenden zu generieren.[41] Durch die Veröffentlichung der Adresse ist es möglich, alle Transaktionen dieser Adresse zu analysieren und Rückschlüsse auf die Vermögensverhältnisse von Wikileaks zu ziehen. Bei der Generierung von Spenden kann diese Nachvollziehbarkeit von Vorteil sein. Bei natürlichen Personen stellt dies jedoch eher ein Risiko dar, dem höchstens durch die bereits erwähnte Verwendung stetig neuer Schlüssel für Transaktionen entgegengewirkt werden kann. Andernfalls lässt sich eine solche Profilbildung nicht verhindern, und es können innerhalb des *Bitcoin*-Systems oder auch in anderen *Blockchain*-Netzwerken Rückschlüsse auf die Vermögensverhältnisse gezogen werden. Ob es sich also um die Verarbeitung personenbezogener Daten handelt, hängt insbesondere von den Interessen und technischen Möglichkeiten des Verantwortlichen oder einer anderen Person ab.[42]

Verantwortlicher nach Art. 4 Nr. 7 DS-GVO ist »die natürliche oder juristische Person, [...] die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet«. Dadurch soll einer Stelle die Verantwortung, u. a. für die Einhaltung der Datenschutzbestimmungen, zugewiesen werden. Allerdings zeichnet sich ein *Blockchain*-Netzwerk insbesondere durch die dezentrale Struktur und das Fehlen einer zentralen Verantwortlichkeit aus. [43]

In der Praxis würde eine Kontrolle durch die *Miner* das Vertrauen in das Netzwerk und dessen Sicherheit erheblich beeinträchtigen. Daher achten Miner innerhalb des *Bitcoin*-Systems stets von sich aus darauf, dass sie den Grenzwert von 51 % nicht überschreiten. Eine gemeinsame Verantwortlichkeit der *Miner* ist abzulehnen.[44] Die *Miner* können lediglich die Transaktionen zusammenfassen und *Hashwerte* errechnen, aber dabei die entsprechenden Daten nicht verändern, weshalb ihnen für die u. U. enthaltenen personenbezogenen Daten nicht die Verantwortung auferlegt werden kann. Prinzipiell besteht für alle Mitglieder des *Blockchain*-Netzwerks keine Möglichkeit, einzelne Transaktion zu löschen. Der einzelne Nutzer kann keine Transaktionen für andere erstellen oder beeinflussen und ist auch nicht in der Lage, seine eigenen Transaktionen rückwirkend zu bearbeiten.[45]

41 WikiLeaks: Donate to WikiLeaks, unter: https://shop.wikileaks.org/donate#db3 (15.10.2018).

42 Eduard Hofert: Blockchain-Profiling – Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke, in: ZD – Zeitschrift für Datenschutz, 7/4 (2017), S. 161–165.

43 Buchner und Kühling: Datenschutz-Grundverordnung, (wie Anm. 34).

44 Jörn Erbguth, Joachim Fasching: Wer ist Verantwortlicher einer Bitcoin-Transaktion?, in: ZD – Zeitschrift für Datenschutz ZD Heft 7/12 (2017), S. 12/2017, S. 560–565.

45 Martini und Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, (wie Anm. 39).

Die DS-GVO normiert in Art. 16 S. 1 und 17 Abs. 1 diverse Rechte, die betroffene Personen gegenüber den Verantwortlichen in Bezug auf ihre personenbezogenen Daten geltend machen können. Im Hinblick auf die Unveränderbarkeit der *Blockchain* lässt sich hier das größte Konfliktpotenzial vermuten. Zunächst normiert Art. 16 S. 1 DS-GVO das Recht betroffener Personen, von dem Verantwortlichen unverzüglich die Berichtigung der die Personen betreffenden, unrichtigen Daten zu verlangen. Dieses Berichtigungsrecht ist für den Betroffenen essenziell, da unrichtig gespeicherte Daten Einfluss auf Entscheidungen wie beispielsweise eine Kreditvergabe haben können. Auch scheinbar bedeutungslose Unrichtigkeiten sind von diesem Recht erfasst, da keine Prognose getroffen werden kann, ob diese künftig nicht noch Relevanz entfalten.[46] Einträge in der *Blockchain* können nachträglich nicht mehr verändert werden. Art. 16 S. 1 DS-GVO steht somit im vollkommenen Gegensatz zu den eigentlich unveränderlichen Transaktionsdaten, und es bedarf spezieller technischer Implikationen, um ein solches Recht praktisch umzusetzen.

Art. 17 Abs. 1 DS-GVO regelt das Recht auf Löschung in bestimmten Fällen. Demnach dürfen die Daten nur solange gespeichert werden, wie sie auch tatsächlich benötigt werden. Sobald der jeweilige Zweck, für den die Daten verarbeitet wurden, erfüllt ist, sind die Betroffenen berechtigt, die Löschung der Daten zu verlangen. Der Verantwortliche hat also sicherzustellen, dass ein Zugriff auf die Daten nicht mehr oder nur noch mit unverhältnismäßig hohem Aufwand möglich ist. Allerdings lässt sich einer derartigen Aufforderung technisch nur schwer nachkommen, da so auch sämtliche *Hashwerte* ungültig und damit die gesamte Kette inkonsistent werden würde. Um das Recht auf Löschung zu umgehen, könnte man auch argumentieren, dass gerade in der stetigen Fortschreibung der Transaktionshistorie der Zweck des Netzwerks besteht und ein Recht auf Löschung somit gar nicht zur Anwendung kommen würde.[47]

Es zeigt sich, dass das Datenschutzrecht zwar durchaus Anwendung in einem öffentlichen *Blockchain*-Netzwerk finden kann, allerdings scheint die Umsetzung der Betroffenenrechte in der Praxis als nicht leicht handhabbar. Dazu bedarf es gesonderter Regelungen, wie der Datenschutz in *Blockchain*-Netzwerken anzuwenden ist oder wie technische Implikationen, die die Umsetzung und Wahrung des Datenschutzes gewährleisten, grundsätzlich einzusetzen sind.

46 Buchner und Kühling: Datenschutz-Grundverordnung, (wie Anm. 34).

47 Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14); Mario Martini und Quirin Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ – Neue Zeitschrift für Verwaltungsrecht 26/17 (2017). S. 1251 – 1270.

5. Zivilrechtliche Aspekte der *Blockchain*-Technologie am Beispiel von *Smart Contracts*

Eine Anfechtung von Verträgen erfolgt gem. § 143 Abs. 1 BGB durch Erklärung gegenüber dem Anfechtungsgegner und bewirkt nach § 142 Abs. 1 BGB, dass ein Rechtsgeschäft als von Anfang an nichtig anzusehen ist. Für Verträge innerhalb des *Blockchain*-Netzwerks würde dies bedeuten, dass bereits validierte und in den Blöcken gespeicherte Transaktionen bei einer wirksamen Anfechtung rückwirkend als nichtig betrachtet werden müssten. Die Technologie zeichnet sich jedoch gerade durch die Unveränderlichkeit der Transaktionshistorie aus.

Die Wirkung des Rücktritts normiert § 346 Abs. 1 BGB. Demnach sind die empfangenen Leistungen zurück zu gewähren und die gezogenen Nutzungen herauszugeben, wenn sich eine Vertragspartei den Rücktritt vertraglich vorbehalten hat oder ihr ein gesetzliches Rücktrittsrecht zusteht. Es stellt sich die Frage wie eine Rückabwicklung in der *Blockchain* abgebildet werden kann, insbesondere wenn der Verkäufer nicht mitwirkt. So kann in einer *Blockchain* niemand Transaktionen für andere Nutzer erstellen, da es stets des jeweiligen zur Adresse gehörenden Schlüsselpaares bedarf.

Im Übrigen stellt sich die Frage, wie innerhalb eines *Blockchain*-Netzwerks gewährleistet werden kann, dass lediglich berechtige Personen Verträge schließen. Zwar ist bei traditionellen Geschäften ebenfalls nicht ausgeschlossen, dass eine nicht berechtigte Person ein solches vornimmt, allerdings birgt die *Blockchain* durch die Unveränderlichkeit meist höhere Hürden in der Rückabwicklung oder Auflösung von Geschäften. So ist ein Rechtsgeschäft beispielsweise schwebend unwirksam, wenn es sich bei einer Vertragspartei um einen Minderjährigen handelt. Zur Wirksamkeit des Rechtsgeschäfts bedarf es dann in diesem Fall gem. § 107 BGB der Einwilligung seines gesetzlichen Vertreters, sofern der Minderjährige nicht lediglich einen rechtlichen Vorteil erlangt. Es ist fraglich, wie eine solche schwebende Unwirksamkeit in einer *Blockchain* abgebildet werden kann, ebenso wie geprüft werden soll, ob ein Minderjähriger Transaktionen ausführt.

Die *Blockchain* ist ein unabhängiges, dezentrales Netzwerk. Daher ist fraglich, wie in diesem Rahmen gewährleistet werden soll, dass Transaktionen nicht einem gesetzlichen Verbot i.S.v. § 134 BGB unterliegen. Da es meist keine zentrale Kontrollinstanz gibt, existiert zunächst auch keine Überprüfung der Transaktionsinhalte. Für diesen Fall könnte man mitunter einen Automatismus im *Blockchain*-Netzwerk einbauen, welcher routinemäßig Transaktionen mit gewissen Gesetzen abgleicht.[48] Allerdings ist es hierbei meist notwendig, das entsprechende Verbots-

48 Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14).

gesetz auszulegen.[49] Die *Blockchain* speichert jedoch lediglich feste Parameter und lässt keinen Raum für Auslegungsfragen. Dies führt auch zu Kollisionen mit der Sittenwidrigkeit gem. § 138 BGB. Ob Sittenwidrigkeit vorliegt, wird meist unterschiedlich beurteilt und kann somit nur schwer durch Automatismen geprüft werden.[50] Dies wirft die Frage auf, ob und wie in einem *Blockchain*-Netzwerk juristische Terminologie wie Treu und Glauben, Ermessen, Unzumutbarkeit oder auch höhere Gewalt in der Zukunft Berücksichtigung finden können.[51]

6. Lösungsansätze

In diesem Kapitel werden drei exemplarische Lösungsansätze vorgestellt, mit denen die oben angesprochenen Probleme zumindest ansatzweise behoben werden können. Die sog. *Reverse Transactions* führen fehlerbehaftete Transaktionen noch einmal umgekehrt aus, wodurch der wirtschaftliche Zustand, der vor der falschen Transaktion bestand, wiederhergestellt wird. Allerdings bleiben dabei sämtliche Transaktionen transparent einzusehen.[52]

Beim sog. *Pruning* handelt es sich um die teilweise Löschung bereits vergangener Transaktionen durch eine zentrale Instanz. Dabei ist zu beachten, dass die Daten, die gelöscht werden sollen, bereits wieder in einer neuen Transaktion enthalten sein müssen. Dieser Vorgang ermöglicht es, Daten zu entfernen, ohne den Nachweis über die jeweilige Legitimation zu verlieren und die *Blockchain* weiterzuführen. Dadurch wird die Funktionsfähigkeit der gesamten *Blockchain* bewahrt, da der *Hashwert* des Blocks nicht verändert wird. Dies führt jedoch aller Wahrscheinlichkeit nach zu einem Verlust der Nachvollziehbarkeit und Fälschungssicherheit.[53]

Die Nutzung des *Chameleon Hashs* ermöglicht es, die eigentliche Unveränderbarkeit, die der *Blockchain*-Technologie zugrunde liegt, zu umgehen, indem Änderungen an bereits verifizierten Transaktionen erlaubt werden. Allerdings erfordert diese Implementierung den Einsatz einer zentralen Instanz, welche nach bestimmten Parametern Löschungen vornimmt und dafür die Zuständigkeit innehat.[54]

---

49 Otto Palandt: Kommentar zum Bürgerlichen Gesetzbuch, 77. Auflage, München 2018.
50 Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14).
51 Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).
52 Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14).
53 Mario Martini und Quirin Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ – Neue Zeitschrift für Verwaltungsrecht 26/17 (2017). S. 1251 – 1270.
54 Ebd.

7. Fazit

»Es gibt destruktive Revolutionen, die das Bestehende angreifen. Und es gibt produktive Revolutionen, die den Weg über das Neue gehen und eben dadurch versuchen, das Alte überflüssig zu machen.«[55] Bereits im Jahre 2015 veröffentlichte das World Economic Forum eine Studie, die prognostizierte, dass bis zum Jahre 2025 bereits 10 % des weltweiten Bruttoinlandsproduktes mithilfe der *Blockchain*-Technologie generiert werden.[56]

Darüber hinaus soll die *Blockchain*-Technologie es ermöglichen, u. a. Korruption zu umgehen, indem man Transaktionen direkt miteinander, ohne eine dritte Instanz, tätigt. Doch sind u. U. potenzielle Nutzer in Ländern mit hoher Korruptionsquote oder schwacher Infrastruktur noch nicht in der Lage, die Voraussetzungen für die Teilnahme an einem *Blockchain*-Netzwerk, wie einen PC mit entsprechender Internetgeschwindigkeit, zu nutzen.

Weltweit besitzen heutzutage noch immer fast 1,7 Milliarden Menschen keinen Zugang zu einem Bankkonto, dennoch ist die Mehrheit dieser Menschen im Besitz eines Mobiltelefons.[57] Dieses Ungleichgewicht versucht sich die *Libra Association* zunutze zu machen, zu deren Mitgliedern u. a. Facebook, Uber oder PayPal gehören, indem eine eigene digitale Währung namens *Libra* auf Basis eines *Blockchain*-Netzwerkes etabliert werden soll. Auf diese Weise soll Zugang zu einer einfachen globalen Währungs- und Finanzinfrastruktur für Milliarden von Menschen geschaffen werden, unabhängig von Wohnort, Tätigkeit oder Einkommen. Es handelt sich dabei aktuell jedoch nicht um ein öffentlich zugängliches *Blockchain*-Netzwerk, sondern um ein genehmigungspflichtiges, welches binnen fünf Jahren öffentlich werden soll. Das Mining wird zunächst nur durch die Mitglieder der Libra Association betrieben.[58] Die drohende Konkurrenz scheint dem Kurs der Kryptowährung *Bitcoin* hingegen nicht zu schaden, seit April dieses Jahres steigt der Kurs wieder an. Aktuell ist ein *Bitcoin* rund 9.389 Euro wert.

Für die derzeitigen rechtlichen Herausforderungen im Hinblick auf die *Blockchain*-Technologie lässt sich festhalten, dass es zumindest Lösungsansätze für die

55 Milosz Matuschek: Blockchain – eine Technologie revolutioniert unser ganzes Denken, unter: https://www.nzz.ch/meinung/kommentare/new-kids-on-the-blockchain-ld.1319020 (02.10.2017).

56 World Economic Forum: Deep Shift – Technology Tipping Points and Societal Impact, unter: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (01.09.2015).

57 World Bank Group: The Global Findex Database 2017 Measuring Financial Inclusion and the Fintech Revolution, unter: http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf (01.09.2017).

58 Libra Association: White Paper – An Introduction to Libra, unter: https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf (05.05.2019).

Problematiken gibt, wenn auch nicht alle Hürden ohne Weiteres zu bewältigen sind. Inwieweit diese die Integrität beeinflussen oder der eigentlichen Anwendung abträglich sind, hängt von den Intentionen der Anwender im jeweiligen Einsatzgebiet ab und welche Ziele damit verfolgt werden sollen. Es bedarf keinen neuen gesetzlichen Regelungen, sondern einer entsprechenden Auslegung in Bezug auf die *Blockchain*-Technologie und der Entwicklung von Ausnahmen, wie die Akzeptanz von *Reverse Transactions* zur Erfüllung der Rückabwicklung von einem anfechtbaren Rechtsgeschäft.

Auch aufseiten des Gesetzgebers bleibt abzuwarten, ob nicht noch entsprechende rechtliche Rahmenbedingungen für die *Blockchain*-Technologie geschaffen werden, so wie sie in anderen Ländern bereits implementiert wurden. Die CDU/CSU und die SPD haben in ihrem Koalitionsvertrag bestimmt, wie sie sich in Bezug auf die *Blockchain*-Technologie aufstellen wollen. Darin heißt es u. a., dass sie »eine umfassende Blockchain-Strategie entwickeln und sich für einen angemessenen Rechtsrahmen für den Handel mit Kryptowährungen und Tokens auf europäischer und internationaler Ebene einsetzen wollen.« Ferner sollen »innovative Technologien wie Distributed Ledger erprobt werden und basierend auf diesen Erfahrungen ein Rechtsrahmen geschaffen werden.«[59]

Aber nicht nur auf nationaler Regierungsebene wird die Technologie weiter erforscht. Auch auf europäischer Ebene wurde mit der Europäischen Blockchain-Partnerschaft eine Institution geschaffen, welche in verschiedene Projekte investieren möchte, welche die Nutzung der *Blockchain* unterstützen und fördern.[60] Mitglieder sind nicht nur EU-Mitgliedstaaten, sondern auch einige Mitglieder des europäischen Wirtschaftsraums. Ziel ist es, eine europäische *Blockchain*-Infrastruktur aufzubauen, welche die Bereitstellung grenzüberschreitender digitaler öffentlicher Dienste mit den höchsten Sicherheits- und Datenschutzstandards bis 2020 unterstützt. Außerdem hat es sich die Europäische Kommission zur Aufgabe gemacht, eine internationale Standardisierung der *Blockchain* zu erreichen.[61]

Darüber hinaus hat sie gemeinsam mit dem Europäischen Parlament das European Blockchain Observatory gegründet, welches u. a. *Blockchain*-Initiativen in Europa bündeln und ein transparentes Forum für den Informations- und Mei-

59 Deutsche Bundesregierung: Koalitionsvertrag zwischen CDU/CSU und SPD vom 14. März 2018, unter: https://www.bundesregierung.de/Content/DE/_Anlagen/2018/03/2018–03–14-koalitionsvertrag.pdf?__blob=publicationFile&v=6 (14.03.2018).

60 Europäische Kommission: Erklärung zur Europäischen Blockchain Partnerschaft, unter: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership (10.04.2018).

61 Europäische Kommission: Blockchain Technologies, unter: https://ec.europa.eu/digital-single-market/en/blockchain-technologies (05.05.2019).

nungsaustausch schaffen soll. Ferner sollen u. a. Austausch und Debatten zum Thema *Blockchain* gefördert werden.

Darüber hinaus wurde eine neue Interessenorganisation, die Internationale Vereinigung für vertrauenswürdige Blockchain-Anwendungen, kurz INATBA, gegründet.[62] Ziel der INATBA ist es die Potenziale und Vorteile von *Blockchain* und *Distributed Ledger Technology* auszuschöpfen und Rechtssicherheit, Transparenz und Integrität zu fördern.[63] Fraglich ist hierbei jedoch, inwieweit bei dieser Vielzahl an Einrichtungen die Seriosität noch gewährleistet ist. Gerade bei der Initiative INATBA sind aktuell weder Vertreter von *Ethereum* oder *Bitcoin* vertreten.[64]

Es werden aber nicht nur unzählige Institutionen gegründet, die mit *Blockchain* als Schlagwort werben. Es wird auch in den verschiedensten Branchen nach neuen innovativen Einsatzmöglichkeiten für die Technologie gesucht. So hat beispielsweise die österreichische Post nun eine sogenannte *Crypto Stamp* angeboten. Dabei handelt es sich um Briefmarken, die zum einen aus einer realen Papierbriefmarke und zum anderen aus einem virtuellen Gegenpart bestehen. Der virtuelle Teil ist mit der *Ethereum Blockchain* verknüpft und ermöglicht somit Zugang zur Kryptowährung *Ether*.[65] Ob diese Angebote nun helfen, die *Blockchain* in der Gesellschaft zu etablieren, bleibt fraglich.

Die *Blockchain* soll Vertrauen, Sicherheit und Integrität gewährleisten. Dennoch besteht auch dort ein Sicherheitsrisiko, insbesondere für externe Schnittstellen, welche für das Ein- und Auslesen der Daten benötigt werden. Auch bleibt abzuwarten, ob die verwendeten Algorithmen mit der Zeit überholt werden und inwieweit diese dann noch untereinander kommunizieren können. Der Mangel an Standards im Bereich der *Blockchain*-Anwendungen hat zur Folge, dass die verschiedenen Netzwerke untereinander nicht kompatibel sind. Die Vielzahl an Lösungsansätzen macht es insbesondere für unerfahrene Nutzer schwierig, sich für eine bestimmte Anwendung zu entscheiden.[66]

---

62 Europäische Kommission: Launch of the International Association of Trusted Blockchain Applications – INATBA, unter: https://ec.europa.eu/digital-single-market/en/news/launch-international-association-trusted-blockchain-applications-inatba (05.05.2019).

63 Europäische Kommission: Blockchain Technologies, unter: https://ec.europa.eu/digital-single-market/en/blockchain-technologies (05.05.2019).

64 Block-Builders: INATBA startet: Verband für Blockchains mit Ripple, IOTA und Cardano an Bord, unter: https://block-builders.de/inatba-startet-verband-fur-blockchains-mit-ripple-iota-und-cardano-an-bord/ (05.05.2019).

65 T3n: Die erste Blockchain Briefmarke der Welt gibt's im Onchain-Shop der Österreichischen Post, unter: https://t3n.de/news/krypto-oesterreichische-post-1172058/ (22.06.2019).

66 Bundesamt für Sicherheit in der Informationstechnik: Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen, unter: https://www.bsi.bund.de/SharedDocs/

Ferner bleibt fraglich, wie sich im Gegensatz zu den Institutionen und Forschungsideen die Negativschlagzeilen langfristig auf Kryptowährung und infolgedessen womöglich auch auf die *Blockchain*-Technologie auswirken. So wurden mit *Bitcoins* u. a. auch schon Käufe über die Internetplattform *Silk Road* bezahlt. Dabei handelte es sich um eine Verkaufsplattform im *Dark Web,* auf der u. a. Drogen oder Hacker-Software angeboten wurde, welche bei einem Kauf mit *Bitcoins* bezahlt werden konnten. Das *Dark Web* ist nicht über gängige Webbrowser und Suchmaschinen erreichbar. Es handelt sich um ein anonymisiertes Netzwerk.[67] Allerdings werden sich diese Probleme auf der einen Seite bei einem öffentlich zugänglichen Netzwerk ohne Kontrollinstanz oder Zugangsvoraussetzungen niemals vermeiden lassen. *Silk Road* war nur ein Beispiel für eine Vielzahl illegaler Plattformen im Internet. Erfolgt keinerlei Kontrolle, lässt sich vermuten, dass auch über öffentliche *Blockchain*-Anwendungen illegale Geschäfte getätigt werden oder deren Bezahlung weitestgehend anonym über Systeme wie *Bitcoin* vorgenommen werden.

In jedem Fall bleibt auch in Zukunft noch zu untersuchen, inwieweit die Daten einer *Blockchain* in der realen Welt valide sind. Die Unveränderbarkeit der Daten in der *Blockchain* garantiert nicht zeitgleich auch die Validität der Daten außerhalb der *Blockchain*.[68]

In welche Richtung die *Blockchain*-Technologie steuert, ist derzeit noch nicht abzusehen. Die Technologie bedarf noch einiger Weiterentwicklung, und es wird sich erst in Zukunft herauskristallisieren, ob die angekündigte Revolution durch die *Blockchain*-Technologie tatsächlich eintritt und langfristig Bestand haben wird. In jedem Fall ist aber bei der Vielzahl an Angeboten Vorsicht geboten. Viele Anbieter und Institutionen möchten u. U. von dem Hype um *Blockchain* profitieren, haben letztlich aber kaum Berührungspunkte damit. Nicht überall, wo *Blockchain* draufsteht, ist auch *Blockchain* drin.

Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5 (05.05.2019).

67 Frankfurter Allgemeine Zeitung: Höchststrafe für den Silk Road-Gründer, unter: https://www.faz.net/aktuell/gesellschaft/kriminalitaet/lebenslange-haft-hoechststrafe-fuer-den-silk-road-gruender-13620148.html (30.05.2015).

68 Bundesamt für Sicherheit in der Informationstechnik: Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen, unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5 (05.05.2019).