vbw

Die bayerische Wirtschaft




Studie

# Blockchain und Smart Contracts
# Recht und Technik im Überblick

Eine vbw Studie, erstellt vom Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau

Stand: Oktober 2017

# Vorwort

Neue Digitalisierungstrends und ihre rechtliche Einordnung

---

Die digitale Transformation kann nicht losgelöst von dem Rechtsrahmen betrachtet werden, in dem sich neue Technologien, Produkte oder Geschäftsmodelle bewegen. Unter den zahlreichen aktuellen Trends greift die vorliegende Studie die Blockchain-Technologie heraus, sowie sog. Smart Contracts als einen ihrer möglichen Anwendungsfälle.

Mit der Blockchain-Technologie sollen – je nach konkretem Einsatzgebiet – hohe Transparenz, Manipulationssicherheit, Beschleunigung und Kostenersparnis bei Transaktionen jeder Art möglich werden, und das im Rahmen einer dezentralen Organisation. Die damit verbundenen Chancen sind dementsprechend groß, möglicherweise aber auch das disruptive Potenzial für jene Branchen, die die entsprechenden Transaktionen bisher zentral als Mittelsmann organisieren.

Der Zukunftsrat der Bayerischen Wirtschaft rät in seinen aktuellen Handlungsempfehlungen von 2017 dazu, solche Veränderungen frühzeitig zu identifizieren und zu prüfen, welche Wertschöpfungspotenziale in der neuen Technologie liegen. Mit Pilotprojekten und gezielter Forschung soll insbesondere auch der Staat die Chancen ausloten.

Wichtig für mehr Wertschöpfung am Standort ist, dass auch unser Rechtsrahmen Innovationsoffenheit gewährleistet. Dazu gehört immer, zunächst zu analysieren, wie neue Sachverhalte und neue Technologien nach geltendem Recht zu beurteilen sind, wo sie an Grenzen stoßen und welche Risiken möglicherweise mit ihrem Einsatz verbunden sind. Erst dann kann und muss geprüft werden, wo möglicherweise gesetzgeberisches Handeln vonnöten ist.

Ob gerade die Blockchain nun das „nächste große Ding“ wird, ist dabei letztlich gar nicht entscheidend. Die zunehmend dezentrale Organisation der verschiedensten Lebens- und Arbeitsbereiche im Internet der Dinge wird in jedem Fall eine Technologie benötigen, die auch ohne zentrale Instanz verlässlich Transaktionen dokumentiert. Die hier skizzierten Rechtsfragen stellen sich in ganz ähnlicher Weise bei jeder Anwendung, die das leistet.

Bertram Brossardt
24. Oktober 2017

# Inhalt

# 1 Die Blockchain-Technologie

Ein technologischer Trend im Fokus

Nach Ansicht etlicher Experten ist Blockchain „the next big thing“ oder gar „the next internet“. Andere gehen hingegen davon aus, dass das disruptive Potenzial bzw. die Breitenwirkung überschätzt werde oder aber zumindest praktische Anwendungen noch weit von der Marktreife entfernt seien.

## 1.1 Erwartungen an die Blockchain-Technologie

Was verbirgt sich hinter Blockchain, dieser Technologie, die gar die Finanzwelt revolutionieren, Banken abschaffen und Börsen überflüssig machen können soll? Als Blockchain bezeichnet man – zunächst verkürzt ausgedrückt – eine Datenbank, die von mehreren Teilnehmern („Nodes“) eines Netzwerkes (bestehend aus Clients und sog. Minern) vorgehalten wird und deren Integrität mittels einer fortlaufenden Prüfsumme sowie durch eine kryptographische Verrechnung gewährleistet wird. Der große Vorteil gegenüber konventionellen Datenbanksystemen ist, dass eine einmal in ein solches datenbankbasiertes Register aufgenommene Information nachträglich nicht mehr verändert werden kann.[1] Das gemeinsame und sichere Nutzen von Daten soll somit möglich werden.[2] Der Quellcode für den Einsatz einer Blockchain steht jedem kostenlos im Internet zur Verfügung.[3]

Ein Ziel der Technologie ist es, durch Transparenz und Dezentralisierung Intermediäre von Transaktionen, wie etwa Banken, überflüssig zu machen.[4] Aus diesem Grund versetzt derzeit die Blockchain-Technologie die Finanzwelt in Aufruhr. Ein Zusammenschluss von mehreren namhaften Banken widmet sich dem Thema Blockchain im Finanzwesen.[5] Der potentielle Anwendungsbereich der Blockchain-Technologie geht aber weit über das Finanzwesen hinaus. Er erfasst insbesondere auch Versicherungen, Medien, den Energiesektor sowie die öffentliche Verwaltung, darunter z.B. staatliche Register wie das Grundbuch. In Zukunft könnte es dank Blockchain öffentliche Verzeichnisse geben, die unabhängig von zentralen, kontrollierenden Instanzen sind

[1] https://www.der-bank-blog.de/smarte-vertraege-zahlungsverkehr/technologie/22480/ (abgerufen am 07.08.2017).
[2] *Stanczyk*, VW 2016, 36, 37.
[3] Vgl. *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 23.
[4] *Blocher*, AnwBl 2016, 612, 612; *Kaulartz*, CR 2016, 474, 476.
[5] http://www.sueddeutsche.de/digital/banken-das-naechste-grosse-ding-1.2764410 (abgerufen am 07.08.2017); http://www.wallstreet-online.de/nachricht/7954698-kampf-ums-ueberleben-begonnen-adaption-zerstoerung-finanzindustrie-schmiedet-unheimliche-blockchain-allianz (abgerufen am 07.08.2017); *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 100.

und dennoch ein gleiches oder sogar höheres Maß an Fälschungssicherheit bringen.[6] Zum Teil wird der Technologie daher das Potential zugeschrieben, unser gesamtes Verständnis von Recht und Staat zu verändern.[7]

## 1.2 Technische Funktionsweise

### 1.2.1 Die Distributed Ledger Technology

Die Blockchain ist eine *Distributed Ledger Technology (DLT)*. Der Begriff lässt sich am besten mit *verteilter Datenbanktechnologie* übersetzen. Die Blockchain kann man sich als eine Liste aller in einem *Peer-To-Peer-Netzwerk (P2P-Netzwerk)* vorgenommenen Transaktionen vorstellen.[8] Jeder Teilnehmer, der die zur Nutzung nötige Software bei sich verwendet, nimmt am Netzwerk teil.[9] Das Netzwerk setzt sich daher aus allen teilnehmenden Rechnern („*Nodes*“) zusammen, die über das Internet miteinander kommunizieren, ohne dass dabei eine zentrale Verwaltung nötig wäre.[10] Eine Speicherung der Blockchain erfolgt für gewöhnlich bei allen Nodes. Bei der Installation der gängigsten Software „Bitcoin-Core“ beispielsweise lädt diese automatisch die *aktuelle Blockkette* aus dem Bitcoin-Netzwerk. Dies kann unter Umständen längere Zeit in Anspruch nehmen, ist aber *Garant für die Sicherheit* des Netzes, da in dieser Blockkette alle Transaktionen zwischen den Nutzern des Netzwerkes enthalten sind.[11]

Jede Transaktion ist damit dezentral auf allen im Netzwerk teilnehmenden Rechnern gespeichert; sobald ein Teilnehmer eine Transaktion ausführt, wird sie allen anderen Teilnehmern bekanntgegeben.[12] Eine Transaktion kann dabei jede Art von Information sein. Die Liste der Transaktionen wird in Blöcken fortgeschrieben, die aufeinander aufbauen und jeweils an den vorherigen Block angehängt werden.[13] Der erste Block der Blockchain nennt sich Genesis-Block und wird zu Beginn programmiert. Jeder neue, hierauf folgende Block ist mit den vorherigen mathematisch verbunden, sodass eine Kette von Blöcken, die Blockchain, entsteht.[14]

---

[6] *Blocher*, AnwBl 2016, 612, 616.
[7] http://www.nzz.ch/finanzen/private-finanzen/herausforderung-fuer-banken-und-den-staat-blockchain-der-naechste-wohlstandsschock-ld.17609 (abgerufen am 07.08.2017).
[8] *Heine*, NStZ 2016, 441, 442; *Weber/ Grauer/ Schmid*, WPg 2016, 916, 923.
[9] *Kuhlmann*, CR 2014, 691, 692.
[10] *Kaulartz*, CR 2016, 474, 475.
[11] https://bitcoinblog.de/bitcoin-client/ (abgerufen am 07.08.2017).
[12] *Kaulartz*, CR 2016, 474, 477; *Spancken/ Hellenkamp/ Brown/ Thiel*, Kryptowährungen und Smart Contracts, 2016, S. 12.
[13] *Kütük/Sorge*, MMR 2014, 643.
[14] *Kaulartz*, CR 2016, 474, 476; *Safferling/ Rückert*, MMR 2015, 788, 790; *Holthusen/ Kufeld/ Glatz*, Vorstellung der Blockchain-Technologie, S. 2.

### 1.2.2 Mining

Das Erzeugen eines neuen Blocks wird *Mining* genannt, die Erzeuger der Blöcke *Miner*. Dabei werden die Transaktionen, die noch nicht in der Blockchain gespeichert sind, in den Block aufgenommen. Jeder Nutzer im Bitcoin-Netzwerk kann seine Rechenkapazität nutzen, um „Mining" zu betreiben.[15] Die Miner verarbeiten nicht nur sämtliche Transaktionsdaten,[16] sie sind zugleich das Herz der „Blockchain-Infrastruktur", da nur sie neue Daten in die Blockchain aufnehmen können. Faktisch sind die Miner die *Betreiber* der Blockchain und als solche in der Lage, auf den Betrieb des Systems massiven Einfluss zu nehmen.

Dies erfordert erheblichen Rechenaufwand. Bei dem regulären Blockchain-Nutzer erfolgt keine solche Berechnung, er hat nur Lese- und keinen Schreibzugriff auf die Blockchain. Die Speicherung der gesamten Blockchain dient hier lediglich der Integritätssicherung und der Ankündigung neuer Transaktionen.[17]

Die Miner betreiben oftmals große Rechenzentren, um den notwendigen Rechenaufwand für das Sammeln neuer Transaktionen in Blöcken, die der Blockchain hinzugefügt werden. Als Gegenleistung erhalten die *Miner* neu geschöpfte Bitcoin-Einheiten gutgeschrieben.[18] Seit Juli 2016 sind dies 12,5 Bitcoins[19]. Das Inverkehrbringen von Bitcoins erfolgt damit im Gegensatz zu üblichem Geld ebenfalls dezentral. Aufgrund der Belohnung, die ein Miner für das Bilden eines neuen Blocks erhält, wird derjenige, der über einen großen Anteil an Rechenleistung im Netzwerk verfügt, diesen im Zweifel für die Bildung neuer Blöcke und nicht für Manipulationen nutzen.[20] Um eine Inflation zu vermeiden, ist die Anzahl der Bitcoins, die so erzeugt werden können, auf ca. 21 Millionen Einheiten begrenzt.[21] Je mehr Bitcoins bereits erzeugt wurden, desto komplexer werden die zur Erzeugung notwendigen Rechenschritte.[22]

### 1.2.3 Verifikation

Vereinfacht gesprochen ist in jedem neuen Block ein „digitaler Fingerabdruck"[23] des vorherigen Blocks enthalten. Dieser wiederum enthält die Prüfsumme seines vorhergehenden Blocks usw. Der Vorteil an dieser Verkettung: Wer einen Block manipuliert, d.h.

---

[15] *Hildner*, BKR 2016, 485, 486.
[16] *Spindler/ Bille*, WM 2014 Heft 29, 1357, 1358.
[17] *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 481.
[18] *Pesch/ Bähme,* DuD 2017, 93, 94.
[19] aktuelle Umrechnungskurse abrufbar z.B. unter www.finanzen.net; im August 2017 entsprach ein Bitcoin gut 3.500 Euro. Ob sich das Mining angesichts von Stromkosten etc. voraussichtlich lohnt, kann man etwa mit dem „Bitcoin Mining Calculator" auf der Seite www.99bitcoins.com ermitteln.
[20] *Blocher*, AnwBl 2016, 612, 616.
[21] *Beck*, NJW 2015, 580, 581.
[22] *Beck*, NJW 2015, 580, 581.
[23] *Blocher*, AnwBl 2016, 612, 615.

eine Information nachträglich verändert oder austauscht, würde die gesamte Kette brechen, was alle anderen Teilnehmer des Netzwerks bemerken und deshalb die Anerkennung der Transaktion verweigern würden.[24]

Eine neue Information, die dem Netzwerk von einem Rechner aus mitgeteilt wird, wird dahingehend überprüft, ob sie nicht den vorherigen Blöcken widerspricht.[25] Dieser Verifikationsprozess wird von Teilnehmern des Netzwerkes geleistet, sodass keine zentrale Instanz benötigt wird.[26] Das Netzwerk erkennt nur die längste Kette an Blöcken als richtig an.[27] Alle Transaktionen, die nicht mit der längsten Kette vereinbar sind, werden als ungültig betrachtet,[28] es findet eine Verifizierung durch Konsens statt.[29] Der in der Blockchain gefundene Konsens über Transaktionen ist damit praktisch unveränderlich.[30] Die Verifizierung durch das P2P-Netzwerk ersetzt damit den Intermediär, der in üblichen Verfahren eine Transaktion anerkennt,[31] also beispielsweise die Bank oder das Grundbuchamt. Diese Verifizierung ist notwendig, weil sonst wegen des Fehlens eines Intermediärs nicht klar wäre, welchen Teilnehmern vertraut werden kann, d.h. welche Blöcke korrekt sind.[32]

Der Verifikationsprozess besteht dabei aus zwei Komponenten: Zunächst wird für eine bestimmte Anzahl von Transaktionen ein bestimmter Hashwert (= Zusammenfassung und Überprüfung der vorangegangenen Transaktionen, der o.g. digitale Fingerabdruck) berechnet und dem neuen Block angefügt. Darüber hinaus muss, als weiterer Sicherungsmechanismus, zusätzlich eine kryptographische Rechenaufgabe gelöst werden (*proof of work*).[33] Dem Block werden nach einem bestimmten Schema Bits hinzugefügt und dessen Hashwert immer wieder neu berechnet. Sobald eine bestimmte Anzahl von Nullen am Anfang des Hashwertes vorliegt, ist die Aufgabe gelöst. Dadurch, dass die Lösung der Rechnung vorab bekannt ist, jedoch nicht der Lösungsweg, ist die Berechnung zwar außerordentlich schwierig, die Prüfung des Ergebnisses aber sehr leicht. Zur Aufgabenlösung werden zumeist so lange verschiedene Möglichkeiten ausprobiert, bis eine passende gefunden wird (Zufallsprinzip).

---

[24] *Boehm/ Pesch,* MMR 2014, 75, 76; Kaulartz, CR 2016, 474, 476.
[25] *Kuhlmann*, CR 2014, 691, 693.
[26] *Kütük/ Sorge*, MMR 2014, 643.
[27] *Safferling/ Rückert*, MMR 2015, 788, 790.
[28] *Safferling/ Rückert*, MMR 2015, 788, 790; Tapscott/ Tapscott, Die Blockchain Revolution, 2016, S. 24.
[29] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 6.
[30] *Blocher*, AnwBl 2016, 612, 618.
[31] *Klein*, Blockchains als Verifikationsinstrument für Transaktionen im IoT, in: Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband Herbstakademie 2015, S. 433; *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 5.
[32] http://whitecoin.eu/category/kryptowaehrungen/bitcoin/ (abgerufen am 07.08.2017).
[33] *Meiners*, Bitcoin Mining-Hardware.

Die Schwierigkeit der mathematischen Aufgabe wird in periodischen Abständen an die vorhandene Rechenleistung angepasst, so dass das Zeitfenster der Blockerzeugung konstant bei 10 Minuten verbleibt. Der Schutzmechanismus der kryptographischen Rechenaufgabe ergibt sich aus dessen Komplexität: Die zugrundeliegende Idee geht von der Annahme aus, dass die Rechenkapazität der redlichen Nutzer wesentlich höher ist und somit eine höhere Wahrscheinlichkeit besteht, dass die kryptographische Rechenaufgabe zuerst durch diese gelöst wird.[34]

Wer eine Transaktion nachträglich verändern oder löschen will, muss den Block, in dem die Transaktion gespeichert ist, und alle auf diesem Block aufbauenden Blöcke neu berechnen, weil sie miteinander verknüpft sind.[35] Dabei muss er die restlichen Teilnehmer überholen, die weiterhin die längste Kette mit neuen Blöcken verlängern.[36] Aufgrund des Umstandes, dass bei den für die Blockerzeugung zu lösenden Rechenaufgaben der Zufall eine Rolle spielt, sind diese sehr aufwändig.[37] Durch die Verbindung von Konsensfindung im Netzwerk und der dafür notwendigen Rechenoperationen bietet die Blockchain-Technologie eine hohe Sicherheit gegen Manipulationen.

Viele Nutzer schließen sich zu sogenannten *Miningpools* zusammen, in welchem gemeinsam an dem nächsten *Proof of work* gearbeitet wird.[38] Die erwirtschafteten Bitcoins werden sodann anteilsmäßig an die Miner im Pool aufgeteilt. Die Gefahr, dass ein Nutzer mit unlauteren Absichten auf mehr Rechenleistung als alle redlichen Teilnehmer kommt, ist also theoretisch nicht völlig ausgeschlossen, aber äußerst gering.[39] Wenn allerdings die Mehrheit der Miner in einem Land ansässig ist – wie es gegenwärtig bei Bitcoin mit China der Fall ist – könnte eine dortige staatliche Regulierung durchaus Einfluss auf das System ausüben.

### 1.2.4 Arten von Blockchains (offene und geschlossene)

Im Grundfall der offenen Blockchain steht die Teilnahme jedem frei.[40] Der Nutzer muss sich nicht identifizieren, er kann unter einem Pseudonym auftreten.

Doch auch eine private Blockchain mit Zugangsbeschränkung ist denkbar. Hier ist im Unterschied zur öffentlichen Blockchain dann ein zentraler Betreiber notwendig, der die Zugangsvoraussetzungen zu der privaten Blockchain festlegt und deren Einhaltung

---

[34] Zum Vorstehenden *Entrup*, Bitcoin – Der Stärkere gewinnt, S. 5 f.
[35] *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 480.
[36] *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 480.
[37] *Blocher*, AnwBl 2016, 612, 615 f.
[38] *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 481.
[39] Vgl. *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 481.
[40] *Kaulartz*, CR 2016, 474, 475.

überwacht. Um daran teilnehmen zu können, muss der Betreiber der Blockchain einen Nutzer zuvor zulassen, was in der Regel mit einer Identifizierung einhergeht.[41]

Eine private Blockchain entfernt sich somit bereits deutlich von den Ursprüngen der Technologie, die einen Betreiber gerade überflüssig machen will. Letztlich macht sich der Betreiber hier nur die technischen Vorteile der Blockchain zunutze. Bei einer privaten Blockchain mit einer begrenzten Anzahl an Nutzern sinkt zudem das mit der Blockchain-Technologie erreichbare Niveau an IT-Sicherheit. Denn einerseits geht dies mit einer geringeren Anzahl an Minern einher, die die Validität einer Transaktion überprüfen. Andererseits lebt die Blockchain-Technologie aber auch durch die ständige Fortsetzung der Kette um neue Blöcke und damit um neue Transaktionen. Werden in einer privaten Blockchain nur sporadisch neue Blöcke erzeugt, steigt insofern die Wahrscheinlichkeit, dass ein Angreifer eine kompromittierte Neuberechnung der gesamten Kette vorzunehmen vermag.

Weiterhin können sich die Berechtigungen der Teilnehmer an der Blockchain unterscheiden: Entweder dürfen alle Teilnehmer Transaktionen vornehmen oder nur bestimmte Teilnehmer. Damit sind verschiedene Kombinationen möglich, zwischen denen im Einzelfall je nach Einsatzbereich gewählt werden kann.

*Tabelle 1*
***Übersicht: Unterschiede der verschiedenen Arten einer Blockchain***

| *Art* | *Transparenz (Identifizierung)* | *Dezentralisierung (Verifizierung)* |
|---|---|---|
| **öffentlich** | Alle Transaktionen sind für jeden Teilnehmer des Netzwerks sichtbar, dieser muss sich nicht identifizieren | Kein vertrauenswürdiger Intermediär nötig, da Verifizierung der Transaktionen durch Konsens aller Teilnehmer |
| **privat** | Transaktionen sind nur für zugelassene und identifizierte Teilnehmer einsehbar | Betreiber oder begrenzte Gruppe von Betreibern regelt den Zugang zur Blockchain und nimmt Verifizierung vor |

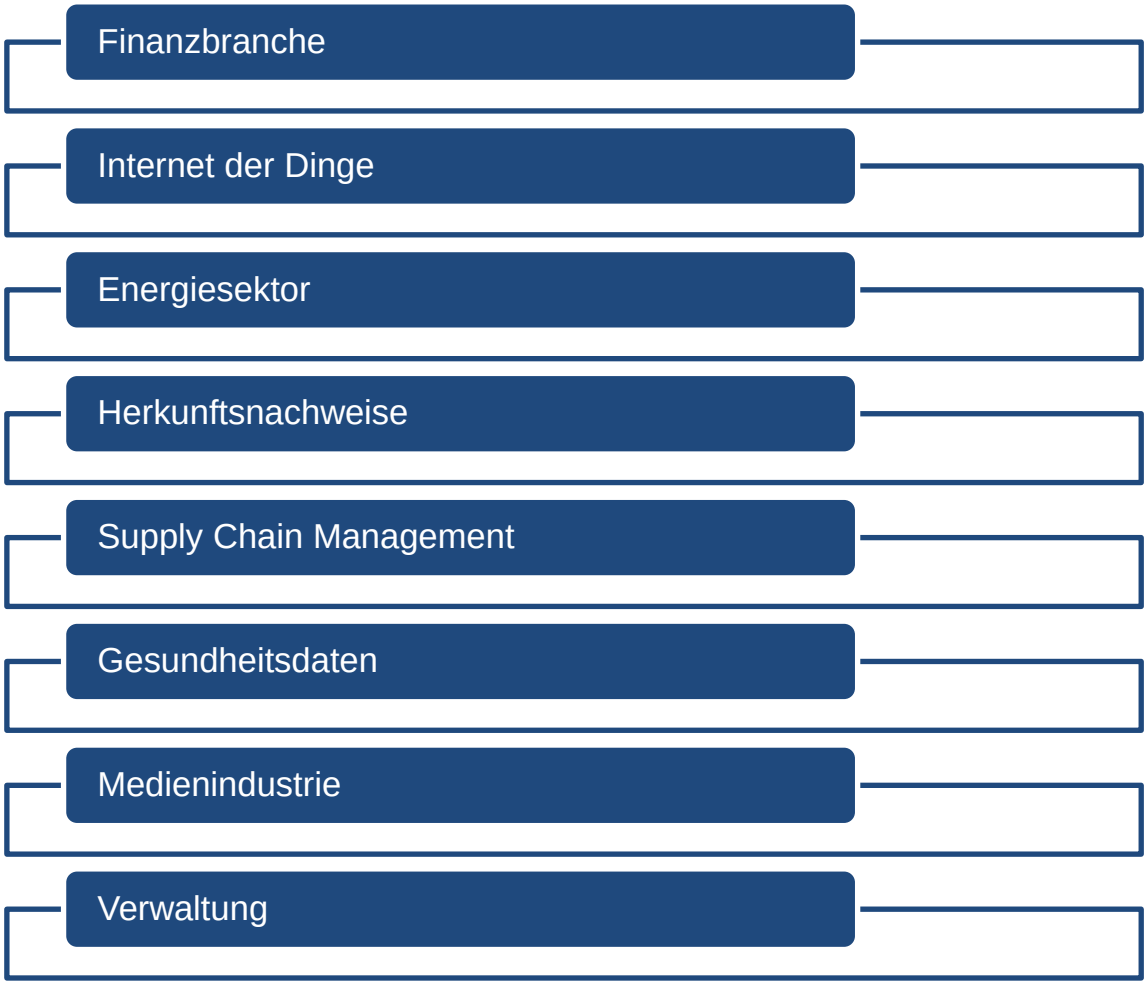
[41] *Kaulartz*, CR 2016, 474, 475.

## 1.3 Anwendungsmöglichkeiten

### 1.3.1 Themenfelder

Die Blockchain-Technologie ist in vielen verschiedenen Bereichen nutzbar, weil sie nur die Grundlage für eigene Anwendungen schafft. Dabei sind jeweils verschiedene Eigenschaften der Blockchain relevant.

*Abbildung 1*
***Übersicht: Anwendungsfelder der Blockchain-Technologie***




Quelle: eigene Darstellung

Eine intensive Untersuchung der Anwendung von Blockchains findet in der Finanzbranche statt. Zum einen kann die Blockchain Zahlungsprozesse beschleunigen und kostengünstiger machen. Zahlungsprozesse sind bislang sehr ressourcenintensiv, da viele Finanzintermediäre involviert sind. Ferner entstehen Zeitverzögerungen, da Abwicklungsprozesse nicht kontinuierlich, sondern nur einige Male pro Tag von statten gehen. Insbesondere bei internationalen Überweisungen ist dies von Belang. Die Anwendung von Blockchain kann hier die bislang hohen Gebühren reduzieren und das Wechselkursrisiko durch eine Reduktion der Transaktionszeit verringern. Zum anderen können Blockchains im Kapitalmarkthandel den direkten Handel zwischen Akteuren ermöglichen. Bis dato ist eine Vielzahl an Akteuren in den Handel eingebunden. Dies bringt hohe Kosten, lange Transaktionszeiten und operationale Risiken mit sich und macht entsprechenden Validierungsprozesse notwendig. Der Einsatz der Blockchain-Technologie kann Transaktionsprozesse vereinfachen und auf Minuten oder gar Sekunden verkürzen. Dadurch werden Kosten minimiert und das operationale Risiko, sowie das Kontrahentenrisiko reduziert. In der Konsequenz könnten sich dadurch die Liquiditäts- und Eigenkapitalanforderungen für Banken potentiell verringern. Ferner kann Blockchain im Bereich Compliance eingesetzt werden. Denkbar ist beispielsweise die Verwendung von Blockchains als Register zur konsolidierten Buchführung oder als „Konsortium-Blockchain“ für Kundendaten. So können Blockchainprozesse dabei helfen, die Kontenführung und Konsolidierung zu automatisieren und somit Fehlverhalten in der Buchhaltung zu verhindern. Auch im Bereich des Wertpapierhandels kann die Blockchain helfen, Vorgänge zu vereinfachen.[42] Der Handel würde schneller ablaufen, da insbesondere private Anleger Aktien ohne Bank in Echtzeit untereinander kaufen und verkaufen könnten. Für Banken, die selbst die Technologie nutzen wollen, bietet sich wegen der vorherigen Identifizierung im Bereich des Zahlungsverkehrs oder des Wertpapierhandels das Einrichten einer privaten Blockchain an.[43] Bei einer privaten Blockchain können die Vorteile der Technologie in einem geschlossenen System genutzt werden.[44] Das macht die Technologie flexibler, entfernt sie aber zugleich von ihren Ursprungsgedanken.[45]

Im auf Dezentralität ausgerichteten Internet der Dinge kann die Blockchain ein Ansatz sein, um die durchgeführten Wertschöpfungsprozesse zu dokumentieren und allen Beteiligten transparent und manipulationsfrei zur Verfügung zu stellen. Dabei muss sichergestellt werden, dass virtuelle Einträge und physische Objekte sicher und eindeutig miteinander verbunden sind. Mit Hilfe von Smart Contracts könnten ferner über Maschinen Vereinbarungen mit Nutzern getroffen werden, deren Einhaltung in beide Richtungen gewährleistet ist. In der Folge können Maschinen „ihre“ Dienstleistungen direkt mit ihren Nutzern selbständig abrechnen. Es ist beispielsweise denkbar, dass

---

[42] Vgl. auch „Blockchain ist keine Revolution“ - Interview mit Prof. Dr. Hans-Gert Penzel, Wirtschaftszeitung August 2017.
[43] *Kaulartz*, CR 2016, 474, 477.
[44] *Tapscott/Tapscott*, Die Blockchain Revolution, 2016, S. 26.
[45] *Tapscott/Tapscott*, Die Blockchain Revolution, 2016, S. 98.

selbstfahrende Autos ohne menschliches Zutun Taxifahrten oder auch an ihnen vorgenommene Wartungsarbeiten abrechnen.

Im Energiesektor könnten Blockchains ein Koordinationsproblem lösen. Der Strommarkt ist von zwei großen Trends geprägt. Zum einen erfolgt die Einspeisung des Stroms nicht mehr nur zentral an wenigen Punkten (den Großkraftwerken), sondern zunehmend dezentral etwa durch einzelne Eigenheimbesitzer mit Photovoltaikanlagen. Zum anderen stellt die hohe Volatilität der Einspeisung von erneuerbarem Strom steigende Anforderungen an die bislang zentral organisierte Koordination von Angebot und Nachfrage. Es liegt daher nahe, nicht nur die Einspeisung, sondern auch die Koordination durch den Einsatz von Blockchains zu dezentralisieren um das Koordinationsproblem zu lösen. Dadurch könnten Prosumer im Netz direkt mit den Endabnehmern handeln, ohne auf ihren jeweiligen Stromanbieter als Intermediäre angewiesen zu sein. In Expertenkreisen wird allerdings auch diskutiert, die zentralisierte Lösung weiter zu verbessern. Daher bleibt abzuwarten, ob Blockchains im Energiesektor tatsächlich Anwendung finden.

Ganz grundsätzlich können Blockchains dabei helfen, die Herkunft von Produkten und Rohstoffen eindeutig nachzuvollziehen, da die verwalteten Transaktionen einer Blockchain irreversibel sind. Für Diamanten wird bereits das Blockchain-basierte System Everledger eingesetzt um Eigentümer und Besitzerwechsel nachzuverfolgen. Eindeutige Herkunftsnachweise (Provenance) sind auch für andere Industriesektoren und Produktarten relevant. Beispielsweise bieten sich Anwendungsmöglichkeiten für die Zulassung von Produkten bei denen nachgewiesen werden muss, dass bestimme Materialien wie Zinn, Wolfram oder Tantal nicht eingesetzt wurden. Auch Hersteller zertifizierte Ersatzteile könnten die Technologie verwenden, um nachzuweisen, dass keine gefälschten Bauteile verwendet wurden.

Im Supply Chain Management können Blockchains Betriebsabläufe sicherer machen und beschleunigen. Zum einen ist im Supply Chain Management eine Vielzahl von Wertschöpfungspartnern durch Leistungsvereinbarungen miteinander verbunden. Dies erfordert eine hohe Integrität des Datenaustausches. Blockchains können dies durch die Irreversibilität der verwalteten Transaktionen gewährleisten. Zum anderen sind Finanzprozesse oft noch manuell und damit deutlich langsamer und fehleranfälliger als die vielfach bereits automatisierte physische Leistungserbringung. Die Verwendung von Blockchains kann hier eine selbständige Transaktionsabwicklung mittels Smart Contracts ermöglichen, die dann unabhängig von der Rechnungserstellung erfolgt. Ferner bieten Blockchains insbesondere im operativen und strategischen Einkauf die Möglichkeit, Prozesse durch die autonome Ausführung von Bestellungen transparenter und effizienter zu gestalten.

Im Gesundheitsbereich könnten Blockchains helfen, den Weg zu einer datengetriebenen, personalisierten Medizin zu ebnen. Im Zeitalter der digitalisierten Medizin liegen immer mehr gesundheitsbezogene Daten vor, deren Auswertung und Verwendung medizinisch sinnvoll erscheint. Diesem Vorhaben stehen bislang aber Fragen des Datenschutzes und der Datensicherheit entgegen. Blockchains könnten hier einen Aus-

weg ermöglichen, indem sie eine transaktionelle und auditierbare Kontrolle über die Verwendung der Daten gewährleisten.

Auch in der Medienindustrie gibt es mögliche Anwendungsfelder. Bislang verhindern uneinheitliche Registrierungs- und Lizensierungsstandards bei Medienprodukten eine korrekte Abrechnung. So sind Verwendungsrechte oft fragmentiert und lokal unterschiedlich. Durch Blockchains könnte ein geteilter, transparenter Aufbewahrungsort für Lizenzinformationen, Metadaten und digitale Inhalte erzeugt werden (Shared Repository), der von mehreren Personen genutzt werde kann. Dieses Lizenzsystem wird dann von einer kleinen Anzahl von berechtigten Marktteilnehmern kontrolliert und völlig transparent betrieben.

Potentielle Anwendungsbereiche in der öffentlichen Verwaltung sind E-Payment, Herkunftsnachweise, Verifikations- und Bestätigungsdienste, Abbildung digitaler Identitäten, sowie Absicherung elektronischer Wahlen. Die Gewährleistung der Integrität von Daten und Dokumenten durch die Blockchain kann zumindest aus Nutzerperspektive eine anwenderfreundliche Alternative zu digitalen Signaturen darstellen. Als mögliche Einsatzbereiche von Blockchain werden im Hinblick auf die nachweisbare, transparente und unveränderbare Dokumentation von Transaktionen ferner öffentlich geführte Register und die Verwaltung von Eigentumsverhältnissen und -übertragungen genannt. In Regionen ohne etablierte staatliche Strukturen kann dadurch insbesondere Vertrauen geschaffen werden; in anderen Regionen der Prozess transparenter und ggf. schneller abgewickelt werden. Erste konkrete Anwendungsbeispiele im öffentlichen Sektor liefert der Vorreiter Estland. Zum einen bietet das Land seit 2015 einen Blockchain-basierten Notardienst namens E-Residency an. Zum anderen verwendet das Land bereits seit einigen Jahren eine Blockchain-ähnliche Technologie, um die Integrität medizinischer Dokumente abzusichern. [46]

Auch darüber hinaus gibt es noch weitere Themenfelder, in denen die Blockchain Verwendung finden kann. Kombiniert man die bereits beschriebenen Vorteile der Blockchain-Technologie mit der Idee der sogenannten *Smart Contracts*, ergeben sich insbesondere für Versicherungen Möglichkeiten, Verträge anhand von Daten automatisch abzuwickeln und anzupassen.[47]

---

[46] Zum Vorstehenden vgl. Prinz, W. und Schulte, A. (2017): *Blockchain - Technologien, Forschungsfragen und Anwendungen*. Positionspapier, Sankt Augustin: Fraunhofer Institute for Applied Information Technology FIT sowie die auf dieser Grundlage erstellte Darstellung in der vbw-Studie *Neue Wertschöpfung durch Digitalisierung*, 2017

[47] Vgl. hierzu noch 1.3.3.

### 1.3.2 Praktische Anwendung: Bitcoin

Die Digitalisierung insgesamt ändert die Märkte und Wertschöpfungsketten in der Finanzwirtschaft grundlegend. Die Blockchain-Technologie kann künftig ein wichtiger Aspekt dieses Wandels sein, da sie droht, Teile des Privatkundengeschäfts im elektronischen Zahlungsverkehr überflüssig zu machen.

Bitcoin und andere digitale Währungen haben im Grunde den gleichen Anwendungsbereich wie übliches Geld.[48] Schon heute können Bitcoins bei vielen Händlern als Zahlungsmittel genutzt werden.[49] Besonders im Internet lassen sich Waren und Dienstleistungen damit erwerben.[50] Bitcoins darf man sich dabei aber nicht wörtlich als virtuelle Münzen vorstellen. Bitcoins gibt es nur in digitaler Form im Sinne von Guthabenbeständen, vergleichbar mit Bankkonten.[51] Ein Zahlungsvorgang entspricht damit einer bloßen Änderung von Daten.[52]

***Bitcoin: Funktionsweise***

---

*Wie die meisten Blockchain-Implementierungen bedient sich Bitcoin gängiger, sogenannter „asymmetrischer" kryptographischer Verfahren, welche es einem Teilnehmer erlaubt, Transaktionen mit einem nur ihm zugänglichen „privaten" Schlüssel zu signieren, der damit als Passwort zur Vornahme seiner Transaktion dient.[53]*

*Die privaten Schlüssel eines Nutzers befinden sich auf seinem Computer oder online in sogenannten Wallets.[54] Die Wallet-Datei kann zwar auf einem physischen Speichermedium abgelegt werden, ist dort aber der Gefahr von Entwendung und Löschung ausgesetzt. Der Inhaber von Bitcoins kann diese auch bei Online-Anbietern speichern, die besondere Sicherheitssysteme bereitstellen, um diesen Gefahren zu begegnen. Zur Verwaltung von Bitcoins gibt es mittlerweile auch passende Apps für Smartphones.[55]*

*Mit Hilfe des dem privaten Schlüssel zugehörigen „öffentlichen" Schlüssels des Teilnehmers, welcher allgemein zugänglich ist, können die anderen Teilnehmer die Gültigkeit der Signatur und damit die Rechtmäßigkeit der Transaktion überprüfen. Der öffent-*

---

[48] *Kuhlmann*, CR 2014, 691, 693.
[49] *Spindler/ Bille*, WM 2014, 1357, 1361.
[50] *Kuhlmann*, CR 2014, 691, 693.
[51] *Beck*, NJW 2015, 580, 581.
[52] *Beck*, NJW 2015, 580, 581.
[53] *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 480; *Kaulartz*, CR 2016, 474, 475; *Kuhlmann*, CR 2014, 691, 693.
[54] *Safferling/ Rückert*, MMR 2015, 788, 790; *Kuhlmann*, CR 2014, 691, 692.
[55] Zum Vorstehenden *Kuhlmann*, CR 2014, 691, 692.

*liche Schlüssel ist im Grunde eine Empfangsadresse (vergleichbar mit einer Kontonummer).*[56]

*Will der Inhaber von Bitcoins diese nun übertragen, greift er mit seinem privaten Schlüssel auf seine Bitcoins zu und sendet sie in Richtung des öffentlichen Schlüssels des Adressaten.*[57] *Mit Absenden der Transaktion erfahren alle Teilnehmer des Netzwerks davon und die Transaktion ist für alle anderen nachvollziehbar.*[58]

*Bitcoins können auf Handelsplattformen wie bitcoin.de gegen Euro umgetauscht werden und umgekehrt. Bei Finanztransaktionen wäre der Nutzer ohne einen Sicherheitsmechanismus nicht daran gehindert, sein virtuelles Geld mehrfach auszugeben.*[59] *Dieses sogenannte Double-Spending-Problem betrifft alle digitalen Güter, da sie nicht rivalisierend sind, d.h. von mehreren Menschen gleichzeitig konsumierbar.*[60] *Aus diesem Grund überprüfen Banken vor einer Überweisung stets, ob das Konto des Überweisenden noch gedeckt ist, das Geld also nicht zuvor bereits ausgegeben wurde.*[61]

*Die Blockchain-Technologie, die auf solche Intermediäre gerade verzichten möchte, löst dieses Double-Spending-Problem in der Weise, dass alle Transaktionen chronologisch gespeichert werden.*[62] *Da auf diese Weise alle Transaktionen in der Blockchain einsehbar sind, sind sie von den anderen Teilnehmern des Netzwerks überprüfbar. Der Blockchain kommt daher eine Publizitätsfunktion zu.*[63] *Aufgrund der Tatsache, dass die Blöcke nur miteinander verkettet werden, sofern sich kein Widerspruch zu einem vorherigen Block ergibt, ist schließlich gewährleistet, dass dieselbe Finanztransaktion nicht an mehrere Empfänger gesendet wird.*[64]

---

Die Transaktionen sind in der Blockchain in sehr kurzer Zeit rechtssicher ausgeführt.[65] Die Verifizierung einer Transaktion durch das Netzwerk dauert bei Bitcoin beispielsweise in der Regel[66] nur wenige Minuten. Besonders Zahlungsvorgänge ins Ausland laufen wesentlicher schneller und ggf. auch günstiger ab als bei der Inanspruchnahme

---

[56] *Sorge/ Krohn-Grimberghe*, DuD 2012, 479, 480; *Kuhlmann*, CR 2014, 691, 693.
[57] *Kuhlmann*, CR 2014, 691, 693; *Kaulartz*, CR 2016, 474, 476.
[58] *Kaulartz*, CR 2016, 474, 477.
[59] *Blocher*, AnwBl 2016, 612, 615.
[60] *Blocher*, AnwBl 2016, 612, 612; *Holthusen/ Kufeld/ Glatz*, Vorstellung der Blockchain-Technologie, S. 2.
[61] *Geiling*, BaFin Journal, Februar 2016, S. 29; *Kaulartz*, CR 2016, 474, 476.
[62] *Blocher*, AnwBl 2016, 612, 615.
[63] *Boehm/ Pesch*, MMR 2014, 75, 76; *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 4.
[64] *Kuhlmann*, CR 2014, 691, 693.
[65] *Kuhlmann*, CR 2014, 691, 694; Boehm/ Pesch, MMR 2014, 75.
[66] Zu einem „Stau“ bei den unbestätigten Bitcoin-Transaktionen vgl. etwa bitcoin.blog.de, Eintrag vom 18.05.2017 (abgerufen am 28.08.2017)

von Banken.[67] Des Weiteren können auch Menschen Transaktionen ausführen, die kein Bankkonto besitzen.[68] Das bietet Vorteile für Einwohner von Staaten ohne entsprechende Zahlungsinfrastrukturen.[69] Der Empfänger der Transaktion, bspw. der Betreiber eines Online-Shops, kann sich sicher sein, dass das Geld eingegangen ist, weil eine einmal in der Blockchain verifizierte Zahlung nicht mehr rückgängig gemacht werden kann.[70] Betrachtet man nun noch die sehr kurze Transaktionszeit,[71] so erleichtert die Akzeptanz von Bitcoins als Zahlungsmittel Händlern ihre Geschäfte. Auch das Europäische Parlament sieht insbesondere die Chance, mit Hilfe der Blockchain-Technologie den elektronischen Handel für Nutzer zu vereinfachen, während sich Risiken in Bereichen wie Aufsicht und Verbraucherschutz ergäben.[72]

Gleichwohl spielt die auf der Blockchain-Technologie basierende Währung Bitcoin im weltweiten Wirtschaftsgeschehen bisher nur eine unbedeutende Rolle. Die Zahl von Bitcoin-Transaktionen steigt jedoch weiterhin an. Wurden Anfang des Jahres 2013 täglich ca. 50.000 Transaktionen abgewickelt,[73] lag die Zahl im Mai 2016 weltweit bei täglich ca. 220.000[74] und im Mai 2017 bereits bei täglich ca. 359.000.[75] Insgesamt wurden mit Stand zum Mai 2017 ca. 221 Millionen Transaktionen über Bitcoin abgewickelt, wobei die Entwicklung im letzten Jahr beinahe linear steigend war. Das Interesse an Bitcoin steigt auch in Deutschland stetig.

### 1.3.3 Smart und Self executing Contracts

Als *Smart Contract* bezeichnet man einen Programmcode, der sich beim Eintritt bestimmter Bedingungen, z.B. einer Kaufpreiszahlung, automatisch ausführt, d.h. es bedarf keines menschlichen Eingreifens und keiner weiteren menschlichen Überprüfung mehr.[76] Damit ist im Extremfall eine staatliche Zwangsvollstreckung nicht mehr nötig.[77] Vereinfacht ausgedrückt: Man muss seinem Vertragspartner nicht vertrauen, weil dieser die Durchführung des Vertrages gar nicht unterlassen kann, sobald die Zahlung eingegangen ist.

---

[67] *Spindler/ Bille*, WM 2014, 1357, 1358; vgl. kritisch hinsichtlich der Anwendbarkeit im einfachen Zahlungsverkehr „Blockchain ist keine Revolution“ - Interview mit Prof. Dr. Hans-Gert Penzel, Wirtschaftszeitung August 2017.
[68] *Boehm/ Pesch*, MMR 2014, 75.
[69] *Boehm/ Pesch*, MMR 2014, 75.
[70] *Spindler/ Bille*, WM 2014, 1357, 1358, *Basu/ Sreenivasan/ Tang*, CRi 2014, 73, 74; Boehm/ Pesch, MMR 2014, 75.
[71] *Kuhlmann*, CR 2014, 691, 694.
[72] Entschließung des Europäischen Parlaments vom 26.05.2016 zu virtuellen Währungen (2016/ 2007(INI)), S. 5.
[73] *Knops*, BKR 2013, 240.
[74] *Goger*, MMR 2016, 431, 432.
[75] https://blockchain.info/de/charts (abgerufen am 07.08.2017).
[76] *McLean/Deane-Johns*, CRi 2016, 97, 99; Kaulartz, CR 2016, 474, 477; Heckmann, CR 2016, R99.
[77] *Blocher*, AnwBl 2016, 612, 618.

Solche Smart Contracts müssen dabei zwar nicht zwingend auf einer Blockchain abgebildet werden. In Betracht kommen hierbei insofern auch einfache Computerprogramme, die zu bestimmten Zeitpunkten oder Ereignissen einen vorher einprogrammierten Programmcode ausführen. Die Hinterlegung in der Blockchain gewährleistet hier aber deren Unverfälschtheit und garantiert insofern, dass der jeweilige, dem Smart Contract zugrundeliegende, Algorithmus auch tatsächlich bei Fälligkeit ausgeführt wird.

***Beispiel***

---

*Das Grundbuch wird mit einer Blockchain verwaltet. In einem Smart Contract ist vorgesehen, dass das Eigentum an einem Grundstück automatisch in der Blockchain umgeschrieben wird, sobald der Käufer den Kaufpreis gezahlt hat. Der Käufer kann die Transaktion nur ausführen, wenn er genügend Bitcoin zur Verfügung hat, weil sie sonst nicht im Einklang mit der Liste aller Transaktionen steht. Geht die Transaktion ein, führt der Smart Contract im Sinne des Wenn-Dann-Prinzips die Änderung in der Blockchain durch, ohne dass der Verkäufer noch mitwirken müsste bzw. könnte. Die Parteien benötigen für den Eigentumswechsel weder ein Notar-Anderkonto noch einen Grundbuchbeamten.*

---

Auch mögliche Vertragsstörungen sollen in der Theorie nicht dazu führen, dass es eines Dritten bedarf, der den Vertrag auslegt: Alle denkbaren Varianten sollen bereits im Programmcode festgelegt sein. An solchen Fantasien bestehen wegen der Komplexität der Fallgestaltungen große Zweifel.[78] Nichtsdestotrotz bietet das Fixieren von Vertragsbedingungen und anderen für den Vertrag relevanten Daten in der Blockchain für die Parteien eine erhöhte Vertragssicherheit und Transparenz.[79] Weil in eine Blockchain jede Information geschrieben werden kann, besteht auch die Möglichkeit, den Vertragstext in einer Blockchain zu fixieren, ohne dabei einen Programmcode vorzusehen, der den Vertrag automatisch ausführt. Auf diese Weise kann die erhöhte Vertragssicherheit auch ohne *Smart Contract* in Anspruch genommen werden.

#### *1.3.3.1* Unterscheidung verschiedener Arten von *Smart Contracts*

Der Begriff des *Smart Contracts* setzt gerade nicht voraus, dass er im eigentlichen Sinne *smart* ist, also eine eigene Intelligenz besitzt.[80] Die Bezeichnung als *automati-*

---

[78] Vgl. *Kaulartz/Heckmann*, CR 2016, 618, 623.
[79] *Glatz*, EuCML 2016, 67; *Kaulartz/Heckmann*, CR 2016, 618, 618; http://www.lto.de/recht/kanzleien-unternehmen/k/smart-contracts-digitale-vertraege-computer-rechteuebertragung/ (abgerufen am 07.08.2017).
[80] *Kaulartz/Heckmann*, CR 2016, 618, 618 f.

*sierter* oder *programmierter Vertrag* ist daher passender.[81] Bei genauerer Betrachtung zeigt sich, dass der Begriff nicht einheitlich verwendet wird:

Einerseits kann der Begriff einen Vertragsschluss mittels Transaktionen meinen, wenn die Parteien den Programmcode als Vertragssprache (vergleichbar mit der Verwendung einer Fremdsprache) nutzen, um ihren Willen auszudrücken.[82] Die Transaktionen können dann als Antrag und Annahme ausgelegt werden.[83] Denn die Gestaltungs- und Formfreiheit aus der Privatautonomie (Art. 2 Abs. 1 GG, § 311 Abs. 1 BGB) erstreckt sich auch auf die freie Wahl der Vertragssprache.[84] Kommt es zum Streitfall vor Gericht, wird es insoweit regelmäßig der Hinzuziehung eines Sachverständigen bedürfen.[85]

Andererseits kann der Begriff *Smart Contract* in der Art verwendet werden, dass die Vertragsparteien einen Vertrag geschlossen haben und der *Smart Contract* nur das Vereinbarte automatisch umsetzen soll.[86] Aus diesem Grund ist auch der Begriff des *Self-executing Contracts* geläufig.[87] Damit ist nur die Umsetzung des zuvor geschlossenen Vertrags durch eine Software gemeint. Die Tatsachen eines rechtlichen Sachverhalts und die Tatbestandsmerkmale einer Rechtsnorm werden auf ihre logischen Bedingungen heruntergebrochen und in einen Code übersetzt.[88] Die Software prüft dann selbstständig, ob diese eingetreten sind und vollzieht das Vereinbarte automatisch.[89] Entscheidende Bedeutung kommt der jeweiligen Ausgestaltung der Transaktionen im Einzelfall zu.[90]

#### *1.3.3.2 Anwendungsbereiche von Smart Contracts*

Aufgrund der hohen Transparenz und der niedrigen Transaktions- und Rechtsdurchsetzungskosten kommt zum einen die Durchführung von Überweisungen in Betracht. Um ein angemessenes Sicherheitslevel zu gewährleisten, wird hier die Nutzung der

---

[81] *Kaulartz/Heckmann*, CR 2016, 618.
[82] *Kaulartz/Heckmann*, CR 2016, 618, 621.
[83] *Kaulartz/Heckmann*, CR 2016, 618, 621.
[84] *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, in: Taeger (Hrsg.), Smart World – Smart Law?, DSRI Tagungsband Herbstakademie 2016, S. 1028 f.; *Börding/Jülicher/Röttgen/v.Schönfeld*, CR 2017, 134, 139; *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1.
[85] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Börding/Jülicher/Röttgen/v.Schönfeld*, CR 2017, 134, 139 m.w.N.
[86] *Kaulartz/Heckmann*, CR 2016, 618, 621.
[87] Vgl. http://www.blockchaintechnologies.com/blockchain-smart-contracts (abgerufen am 07.08.2017).
[88] Vbw-Studie: Die Blockchain Technologie, Kapitel 2.2.3.2
[89] *Djazayeri*, jurisPR-BKR 12/2016.
[90] *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, in: Taeger (Hrsg.), Smart World – Smart Law?, DSRI Tagungsband Herbstakademie 2016, S. 1032.

Blockchain-Technologie erwogen.[91] Self Executing Contracts können auch bei Verträgen zum Einsatz kommen, die nicht spezielle auszuhandelnde Vertragsinhalte betreffen,[92] sondern zum Beispiel regelmäßig erforderliche Lieferungen von Massenwaren. So könnte ein Lebensmittelhersteller von Mehlspeisen einen Self Executing Contract mit Zulieferern zur Nachbestellung von Getreide im Rahmen eines Kaufvertrags einsetzen. Teilweise handelt es sich nicht um Verträge im Rechtssinne, sondern vielmehr um einen automatisierten Leistungsaustausch, vergleichbar mit einem Warenautomaten.[93]

***Beispiel***

---

*Ein Versicherer und ein Versicherungsnehmer schließen einen Versicherungsvertrag in Papierform. In der Blockchain hinterlegen die Parteien einen Programmcode, der beim Eintritt von vorab vereinbarten Messwerten einer Wetterstation, die ebenfalls in die Blockchain gespeist werden, automatisch eine Auszahlung an den Versicherungsnehmer vornimmt.[94] In diesem Fall findet der Vertragsschluss wie üblich statt. Der in der Blockchain hinterlegte Smart Contract übernimmt nur die Ausführung der zuvor vereinbarten Vertragsbedingungen.*

---

Als weiteres konkretes Anwendungsbeispiel für eine automatische Vertragsanpassung wird unter 3.2 der *Smart Contract* nach dem Pay-as-you-drive-Prinzip in der Versicherungsbranche näher beleuchtet. Versicherungen hantieren ähnlich wie Banken täglich mit einer großen Menge an Daten, an deren manipulationssicherer Dokumentation sie ein hohes Interesse haben. Kombiniert man die bereits beschriebenen Vorteile der Blockchain-Technologie mit der Idee der sogenannten *Smart Contracts*, ergeben sich insbesondere für Versicherungen Möglichkeiten, Verträge anhand von Daten automatisch abzuwickeln und anzupassen. Anpassungsklauseln sind in Versicherungsverträgen regelmäßig vorgesehen und lassen sich gut mit einem *Smart Contract* gestalten.

Weitere praktische Anwendungsfälle gibt es aber beispielsweise im Bereich von Industrie 4.0 bzw. des Internet of Things. Man denke nur an die Maschine, die ihre Ersatzteile ordert oder der oftmals zitierte Kühlschrank, der sich selbständig auffüllt.

---

[91] Wenngleich die Blockchain-Technologie vielfach nur durch ihren prominentesten Anwendungsfall Bitcoin bekannt ist, ist ihre Nutzung auch im Rahmen von Bezahlvorgängen in herkömmlichen Währungen möglich.
[92] *Kaulartz/Heckmann*, CR 2016, 622.
[93] *Kaulartz/Heckmann*, CR 2016, 624.
[94] *Kaulartz/Heckmann*, CR 2016, 618, 621; *Heckmann*, CR 2016, R99.

#### 1.3.3.3 Gefahren des Einsatzes von *Smart Contracts*

Potentielle negative Folgen des Einsatzes von Smart Contracts liegen in der technischen Ausgestaltung. Da der Computer im Rahmen eines Smart Contract lediglich den Programmcode ausführt, können bei Programmierfehlern Abweichungen vom vertraglich Vereinbarten vorliegen oder ungewollte Vermögenstransaktionen vorgenommen werden. In derartigen Fällen muss sich zur Rückabwicklung der Instrumente des allgemeinen Zivilrechts bedient werden. Auch unbestimmte Rechtsbegriffe können nicht verarbeitet und Gesetzesverstöße nicht erkannt werden.[95] Mit zunehmender Leistungsfähigkeit von KI kann sich das allerdings ändern.

[95] *Kaulartz/Heckmann*, CR 2016, 623.

# 2 Rechtsrahmen

Zusammenspiel unterschiedlichster Rechtsbereiche

Die Anwendungsfälle der Blockchain-Technologie in den verschiedensten Bereichen werfen eine Vielzahl komplexer Rechtsfragen aus den unterschiedlichsten Gebieten auf – von der zivilrechtlichen Behandlung von Bitcoin-Zahlungsvorgängen oder Smart Contracts einschließlich der Haftungsproblematik über Datenschutz und IT-Sicherheit, aufsichts- und verbraucherschutzrechtliche Fragen bis hin zu strafrechtlichen Aspekten. Einige Fragen insbesondere aus dem Bereich des Vertragsrechts lassen sich mit den heute zur Verfügung stehenden Rechtsnormen lösen. Andere Fragen verlangen in Zukunft nach Entscheidungen des Gesetzgebers, beispielsweise im Hinblick auf die Erfüllung von Formvorschriften[96] oder die Frage, wie viel Verbraucherschutz in dezentralen Netzwerken geboten ist und wie er ggf. gewährleistet werden kann.[97]

## 2.1 Datenschutzrecht

### 2.1.1 Das Spannungsfeld zwischen Transparenz und Datenschutz

Die Blockchain-Technologie und der Datenschutz scheinen auf den ersten Blick zwei unversöhnliche Gegensätze zu bilden. Wie soll ein öffentlich einsehbares Register mit dem Datenschutz vereinbar sein, das dauerhaft und unveränderlich alle Transaktionen jedes Teilnehmers enthält und damit umfassende Transparenz bietet?

Tatsächlich ist Transparenz ein Kernelement der Blockchain.[98] Die Transaktionsdaten in der Blockchain sind leicht zugänglich und von anderen nutzbar.[99] Wer einen *Smart Contract* in die Blockchain schreibt, macht den Vertragsinhalt allen Teilnehmern des Netzwerks zugänglich,[100]sofern nicht der Inhalt der Transaktion verschlüsselt in der Blockchain abgelegt wird.

---

[96] Denkbar wäre es, eine Rechtsnorm des Inhalts zu erlassen, dass eine gesetzlich vorgeschriebene Form durch eine Protokollierung in der Blockchain wirksam ersetzt werden kann, vgl. https://irights.info/artikel/schlaue-vertraege-blockchain-technologie-befluegelt-die-entwickler-phantasien/26991 (abgerufen am 07.08.2017).
[97] vgl. vertiefend zu diesen und weiteren Fragen die Studie Blockchain und Recht, vbw/ Heckmann, 2017
[98] *Von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 35.
[99] *Spindler/Bille*, WM 2014, 1357, 1368.
[100] *Spancken/Hellenkamp/Brown/Thiel*, Kryptowährungen und Smart Contracts, 2016, S. 9.

Im Gegensatz dazu ist zentrales Wesenselement des Datenschutzes, Daten vor ungewollten Einblicken zu schützen.[101] Insbesondere die Grundsätze der Datensparsamkeit und Datenvermeidung, der Zweckbindung[102] sowie der Erforderlichkeit der Datenverarbeitung sind mit der Blockchain-Technologie zunächst nur schwer vereinbar. Allerdings bietet die Technologie zugleich Chancen für den Datenschutz. Die Teilnahme an der Blockchain erfolgt in aller Regel pseudonym, da sich Absender und Adressat lediglich durch eine ID ausweisen müssen.[103] Die Blockchain bietet damit die Möglichkeit *„Privacy by Design"* im Sinne des Art. 25 Abs. 1 EU-DSGVO tatsächlich umzusetzen.[104] Die Chancen für den Datenschutz ergeben sich dabei insbesondere aus der Sicherheit der Technologie auf Grund der kryptographischen Mechanismen und der Möglichkeit der Nutzer, selbst zu entscheiden, welche Daten preisgegeben werden sollen (*„Privacy by Default"*).[105]

### 2.1.2 Anwendbarkeit des Datenschutzrechts in der Blockchain

Ob das BDSG respektive ab 2018 die EU-DSGVO sowie das TMG im Falle einer öffentlichen Blockchain anwendbar sind, ist fraglich. Die Anwendbarkeit wird teilweise mit Verweis darauf abgelehnt, dass die jeweiligen Transaktionen für sich genommen keine personenbezogenen Daten enthalten, sondern lediglich eine pseudonymisierte ID des jeweiligen Nutzers, welche grundsätzlich nicht als personenbezogenes Datum zu werten ist.[106] Dem wird jedoch entgegengehalten, dass diese Transaktionsdaten jedenfalls Angaben über wirtschaftliche beziehungsweise geschäftliche Verhältnisse der Nutzer enthalten und somit personenbeziehbar sind.[107] Theoretisch ist eine Bestimmung des Nutzers hinter der ID möglich.[108] Dann können alle Transaktionen eindeutig zugeordnet werden.[109] Das ist beispielsweise der Fall, wenn sich der Käufer von Bitcoins bei der Plattform, auf der er diese erwirbt, identifiziert. Um sich dagegen zu schützen, besteht jedenfalls bei digitalen Währungen die Möglichkeit, für jeden Zahlungsvorgang eine neue ID zu verwenden.[110] Diese erhält man ohne die Angabe von persönlichen Daten.[111]

---

[101] *Guggenberger*, ZD 2017, 49.
[102] Dieser allgemeine Grundsatz des Datenschutzrechts ist nicht ausdrücklich im BDSG normiert, anders hingegen in der EU-DSGVO, in welcher dieser nunmehr in Art. 5 Abs. 1 Lit. b) EU-DSGVO festgelegt ist, vgl. *Wolff*, in: BeckOK, Datenschutzrecht,18. Edit. Stand: 01.11.2016, Prinzipien, Rn. 14.
[103] *Kaulartz*, CR 2016, 474, 479. Anders stellt sich die Situation dagegen in der privaten Blockchain dar.
[104] *Guggenberger*, ZD 2017, 49.
[105] *Guggenberger*, ZD 2017, 49.
[106] *Kaulartz*, CR 2016, 474, 480.
[107] *Pesch/Böhme*, DuD 2017, 93, 95.
[108] *Chaplin*, CR 2016, R81, R82.
[109] *Von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 35.
[110] *Spindler/Bille*, WM 2014, 1357, 1368.
[111] *Basu/Sreenivasan/Tang*, CRi 2014, 73, 74.

Damit dürften BDSG sowie TMG im Falle einer öffentlichen Blockchain nicht anwendbar sein, sofern für den einzelnen Teilnehmer nicht zusätzliche Möglichkeiten bestehen, andere Teilnehmer zu bestimmen. Sollte der Anwendungsbereich des Datenschutzrechts gleichwohl eröffnet sein, ist auf die Frage nach der verantwortlichen Stelle keine pauschale Antwort möglich.

Beim Einsatz einer privaten Blockchain sind die Nutzer hingegen regelmäßig bekannt, weil sie vorher identifiziert wurden.[112] Dann finden das TMG und BDSG bzw. die Europäische Datenschutz-Grundverordnung Anwendung.[113] In diesem Fall ist der den Zugang regelnde Intermediär verantwortliche Stelle im Sinne des Datenschutzrechts.

Sofern kein gesetzlicher Erlaubnistatbestand vorliegt, ist auf die Einwilligung des Betroffenen im Einzelfall zurückzugreifen. Wie eine solche im Kontext verschiedener Blockchain-Anwendungen rechtskonform eingeholt werden kann, ist derzeit noch fraglich. Konfliktpotential ergibt sich insbesondere daraus, dass die Einwilligung jederzeit frei widerruflich sein muss,[114] dies aber auf Grund der technischen Gestaltung der Blockchain nicht umgesetzt werden kann, da Eintragungen in der Blockchain nicht gelöscht werden können.[115] Im geschäftlichen Bereich kann dieses Defizit möglicherweise durch gesetzliche Speicherpflichten überwunden werden. Zudem bietet die Blockchain, anders als zum Beispiel die Oberfläche eines Webshops, keine Möglichkeit den Einwilligungsprozess als solchen rechtskonform abzubilden.

Noch nicht geklärt ist, wie die Rechte des Betroffenen, zum Beispiel das „Recht auf Vergessenwerden“ (zukünftig in Art. 17 EU-DSGVO normiert), bei Blockchain-Anwendungen, umgesetzt werden soll. Etwaige Löschungs- und Sperransprüche der Betroffenen stehen in einem derzeit noch nicht auflösbaren Konflikt zu der Blockchain-Technologie, welche gerade durch ihre Unveränderbarkeit besticht.

## 2.2 IT-Sicherheitsrecht

Die Anwendung der Blockchain-Technologie kann zudem IT-sicherheitsrechtliche Fragen aufwerfen. IT-Sicherheit bedeutet dabei zunächst, dass die *Verfügbarkeit*, *Integrität*, *Vertraulichkeit* und *Authentizität* des informationstechnischen Systems gewährleistet werden muss.[116] Neben den Vorgaben des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) können auch die Vorgaben des Telemediengesetzes (TMG) einschlägig sein.

---

[112] *Kaulartz*, CR 2016, 474, 480.
[113] *Kaulartz*, CR 2016, 474, 480.
[114] Vgl. dazu *Simitis*, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, § 4a Rn. 94.
[115] *Kuhlmann*, CR 2014, 691, 694.
[116] *Heckmann*, MMR 2006, 280, 281.

Je nach konkreter Ausgestaltung bzw. je nach Einsatzbereich der Blockchain-Technologie kann diese als kritische Infrastruktur im Sinne des § 2 Abs. 10 BSIG gewertet werden. Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die den in § 2 Abs. 10 Nr. 1 BSIG genannten Sektoren, wie zum Beispiel Energie, Finanz- und Versicherungswesen, angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Insbesondere für den Fall, dass Banken, Versicherungen oder große Energieversorger auf die (private) Blockchain-Technologie setzen, ist denkbar, dass diese dem sachlichen Anwendungsbereich des § 2 Abs. 10 BSIG unterfallen. Das wird jedoch erst dann in der Praxis relevant, wenn die Blockchain-Technologie tatsächlich im Geschäftsverkehr eingesetzt wird.

Je nach Ausgestaltung der jeweiligen Blockchain-Anwendung sind auch die Vorgaben des Telemediengesetzes zu beachten. Grundsätzlich unterfallen alle unternehmerischen Telemediendienste der Regelung,[117] insbesondere Online-Shops, Online-Dienste, Cloud-Dienste, SaaS-Dienste.[118] Es spricht daher vieles dafür, dass auch Blockchain-Anwendungen, bei entsprechender Ausgestaltung, als *geschäftsmäßig angebotene Telemedien* gewertet werden können. Sofern der Anwendungsbereich der Norm eröffnet ist, sind gem. § 13 Abs. 7 TMG technische und organisatorische Maßnahmen zu ergreifen, die den Stand der Technik berücksichtigen[119], etwa im Hinblick auf die Verschlüsselungstechnik.

Die Sicherungspflichten bei Telemediendiensten sind allerdings, im Gegensatz zu den Pflichten bei dem Betrieb kritischer Infrastrukturen (vgl. § 8a Abs. 1 BSIG), auf das technisch mögliche und wirtschaftlich zumutbare beschränkt.[120]

## 2.3 Allgemeines Vertragsrecht

### 2.3.1 Grundsätzliche Überlegungen

Die Blockchain wirft auch Fragen der Rechtsgeschäftslehre bzw. des Vertragsrechts auf. Dabei ist allerdings zu beachten, dass die Blockchain-Technologie nicht der Vertragsanbahnung, sondern eher der Dokumentation des Vertragsschlusses und unter Umständen auch der (automatisierten) Durchführung eines Vertrages („smart contract“) dient. So liegt der Anlass bzw. die „Vorgeschichte“ für den Vertragsschluss unter Anwendung der Blockchain-Technologie nach wie vor sowohl in der analogen als auch in der digitalen Welt in Form von klassischen Online-Shops oder mobilen Anwendungen (Applikationen, kurz Apps). Über die Blockchain selbst lassen sich wiederum Willens-

[117] *Lepperhoff/Papendorf*, DuD 2016, 107, 108.
[118] *Bartels/Backer*, DuD 2016, 22.
[119] *Djeffal*, MMR 2015, 716, 718.
[120] *Djeffal*, MMR 2015, 716, 718.

erklärungen und Vertragsschlüsse ebenso abbilden wie über herkömmliche Internetanwendungen. Insofern ist eine genaue Unterscheidung zwischen zwei Ebenen zu beachten: der Ebene außerhalb und innerhalb der Blockchain.

Auf der Ebene außerhalb der Blockchain gelten ausnahmslos die allgemeinen Regeln des Vertragsrechts, sei es mit Blick auf das Recht der Willenserklärungen, die Besonderheiten im elektronischen Geschäftsverkehr in Gestalt der sog. Buttonlösung (§ 312i Abs. 4 BGB) und/oder den gesonderten verbraucherrechtlichen Informationspflichten, z.B. aus Fernabsatzrecht. Betrachtet man etwa die „juristische Sekunde“ vor Abgabe einer Erklärung des Bestellers – gewissermaßen dem „finalen Mausklick“ –, so müssen dem Kunden auch hier angemessene, wirksame und zugängliche technische Mittel zur Verfügung gestellt werden, mit deren Hilfe er Eingabefehler vor Abgabe seiner Bestellung erkennen und berichtigen kann. Denn die Pflichten aus § 312i Abs. 1 Satz 1 Nr. 1 BGB treffen jeden Unternehmer i.S.d. § 14 BGB, der sich zum Zwecke des Vertragsabschlusses über die Lieferung von Waren oder Erbringung von Dienstleistungen der Telemedien bedient, und wobei der Vertragsschluss nicht ausschließlich durch individuelle Kommunikation zwischen den Parteien zustande kam.

Mittels des Instruments Blockchain kann der Vertrag am Ende manifestiert werden, wobei die früheren, darin bereits vorhandenen Daten nicht gelöscht werden, sondern lediglich eine Ergänzung des Datensatzes stattfindet. Die Blockchain ist mithin als eine „neutrale“ Technologie mit der Möglichkeit der Abbildung digitaler Datensätze anzusehen. Sie bietet den Vertragsparteien eine hohe Gestaltungsfreiheit. Unter den diversen denkbaren Anwendungsmöglichkeiten haben bislang Bitcoins und Smart Contracts am meisten Beachtung erfahren. Gerade bei Letzteren stellen sich zahlreiche ungeklärte Fragen aus dem allgemeinen Vertragsrecht (2.3.3; zum Anwendungsszenario Bitcoins siehe 1.3.2 sowie 3.1). Störungen innerhalb der Blockchain werden unter 2.6.2 behandelt.

### 2.3.2 Wahrung von Formvorschriften

Die Formvorschrift der Textform, welche v.a. zur Erfüllung von unternehmerischen Informations- und Mitteilungspflichten eingesetzt werden kann (§ 126b BGB), dürfte regelmäßig bei einer endgültigen Speicherung in der Blockchain erfüllt sein. Ob bei der Verwendung der Blockchain-Technologie eine qualifizierte elektronische Signatur nach Art. 3 Nr. 12 der eIDAS-Verordnung[121] verwendet werden kann, hängt von deren konkreter technischer Ausgestaltung ab. Zusammengefasst kommt es darauf an, ob einer dergestalt digital signierten Erklärung derselbe hohe Stellenwert zukommen kann wie der eigenhändigen Unterschrift des Erklärenden. In der Konsequenz würden solche

[121] VO (EU) Nr. 910/2014; derzeit findet sich in § 126a Abs. 1 BGB noch der – veraltete – Verweis auf das Signaturgesetz, welcher durch das Vertrauensdienstegesetz demnächst ersetzt werden soll.

über die Blockchain abgebildete Erklärungen der elektronischen Form (§ 126a BGB) entsprechen, die in den meisten Fällen auch schriftformersetzend wirkt.

Schreibt ein Gesetz die Mitwirkung eines Dritten - typischerweise eines Notars oder des Gerichts als Hinterlegungsstelle - vor, ist diese bei Einsatz der Blockchain-Technologie bei Vertragsschluss freilich nicht erfüllt. Auch nach dem Sinn und Zweck dieses Formerfordernisses kann eine ggf. rechtspolitisch sinnvolle Anpassung an die neue Technologie nur insoweit befürwortet werden, als es nicht gerade auf die Aufklärungs-, Beratungs- und Warnfunktion etwa der notariellen Beurkundung (§ 128 BGB) ankommt. Gerade Grundstücksgeschäfte sollten damit sinnvollerweise auch in Zukunft nicht lediglich mittels digitaler Transaktionen möglich sein. Auch bei Vorschriften, welche – aus Schutzgesichtspunkten – die gleichzeitige Anwesenheit beider Vertragsparteien vor einem Notar verlangen, worunter etwa der Ehevertrag fällt (§ 1410 BGB), sollte nicht nur nach derzeitiger Rechtslage das Festhalten derartiger Vereinbarungen in der Blockchain nicht formgerecht möglich sein.

Kommt es hingegen alleine auf die vertrauensvolle Anwesenheit einer *Trusted Third Party* an – etwa im Rahmen der Vertragsabwicklung – kann die Ersetzung des neutralen Dritten durch die Blockchain vorteilhaft sein. Dies betrifft jedoch dann nicht mehr die Formbedürftigkeit einzelner Handlungen im engeren Sinne.

### *2.3.3* Besondere vertragsrechtliche Fragen bei *Smart Contracts*

Kapitelübersicht



#### 2.3.3.1 Zurechnung von Willenserklärungen

Ist vorgesehen, dass im Fall des Bedingungseintritts eine Rechtsfolge i.R.e. *Smart Contracts* automatisch ausgelöst wird, können Verpflichtungs- und Verfügungsgeschäft zusammenfallen.[122] Die Verfügung ist – auch wenn sie automatisch ausgeführt wird – eine wirksame menschliche Willenserklärung**,** denn sie ist demjenigen Menschen zure-

[122] *Kaulartz/Heckmann*, CR 2016, 618, 623; Klein, Blockchains als Verifikationsinstrument für Transaktionen im IOT, in: Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband Herbstakademie 2015, S. 434.

chenbar, der den ausgeführten Befehl festgelegt hat.[123] Die menschliche Handlung setzt also die Bedingungen für die Ausführung fest.[124] Diese Zurechnung wird umso problematischer, je mehr die menschliche Mitwirkung in den Hintergrund tritt. Man denke an zwei autonom handelnde Maschinen, beispielsweise wenn eine Waschmaschine selbstständig Waschpulver nachbestellt und dieses automatisch ausgeliefert wird.[125] De lege lata müssen wirksame Willenserklärungen jedoch zwingend auf der Willensbetätigung eines Menschen beruhen.[126] In der Literatur finden sich bereits erste Lösungsansätze zu diesem Problem: Einerseits wird die gesetzliche Verankerung einer elektronischen Person mit eigener Rechtspersönlichkeit (sog. E-Person) befürwortet,[127] andererseits wird über eine generelle Einwilligung der hinter der Maschine stehenden natürlichen Person nachgedacht.[128] Letzteres erscheint vor dem Hintergrund, dass die selbstbestimmte Entscheidung, eigenständig oder mittels Vertreter zu handeln sowie eigenständig zu wirtschaften, natürliche und juristische Personen gerade auszeichnet, um ein Vielfaches vorzugswürdiger.[129]

#### 2.3.3.2 Unbestimmte Rechtsbegriffe

Bei der Verwendung von *Smart Contracts* stellt sich noch ein weiteres Problem: Sie bestehen aus maschinell gesteuerten Wenn-Dann-Beziehungen. Tritt eine Bedingung ein, führt der Vertrag automatisch die Folge aus. Der Programmcode muss aber eindeutig bestimmen können, ob die Bedingung eingetreten ist. *Smart Contracts* bieten sich deshalb nur für Ereignisse und Bedingungen an, die sich in den Kategorien *wahr / falsch* ausdrücken lassen.[130] Unbestimmte Rechtsbegriffe eignen sich hier praktisch nicht.[131] Zu beachten ist überdies, dass programmierte Verträge der Auslegung nicht zugänglich sind; Softwarecode wird vielmehr von Computern nach strikten Regeln interpretiert oder ausgeführt.[132]

---

[123] *Klein*, Blockchains als Verifikationsinstrument für Transaktionen im IOT, in: Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband Herbstakademie 2015, S. 437.
[124] *Klein*, Blockchains als Verifikationsinstrument für Transaktionen im IOT, in: Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband Herbstakademie 2015, S. 437.
[125] *Klein*, Blockchains als Verifikationsinstrument für Transaktionen im IOT, in: Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband Herbstakademie 2015, S. 430, 438.
[126] *Börding/Jülicher/Röttgen/v.Schönfeld*, CR 2017, 134, 139.
[127] *Wendehorst*, NJW 2016, 2609; Djazayeri, jurisPR-BKR 12/2016 Anm. 1.
[128] *Börding/Jülicher/Röttgen/v.Schönfeld*, CR 2017, 134, 139 f.
[129] *Heckmann*, NJW-Aktuell 20/2016, 3; ähnlich *Börding/Jülicher/Röttgen/v.Schönfeld*, CR 2017, 134, 139.
[130] *Kaulartz/Heckmann*, CR 2016, 618, 623.
[131] *Kaulartz/Heckmann*, CR 2016, 618, 620.
[132] *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, in: Taeger (Hrsg.), Smart World – Smart Law?, DSRI Tagungsband Herbstakademie 2016, S. 1031, 1035.

***Beispiel Smart Contracts und unbestimmte Rechtsbegriffe***

*Im Programmcode eines Smart Contracts ist vorgesehen, dass automatisch eine Schadensersatzzahlung ausgelöst wird, sofern eine angemessene Frist abgelaufen ist gem. § 281 Abs. 1 Satz 1 BGB.[133] Der Smart Contract erhält nun die Information, dass seit der Fristsetzung eine Woche vergangen ist. Wenn keine Kriterien für die Angemessenheit der Frist mit im Programmcode verankert sind, bleibt für den Programmcode offen, ob eine Woche eine angemessene Frist darstellt oder nicht. Man könnte die Kriterien, aus denen der Programmcode die Wertung „angemessen" ziehen soll, zwar mit in den Smart Contract einprogrammieren. Dann verliert man jedoch zum einen die Flexibilität des unbestimmten Rechtsbegriffs. Zum anderen entstehen dadurch erhöhte Vertragskosten im Sinne von Transaktionskosten genau wie beim Vereinbaren einer bestimmten Nachfrist. Allgemein können daher sinnvollerweise nur solche Geschäfte über selbstvollziehende Verträge abgewickelt werden, deren Leistungen und Leistungsmodalitäten – bereits im Vorfeld – klar definiert werden können, die digital abbildbar sind[134] und überdies eine geringe Anfälligkeit für Leistungsstörungen aufweisen.[135]*

#### 2.3.3.3 Ausübung von Gestaltungsrechten

Gerade angesichts der aufgezeigten Herausforderungen im Rahmen der praktischen Umsetzung stellt sich die Frage, wie sich die Vertragspartner – im Falle von beachtlichen Irrtümern – wieder von dem Vertrag lösen können. Rechtlich kommt hierbei etwa die Anfechtung in Betracht. Ein denkbarer Einwand des Vertragspartners könnte sein, er habe sich eine falsche Vorstellung vom Inhalt des Vertrages gemacht, welche für seine Erklärung kausal gewesen sei, sodass eine Anfechtung wegen Inhaltsirrtums (§ 119 Abs. 1 Alt. 1 BGB) durchgreifen könnte.[136] Zu beachten ist jedoch, dass der Vertragspartner hierfür darlegungs- und beweispflichtig ist, was zu gewissen Schwierigkeiten bei der Rechtsdurchsetzung führen kann.

Auch die berechtigte Ausübung eines – vertraglichen oder gesetzlichen – Rücktritts- bzw. Widerrufsrechts darf bei einem Smart Contract nicht unmöglich sein. Bei der Rückabwicklung eines hierdurch umgesetzten Vertrages müsste die Selbstvollziehung des Codes außer Kraft gesetzt werden.[137]

---

[133] Vgl. *Kaulartz/Heckmann*, CR 2016, 618, 620.
[134] *Börding/Jülicher/Röttgen/v.Schönfeld*, CR 2017, 134, 138 m.w.N.
[135] *Jacobs/Lange-Hausstein*, ITRB 2017, 10, 13 f.
[136] *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, in: Taeger (Hrsg.), Smart World – Smart Law?, DSRI Tagungsband Herbstakademie 2016, S. 1031; *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1.
[137] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1.

Auch Bedingungen, die in einem Smart Contract formuliert sind, können der AGB-Kontrolle gem. §§ 305 ff. BGB unterliegen.[138] Voraussetzung dafür, dass eine Klausel der AGB-Kontrolle unterliegt, ist gem. § 305 Abs. 1 Satz 1 BGB, dass sie vorformuliert ist. Der hinter dieser Regelung stehende Gedanke liegt in der Standardisierung von Vertragsklauseln im Wirtschaftsleben.[139] Eine Klausel ist dann vorformuliert, wenn vorprogrammierte Teile aus einem vorhandenen Bestand in den Vertrag aufgenommen werden.[140] Bei einem Smart Contract kann – wie bereits ausgeführt – der Vertragstext selbst aus einem in einer Programmiersprache geschriebenen Quellcode für ein Programm bestehen.

***Beispiel für einen Programmcode***

*Statt der Formulierung „Das Eigentum geht mit vollständiger Bezahlung über" nutzen die Parteien den Programmcode*

*„if ($AmountReceived >= $Price) $OwnerDB[$AssetID] = $BuyerID".*[141]

*Beide Male vereinbaren die Parteien einen Eigentumsvorbehalt.*

Davon zu trennen ist wiederum der Fall, dass ein in sonstiger Form geschlossener Vertrag sich bloß selbst ausführt. Dort kann die AGB-Kontrolle auch relevant sein. Es stellt sich jedoch nicht das spezielle Problem, dass der Vertragstext selbst in einer Programmiersprache geschrieben ist.

Gem. § 307 Abs. 1 Satz 1, Satz 2 BGB ist eine Bestimmung in Allgemeinen Geschäftsbedingungen unwirksam, wenn die Bestimmung nicht klar und verständlich ist. Die Vorschrift verfolgt das Ziel, Rechte und Pflichten in Verträgen für den Vertragspartner klar und präzise zu fixieren, damit dieser weiß, worauf er sich einlässt.[142] Damit stellt sich das Problem, dass der Vertrag kaum den Transparenzanforderungen genügen kann, solange viele Menschen keine Programmierkenntnisse besitzen.[143] Das hat zur Folge, dass eine ausschließlich in einer Programmiersprache geschriebene Klausel unwirksam ist, sofern der Verbraucher nicht in der Lage ist, ihren Inhalt nachzuvollziehen. Sicherlich ist es möglich, dem Verbraucher den Programmcode im Einzelfall zu

[138] Vgl. *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, in: Taeger (Hrsg.), Smart World – Smart Law?, DSRI Tagungsband Herbstakademie 2016, S. 1029; *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1.
[139] *Becker*, in: Bamberger/Roth, Beck'scher Online-Kommentar BGB, 41. Edition (Stand 01.05.2016), § 305 Rn. 1.
[140] *Kaulartz/Heckmann*, CR 2016, 618, 622.
[141] Beispiel nach *Kaulartz/Heckmann*, CR 2016, 618, 621.
[142] Stadler, in: *Jauernig*, BGB, 16. Aufl. 2015, § 307 Rn. 6.
[143] http://diepresse.com/home/recht/rechtallgemein/5042568/Wenn-Vertraege-automatisiert-werden (abgerufen am 07.08.2017).

erläutern. Dadurch geht allerdings der Vorteil von AGB verloren, die Vertragskosten infolge Standardisierung gering zu halten. Wer die Vorteile der Standardisierung von Klauseln nutzen möchte, muss daher darauf achten, dass die Inhalte (Bedingungen) des Programmcodes zutreffend und vollständig zum Vertragsgegenstand geworden sind, so dass der Code lediglich deren technische Umsetzung darstellt.
Klauseln im Rahmen eines Smart Contracts dürften schließlich für den Vertragspartner auch nicht überraschend i.S.d. § 305c Abs. 1 BGB sein, nachdem der Vertragsschluss in einer Programmiersprache (auch) von diesem so gewählt wurde.[144]

## 2.4 Verbraucherschutz

Die Blockchain-Technologie kann zu einer verbesserten Durchsetzung von Rechten für Verbraucher führen. Dabei können auch *Smart Contracts* helfen: Da sich diese ohne menschliche Tätigkeit selbst ausführen, erhält der Verbraucher eine ihm zustehende Leistung automatisch, sobald die vertraglichen Bedingungen dafür vorliegen.[145] Die Blockchain ihrerseits stellt die lückenlose Dokumentation sicher.

***Beispiel***

---

*In dem bereits im Rahmen der Anwendungsmöglichkeiten dargestellten Beispiel des Smart Contracts für eine Unwetterversicherung kann sich der Verbraucher sicher sein, dass die Auszahlung erfolgt, sobald die Voraussetzungen eines Schadensfalles vorliegen. Er ist davor geschützt, dass die Versicherung die Auszahlung grundlos verweigert. Dass die Versicherung sich auf eine solche Fixierung des Vertrags in der Blockchain einlässt, ergibt sich daraus, dass sie durch die automatische Abwicklung Kosten sparen kann. Zudem ist sie davor geschützt, dass der Verbraucher unberechtigte Ansprüche geltend macht, weil in der Blockchain gleichfalls die Anspruchsvoraussetzungen dokumentiert sind.*

---

Der bestehende Verbraucherschutz darf nicht dadurch ausgehebelt werden, dass eine neue Technologie beispielsweise von Banken beim Erbringen ihrer Leistungen eingesetzt wird. Normen, die etwa den Darlehensnehmer eines Verbraucherdarlehens nach den §§ 491 ff. BGB schützen, bleiben anwendbar. Zu beachten ist auch, dass der oben skizzierte Effekt einer automatischen Ausführung grundsätzlich auch umgekehrt für die vom Verbraucher zu erbringende Leistung eingreift.

---

[144] *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, in: Taeger (Hrsg.), Smart World – Smart Law?, DSRI Tagungsband Herbstakademie 2016, S. 1030.
[145] *McLean/Deane-Johns*, CRi 2016, 97, 101; *Kaulartz/Heckmann*, CR 2016, 618, 620.

## 2.5 Bankenrecht

Die Speicherung von Informationen in einer Blockchain kann mit dem Bankgeheimnis in Konflikt geraten. Das Bankgeheimnis ergibt sich aus dem Bankvertrag zwischen Bank und Kunden und ist Ausfluss des Prinzips von Treu und Glauben.[146] Aus ihm ergibt sich die Pflicht, über kundenbezogene Tatsachen und Wertungen Verschwiegenheit zu wahren.[147] Dieses Geheimnis gilt für die Bank gegenüber jedem Dritten[148] und gilt selbstverständlich auch im Zahlungsverkehr.[149]

Stellt die Bank also Zahlungsvorgänge in eine Blockchain, in der alle Transaktionen für jeden Teilnehmer einsehbar sind, könnte sie damit gegen diese Pflicht verstoßen. Wie bereits beim Datenschutz erläutert, besteht bei einer Blockchain aber die Besonderheit, dass alle Transaktionen pseudonymisiert sind bzw. sein können. Die Frage ist daher, ob das Bankgeheimnis auch durch das Veröffentlichen von pseudonymisierten Informationen verletzt wird. Dafür spricht die folgende Überlegung: Selbst bei einer Pseudonymisierung ist nicht ausgeschlossen, dass die Informationen einem konkreten Bankkunden zugeordnet werden können. Davor will das Bankgeheimnis gerade schützen; es richtet sich gegen die Mitteilung von kundenbezogenen Informationen an Dritte.[150] Insofern hat das Bankgeheimnis einen engeren Anwendungsbereich als das Datenschutzrecht: Das Datenschutzrecht gilt im Gegensatz zum Bankgeheimnis auch für die bankinterne Verarbeitung von kundenbezogenen Informationen.[151]

Um die Transaktionen so zu verwalten, dass sie nicht für jeden einsehbar sind, bietet sich eine private Blockchain an. Denn diese kann nur von einem begrenzten Personenkreis eingesehen werden. Nutzen jedoch mehrere Banken eine private Blockchain, um Zahlungsvorgänge abzuwickeln, besteht die Gefahr, dass Mitarbeiter der Banken, zu denen der Kunde keine Vertragsbeziehung hat, alle Informationen – wenn auch pseudonymisiert – einsehen können. Das Bankgeheimnis ist zwar nicht verletzt, wenn der Kunde sein Einverständnis zur Offenlegung erklärt.[152] Das Einverständnis wird jedoch beispielsweise bei einer Überweisung nur so weit gehen, wie es für die Durchführung der Überweisung erforderlich ist.

---

[146] *Bunte*, in: Schimansky/Bunte/Lwowski, Bankrechtshandbuch, 4. Aufl. 2011, § 2 Rn. 11.
[147] *Bunte*, in: Schimansky/Bunte/Lwowski, Bankrechtshandbuch, 4. Aufl. 2011, § 2 Rn. 11; Hopt, in: Baumbach/Hopt, Handelsgesetzbuch, 37. Aufl. 2016, V, (7), Rn. A/9.
[148] *Bunte*, in: Schimansky/Bunte/Lwowski, Bankrechtshandbuch, 4. Aufl. 2011, § 7 Rn. 9.
[149] *Häuser*, in: Schmidt, Münchener Kommentar zum Handelsgesetzbuch, 3. Aufl. 2014, Rn. B 285.
[150] *Kahler/Werner*, Electronic Banking und Datenschutz, 2008, S. 194.
[151] *Kahler/Werner*, Electronic Banking und Datenschutz, 2008, S. 194.
[152] *Häuser*, in: Schmidt, Münchener Kommentar zum Handelsgesetzbuch, 3. Aufl. 2014, Rn. B 285.

***Chancen und Perspektiven***

*Sowohl im Datenschutzrecht als auch bei der Entbindung vom Bankgeheimnis stellt der Grundsatz der Erforderlichkeit der Datenerhebung und -verarbeitung eine nicht unerhebliche Hürde dar. Danach dürften nur diejenigen Daten genutzt werden, ohne die die jeweilige Aufgabe – zum Beispiel eine Überweisung – nicht oder nicht vollständig erfüllt werden kann. Richtig verstanden, muss der Grundsatz aber in Abhängigkeit von der jeweils eingesetzten Technologie gesehen werden. Wenn die Blockchain-Technologie für die Durchführung einer Finanztransaktion die Offenlegung von weiteren, nicht für die Transaktion erforderlichen Informationen technisch notwendigerweise verlangt, kann ihr Einsatz nicht bereits deshalb am Grundsatz der Erforderlichkeit scheitern. Es dürfte zu weit gehen, aus dem Grundsatz der Erforderlichkeit zu schließen, dass Unternehmen eine bestimmte Technologie verwenden müssen, weil diese im Vergleich mit anderen Technologien datensparsamer arbeitet. Vielmehr wird sich die Frage, was für eine Transaktion erforderlich ist, auf die Gestaltungsmöglichkeiten beschränken, die eine genutzte Technologie zur Verfügung stellt. Anderenfalls bliebe Unternehmen keine ausreichende Wahlmöglichkeit, welche Technologie sie für ihre Geschäfte verwenden möchten. Der Grundsatz der Erforderlichkeit ist kein unumstößliches Prinzip, sondern immer mit anderen Interessen in Ausgleich zu bringen. Etwas anderes gilt aber dann, wenn im Rahmen einer genutzten Technologie zwei verschiedene Möglichkeiten vorhanden sind, eine Transaktion auszuführen. Dann ist diejenige zu wählen, die weniger Daten benötigt.*

## 2.6 Haftung und Regulierung

### 2.6.1 Ausgangslage

Obwohl die Blockchain-Technologie als sehr sicher eingestuft werden kann, können sich Haftungsfälle ergeben. Die Rechtsdurchsetzung der Geschädigten erschwert in ganz erheblichem Maße ein wesentlicher Punkt: Mangels Betreiber fehlt es zumindest bei der offenen („echten“) Blockchain an der eindeutigen Identifizierbarkeit des Verletzers. Denn in einem P2P-Netzwerk gibt es niemanden, der für die ordnungsgemäße Durchführung von Transaktionen verantwortlich ist.[153] In rechtlichen Kategorien betrachtet, stellt sich damit die zentrale Frage, wer in Bezug auf allgemeine Haftungsregelungen der richtige Anspruchsgegner ist, wenn z.B. technische Defekte oder Manipu-

[153] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 31.

lationen auftreten.[154] Erschwerend tritt der Umstand hinzu, dass sich die Transaktionen nicht rückgängig machen lassen, sondern die Vornahme einer weiteren, auf Wiederherstellung der Ausgangslage gerichteten, Transaktion erforderlich ist. .

### 2.6.2 Mögliche Schadensszenarien

Um sich der Frage nach dem richtigen Anspruchsgegner besser nähern zu können, bietet sich eine Kategorisierung möglicher Schadensszenarien an:

- Zunächst kommen Rechtsverletzungen innerhalb der Blockchain in Betracht. Hierbei fungiert die Blockchain sozusagen als „Tatort“, indem beispielsweise Links auf rechtswidrige Inhalte in der Datenbank gespeichert werden. Ein weiteres denkbares Schadensszenario ergibt sich aus der möglichen Nutzung der Distributed Ledger für bestimmte Register wie z.B. das Zentrale Fahrzeugregister, das Markenregister oder auch das Grundbuch. Ein Teilnehmer könnte hierbei nämlich ein nicht auf ihn eingetragenes Grundstück mittels Blockchain verkaufen und übertragen.[155]
- Das zweite Haftungsszenario betrifft die Störung der Blockchain selbst. In diese Kategorie lassen sich bspw. diejenigen Fälle einordnen, bei denen sich im Nachhinein herausstellt, dass eine Transaktion nicht hätte validiert werden dürfen, weil der Rechner des Miners Doppelausgaben (*Double Spending*) übersehen hat. Dies kann insbesondere dazu führen, dass ein Aktionär dieselbe Aktie mehrfach verkaufen könnte.[156]
- Das dritte Haftungsszenario bilden Störungen, die zwar außerhalb der Blockchain auftreten, allerdings – zumindest mittelbar – Einfluss auf die Blockchain ausüben. Ein konkreter Anwendungsfall in Bezug auf Bitcoins ist dabei dahingehend denkbar, dass der Datenträger, der den privaten Schlüssel zum Signieren von Transaktionen enthält und der den Zugang zum Wallet sowie das Übertragen von Bitcoins erst ermöglicht, zerstört wird. Ohne privaten Schlüssel sind die erhaltenen Transaktionen nämlich wertlos.[157]

---

[154] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 31.
[155] *Bitkom*, Blockchain und #Banking, Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien, S. 38, https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Blockchain/161104-LF-Blockchain-final.pdf (abgerufen am 07.08.2017).
[156] *Bitkom*, Blockchain und #Banking, Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien, S. 38, https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Blockchain/161104-LF-Blockchain-final.pdf (abgerufen am 07.08.2017).
[157] *Kaulartz*, CR 2016, 474, 479.

***Beispiele***

*Als Angriff „von innen" ist etwa ein kollusives Zusammenwirken von mindestens 51% der Miner dahingehend denkbar, als dass Fehler in der Blockchain von allen teilnehmenden Minern ignoriert werden.*

*Im Bereich des Projekts Ethereum, das mit der Kryptowährung Ether die zweitgrößte Marktkapitalisierung nach Bitcoin aufweist und ebenfalls auf der Blockchain-Technologie basiert, sorgte der sog. DAO-Hack jüngst für Aufsehen.[158] Er kann als Beispiel für einen Angriff „von außen" dienen. Der die DAO (dezentrale autonome Organisation) beschreibende Smart Contract enthielt eine sog. Split-Funktion, die es Investoren ermöglichen sollte, aus der Gesellschaft auszuscheiden und das Kapital auf eine Gesellschaft zu transferieren.[159] Die wiederholte Ausführung dieser Funktion ermöglichte es einer Person daraufhin, ca. 3,6 Mio. Ether auf eine Tochtergesellschaft zu transferieren. Dieser Transfer wurde dadurch ermöglicht, dass die Split-Funktion im Smart Contract in unerwünschter Weise auch rekursiv über die Höhe des ursprünglichen Anlagevermögens hinaus ausgeführt werden konnte.[160]*

*Ein weiteres Angriffsszenario „von außen" lässt sich anhand gerichtlicher Sachverhaltskonstellationen aufzeigen. So mussten sich bereits die (Straf-)Gerichte mit illegalem Bitcoin-Mining beschäftigen.[161] Hierbei schaffte es der Angreifer durch die Infizierung der Mining-Rechner mit einer Schadsoftware, ein Botnetz aufzubauen und das hoch performante Rechnersystem so für seine Zwecke zu nutzen.[162] Nach 120 Sekunden Inaktivität des Benutzers setzte sich die Schadsoftware selbstständig mit dem Server des Täters in Verbindung und fragte dort Rechenaufgaben ab, die dem Bitcoin-Mining dienten.[163] Auf diese Weise ersparten sich schließlich auch Täter in den USA Energiekosten in Höhe von 560.887 $ pro Tag, indem sie ein großes Bitcoin-Mining-Netzwerk mit 1,9 Mio. Rechnern mit einer Schadsoftware infizierten.[164]*

[158] Vgl. *Heckmann*, CR 2016, R99.
[159] Vgl. *Heckmann*, CR 2016, R99.
[160] Vgl. *Heckmann*, CR 2016, R99.
[161] BGH, Urt. v. 21.07.2015 - 1 StR 16/15 - NJW 2015, 3463; *Heine*, NStZ 2016, 441.
[162] *Heine*, NStZ 2016, 441.
[163] *Heine*, NStZ 2016, 441.
[164] Heise: Bitcoin-Mining-Botnetz um 500.000 Bots erleichtert, https://www.heise.de/security/meldung/Bitcoin-Mining-Botnetz-um-500-000-Bots-erleichtert-1970116.html (abgerufen am 07.08.2017).

### 2.6.3 Mögliche Anspruchsgegner

Anhand der aufgezeigten ersten Kategorie möglicher Schadensszenarien und des darin erwähnten konkreten Fallbeispiels, dass eine Transaktion von einem tatsächlich dazu nicht Berechtigtem durchgeführt wurde, soll die Problematik in Bezug auf mögliche Anspruchsgegner verdeutlicht werden.

In erster Linie ist an einen Schadensersatzanspruch gegen den unmittelbaren Täter zu denken, der beispielsweise einen ihm nicht gehörenden Gegenstand verkauft hat. Ein solcher Anspruch wird in der Regel bestehen, beispielsweise aus § 823 Abs. 2 BGB i.V.m. § 263 StGB. Wie bei sämtlichen Rechtsverletzungen im Onlinebereich besteht jedoch auch an dieser Stelle die Schwierigkeit, dass ein Vorgehen gegen den unmittelbaren Täter nur selten Erfolg bringt.

Mögliche Haftungsansprüche könnten sich ferner gegen den Software-Hersteller aus einer Verletzung von Produktbeobachtungspflichten (§§ 280 Abs. 1, 823 Abs. 1 BGB) oder der Produkthaftung (§ 1 ProdHaftG; bzw. §§ 823 ff. BGB) in Bezug auf die Software richten, wenn bereits ein Fehler in der verwendeten Software vorliegt. Jedoch ist im Rahmen der Produkthaftung fraglich und bislang nicht abschließend geklärt, ob Software eine bewegliche Sache i.S.d. § 2 ProdHaftG ist.[165] Bei einer Open Source Software kommt als weiteres Problem hinzu, dass es einen Produzenten im engeren Sinne gar nicht gibt.

Damit stellt sich die Frage, ob Unterlassungs- und Beseitigungsansprüche nach den Grundsätzen der sog. (zivilrechtlichen) Störerhaftung geltend gemacht werden können.[166] Die Erzeugung zusätzlicher Blöcke innerhalb einer Bitcoin-Blockchain wird durch die Miner vorgenommen,[167] sodass diese insoweit – in Parallelität zur Verantwortlichkeit bestimmter Knotenpunkte (sog. *Super-Nodes*) in dezentralen Filesharing-Tauschbörsen – als mögliche Anspruchsgegner in Betracht kommen.

Störer ist nach ständiger höchstrichterlicher Rechtsprechung, wer in irgendeiner Weise willentlich und adäquat kausal an der Herbeiführung oder der Aufrechterhaltung einer rechtswidrigen Beeinträchtigung (Störung) mitwirkt, sofern es ihm tatsächlich und rechtlich möglich sowie zumutbar ist, die konkrete Rechtsverletzung zu verhindern und er ihm zumutbare Prüfpflichten verletzt hat.[168] Während man die Kausalität der Störung durch die Miner wohl annehmen kann – die Miner stellen immerhin die Rechenleistung

---

[165] Vgl. *Jaeger/Metzger*, OpenSource, Rechtliche Rahmenbedingungen der Freien Software, 4. Aufl. 2016, Rn. 227.
[166] Die dogmatische Einordnung erfolgt dabei über § 1004 BGB analog, Hoeren, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 43. Ergänzungslieferung 2016, Teil 18.2 Rn. 19.
[167] *Kütük/Sorge*, MMR 2014, 643, 644.
[168] *Hoeren*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 43. Ergänzungslieferung 2016, Teil 18.2 Rn. 27 u.a. unter Verweis auf BGH, Urt. v. 17.05.2001 - I ZR 251/99 - www.ambiente.de; BGH, Urt. v. 15.10.1998 - I-ZR 120/96 - Möbelklassiker.

zur Verfügung und verifizieren die neuen Blöcke - ergeben sich bei der willentlichen Herbeiführung und der Zumutbarkeit der Verhinderung der Beeinträchtigung sowie auch bei der Verletzung zumutbarer Prüfpflichten durchaus erhebliche Bedenken. Gegen eine Verantwortlichkeit spricht schon, dass die entstandenen Fehler für den Miner vielfach nicht vorhersehbar[169] und ihm daher Verhinderungen der Beeinträchtigung nicht zumutbar sein werden.

Mit Blick auf die gegenwärtig bestehende Rechenleistung einer Bitcoin-Blockchain ist eine Manipulation eher unwahrscheinlich,[170] was im Ergebnis für einen nur auf offensichtliche Rechtsverletzungen beschränkten und damit – schon jetzt – für einen äußerst geringen Umfang der Prüfpflichten spricht. Diese Überlegungen führen dazu, dass auch die Inanspruchnahme der Miner unter dem Gesichtspunkt der zivilrechtlichen Störerhaftung zumindest unter den derzeitigen gesetzlichen Voraussetzungen wohl nur in Einzelfällen erfolgreich sein wird.

Ferner stellt sich generell mit Blick auf die zivilrechtliche Verantwortlichkeit – und damit insbesondere unabhängig vom hier gewählten Fallbeispiel – noch die Frage nach einer Haftung der einzelnen Nutzer der Blockchain-Technologie. Unter diesen Kreis an potentiellen Anspruchsgegnern sind einerseits diejenigen Personen zu fassen, welche lediglich an der Blockchain partizipieren, ohne diese zugleich auf ihrem Rechner gespeichert zu haben. Andererseits sollen hierunter auch solche Personen fallen, welche – ohne Miner zu sein – aufgrund vorhandener Speicherkapazitäten die Blockchain bei sich gespeichert haben. Beseitigungs- und damit insbesondere Löschungsansprüche müssen bei den einzelnen Nutzern schon daran scheitern, dass diese keine Möglichkeit besitzen, entsprechende Inhalte zu löschen. In Bezug auf Schadensersatzansprüche stellt sich schlicht die Frage, welchen Kausalbeitrag dem einzelnen (!) Nutzer an einem konkret eingetretenen Schaden zugerechnet werden kann. Die einzelne Blockchain wird bekanntlich vielfach gespiegelt und automatisch synchronisiert, so dass die Beteiligung eines einzelnen Nutzern nicht „conditio sine qua non“ ist, also sehr wohl hinweggedacht werden kann, ohne dass der Erfolg (etwa eine Rechtsgutverletzung) entfiele.

---

[169] *Bitkom*, Blockchain und #Banking, Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien, S. 38, https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Blockchain/161104-LF-Blockchain-final.pdf (abgerufen am: 07.08.2017); *Horner/Kaulartz*, Rechtliche Herausforderungen durch Industrie 4.0 in der Praxis – Die Auswirkungen der Vernetzung von Wertschöpfungsketten auf die anwaltliche Beratung, in: Taeger (Hrsg.), Internet der Dinge, Tagungsband DSRI Herbstakademie 2015, S. 501.

[170] *Entrup*, Bitcoin – Der Stärkere gewinnt, S. 8.

### 2.6.4 Regulierungserfordernisse für Blockchain-Modelle

Blockchain-Modelle müssen u.a. im Bereich des Finanz- oder Energiesektors[171] bestimmte regulatorische Vorgaben einhalten. Ein Beispiel dafür sind die Anforderungen an ein angemessenes und wirksames Risikomanagement aus § 25a Abs. 1 Satz 3 des Kreditwesengesetzes (KWG). Denn das derzeitige Regulierungsrecht geht davon aus, dass es einen organisatorischen und rechtlichen Verantwortlichen gibt.[172] Die Blockchain-Technologie will solche Verantwortliche, die zwischen zwei Parteien stehen, dagegen bewusst ausschalten.[173] Daher wird mit gutem Grund bezweifelt, ob sich eine dezentrale Rechnerstruktur sinnvollerweise überhaupt regulieren lässt.[174]

Das Fehlen eines zentralen Verantwortlichen lässt sich weiter am Beispiel des Geldwäschegesetzes (GwG) veranschaulichen. Ziel des sog. *Know-Your-Customer-Prinzips* ist es, Anonymität zu unterbinden.[175] Das Geldwäschegesetz schreibt deswegen eine Identifizierung von Kunden vor, wozu Kredit- und Finanzdienstleistungsinstitute gem. § 2 Abs. 1 Nr. 1, Nr. 2 GwG angehalten sind. Da die Blockchain ohne einen Dritten auskommt, der vermittelnd zwischen zwei Kunden steht, greift dieser Ansatz ins Leere.[176] Die Europäische Kommission möchte deshalb – zu Recht – bei den Plattformen ansetzen, bei denen der Erwerb von virtuellen Währungen gegen Euro möglich ist.[177] Sie schlägt vor, die Vierte Europäische Geldwäscherichtlinie in der Weise zu ändern, dass die Anbieter dieser Plattformen die Identität ihrer Kunden zuvor prüfen müssen.

Auch bei der Regulierung muss erneut dahingehend differenziert werden, ob es sich um eine offene („echte“) oder private („unechte“) Blockchain handelt. Vor der Aufnahme in eine private Blockchain muss sich der Teilnehmer beispielsweise bei einer Bank identifizieren.[178] Dies hat den Vorteil, dass die angesprochenen Fragen der Regulierung weniger virulent werden, weil die Bank als Verantwortliche auftritt.[179] Bei einer offenen Blockchain hingegen werden die derzeitigen gesetzlichen Anforderungen des Regulierungsrechts nicht erfüllt. Mag die Bewertung aus regulatorischer Sicht damit zwar eindeutig zugunsten der privaten Blockchain ausfallen, so ist dennoch zu beach-

---

[171] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 2.
[172] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 32.
[173] *Gunkel/Richter*, WM 2016, 1517, 1525; von Perfall, in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 32.
[174] *Gunkel/Richter*, WM 2016, 1517, 1525.
[175] *Spindler/Bille*, WM 2014, 1357, 1366.
[176] *Spindler/Bille*, WM 2014, 1357, 1367.
[177] http://europa.eu/rapid/press-release_MEMO-16-2381_de.htm (abgerufen am 07.08.2017).
[178] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 11.
[179] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 5.

ten, dass diese mit dem ursprünglichen Kerngedanken einer öffentlichen und transparenten Technologie bricht.[180]

### 2.6.5 Ausblick

Die beschriebenen haftungsrechtlichen wie regulatorischen Überlegungen sollten deutlich gemacht haben, dass mit den vorhandenen gesetzlichen Bestimmungen die mit der Blockchain-Technologie verbundenen Fragestellungen nur teilweise zufriedenstellend abgebildet werden können. Dies hängt damit zusammen, dass die synallagmatischen Leistungsbeziehungen des BGB in der Grundkonzeption auf das Zweiparteien-System angelegt sind,[181] und insbesondere unsere Rechtsordnung nicht von der Anonymität bzw. Pseudonymität der Rechtssubjekte ausgeht. Dezentrale Netzwerktechnologien wie Blockchain werden in Zukunft jedoch zunehmend an Bedeutung gewinnen und die juristische Auseinandersetzung mit dem Vertragsnetz als Konzeption in Zukunft dringend erforderlich machen.[182] Zugleich steht der Gesetzgeber vor der Herausforderung, eine Überregulierung zu vermeiden, damit Innovationen wie die Blockchain-Technologie auch realisierbar bleiben und nicht „im Keim zu ersticken“ drohen.[183]

---

[180] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 12.
[181] *Börding/Jülicher/Röttgen/v. Schönefeld*, CR 2017, 134, 137.
[182] *Börding/Jülicher/Röttgen/v. Schönefeld*, CR 2017, 134, 137.
[183] *Hildner*, BKR 2016, 485, 495; *Ettl*, Kreditwesen 2016, 15, 16 f.

# 3 Beispielsfälle

Bitcoins und Smart Contracts als Beispiele der rechtlichen Fragestellungen

## 3.1 Fall 1: Der Erwerb von und mit Bitcoins

Die folgenden Ausführungen beziehen sich auf Bitcoin, lassen sich jedoch auf andere digitale Währungen übertragen. Der folgende Beispielsfall eignet sich, um die von Bitcoin aufgeworfenen Fragen diskutieren zu können und Unterschiede zu Sachverhalten aufzuzeigen, bei denen der Kunde bar oder per Überweisung zahlt.

***Beispielfall***

*Ein Kunde sieht in einem Online-Shop eine Ware, die er erwerben möchte. Als er erkennt, dass der Verkäufer als Zahlungsmethode auch Bitcoins akzeptiert, entschließt er sich dazu, diese Möglichkeit zu nutzen. Dazu erwirbt er auf einer Handelsplattform Bitcoins gegen Euro. Sodann bezahlt er die Ware mit den erworbenen Bitcoins. Kurze Zeit später meldet der Händler des Online-Shops Insolvenz an.*

Zunächst stellt sich die Frage, wie Bitcoins sich rechtlich qualifizieren lassen und welche Rechte ihr Inhaber hat. Eindeutig ist, dass Bitcoins mangels Körperlichkeit keine Sachen im Sinne des § 90 BGB sind.[184] Denn es gibt nur Aufzeichnungen über Transaktionen in der Blockchain.[185] An ihnen kann deshalb auch - anders als an Münzen oder Geldscheinen - kein Sacheigentum bestehen.[186] Sie sind ein Immaterialgut.[187] Allerdings besteht an ihnen kein Immaterialgüterrecht, denn für diese gilt der Numerus-Clausus-Grundsatz, wonach Immaterialgüterrechte abschließend gesetzlich geregelt sind. Bitcoins fallen aber unter kein gesetzlich vorgesehenes Recht. Am ehesten kommt ein Urheberrechtschutz in Betracht. Im Falle von Bitcoins fehlt es jedoch an einer persönlichen geistigen Schöpfung im Sinne des § 2 Abs. 2 UrhG.[188] Denn beim *Mining* der Bitcoins führt eine Software mathematische Rechenaufgaben durch. Es handelt sich um einen maschinellen Prozess ohne menschliche Steuerungsmöglichkeit.[189]

[184] *Kuhlmann*, CR 2014, 691, 694; *Kaulartz*, CR 2016, 474, 478.
[185] *Höltge*, ITRB 2016, 215.
[186] *Kuhlmann*, CR 2014, 691, 695.
[187] *Kütük/Sorge*, MMR 2014, 643, 644.
[188] *Kaulartz*, CR 2016, 474, 478; Kuhlmann, CR 2014, 691, 695.
[189] *Kütük/Sorge*, MMR 2014, 643, 644; Kuhlmann, CR 2014, 691, 695; Engelhardt/Klein, MMR 2014, 355, 357.

Da es den Bitcoins an Körperlichkeit und damit der Sacheigenschaft fehlt, kann man sie auch nicht gem. § 929 Satz 1 BGB übertragen.[190] Die Vorschriften für Forderungen in den §§ 413, 398 BGB sind ebenfalls nicht auf Bitcoins anwendbar, weil man durch Bitcoins keine Rechte erhält.[191] Im Hinblick auf die zivilrechtliche Einordnung des Übertragungsvorgangs besteht insoweit also noch Klärungsbedarf.

Die Rechtsordnung stellt den Inhaber von Bitcoins aber nicht schutzlos. Bei Schadensersatzansprüchen kommt § 823 Abs. 2 BGB in Verbindung mit einem Schutzgesetz als Anspruchsgrundlage in Betracht.[192] Als Schutzgesetz ist beispielsweise der Tatbestand der Datenveränderung gem. § 303a StGB heranzuziehen.[193] Unterlassungsansprüche entstehen analog § 1004 Abs. 1 BGB.

Bisher ungeklärt ist, welcher Vertragstyp beim Erwerb von Bitcoins vorliegt. Diese Einordnung ist wichtig, da sich verschiedene Vertragstypen in ihren Rechtsfolgen unterscheiden, beispielsweise hinsichtlich Gewährleistungsrechten. Naheliegend ist es, Bitcoins als sonstigen Gegenstand im Sinne von § 453 Abs. 1 Alt. 2 BGB anzusehen.[194] Das entspricht ihrer Einordnung als Immaterialgut.[195] Dann sind auf den Vertrag wegen der Verweisung die Vorschriften des Kaufrechts in den §§ 433 ff. BGB anwendbar. Zu demselben Ergebnis gelangt man, wenn man den Erwerb als atypischen Kaufvertrag einstuft.[196] Die Anwendung des Kaufrechts ist deswegen angemessen, weil die Vorschriften auch für den Erwerb von ausländischen Währungen gelten.[197]
Eine vom Vertragstyp beim Erwerb von Bitcoins zu unterscheidende Frage ist, was für ein Vertragstyp vorliegt, wenn eine Ware mit Bitcoins bezahlt wird. Den Vertragspartnern ist es wegen der Vertragsfreiheit gestattet, eine Zahlung in Bitcoins zu vereinbaren.[198] Ist eine solche Vereinbarung getroffen, kann der Schuldner die Forderung auch nur durch Absenden der Transaktion gemäß § 362 BGB erfüllen.[199] Die Vertragsfreiheit ist einer der wichtigsten Grundsätze des BGB und ermöglicht den Parteien, Verträge inhaltlich so zu gestalten, wie sie es für sinnvoll halten. Das BGB ist in diesem Punkt bewusst offen gehalten, sodass sich neue Zahlungsarten erfassen lassen.Auf den Vertrag über den Erwerb einer Ware im Austausch gegen eine Bezahlung mit Bitcoins ist das Kaufvertragsrecht – mindestens analog – anwendbar.

---

[190] *Kuhlmann*, CR 2014, 691, 696.
[191] *Kuhlmann*, CR 2014, 691, 696.
[192] *Kuhlmann*, CR 2014, 691, 695; Kaulartz, CR 2016, 474, 479.
[193] *Engelhardt/Klein*, MMR 2014, 355, 356, 358; *Kuhlmann*, CR 2014, 691, 695; *Kaulartz*, CR 2016, 474, 479.
[194] *Kuhlmann*, CR 2014, 691, 694.
[195] *Kuhlmann*, CR 2014, 691, 694.
[196] *Engelhardt/Klein*, MMR 2014, 355, 359.
[197] *Kuhlmann*, CR 2014, 691, 695.
[198] *Engelhardt/Klein*, MMR 2014, 355, 356.
[199] *Beck*, NJW 2015, 580, 585.

Bitcoins werfen steuerrechtliche Fragen auf. Neben der Einkommenssteuerpflichtigkeit ist fraglich, ob beim Umtausch von Bitcoins in andere Währungen Umsatzsteuer zu zahlen ist.[200] Zur Umsatzsteuer hat sich der Europäische Gerichtshof bereits geäußert. Der EuGH entschied, dass Umsätze aus dem Umtausch von Bitcoins in konventionelle Währungen (und umgekehrt) unter die Mehrwertsteuersystemrichtlinie fallen.[201] Gleichzeitig handelt es sich dabei um von der Mehrwertsteuer befreite Umsätze.[202] Gewinne durch Bitcoins sind nach dem Einkommensteuergesetz (EStG) zu versteuern.[203] Die Steuerpflicht folgt aus § 23 Abs. 1 Satz 1 Nr. 2 EStG.[204] Denn Bitcoins fallen unter den Begriff des (sonstigen) Wirtschaftsguts des EStG.[205]

Auch im Hinblick auf aufsichtsrechtliche Fragen sind Bitcoins von Interesse. Für Handelsplattformen ist wichtig zu wissen, ob für gewerbliche Geschäfte mit Bitcoins eine Genehmigung gemäß § 32 Abs. 1 KWG erforderlich ist. Eine solche ist für Bankgeschäfte und Finanzdienstleistungen bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) einzuholen.[206] Die BaFin sieht Bitcoins als Rechnungseinheiten im Sinne von § 1 Abs. 11 Satz 1 Nr. 7 Alt. 2 KWG an und damit als Finanzinstrument.[207] Dies hat zur Folge, dass eine schriftliche Erlaubnis nötig ist.[208] Für den Einsatz von Bitcoins als Zahlungsmittel ist hingegen keine Erlaubnis nötig.[209] Insofern fehlt es an der von § 32 KWG vorausgesetzten Gewerbsmäßigkeit.[210] Dasselbe gilt für den Handel von Waren gegen Bitcoins und für das *Mining*, solange es auf eigene Rechnung geschieht.[211] Dass das Mining keiner Erlaubnis bedarf, obwohl der Miner eigene Rechenleistung für eine Gegenleistung aufwendet, erklärt sich dadurch, dass der Miner kein Bankgeschäft bzw. keine Finanzdienstleistung erbringt. Er nimmt nach Ansicht der BaFin nur an einem bereits bestehenden Markt teil und schafft diesen nicht etwa erst durch Emittieren der Bitcoins.[212]

In der Insolvenz gehören Bitcoins abschließend zum Vermögen des Insolvenzschuldners und damit zur Insolvenzmasse nach § 35 Abs. 1 InsO, da ihnen ein ermittelbarer Preis innewohnt.[213] Um die Möglichkeiten der Zwangsvollstreckung im Zusammenhang mit Bitcoins zu nutzen, muss man sich erneut das Wesen von Bitcoins vor Augen hal-

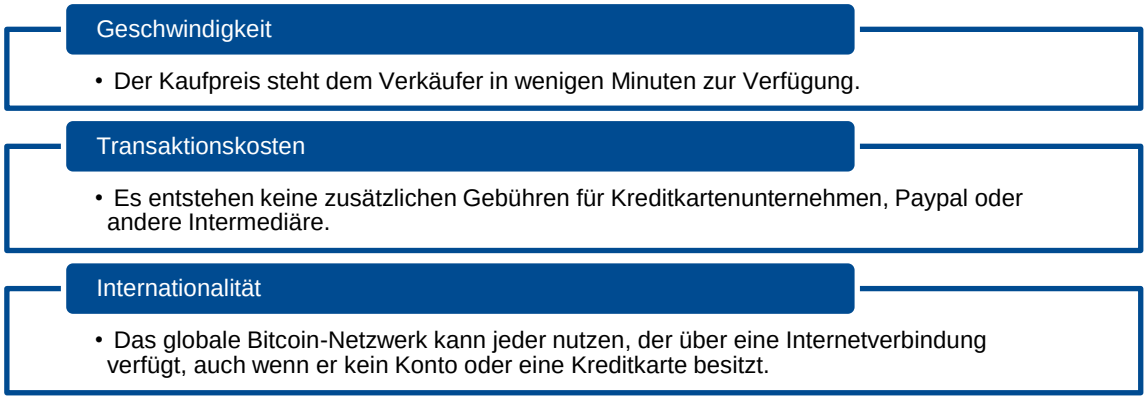
---

[200] Vgl. *Boehm/Bruns* in: Bräutigam/Rücker, Rechtshandbuch E-Commerce, 13. E. Rn. 21 f.
[201] EuGH v. 22.10.2015 - C-264/14 mit Anm. *Pörksen*, jurisPR-ITR 5/2016 Anm. 5.
[202] EuGH v. 22.10.2015 - C-264/14 mit Anm. *Pörksen*, jurisPR-ITR 5/2016 Anm. 5.
[203] *Boehm/Pesch*, MMR 2014, 75, 76.
[204] *Goger*, MMR 2016, 431; Kuhlmann, CR 2014, 691, 696.
[205] *Eckert*, DB 2013, 2108, 2110; Boehm/Pesch, MMR 2014, 75, 76.
[206] *Boehm/Pesch*, MMR 2014, 75, 76.
[207] *Goger*, MMR 2016, 431, 431; *Spindler/Bille*, WM 2014, 1357, 1363; *Sorge/Krohn-Grimberghe*, DuD 2012, 479, 484; *Kaulartz*, CR 2016, 474, 477.
[208] *Spindler/Bille*, WM 2014, 1357, 1365.
[209] *Spindler/Bille*, WM 2014, 1357, 1364.
[210] *Spindler/Bille*, WM 2014, 1357, 1364.
[211] *Schroeder*, JurPC Web-Dok. 104/2014, Abs. 100.
[212] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html (abgerufen am 07.08.2017).
[213] *Kütük/Sorge*, MMR 2014, 643, 645.

ten.[214] Für eine Transaktion benötigt man den privaten Schlüssel.[215] Diesen kennt in der Regel nur der Vollstreckungsschuldner.[216]

Bei der Eingabe des privaten Schlüssels handelt es sich daher um eine unvertretbare Handlung im Sinne von § 888 Abs. 1 ZPO.[217] Im Falle der Weigerung kann der Vollstreckungsgläubiger ferner gem. § 893 Abs. 1 ZPO Schadensersatz verlangen.[218] Doch kann man davon ausgehen, dass der Vollstreckungsschuldner seinen privaten Schlüssel in einer Datei notiert.[219] In diesem Fall ist die Herausgabe der Datei für den Vollstreckungsgläubiger zweckmäßiger.[220] Die Zwangsvollstreckung gestaltet sich damit im Vergleich zu anderen Zahlungsmitteln etwas schwieriger, ist aber nach bestehendem Recht durchführbar.

*Abbildung 2*
***Vorteile der Abwicklung von Zahlungsvorgängen mittels der Blockchain-Technologie***




Quelle: eigene Darstellung

[214] *Kaulartz*, CR 2016, 474, 479.
[215] *Kaulartz*, CR 2016, 474, 479.
[216] *Kütük/Sorge*, MMR 2014, 643, 645.
[217] *Kütük/Sorge*, MMR 2014, 643, 645; *Kaulartz*, CR 2016, 474, 479.
[218] *Kaulartz*, CR 2016, 474, 479.
[219] *Kaulartz*, CR 2016, 474, 479.
[220] *Kaulartz*, CR 2016, 474, 479.

## 3.2 Fall 2: Automatische Vertragsanpassung nach dem Pay-as-you-drive-Prinzip

Im Bereich von *Smart Contracts* für Versicherungen soll mit dem folgenden Beispiel gearbeitet werden.

### *Beispielfall*

---

*Ein Versicherungsnehmer schließt mit seiner Versicherung einen Vertrag ab. Darin ist vorgesehen, dass sich die Versicherungsprämie automatisch erhöht, wenn der Kunde einen riskanten Fahrstil an den Tag legt (sogenanntes Pay-as-you-drive-Prinzip). Zum Erheben dieser Daten besitzt das Auto eine Schnittstelle zur Blockchain. Der in der Blockchain hinterlegte Smart Contract ist so programmiert, dass er die Vertragsänderung automatisch durchführt, sobald die Voraussetzungen dafür vorliegen.*

---

Das Beispiel knüpft an die zunehmende Digitalisierung des Straßenverkehrs an. Dadurch vorhandene Daten können in einer Blockchain nahezu optimal verwaltet werden. Daraus ergeben sich für Versicherungen neue Möglichkeiten, Verträge zu verwalten.

Beim Abschluss des und bei der Ausübung von Rechten aus dem *Smart Contract* können sich zunächst Formfragen stellen. Wird die gesetzlich zwingende Form eines Rechtsgeschäfts nicht eingehalten, so ist das Rechtsgeschäft nichtig (vgl. § 125 Abs. 1 BGB). Im Fall eines Versicherungsvertrags kann beispielsweise das Recht des Versicherers nach § 19 Abs. 2 VVG, bei einer Verletzung der Anzeigepflicht von Gefahrumständen vom Vertrag zurückzutreten, gem. § 21 Abs. 1 Satz 1 VVG nur schriftlich ausgeübt werden. Ein schlichtes automatisches Außerkraftsetzen des Vertrages, das in der Blockchain dokumentiert wird, genügt also nicht.

Für Versicherungen besteht generell die Möglichkeit, Anpassungsklauseln in ihre Verträge aufzunehmen (vgl. § 40 VVG). Daraus folgt aber nicht zwingend die Erlaubnis, den Vertrag auch automatisch per *Smart Contract* anzupassen. Die Ausführung durch den *Smart Contract* muss insbesondere noch mit dem Datenschutzrecht in Einklang stehen.

Die automatische Erhöhung darf nur dann erfolgen, wenn vom Fahrer erhobene Daten sie rechtfertigen. Ein *Pay-as-you-drive-Prinzip* kann grundsätzlich in Bezug auf den Datenschutz rechtskonform umgesetzt werden.[221] Dazu bietet es sich aus Gründen der

---

[221] *Heckmann*, in: vbw, Studie Big Data im Freistaat Bayern Chancen und Herausforderungen, Stand: Juli 2016, S. 101 f.

Datensparsamkeit an, einem Dienstleister, der die Daten zum Fahrverhalten wie Geschwindigkeit und Bremsverhalten analysiert, nicht den Namen des Fahrzeugführers mitzuteilen.[222] Zugleich braucht die Versicherung nicht alle Daten zum Fahrverhalten, sondern nur einen entscheidenden Score-Wert.[223]

In Bezug auf die Schnittstelle des Autos zur Blockchain treten weitere datenschutzrechtliche Fragen auf, die generell unter dem Begriff *Connected Cars* diskutiert werden.[224] Da sie keinen speziellen Bezug zur Blockchain-Technologie aufweisen, sollen sie an dieser Stelle nicht vertieft werden. Die Verknüpfung der Schnittstelle mit der Blockchain kann aber zu einer für den Fahrer ungünstigen Situation führen: Wird der Wagen entwendet und fährt derjenige nicht verkehrsgerecht, so speichert die Blockchain diese fehlerhaften Daten unveränderlich. Diese Unveränderlichkeit ist als Schutz gegen einseitige Manipulationen gerade Sinn und Zweck der Technologie. Damit treten erneut generelle Probleme der Technologie zutage: Die Unabhängigkeit von einer Kontrollinstanz wird durch die Unveränderlichkeit der Informationen erreicht. Da es – jedenfalls in einer öffentlichen Blockchain – keinen zentralen Verantwortlichen gibt, sondern sie dezentral organisiert ist, gibt es selbst für später eindeutig als fehlerhaft festgestellte Sachverhalte keine Möglichkeit zur Löschung. Die Transaktion bleibt fehlerhaft gespeichert. Allerdings lässt sich in manchen Fällen das Ergebnis jedenfalls inhaltlich rückgängig machen: Es kann einfach eine neue, dieses Mal korrekte Information in die Blockchain geschrieben werden.

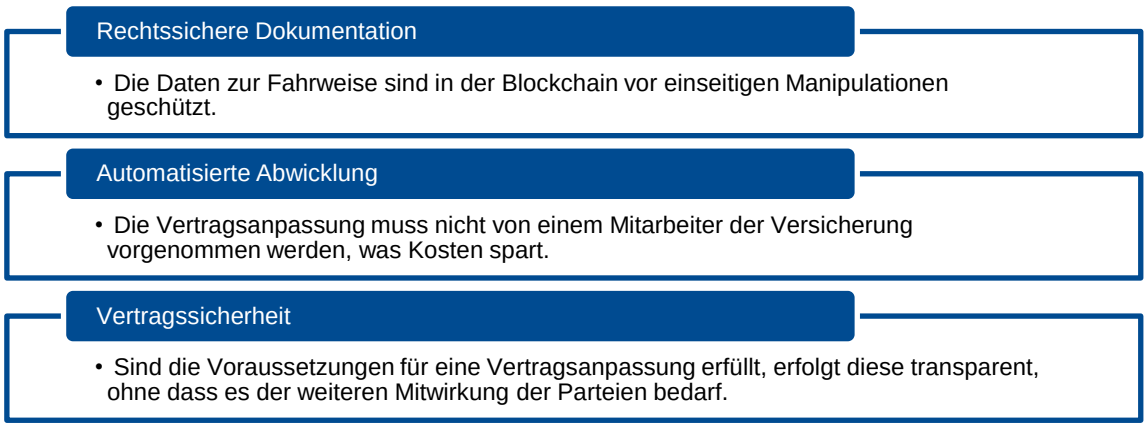
Probleme entstehen aber, wenn die Informationen bereits z.B. durch einen *Smart Contract* weiterverarbeitet wurden und auf ihrer Speicherung basierend Rechtsfolgen ausgelöst wurden. Die Rückabwicklung wird dann mit jedem weiteren bereits ausgeführten Schritt komplexer. Denkbar ist auch, dass der *Smart Contract* seine Ausführung an das Vorliegen einer Information zu einem bestimmten Zeitpunkt knüpft. Dann kann eine zeitlich spätere Speicherung, die nun die korrekten Daten enthält, an seiner Ausführung nichts mehr ändern. Aus der Perspektive der Versicherung kann ein ähnlicher Fall auftreten: Daten können an der Schnittstelle vonseiten des Kunden manipuliert werden, sodass sie für ihn günstig in die Blockchain aufgenommen werden.[225] Im Rahmen einer privaten Blockchain ist zumindest die Korrektur der zu Unrecht aufgenommenen Daten einfacher möglich.

---

[222] *Heckmann*, in: vbw, Studie Big Data im Freistaat Bayern Chancen und Herausforderungen, Stand: Juli 2016, S. 101.
[223] *Heckmann*, in: vbw, Studie Big Data im Freistaat Bayern Chancen und Herausforderungen, Stand: Juli 2016, S. 101 f.
[224] Vgl. dazu *Lüdemann*, ZD 2015, 247 ff.
[225] Vgl. von Perfall, in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 33.

*Abbildung 3*

***Vorteile der Abwicklung von Pay as You Drive Tarifen mittels der Blockchain-Technologie***




Quelle: eigene Darstellung

# 4 Herausforderungen und Grenzen

Einsatzgrenzen und zukünftiger Entwicklungsbedarf

## 4.1 Skalierbarkeit

Grenzen können sich im Hinblick auf die Speicherkapazitäten ergeben, wenn jeder Teilnehmer des Netzwerkes die gesamte Blockchain auf seinem Rechner speichert. Der heutige Speicherbedarf der Bitcoin-Blockchain von ca. 105 GB lässt sich mit handelsüblichen Festplatten noch bewältigen. Doch mit jeder Transaktion wächst die Blockchain weiter an. Der Erfolg einer Blockchain (mehr Teilnehmer bedeuten mehr Transaktionen) stellt damit zugleich ein Risiko dar: Die Skalierbarkeit der Technologie steht infrage.[226] Weil die Blockchain-Technologie durch den Einsatz der *P2P-Kommunikation* problemlos global funktioniert, stellt sich das Problem in besonderem Maße. Mittlerweile sind sogenannte *light clients* verfügbar, die nicht die gesamte Blockchain herunterladen, sondern nur gewisse Teile. Auf diese Weise kann das Problem entschärft werden. Im Fall von *Smart Contracts* sind die *Miner* nicht bloß für die Zusammenfassung von Transaktionen in Blöcken zuständig, sie führen den Code des *Smart Contracts* bei sich aus. *Smart Contracts* sind dezentrale Applikationen (DAPPs).[227] Dem Umfang und der Komplexität des Inhalts solcher Verträge sind damit ebenfalls Grenzen gesetzt.

Als ein weiteres Problem der Skalierbarkeit ergibt sich weiterhin, dass mit der derzeitigen Blockchain-Infrastruktur derzeit etwa sieben Transaktionen pro Sekunde durchführbar sind, was pro Tag 500.000 Transaktionen bedeutet. Alleine in Deutschland werden täglich aber über 70 Millionen und weltweit über eine Milliarde elektronische Transaktionen durchgeführt, sodass die Performance der Blockchain hierfür noch als unzureichend gelten muss.[228]

## 4.2 Effizienz

Die Blockchain Technologie ermöglicht die Konsensfindung in einem dezentralen Netzwerk. Die Art der Lösung ist dabei jedoch alles andere als effizient.[229] Nach aktuellen Schätzungen benötigt eine Bitcoin-Transaktion beispielsweise mehr Strom als ein

[226] https://bitcoinblog.de/2015/08/23/satoshi-nakamoto-ueber-skalierbarkeit/ (abgerufen am 07.08.2017).
[227] *Spancken/ Hellenkamp/ Brown/ Thiel*, Kryptowährungen und Smart Contracts, 2016, S. 7.
[228] „Blockchain ist keine Revolution“ - Interview mit Prof. Dr. Hans-Gert Penzel, Wirtschaftszeitung August 2017.
[229] *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 330.

Haushalt an einem Tag,[230] weshalb die Miner ihre Server oftmals in das billigere Ausland outsourcen. Die Kosten einer einzigen Bitcoin-Transaktion werden derzeit auf etwa 80 Cent geschätzt.[231] Um dieses Problem zu lösen, gibt es alternative Konzepte zur Verifizierung von Transaktionen, die nicht an die Rechenleistung anknüpfen.[232] Das Konzept des *Proof of Stake* knüpft beispielsweise die Wahrscheinlichkeit, dass ein Nutzer einen neuen Block erstellt, an dessen Anteil an der Gesamtwährung.[233] Das erschwert einem Angreifer eine Manipulation in gleicher Weise wie der *Proof of Work*.

## 4.3 Standards

Für die Blockchain-Technologie gibt es noch keine anerkannten Standards. Sowohl für Kryptowährungen als auch für *Smart Contracts* gibt es die unterschiedlichsten Gestaltungen. *Smart Contracts* lassen sich in ganz verschiedenen Programmiersprachen schreiben. Mangels Standards ist der Aufwand für die Verwaltung einer Blockchain zum jetzigen Stand höher als für eine übliche Datenbank. Das gilt auch für das Programmieren komplexer *Smart Contracts*, wobei sich dieser Nachteil durch die geringeren Kosten für die Ausführung ausgleicht.[234] Für die Entwicklung neuer Technologien ist die Entwicklung von Standards jedoch enorm wichtig, da fehlende Standards Investitionen von Unternehmen gefährden.[235] Ohne Standards fehlt zudem die Interoperabilität zwischen verschiedenen Plattformen. Die vielversprechendste Plattform für dezentrale Applikationen ist aktuell Ethereum.[236] Sie bietet ein Grundgerüst, das jedoch genug Freiheiten für Entwickler lässt.

## 4.4 Veränderte Rollen von Verbrauchern und Intermediären

Weil die Blockchain ohne eine Zwischeninstanz auskommt, die zwischen zwei Parteien vermittelt, verändert sich die Rolle der Parteien in der Wertschöpfungskette.

Im Energiesektor spricht man schon heute vom Prosumer, also einem Haushalt, der zugleich Produzent und Konsument ist.[237] Die Blockchain kann dieses Modell weiter stützen, indem sie es Haushalten ermöglicht, Energie direkt und ohne Umwege zu kau-

---

[230] http://blog.frankfurt-school.de/blockchain-technologien-konsens-mechanismen/?lang=de (abgerufen am 07.08.2017).
[231] „Blockchain ist keine Revolution“ - Interview mit Prof. Dr. Hans-Gert Penzel, Wirtschaftszeitung August 2017.
[232] *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 334.
[233] *Spancken/ Hellenkamp/ Brown/ Thiel*, Kryptowährungen und Smart Contracts, 2016, S. 40 f.
[234] *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 142 f.
[235] *Münstermann/ Higginson/ Olesen/ Bohlken/ Ricciardi*, Blockchain in insurance - opportunity or threat, 2016, S. 6.; *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 336.
[236] https://www.ethereum.org/ (abgerufen am 07.08.2017).
[237] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 2..

fen und zu verkaufen.[238] Dieses Modell dürfte sich auf andere Güter übertragen lassen. Das disruptive Potenzial ist im Hinblick auf den ggf. verzichtbaren Intermediär nicht unerheblich, beispielsweise im Finanzbereich. Dort wo die Technik jedoch an Grenzen stößt, werden Intermediäre aber auch weiterhin einen Platz haben. Ferner können durch die neue Technologie auch neue mächtige Intermediäre entstehen, die beispielsweise entsprechende Plattformen schaffen, wie es beispielsweise im Internet mit Suchmaschinen wie Google passiert ist. Zu den möglichen neuen Intermediären zählen neben den Betreibern privater Blockchains bsp. auch Online-Anbieter, bei denen Bitcoins gespeichert werden können.

Dem Verbraucher kommt bei der Nutzung dieser dezentralen Netzwerke eine erhöhte Eigenverantwortung zu.[239] Das stärkt seine Stellung im Markt, wirft aber zugleich die Frage auf, inwieweit eine verbraucherschützende Regulierung hier noch möglich und geboten ist. Die Blockchain-Technologie kann ferner die Position des Verbrauchers bei Regressansprüchen stärken, da die Blockchain beweist, dass eine Transaktion stattgefunden hat. Durch die dezentrale Speicherung ist der Verbraucher vor Manipulationen von Transaktionen sicher.[240] Allerdings können Bitcoins, da sie nur elektronisch vorliegen, auch Gegenstand von Malware- und Hacking-Angriffen werden.[241]

## 4.5 Sicherheit

Hinsichtlich der IT-Sicherheit der Blockchain-Technologie gilt, dass durch die Grundkonzeption als verteilte und durch Hashing gesicherte Datenbank die Verfügbarkeit, Integrität und Authentizität der Transaktionen als gewährleistet gelten darf. Diese Sicherheit steht und fällt jedoch u.a. mit der Sicherheit des verwendeten Hashing-Algorithmus. Hinsichtlich des sog. SHA-1 Hash-Verfahrens gelang es einer Kooperation zwischen der CWI Amsterdam und Google jüngst etwa erstmalig, eine sog. Kollision zu erzeugen, also zwei verschiedene Dokumente mit demselben SHA-1-Wert zu generieren.[242]

Hierdurch wird deutlich, dass die Blockchain-Technologie nicht als Wundermittel für jegliche zukünftigen Gefahrenszenarien gelten darf. Wie jede Sicherheitstechnologie muss diese insofern stets an den jeweils geltenden Stand der Technik angepasst und weiterentwickelt werden. Hierbei ergibt sich bei der Blockchain jedoch die spezifische Besonderheit, dass bereits in die Blockchain geschriebene Transaktionen nicht einfach

---

[238] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 2.
[239] *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 33, 328.
[240] *von Perfall,* in: Blockchain - Chance für Energieverbraucher? - pwc Kurzstudie für die Verbraucherzentrale NRW, 2016, S. 15.
[241] *Höltge*, ITRB 2016, 215.
[242] https://www.heise.de/security/meldung/Todesstoss-Forscher-zerschmettern-SHA-1-3633589.html (abgerufen am 07.08.2017).

auf den Stand der Technik aktualisiert werden können. Soll etwa zukünftig ein aktualisierter Hashing-Algorithmus verwendet werden, müsste dann beispielsweise zunächst eine neue Blockchain eröffnet und die alte Blockchain versiegelt werden.

# 5 Fazit zur Blockchain-Technologie

Blockchain als „das neue Internet“?

Die Blockchain-Technologie hat großes Potenzial, mit ihr lassen sich aber bei Weitem nicht alle Probleme lösen. Gerade im Fall des Einsatzes einer privaten Blockchain ist noch nicht abzusehen, ob sich viele Anwendungen mit einer üblichen Datenbank nicht genauso gut umsetzen lassen. Die Blockchain-Technologie wäre hier dann einfach eine spezielle Technik für konkrete Anwendungsfälle.

Auf der anderen Seite wäre es gut vorstellbar, dass sich die Technologie in ähnlicher Weise gleichsam über Nacht in der Breite durchsetzt, wie zuletzt etwa Cloud Computing. Die Blockchain hat eindeutig disruptives Potenzial, allerdings nur für bestimmte, eingrenzbare Teilbereiche. Für viele Anwendungsfelder scheint sie sehr sinnvolle unterstützende Funktionen zu ermöglichen, beispielsweise im Internet of Things (IoT), ist dafür aber keine notwendige Bedingung. Gleichzeitig steht das IoT exemplarisch für dezentrale Netzwerkanwendungen, deren Bedeutung unzweifelhaft wächst, was die Durchsetzung der Blockchain wiederum befördern könnte.

Das neue Internet wird Blockchain wohl nicht, aber es gilt, die Technologie im Auge zu behalten. Nachdem der Quellcode öffentlich ist[243] und die potenziellen Anwendungsfelder ebenso wie die laufenden Pilotprojekte zahlreich sind, kann man in naher Zukunft viele verschiedene Anwendungen erwarten. Bis sich die Technologie bei Endbenutzern durchsetzt, wird allerdings voraussichtlich noch einige Zeit vergehen.[244] Es bleibt abzuwarten, wie die Technologie Eingang in unseren Alltag finden wird.

Einstweilen gilt es, die Entwicklung aufmerksam zu beobachten und nicht regulativ im Keim zu ersticken,[245] sondern im Gegenteil zu prüfen, an welchen Anwendungsfällen gerade der Staat den Nutzen vergleichsweise risikolos erproben kann.

[243] Vgl. *Tapscott/ Tapscott*, Die Blockchain Revolution, 2016, S. 23.
[244] *Spancken/ Hellenkamp/ Brown/ Thiel*, Kryptowährungen und Smart Contracts, 2016, S. 91.
[245] Vgl. auch *Hildner*, BKR 2016, 485, 495; *Ettl*, Kreditwesen 2016, 15, 16 f.

## Ansprechpartner

**Christine Völzow**
Büroleiterin des Präsidenten
und des Hauptgeschäftsführers

Telefon 089-551 78-104
Telefax 089-551 78-106
christine.voelzow@vbw-bayern.de

## Impressum

Alle Angaben dieser Publikation beziehen sich grundsätzlich sowohl auf die weibliche als auch auf die männliche Form. Zur besseren Lesbarkeit wurde meist auf die zusätzliche Bezeichnung in weiblicher Form verzichtet.

Herausgeber:

**vbw**
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Verfasser:

Prof. Dr. Dirk Heckmann,
Alexander Schmid

Lehrstuhl für Öffentliches Recht,
Sicherheitsrecht und
Internetrecht
Universität Passau

Telefon 0851-509 2290
heckmann@mein-jura.de