BLOCKCHAIN
REALLABOR
RHEINISCHES REVIER

Bericht AP2.4 | Organisatorische, politische und gesellschaftliche Rahmenbedingungen

Philip Sendrowski (Fraunhofer INT) (Hrsg.), Larissa Müller (Fraunhofer INT), Sebastian Brenk (RWTH Aachen TIM), Anna Amft (RWTH Aachen TIM), Christian Gülpen (RWTH Aachen TIM), Kevin Wittek (if(is)), Tina Marquardt (if(is)), Elisaweta Rabovskaja (Universität Münster), Alexander Bauer (Fraunhofer FIT)

März 2020

Inhaltsverzeichnis

1 DIE WICHTIGSTEN ERGEBNISSE IM ÜBERBLICK

Die Ergebnisse des vorliegenden Berichts geben einen Überblick über die aktuellen Erkenntnisse zu gesellschaftlichen, politischen, rechtlichen und organisationalen Rahmenbedingungen der Blockchain-Technologie. Dabei zeigt sich, dass die (wissenschaftliche) Auseinandersetzung mit dem Thema noch in den Kinderschuhen steckt. Vor allem gesellschaftliche und politische Fragestellungen werden momentan noch kaum behandelt, auch sind Forschungslücken kaum definiert. Auf rechtlicher und organisationaler Ebene gibt es hingegen vergleichsweise viele Erkenntnisse, bzw. klar umrissene Forschungslücken. Während wirtschaftliche Akteure schon seit geraumer Zeit Stellung zu dem Thema beziehen, fangen Politik und – zum Teil erst neugegründete – Interessensverbände erst seit verhältnismäßig kurzer Zeit damit an.

Die wichtigsten Ergebnisse der Recherche finden sich hier kurz zusammengefasst. Zu Beginn der Kapitel zu den einzelnen Dimensionen finden sich die jeweiligen Kernaussagen und die Handlungsempfehlungen tabellarisch aufgelistet, mit Verweis in die entsprechenden Kapitel. Dort finden sich dann detailliertere Informationen.

Gesellschaft

Auf gesellschaftlicher Ebene zeigt sich deutlicher Forschungsbedarf, was **Folgenabschätzung** sowie **Akzeptanzfragen** bezüglich der Blockchain-Technologie angeht. Derzeit existieren noch keine relevanten Studien zu gesellschaftlichen Fragestellungen, die sich explizit auf die Blockchain-Technologie beziehen. Abgeleitet aus allgemeinen Erkenntnissen der Technologieakzeptanzforschung kann daher nur empfohlen werden, Nützlichkeit und Bedienbarkeit / Zugänglichkeit von Blockchain-Anwendungen in den Vordergrund zu stellen, um Akzeptanz in der Bevölkerung zu fördern.

Ein großes Akzeptanzproblem zeichnet sich beim **Umweltschutz** ab. Die Bitcoin-Blockchain ist der bekannteste Vertreter der Technologie, wenn auch technologisch gesehen einer der primitivsten und energietechnisch ineffizientesten. Vielfach werden Blockchain und Bitcoin jedoch gleichgesetzt, und der massive Energiebedarf von Bitcoin auf die gesamte Technologie projiziert. Hier durch Information, Transparenz und konsequente Weiterentwicklung der Technologie nach ökologischen Gesichtspunkten gegenzusteuern wird unumgänglich sein.

Die Blockchain-Technologie hat großes Potenzial, durch ihre Eigenschaften wie Fälschungssicherheit und Transparenz neue Formen **digitaler Partizipation** zu unterstützen. Dazu gehören zum Beispiel eVoting, aber auch Beteiligungsplattformen, eGovernment-

Dienste oder ähnliches. Das **Vertrauen** der Bevölkerung wird aber nicht von alleine kommen, sondern muss erst aufgebaut werden. Mit anderen Worten: damit die Blockchain-Technologie Vertrauen aufbauen kann, muss erst Vertrauen in die Blockchain-Technologie selbst aufgebaut werden.

Politik

Auf politischer Ebene lassen sich direkte Parallelen zur **Digitalisierung** als übergeordnetem Thema ziehen. Ein Dreh- und Angelpunkt weiterer Entwicklungen werden **Standardisierung** und **Harmonisierung** sein. Dies ist für Nordrhein-Westfalen insofern eine Herausforderung, als diese Bemühungen auf möglichst hoher Ebene stattfinden müssen, um einen Effekt zu haben. Gleichzeitig bietet sich die Chance, Ergebnisse und Positionen aus NRW über entsprechende Foren in diese Standardisierungsentwicklungen einzubringen.

Ein weiterer maßgeblicher politischer Erfolgsfaktor wird eine kohärente **Strategie** für das Land Nordrhein-Westfalen sein. Im Gegensatz zur Blockchain-Strategie des Bundes sollten hier sehr konkrete Anwendungsfälle und Unterstützungsmaßnahmen benannt werden. So wird Akteuren ein sicherer Handlungsrahmen geboten. Ob dieses Dokument Teil der Digitalisierungs-Strategie wird, ein eigenes Dokument darstellt, oder „nur" ein Aktionsplan ist, ist unerheblich, wichtig sind die Signalwirkung und die Umsetzung von Maßnahmen.

Die Landesregierung kann durch verschiedene **Unterstützungsmaßnahmen** die Verbreitung der Blockchain-Technologie im Land unterstützen. Dazu gehören beispielsweise Vernetzungsaktivitäten, das zur Verfügung stellen von Technologie, Förderprogramme und Bildungsmaßnahmen. Wichtig sind in allen Fällen die Anwendernähe und damit eine zugrunde liegende Bedarfserhebung. Die Etablierung eines Reallabors kann dabei hilfreich sein und wäre konform zur Blockchain-Strategie des Bundes.

Recht

Innerhalb der rechtlichen Rahmenbedingungen ist der Aufbau von **Rechtssicherheit** evident wichtig, um die notwendigen Voraussetzungen für den Ausbau der Blockchain-Technologie zu schaffen. Schon die Frage nach der rechtlichen Qualifikation von Blockchain-basierten Anwendungen wie Token zeigt, dass das Recht de lege lata zwar oftmals schon rechtliche Lösungen bereitstellt. Gleichzeitig bestehen dennoch offene Rechtsfragen, deren Weiterentwicklung durch den stattfindenden rechtlichen Diskurs genau verfolgt werden muss, da sie großen Einfluss auf die weitere rechtliche Behandlung haben können. Bei der **zivilrechtlichen Einordnung** von Token muss dabei vor allem die Frage des gutgläubigen Erwerbs und der Übertragung verfolgt werden. Schließlich ist die Frage der rechtlichen

Einordnung von Token grundsätzlich von der übergeordneten Frage, ob Rechte an virtuellen Gütern bestehen, betroffen.

Auch die **kapitalmarktrechtliche Behandlung** von Currency-, Utility- und Security-Token leidet an offenen Rechtsfragen. Zwar hat sich in der Rechtsliteratur und aufsichtsbehördlichen Praxis die Meinung durchgesetzt, dass Security-Token und zum Teil auch Utility-Token Wertpapiere darstellen, sodass sie den besonderen Regeln hinsichtlich Transparenz und Anlegerschutz unterliegen. Eine eindeutige Klassifizierung von Token ist aber vor allem bei Utility-Token aufgrund ihres oftmals hybriden Charakters nicht möglich. Auch besteht durch die Tokenisierung erstmals die Möglichkeit, bislang nicht verkehrsfähige Rechtspositionen dem Kapitalmarktrecht zu unterwerfen. Gesetzgeberische Entscheidungen zur eindeutigen Abgrenzbarkeit von Token, der Reichweite von Regeln hinsichtlich Transparenz und Anlegerschutz (vor allem die Prospektpflicht) und zur Möglichkeit der Tokenisierung bislang nicht verkehrsfähiger Rechtspositionen sind daher wichtig für die Schaffung von Rechtssicherheit.

Die Blockchain-Technologie stellt auch die **Anspruchsdurchsetzung** vor neue Herausforderungen. So bestehen schon Zweifel, nach welchen Regeln die jeweilige Einzel- und Gesamtvollstreckung stattfinden soll. Des Weiteren stellen die Besonderheiten der Blockchain-Technologie das Verfahren der Anspruchsdurchsetzung vor Probleme hinsichtlich der Effektivität, da kein Intermediär vorhanden ist und es an einer Verkörperung des Vollstreckungsobjekts mangelt. Zwar fehlt es noch an einer weitläufigen Verbreitung der Technologie, wodurch die Anspruchsdurchsetzung derzeit kein praktisches Problem darstellt. Eine steigende Verbreitung und Akzeptanz der Blockchain-Technologie wird jedoch auch zwangsläufig zu einer steigenden Nachfrage hinsichtlich der Anspruchsdurchsetzung führen, sodass frühzeitig an Lösungen gearbeitet werden sollte.

Sollen Blockchain-basierte **Smart Contracts** im Bereich der **Vertragsdurchführung** zum Einsatz kommen, ist der zivilrechtliche Rechtsrahmen grundsätzlich geeignet, um solche Konstellationen zufriedenstellen zu erfassen. Probleme können sich auf Grund der rein virtuellen Natur von Werten, die auf der Blockchain übertragen werden, und der dezentralen Architektur ohne Intermediäre bei der Durchsetzung von Ansprüchen ergeben. Insofern kommen staatliche oder private Konfliktlösungsmechanismen in Betracht, die auf diese Besonderheiten abgestimmt sind.

Eine erhebliche Herausforderung für den Einsatz der Blockchain-Technologie stellt das **Datenschutzrecht** dar. Das ergibt sich zunächst aus den generellen Auslegungsschwierigkeiten bezüglich der Vorschriften des Datenschutzrechts und ferner

aus einem Konflikt zwischen Grundannahmen der DSGVO und diversen Charakteristika der Blockchain-Technologie. Das führt dazu, dass erhebliche Rechtsunsicherheit auf diesem Gebiet herrscht und die rechtskonforme Gestaltung von Anwendungsfällen nur schwer möglich ist. Transaktionsdaten und Public Keys stellen personenbezogene Daten i.S.d. DSGVO dar, sodass die Entwicklung datenschutzrechtlich zulässiger Lösungen unerlässlich für einen erfolgreichen Einsatz der Technologie ist. Unklarheit besteht bezüglich der **datenschutzrechtlichen Verantwortlichkeit** der einzelnen Nodes in öffentlichen, zulassungsfreien Systemen. Die Alternativen sind, dass entweder alle Nodes als Verantwortliche anzusehen sind oder keiner von ihnen. Dies führt für Betroffene und Behörden zu unbefriedigenden Ergebnissen. Gleichzeitig ist es auch für die Teilnehmer des Netzwerks von erheblicher Bedeutung, ob sie Verantwortliche im Sinne der DSGVO sind und die entsprechenden Pflichten zu erfüllen haben, da sie sich ansonsten Haftungsrisiken aussetzen. Weniger Probleme bestehen in privaten, zulassungsbeschränkten Blockchains, da hier eine zentrale Stelle (oder ein Konsortium) als Verantwortlicher identifiziert werden kann. Die **Betroffenenrechte** auf Berichtigung und Löschung nach der DSGVO lassen sich aufgrund der Unveränderlichkeit von Daten in der Blockchain nur schwer erfüllen. Deswegen sollten möglichst keine personenbezogenen Daten in die Blockchain geschrieben werden. Wo dies unmöglich ist, muss eine zuverlässige Anonymisierung erfolgen. Bisher bestehen allerdings keine gesicherten Erkenntnisse, bei welcher technischen Gestaltung eine ausreichende Anonymisierung im Sinne der DSGVO anzunehmen ist. Eine solche ist zudem nicht immer erwünscht, z.B. aus Sicht von Behörden.

Auf dem Gebiet des Datenschutzrechts wäre eine Beseitigung der bestehenden Rechtsunsicherheit wünschenswert. Dies könnte einerseits durch Anpassungen des Rechtsrahmens erfolgen, andererseits durch Hilfestellungen und Leitlinien für Anwender*innen.

Auf dem Gebiet des **Verbraucherschutzrechts** kann sich Anpassungsbedarf ergeben, um ein ausreichend hohes Verbraucherschutzniveau im Verhältnis zu neuartigen Risiken der Blockchain-Technologie zu gewährleisten. Dies wird aber erst absehbar, wenn es ein breiteres Feld an praxistauglichen Anwendungen gibt.

Über die Grenzen des vorhandenen Rechtsrahmens hinaus ist denkbar, dass Blockchain-Lösungen vom Gesetzgeber in verschiedenen Bereichen anerkannt werden. Hier kann sich ein gewisses Vereinfachungs- und Digitalisierungspotenzial ergeben. Nicht zu verkennen ist aber, dass jede Anerkennung dieser Art vorab eingehend aus rechtspolitischer Sicht geprüft werden muss.

Organisational

Entscheidet sich ein Unternehmen dafür die Blockchain einzusetzen, ist es relevant eine geeignete **Strategie** auszuwählen, um die Technologie im Unternehmen erfolgreich nutzbar zu machen. Hierbei leitet sich die Wahl der Strategie von dem Offenheitsgrad der Blockchain ab. Das **Geschäftsmodell** wird von der Strategie unmittelbar determiniert. Somit hat diese einen direkten Einfluss auf die Geschäftsmodellelemente Wertangebot, Wertschöpfungsarchitektur und Werteerfassung. Jedes dieser Elemente spaltet sich in weitere Dimensionen auf, wodurch die Auswirkungen der Blockchain-Technologie auf die einzelnen Unternehmenssegmente analysiert und dadurch taktische Handlungsmechanismen abgeleitet werden können.

Seitdem die Kryptowährung Bitcoin im Jahre 2009 am Markt eingeführt wurde, ist die Blockchain-Technologie, auf der die Kryptowährung basiert, mit eine der meistdiskutierten Innovationen des digitalen Zeitalters für Wirtschaft und Gesellschaft geworden. Die Nutzung der Bitcoin-Blockchain hat deutlich gemacht, dass die **Infrastruktur** der Banken abgelöst werden kann. Nicht nur Banken, sondern auch andere **Intermediäre** deren Geschäftsmodell es ist, als Mittler zwischen zwei Parteien zu agieren, sollten ihr Geschäftsmodell nunmehr im Rahmen dieser Technologie kritisch hinterfragen.

Demgegenüber birgt die Blockchain-Technologie diverse **Mehrwerte** wie Kosteneinsparungen, Prozessoptimierungen, Vertrauen, Sicherheit und Transparenz. Auf Basis dieser Mehrwerte ist es bspw. möglich neue Serviceangebote zu generieren sowie Kundensegmente zu erreichen, dessen Zugang zuvor nicht möglich war. Kunden wird mit der Blockchain-Technologie nun bspw. die Möglichkeit eröffnet, eine deutlich aktivere Rolle einzunehmen (C2B), als dies derzeit im Markt der Fall ist (B2C). Kundesegmente wie „**Prosumers**“ rücken verstärkt in den Fokus. Diese und weitere Szenarien eröffnen Unternehmen diverse Opportunitäten, die u.a. zur Stabilisierung, Erweiterung oder Neugestaltung des eigenen Geschäftsmodells beitragen kann.

2 METHODIK UND VORGEHEN

Die Identifizierung der relevanten Rahmenbedingungen und die Ableitung von Handlungsempfehlungen wurden vor allem durch Literaturrecherche betrieben. Über einschlägige Portale wie Web of Science, Scopus und Google Scholar wurde nach Fachliteratur gesucht.

Bei der Identifizierung gesellschaftlicher und politischer Rahmenbedingungen zeigte sich eine deutliche Forschungslücke. Hier gibt es nur sehr wenige Erfahrungsberichte und nahezu keine spezielle Forschung. Daher wurden auf allgemeine Erkenntnisse der Techniksoziologie sowie des politischen Umgangs mit neuen Informationstechnologien zurückgegriffen. Dies wurde ergänzt durch eine Analyse von ausgewählten politischen Initiativen sowie Analysen und Berichten von Unternehmensberatungen und politischen Institutionen zur Bedeutung der Blockchain-Technologie und sich daraus ableitenden (politischen) Handlungsoptionen. Diese Veröffentlichungen wurden durch zielgerichtete Internetrecherche bei großen Beratungsunternehmen sowie politischen Institutionen und nach dem Schneeballsystem identifiziert.

Die Identifikation relevanter rechtlicher Fragestellungen erfolgte ausgehend von bekannten Anwendungsszenarien der Blockchain-Technologie. Anschließenden erfolgte eine Literaturrecherche in diversen Fachdatenbanken (beck-online, juris, SSRN) und eine Auswertung der vorhandenen Fachliteratur in Bezug auf die gefundenen Themen.

Ferner wurde der vorhandene Rechtsrahmen analysiert. Vorgeschlagene Konzepte wurden auf Rechtskonformität hin überprüft (de lege lata-Betrachtung). Aktuelle Regulierungsansätze auf nationaler und europäischer Ebene wurden zusammengestellt. Auf Basis aller gefundenen Erkenntnisse wurde der weiterführende Forschungsbedarf identifiziert. Ebenso wurden Regelungslücken identifiziert (de lege ferenda-Betrachtung).

Zur Identifikation der Rahmenbedingungen hinsichtlich Geschäftsmodellinnovation wurde Literaturrecherche basierend auf den Portalen Web of Science und Google Scholar betrieben. Hierzu wurden rund 3372 wissenschaftliche Publikationen von „Web of Science“ zum Thema Blockchain heruntergeladen. Darauf aufbauend wurde ein Skript zur Auswertung dieser Meta-Daten auf Basis eines Topic Modeling Ansatzes in Verbindung mit einer Netzwerk-Cluster-Analyse erstellt. Dadurch konnte eine bibliografische Analyse der Meta-Daten vorgenommen werden, wodurch u.a. ein Forschungsthemencluster erstellen werden konnte. Anhand dieser Auswertungen konnten gezielt die Rahmenbedingungen zu

Geschäftsmollinnovation im Kontext von Blockchain eruiert werden. Ergänzend dazu wurden qualitative Interviews von Blockchain Fallbeispielen und Blockchain Experten durchgeführt.

3 GESELLSCHAFTLICHE RAHMENBEDINGUNGEN

Kernaussagen und Rahmenbedingungen	
GR1	Damit Blockchain-Anwendungen auch in der breiten Öffentlichkeit akzeptiert und genutzt werden, muss Vertrauen in die Technologie geschaffen werden. (Kapitel 3a, 3b, 3c)
GR2	Die Blockchain-Technologie bietet großes Potenzial, Versprechungen der digitalen Partizipation endlich einzulösen. Dreh- und Angelpunkt dabei ist natürlich das Vertrauen der Bevölkerung in die Technologie selber. (Kapitel 3c)
GR3	Die CO^2-Billanz einiger bekannter Blockchains erzeugt im Vergleich zu anderen Aspekten der Technologie viel Aufmerksamkeit und wird von der Bevölkerung kritisch gesehen. Dies könnte im Hinblick auf die Akzeptanz der Nutzer*innen ein kritischer Faktor werden. (Kapitel 3a)
GR4	Der Sicherheitsstandard einer Blockchain hängt zu großen Teilen vom Verhalten der Nutzer*innen ab. (Kapitel 3b)
GR5	Die Anwendung neuer Technologien in der Breite hängt auch mit einer offenen Innovations- und Unternehmerkultur zusammen. (Kapitel 3d)
GR6	Die Blockchain-Technologie wird sowohl beabsichtigte als auch unbeabsichtigte Folgen mit sich bringen. (Kapitel 3a)
GR7	Bisher gibt es im Bereich der Technikfolgenabschätzung fast ausschließlich Untersuchungen zu Kryptowährungen. (Kapitel 3a)
GR8	Im Bereich der Technikakzeptanz gibt es vereinzelte Studien beispielsweise zur Adaption, viele Fragen bleiben dazu aber bisher unerforscht. (Kapitel 3a)

Handlungsempfehlungen	
GH1	Zur Vertrauensbildung beitragen können skalierbare Pilotprojekte im kleinen Rahmen, größtmögliche Transparenz und Nachvollziehbarkeit bei der Wahl der

	technologischen Rahmenbedingungen, und überprüfbare Standards an die Sicherheit privater Daten und der Blockchain allgemein. (Kapitel 3c)
GH2	Im Fall der Partizipation ist Vertrauen in die partizipativen Prozesse selbst wichtig. Sofern Blockchain-basierte Formen digitaler Partizipation implementiert werden, müssen diese auch Konsequenzen haben. (Kapitel 3c)
GH3	Aufgrund ihres potenziell disruptiven Charakters und der damit verbundenen weitreichenden (aber bisher unbekannten) Folgen der Blockchain-Technologie sollten frühzeitig Technikfolgeabschätzungsanalysen zu ihr erstellt werden. (Kapitel 3a)
GH4	Um Akzeptanz in der Bevölkerung zu schaffen, müssen auch kritische Themen wie Umweltschutz aktiv behandelt werden. Besonders der Zusammenhang von Blockchain und ökologischen Konsequenzen sollte näher untersucht werden, da dieses Thema gesellschaftlich an Bedeutung gewinnt. Damit verbunden sind aber auch die konsequente Weiterentwicklung der Technologie, sowie die zielgerichtete Auswahl der richtigen Blockchain für einen Anwendungsfall um möglichst energieeffizient zu arbeiten. (Kapitel 3a)
GH5	Eine staatliche Intervention zur Sicherung digitaler Identitäten der Bürger*innen kann ebenfalls vertrauensbildend wirken. Im Sinne der Verbraucher*innen würde der Staat dabei die Verwaltung digitaler Identitäten basierend auf einer zu entwickelnden Blockchain übernehmen, die Bürger*innen könnten selbst entscheiden, wer ihre digitale Identität nutzt. Auch hier sind Transparenz und Sicherheit maßgebliche Kriterien. Zudem müsste eine solche Infrastruktur auf größtmöglicher Ebene angesiedelt sein. (Kapitel 3c)
GH6	Für ein hohes Sicherheitsniveau muss durch hohe Sicherheitsstandards Vertrauen ermöglicht werden. Gleichzeitig ist die Sensibilisierung der Bevölkerung für den Umgang mit digitalen Technologien maßgeblich dafür verantwortlich, das Sicherheitsniveau dann auch aufrecht zu erhalten und Vertrauen zu wahren. (Kapitel 3b)
GH7	Unterschiedliche Fragestellungen im Bereich der Nutzer*innen-Akzeptanz sollten zeitnah wissenschaftlich untersucht werden. (Kapitel 3a)

GH8	Zur Förderung einer gesamtgesellschaftlichen Innovationskultur empfiehlt es sich, sämtliche Fördermöglichkeiten auszunutzen und die Weiterentwicklung von Zukunftstechnologien gezielt voran zu treiben. Dazu gehören politische und rechtliche Rahmenbedingungen ebenso, wie die Förderung einer innovationsoffenen Mentalität. (Kapitel 3d)

3.1 Techniksoziologie

Techniksoziologie beschäftigt sich im Allgemeinen mit dem Verhältnis von Technik/Technologien und der Gesellschaft oder den sozialen Rahmenbedingungen, sowie den Auswirkungen von technologischen Entwicklungen. Soziolog*innen begannen, sich mit dem Wirkungsgrad und dem Wechselspiel zwischen Technik und Gesellschaft/Technik und Mensch auseinanderzusetzen. Innerhalb der techniksoziologischen Forschung gibt es zwei größere Teilgebiete, die sich jeweils mit unterschiedlichen Schwerpunkten mit der soziologischen Perspektive auf Technik beschäftigen: die Technikfolgenabschätzung und die Technikakzeptanz. Diese beiden Strömungen und ihre Erkenntnisse spielen in der heutigen Zeit, auch in Bezug auf die zunehmende allgemeine Technologisierung eine immer größere Rolle, sodass sie mit Fokus auf die Blockchain-Technologie im Folgenden näher beleuchtet werden.

3.1.1 Technikfolgenabschätzung

Das Forschungsgebiet Technikfolgenabschätzung entstand in den 60er Jahren und beschäftigt sich mit der Beobachtung von Technologien, deren Analyse und den mit ihr zusammenhängenden gesellschaftlichen Auswirkungen. Hier fokussiert sie besonders die Abschätzung der Chancen und Risiken, die durch Technologien entstehen. Somit kann sie als Teilgebiet der Techniksoziologie verstanden werden.

Die Grundannahme in der Technikfolgenabschätzung besagt, dass Technik nicht nur dem Erreichen eines speziellen Ziels dient, sondern sehr wahrscheinlich auch andere Konsequenzen hat – zum Beispiel auf die Umwelt und die sozialen Rahmenbedingungen. Dazu können neben beabsichtigten Folgen auch nicht-intendierte Folgen gehören. Je nach Technologie kann es sich um weitreichende, sehr komplexe und/oder undurchschaubare Auswirkungen handeln. Deshalb ist die Prognose nicht immer einfach zu vollziehen. Vor allem wenn Technik und Technologien erst in der Entwicklungsphase sind, oder noch nicht stark verbreitet sind und sich noch stark weiterentwickeln ist eine Abschätzung ihrer Folgen oft nicht einfach und kann nicht vollumfänglich sein, sondern fokussiert eher einzelne Aspekte oder Prozesse.

Da es bisher keine detaillierten Untersuchungen zu der Technikfolgenabschätzung der Blockchain-Technologie gibt und ihre Folgen deshalb noch nicht ausführlich beleuchtet wurden, lassen sich schwer Aussagen über spezifische gesellschaftliche Konsequenzen ableiten. Es gibt erste Untersuchungen und Einschätzungen zu der Anwendung von Blockchain in Kryptowährungen, welche mit zu den bekannteren Anwendungsgebiete der Blockchain zählen (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)

2018). Es zeigt sich also, dass es noch kaum wissenschaftlich fundierte Erkenntnisse zur Technikfolgenabschätzung der Blockchain gibt. Deshalb sollten solche Untersuchungen möglichst schnell gemacht werden, damit man entsprechend vorbereitet ist bei der Einführung von Blockchain und möglichen Hindernissen und Vorbehalten entgegen wirken kann.

3.1.2 Technikakzeptanz

Der Beginn der Technikakzeptanzforschung als weiteres Teilgebiet der Techniksoziologie war in den 70er Jahren. Zu der Zeit stellten Forscher*innen eine Feindlichkeit gegenüber einigen Technologien, wie bspw. der Atomenergie fest (Schäfer und Keppler 2013). Im Rahmen der Technikakzeptanzforschung werden die Nutzung und die Akzeptanz technologischer Lösungen durch die (potentiellen) Nutzer*innen vorhergesagt oder die bereits vorhandene Akzeptanz der Nutzer*innen bei bereits existierenden Technologien gemessen.

Es gibt unterschiedliche Modelle in der Akzeptanzforschung. Eines der bekanntesten ist das „Technology Acceptance Model (TAM)“ (Davis et al.): Es identifiziert zwei Faktoren, die die Einstellungen der Nutzer*innen zu der technologischen Lösung beeinflussen: die wahrgenommene Nützlichkeit und die wahrgenommene Benutzerfreundlichkeit. Sie sind in unterschiedlichen Kontexten unterschiedlich wichtig, ihre Gewichtung kann jeweils variieren und sie können durch weitere Faktoren beeinflusst und/oder ergänzt/ausgetauscht werden. Deshalb werden sie in diversen Kontexten in variierenden Methoden erforscht. Grundsätzlich kann man zwischen sozialwissenschaftlichen (soziologisch/psychologisch und ökonomischen) Ansätzen in der Forschung unterscheiden (Schäfer und Keppler 2013). Neben dem TAM-Modell haben sich in der Forschung der vergangenen Jahrzehnte noch eine Vielzahl neuer Modelle und Theorien herausgebildet, die unterschiedliche Aspekte beleuchten (Schäfer und Keppler 2013). Manche Modelle untersuchen bspw. die Akzeptanz der Nutzer*innen in unterschiedlichen Phasen: in der Einstellungs-Phase, also der Phase bevor die Nutzer*innen die Technologie kaufen/nutzen, in der Handlungs-Phase, in der die Technologie gekauft/genutzt wird und in der Nutzungs-Phase, in die Nutzer*innen die Technologie verwenden (Kollmann 1998).

In Bezug auf Blockchain könnten die Frage nach der wahrgenommenen Nützlichkeit und der Benutzerfreundlichkeit und weitere damit zusammenhängende Fragen, besonders vor der Einführung hilfreich sein, weil sie so noch in der Technologie, in ihrem Design und ihren Funktionalitäten oder in den darum entstehenden Prozessen berücksichtigt werden könnten. Wenn man sich erst nach Einführung einer solchen Technologie die Fragen stellt und die Aspekte beleuchtet, die den beschriebenen Modellen entspringen, kann es sein, dass zu

einem späteren Zeitpunkt diese unbeantworteten Fragen Hindernisse darstellen: bspw. kann die Zielgruppe die Blockchain nicht akzeptieren oder verstehen, sodass sie sie nicht (richtig) anwenden oder es könnten nochmals Kosten anfallen, um im Nachgang entsprechende Änderungen einzuarbeiten. Es ist daher sinnvoll, bei einzelnen Anwendungen bspw. Akzeptanzuntersuchungen in den einzelnen Phasen (wie oben beschrieben) durchzuführen.

Derzeit fehlen weitgehend noch langfristige Studien und Analysen zu der allgemeinen Akzeptanz der Blockchain-Technologie. Es gibt bisher vereinzelte Untersuchungen, die sich mit unterschiedlichen Teilaspekten, bspw. der Adaption von Blockchain beschäftigen. Beispielsweise identifizieren Francisco und Swanson (Francisco und Swanson 2018) unter anderem folgende Fragestellungen, die in Zukunft im Hinblick auf die Adaption von Blockchain relevant werden könnten:

- Hat der spezielle Anwendungsbereich, in dem die Blockchain eingesetzt wird, einen Einfluss darauf, ob User Blockchain benutzen werden?
- Welche Synergien können durch Verwendung einer Blockchain zwischen unterschiedlichen Bereichen eines Unternehmens/einer Organisation entstehen?
- Wie können Internet of Things (IoT) und Blockchain gemeinsam genutzt werden/wie kann IoT in Blockchain integriert werden?
- Wie werden nicht-technische Entwicklungen wie Regulationen/Gesetze, Organisationskulturen die Verwendung von Blockchain beeinflussen?
- Wie werden die Nutzer*innen auf neue Kosten und Risiken reagieren, die mit der Blockchain einhergehen können (bspw. der Möglichkeit bestimmte Prozesse im Job zu rationalisieren/straffen, um Kosten zu vermeiden)?

Momentan gewinnt gesellschaftlich die Diskussion um ökologische Folgen immer mehr an Bedeutung. Besonders in diesem Bereich der ökologischen Folgen besteht Kritik an der Blockchain-Technologie, die besonders im Hinblick auf eine große Verbreitung enorme ökologische Kosten mit sich bringt (WBGU - Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen 2019). Die meisten Blockchains nutzen derzeit das Proof-of-Work Konzept zur Konsensfindung innerhalb des Netzwerks, also zur Validierung von Informationen in der Blockchain. Dieser Prozess ist sehr energieaufwändig und benötigt viel Rechenleistung (Nascimento und Pólvora 2019; BNetzA 2019). Bitcoin als prominentestes Beispiel einer Blockchain hat einen extrem hohen Energiebedarf. Wie hoch er tatsächlich ist, lässt sich aber nur schwer sagen. Schätzungen zufolge dürfte der Energieverbrauch der gesamten Bitcoin-Blockchain momentan etwa so groß sein wie der der gesamten Republik Irland. Und sofern sich Bitcoin weiterentwickelt wie bisher wird der Energiebedarf weiter

steigen und könnte eine ähnliche Größenordnung wie der Österreichs erreichen (Vries 2018). An dieser Stelle muss erwähnt werden, dass Bitcoin als Blockchain nicht sonderlich effizient ist und andere Anwendungen deutlich weniger Energie benötigen. Steigt aber die Gesamtzahl der Anwendungen insgesamt bleibt der Energiebedarf der Blockchain-Technologie ein wichtiges Thema (Yaga et al. 2018). In Bezug auf Akzeptanz könnten also ökologische Konsequenzen zu einem kritischen Punkt werden, daher wären zeitnahe Studien dazu empfehlenswert.

Insgesamt empfiehlt es sich unterschiedliche Aspekte von Akzeptanz im Zusammenhang mit Blockchain frühzeitig in wissenschaftlichen Studien zu beleuchten und ihre Ergebnisse zu berücksichtigen.

3.2 Privatsphäre

Der Schutz privater Daten ist nicht nur ein rechtliches Thema, sondern auch ein gesellschaftliches. So stehen große Unternehmen wie Apple, Facebook oder Google häufig in der Kritik, ihre Nutzer*innen auszuspionieren. Aber auch Online-Werbung ist hier problematisch. In diesem Kontext werden nun Blockchain-basierte Anwendungen erprobt. Dazu gehört etwa ein Browser, der ein privates Werbenetzwerk aufbaut, welches für das freiwillige Anschauen von Werbung mit Tokens belohnt, die sie wiederum an Websites ihrer Wahl ausschütten können. Die Entwickler*innen wollen so nach eigenen Angaben die gesellschaftlichen Bedürfnisse nach Schutz ihrer Privatsphäre und qualitativ hochwertigen Angeboten im Internet bedienen (Berger 2019).

Auch wenn die kryptografischen Verfahren zum Schutz einer Blockchain derzeit sicher sind, kann nicht ausgeschlossen werden, dass sich dies in Zukunft ändert (Nascimento und Pólvora 2019; Schütte et al. 2017). Auch muss aus Sicherheitsperspektive das, in nahezu allen Fällen, schwächste Glied der Kette betrachtet werden: die Nutzer*innen. Zum heutigen Stand ist hier die größte Vulnerabilität einer Blockchain zu sehen (Nascimento und Pólvora 2019).

3.3 Vertrauen

Ein großes Problemfeld, welches mangels Standards und Zertifizierung zu einem Problem werden kann, ist das Vertrauen in Blockchains. Das Beispiel der französischen Supermarktkette Carrefour zeigt etwa, dass eine Blockchain Fälschungssicherheit und Verlässlichkeit auch nur vorgaukeln kann. Da die Server, auf denen die Blockchain gespeichert sind, alle im Rechenzentrum von Carrefour stehen, wird mithilfe des Schlagwortes „Blockchain“ eine vertrauensbildende Maßnahme lediglich vorgetäuscht (Mahn

2019). Sollten entsprechende Fälle publik werden, kann dies zu einem Vertrauensverlust bei der Bevölkerung führen.

Der Vertrauensverlust in demokratische Institutionen wird derzeit intensiv diskutiert (Schneider 2019; Di Fabio 2019; Seibel 2019). Neue Formen von Partizipation können Teil einer Antwort sein, etwa durch Online-Abstimmungen und –Wahlen (eVoting). eVoting wird jedoch vielleicht mehr als andere Aspekte staatlichen Handelns von Vertrauensproblemen geplagt: wie kann etwa sichergestellt werden, dass jede Stimme gezählt wird und doch anonym bleibt? Blockchain-Technologie kann hier Abhilfe schaffen, durch transparente und vertrauenswürdige Abstimmungsmechanismen (Lyons et al. 2018b; Muth et al. 2019). Das Vertrauen in eVoting kann aber nur durch Vertrauen in die zugrunde liegende Technologie erlangt werden. Und im Kern steht wiederum die Frage nach eindeutig zuzuordnenden digitalen Identitäten. Erste Versuche mit Blockchain-basiertem eVoting fanden auf kommunaler Ebene in der Schweiz statt, wenn auch nur in einer beratenden Abstimmung (Lyons et al. 2018b).

Ein weiteres Beispiel ist die Schaffung einer Plattform für Bürgerbeteiligung, basierend auf der Blockchain-Technologie, die BBBlockchain. Durch sichere Zeitstempel von Beiträgen, sicheres Datenmanagement, Diskussionsforen, Mechanismen für Umfragen und Abstimmungen und die Integration von Social Media werden verschiedene Aspekte von Partizipation bedient (Muth et al. 2019). Als grundlegende Aspekte von Partizipation werden von den Autoren des White Papers zur BBBlockchain Transparenz und Verantwortlichkeit gesehen, die von einer entsprechenden staatlichen Infrastruktur gewährleistet werden müssen. Nur ein starker Einfluss der Regierung könne bei digitaler Partizipation den tatsächlichen Einfluss der Bevölkerung auf Entscheidungen sicherstellen (Muth et al. 2019). Dies könnten erste Schritte in einer notwendigen Reihe vertrauensbildender Maßnahmen sein.

Die Blockchain-Technologie kann aber auch helfen, bereits verloren gegangenes Vertrauen wieder herzustellen. Bei den oben erwähnten digitalen Identitäten ist die Situation derzeit für Nutzer*innen alles andere als optimal. Daten liegen nicht nur bei staatlichen Akteuren, sondern vor allem bei einer Vielzahl privatwirtschaftlicher Akteure die diese Daten auch zur Gewinnerzielung nutzen. Sicherheitsstandards werden, wie regelmäßige Berichte zu Datenlecks zeigen, oft nur rudimentär eingehalten. Ein Blockchain-basiertes und einheitliches System zur Verwaltung und Sicherung privater Daten könnte Vertrauen wiederherstellen, persönliche Informationen sichern und Nutzer*innen Kontrolle

zurückgeben – vom Staat garantiert, sofern er diese Rolle spielen will und den nötigen Rahmen an Recht und Standards setzt (Lyons et al. 2018b).

3.4 Unternehmertum

Es herrscht derzeit Unklarheit über das Marktpotenzial neuer Blockchain Start-Ups. Nach einer Phase des Anstiegs wurden 2018 nur noch in China mehr neue Unternehmen in dieser Branche gegründet als im Vorjahr, sonst stagnierte die Zahl neuer Blockchain-Startups. Zusätzlich gab es einen Wechsel der Finanzierungsmodelle von Crowdfunding und Beteiligungen am Netzwerk (sog. Initial Coin Offerings, siehe dazu auch das Kapitel zu rechtlichen Rahmenbedingungen) hin zu klassischeren Finanzierungswegen wie Risikokapital. Ob dies aber bereits auf einen Saturierungseffekt hindeutet, ist umstritten (Nascimento und Pólvora 2019). Die Frage stellt sich also, wie groß das Potenzial der Blockchain-Technologie für Neugründungen in Nordrhein-Westfalen ist. Die weiter unten im Kontext der Digitalisierungsstrategie ausführlicher beschriebene Förderung von Pilotprojekten und Reallaboren bezogen auf die Blockchain-Technologie können helfen, das echte Marktpotenzial zu erschließen.

4 POLITISCHE RAHMENBEDINGUNGEN

Kernaussagen und Rahmenbedingungen	
PK1	Standardisierung ist eine der Haupttriebkräfte um der Blockchain-Technologie Akzeptanz zu verschaffen und weitere Anwendungsgebiete zu eröffnen. Standardisierung und Harmonisierung können potenziellen Anwendern Sicherheit geben. (Kapitel 4a)
PK2	Erfolgreiche Praxisbeispiele haben eine Leuchtturm-Funktion, die andere ermutigt, selbst Blockchain-Anwendungen zu implementieren. So können beispielsweise durch staatliche Förderprogramme oder die Unterstützung von Pilotprojekten durch staatliche Einrichtungen andere Akteure ermuntert werden, sich konkret mit dem Thema Blockchain zu beschäftigen. (Kapitel 4c, 4e)
PK3	Die klare Benennung von strategischen politischen Zielen kann helfen, Akteure zu Pilotprojekten zu animieren. Als Beispiel kann die Blockchain-Strategie des Landes Bayern dienen. (Kapitel 4e)
PK4	Die öffentliche Verwaltung gilt als eines der größten potenziellen Anwendungsfelder, und es gibt bereits erste positive Erfahrungen mit Blockchains

	in der Verwaltung in anderen Ländern. Damit eine Blockchain in der öffentlichen Verwaltung sinnvoll verwendet werden kann, müssen klare Anwendungsfälle konzipiert werden, was eng mit einer kohärenten Digitalisierungsstrategie verbunden ist. (Kapitel 4e)
PK5	Die Initiative „Blockchain in der Verwaltung Deutschland“ zeigt einen länder- und ressortübergreifenden Ansatz, Blockchain-Vorhaben in der Verwaltung umzusetzen. Solche Initiativen und durch sie angestoßene Projekte werden maßgeblich zum Erfolg oder Misserfolg der Blockchain-Technologie in der Verwaltung beitragen. (Kapitel 4e)
PK6	Derzeit sind viele Aspekte bei der Implementierung einer Blockchain juristisch noch unklar, siehe dazu auch das Kapitel zu juristischen Rahmenbedingungen. Der Staat hat die Aufgabe, klare Bedingungen zu schaffen. (Kapitel 4b)
PK7	Die Politik kann durch Unterstützungsmaßnahmen die Verbreitung der Blockchain-Technologie zielgerichtet unterstützen, wenn sie sich dabei an den Bedarfen der (potenziellen) Nutzer*innen orientiert. (Kapitel 4c, 4e)
PK8	Die Schaffung eines Systems zur Überprüfung digitaler Identitäten ist für viele Aspekte der Digitalisierung staatlicher Aufgaben, aber auch viele Blockchain-Anwendungen maßgeblich. (Kapitel 4a, 4c)
PK9	Aus- und Weiterbildungsangebote im Bereich der Blockchain-Technologie sind wichtig, um für ausreichend qualifiziertes Personal zu sorgen. (Kapitel 4d)

Handlungsempfehlungen	
PH1	Politische Entscheidungsträger sollten sich auf allen Ebenen um Standardisierung und Harmonisierung bemühen. Dies kann in Form eines rechtlichen Rahmens geschehen, die Entwicklung einer eigenen staatlichen oder EU-weiten Blockchain, durch runde Tische, oder andere Formen der Selbstverpflichtung. Das Land Nordrhein-Westfalen sollte dabei aber nicht auf Alleingänge setzen, sondern Aktivitäten im Land nach oben vermitteln und gleichzeitig Ergebnisse wo möglich wieder nach unten weitergeben. Dazu kann beispielsweise das Reallabor dienen. (Kapitel 4a)

PH2	Die Förderung von konkreten Anwendungsfällen sollte ausgebaut werden. In der deutschen Blockchain-Strategie wird dabei die dauerhafte Einrichtung von Reallaboren empfohlen. (Kapitel 4c, 4e)
PH3	Die Politik muss klare Themen und Handlungsfelder benennen, innerhalb der durch konkrete Maßnahmen die Implementierung einer Blockchain unterstützt wird. Dies kann beispielsweise durch eine eigene NRW Blockchain Strategie geschehen. Dabei sollten Aspekte wie Interoperabilität, Skalierbarkeit und Sinnhaftigkeit der Blockchain-Anwendungen im Vergleich zu anderen möglichen Lösungen stets mitgedacht werden. Die Verzahnung mit der Initiative „Blockchain in der Verwaltung Deutschland“ sowie den Aktivitäten des Bundesverbandes Blockchain kann viele Vorteile bieten. (Kapitel 4e)
PH4	Die Landesregierung sollte prüfen, im Zug der Digitalisierung staatlicher Aufgaben selbst (weitere) Blockchains zu implementieren. Dem muss eine genaue Bedarfs- und Fähigkeitslückenanalyse zugrunde liegen, etwa durch das Reallabor, um sicherzustellen, dass mit einer Blockchain auch die richtige Lösung für ein Thema gewählt wurde. (Kapitel 4c, 4e)
PH5	Die Schaffung eines sicheren rechtlichen Rahmens für Blockchain-Anwendungen muss schnell vorangetrieben werden. (Kapitel 4b)
PH6	Das Thema Blockchain befindet sich in der politischen Agenda derzeit weit oben, sowohl in Deutschland als auch in der EU. Für Nordrhein-Westfalen empfiehlt es sich daher, Förder- und Kooperationsmöglichkeiten auf Bundes- und Europaebene genau zu prüfen und im Bundesland bekannt bzw. verfügbar zu machen. (Kapitel 4e)
PH7	Die Politik sollte sich mit konkreten Unterstützungsmaßnahmen beschäftigen. Dazu können beispielsweise Vernetzungsaktivitäten der beteiligten Akteure gehören, oder aber das zur Verfügung stellen eigener Ressourcen, wie einer eigenen Blockchain oder von Server-Kapazitäten. Auch die Schaffung eines Registers bekannter Anwendungen zur Vermeidung von Dopplungen und dem Offenlegen von Kooperationspotenzialen wird empfohlen. (Kapitel 4c, 4e)
PH8	Staatliche Aus- und Weiterbildungsangebote bezogen auf die Blockchain-Technologie sollten ernsthaft in Erwägung gezogen werden. Dies betrifft IT-Themen allgemein, je prominenter ein Thema besetzt ist desto dringender werden jedoch

	Fachkräfte gesucht. Auch die Schulung potenzieller Nutzer*innen wird weiter an Relevanz gewinnen, hier ist noch viel Raum für politisches Handeln. (Kapitel 4d)

4.1 Standardisierung

Ein Mindestmaß an Standardisierung wird als Grundlage für die erfolgreiche Etablierung der Blockchain-Technologie genannt (Higginson et al. 2018). Derzeit existieren noch keine (internationalen) Standards bezüglich der Blockchain-Technologie[1]. Diese Standardisierungslücke wirft regulatorische Fragen auf, die eine Koordination über Ressort- und Landesgrenzen erfordern. Ziel muss es sein, einen sicheren Rechtsrahmen für die Blockchain-Technologie zu schaffen, sowohl was die Anwendung selbst, beispielsweise in gesetzlich stärker regulierten Feldern, als auch damit verbundene Funktionalitäten wie etwa Verifizierung oder Authentifizierung angeht (Schütte et al. 2017).

Damit die Blockchain-Technologie eines Tages etwa bei der weiter unten ausführlicher beschriebenen Verwaltung verschiedener digitaler Identitäten verwendet werden kann, braucht es Standards für Identitäts-bezogene Daten (Lyons et al. 2019). Auch die Standardisierung bei Datenformaten von in Blockchains gespeicherten Daten bzw. die ausreichende Interoperabilität verschiedener Blockchains untereinander und mit anderen Informationssystemen wird ebenfalls als für die Zukunft der Technologie immens wichtig erachtet (BNetzA 2019; Treat et al. 2018). So könnte eine ausreichende Interoperabilität staatlichen Akteuren erlauben, Kontrollen und Audits irgendwann automatisiert, aber zumindest aus der Distanz durchzuführen. Dies ist besonders interessant bei kritischen Produktions- und Lieferketten wie Nahrung oder Medizin. Aber auch das Monitoring von Wetterdaten oder Sensordaten kritischer Infrastrukturen könnte dem Staat im Krisenfall früheres und zielgerichteteres Handeln ermöglichen (Lyons et al. 2018b). Aber auch die Vorteile für Unternehmen liegen auf der Hand. Durch Interoperabilität verschiedener Blockchains und den damit ermöglichten Datenaustausch können neue Ökosysteme entstehen, die wiederum neue Anwendungsfälle und Innovationen ermöglichen (Treat et al. 2018).

Bei Standardisierungsbemühungen kann es aber zu Konflikten mit Wirtschaftsinteressen kommen, wie das Unternehmen PayPal sehr deutlich ausformuliert:

[1] Auf internationaler Ebene befinden sich bei der International Standardization Organization (ISO) mehrere Standards in Arbeit, von denen bisher den Status „Approval“ erreicht hat. Wird sie von ausreichend vielen ISO-Mitgliedern angenommen, gilt sie als akzeptiert und wird veröffentlicht. Zehn weitere Standards sind derzeit in Arbeit. (https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0, Stand 25.09.2019).

„Governments and regulators should be careful not to rush into regulating blockchain. (…) [G]overnments and regulators should look at how the technology is utilized in order to determine whether regulation is necessary. Where blockchains are used as a fully distributed platform, governments and regulators should also be aware that it will be challenging to regulate their use on a national or sub-national level, and we encourage standardization and consistency across the regulatory landscape."

„Regierungen und Regulatoren sollten bei der Regulierung von Blockchain Vorsicht walten lassen. (…) [R]egierungen und Regulatoren sollten beachten, wie die Technologie verwendet wird, um den Regulierungsbedarf festzustellen. Wo Blockchains als völlig dezentralisierte Plattformen verwendet werden, sollte es Regierungen und Regulatoren bewusst sein, dass eine Regulierung auf nationaler oder sub-nationaler Ebene schwierig sein wird, und dass wir Standardisierung und Konsistenz über die gesamte regulatorische Bandbreite empfehlen." (PayPal Government Relations 2019)

In Deutschland sollen nun erste Standardisierungsbemühungen für Blockchain-Anwendungen in der Energiebranche stattfinden, durch die Erstellung eines Registers für in Smart Contracts abbildbare vertragliche Sachverhalte. Dieses von der Bundesregierung finanzierte Pilotprojekt soll ein Vorgehen entwickeln, welches später auch auf andere Branchen übertragen werden soll (BMWi und BMF 2019). Neben Wirtschaftsvertretern fordert auch der Blockchain Bundesverband Standardisierungen, wie etwa bei Datenschnittstellen (Bundesverband Blockchain 2020). Diese Entwicklungen müssen von Seiten des Reallabors und aller beteiligten Akteure genau verfolgt werden.

4.2 Rechtssicherheit

Die rechtlichen Fragestellungen werden im nächsten Kapitel noch weiter thematisiert. Es handelt sich dabei aber auch um politische Fragestellungen, da Rechtssetzung in sich ein politischer Akt ist. Die enge Zusammenarbeit zwischen Landes- und Bundesregierung ist dabei ausschlaggebend.

Derzeit haben in einer Blockchain gespeicherte Aussagen, was etwa die Überschreibung von Werten oder die Verifizierung von Identität angeht, nur begrenzte gerichtlich verwertbare Aussagekraft. Dazu ist ein gesetzlicher Rahmen nötig, der solche Aussagen juristisch legitimiert (Schütte et al. 2017). Diesen Rahmen zu schaffen ist eine der Kernaufgaben, um die Blockchain-Technologie in der Breite in die Anwendung zu bringen (Bundesverband Blockchain 2020). Die Blockchain-Strategie der Bundesregierung skizziert, wie dieser Rahmen aussehen könnte (BMWi und BMF 2019).

Der Schutz von Daten und Privatsphäre sowie die Gewährleistung von Gerichtsbarkeit und Haftbarkeit sind im Kern staatliche Aufgaben. Die Schaffung des entsprechenden rechtlichen Rahmens für Blockchain-Anwendungen ist somit auch politische Rahmenbedingung, will der

Staat seinen hoheitlichen Aufgaben und Verpflichtungen weiterhin nachkommen (Lyons et al. 2018b).

4.3 Infrastruktur

Der Blockchain-Technologie fehlt derzeit eine adäquate Infrastruktur für die von Blockchain-Technologie zu erwartende Rolle für Staat, Gesellschaft und Wirtschaft. Da eine Zunahme an Blockchain-Anwendungen zu erwarten ist, könnte eine „Blockchain-Registry" Kooperationspotenziale offenlegen und Dopplungen vermeiden (Schütte et al. 2017; Bundesverband Blockchain 2020). Dies ist besonders unter dem Gesichtspunkt ratsam, dass Blockchains ihr Potenzial nur durch eine gewisse Größe des Netzwerks entfalten, erreicht entweder durch Interoperabilität von Technologien oder eine größere Nutzerzahl. Daher empfiehlt sich die Bildung von Verbünden oder die gemeinsame Nutzung einer Blockchain-Anwendung, oder die Mitwirkung an der Etablierung von Standards (Schütte et al. 2017).

Eine andere Blockchain-bezogene Infrastruktur, die vom Staat bereitgestellt werden könnte, wäre ein „Blockchain Platform as a Service"-Modell. Damit könnten je nach Zielgruppe staatliche Behörden und Organisationen, aber auch Vereine, Unternehmen, Start-Ups etc. schnell und einfach Konzepte entwickeln (lassen) und testen. Dies würde natürlich auch zu einer gewissen Standardisierung beitragen (Lyons et al. 2018b).

Ein wichtiger Bestandteil der Bemühungen, die Blockchain-Technologie weiter zu verbreiten, ist die Schaffung von Reallaboren. Dieses Projekt skizziert die Grundlagen für ein Blockchain-Reallabor für Nordrhein-Westfalen, was auch im Sinne der deutschen Blockchain-Strategie ist (BMWi und BMF 2019). Im Zuge der Strategie sollen Reallabore gezielt gefördert werden. Als Teil der Europäischen Blockchain Partnerschaft beteiligt sich Deutschland auch am Aufbau einer Europäischen Blockchain Services Infrastruktur, die demnächst erste Anwendungsfälle abbilden soll (BMWi und BMF 2019). Zugriff auf dieses Netzwerk kann für das Reallabor durch die Möglichkeit auf eine Versuchsinfrastruktur zuzugreifen einen echten Vorteil darstellen.

Im Zuge der Digitalisierung hoheitlicher Aufgaben wird die Problematik der Identitätsüberprüfung dabei immer drängender, denn für viele Aspekte der staatlichen Daseinsvorsorge spielt die zweifelsfreie Identifizierung von Individuen eine zentrale Rolle (Perez 2019). Wie lässt sich die Identität einer Person im digitalen Raum zweifelsfrei feststellen? Blockchain-basierte Lösungen könnten hier ein Teil der Lösung sein, indem digitale Identitäten erstellt, registriert und beglaubigt werden, und ähnlich dem estnischen Gesundheitssystem eine Zugriffskontrolle und Berechtigungsmanagement bieten (Lyons et

al. 2019). Dezentrale Identitäten haben gewisse Grundvoraussetzungen. Dazu gehören eindeutige Identifikationsmerkmale („decentralised identifiers“) mit einem öffentlichen und einem geheimen Teil, der nur der entsprechenden Person oder Entität bekannt ist und die den Besitz der dezentralen Identität gewährleistet (Lyons et al. 2019). Die Schaffung eines Systems zur Verwaltung digitaler Identitäten wird daher als Hauptaufgabe bei der Verwendung von Blockchains durch staatliche Behörden und Organisationen gesehen, quasi als Rückgrat einer Blockchain der öffentlichen Verwaltung (Lyons et al. 2018b). Die Bundesregierung überlegt in diesem Feld aktiv zu werden (BMWi und BMF 2019).

4.4 Bildung

Die erfolgreiche Implementierung einer Blockchain hängt auch von der Expertise der beteiligten Akteure ab. Es kann daher davon ausgegangen werden, dass der Bedarf in Unternehmen an Fachpersonal steigen wird, ebenso wieder der Bedarf an Beratung. Dies setzt eine große Menge an qualifiziertem Personal voraus, welches derzeit nicht in ausreichendem Umfang der Fall (Fujitsu und CXP Group 2017). Auch potenzielle Anwender einer Blockchain-Anwendung in Behörden, Organisationen, Unternehmen etc., aber auch die breite Öffentlichkeit müssen geschult und ausgebildet werden, um zukunftsfähig zu bleiben (Lyons et al. 2018b). Letztlich kann dieser Umstand nur durch gezielte Ausbildungsangebote behoben werden.

4.5 Digitalisierung

Die Förderung der Blockchain-Technologie wird nur dann langfristige Erfolge erzielen und nachhaltig sein können, wenn sie als Teil einer umfänglichen Strategie stattfindet. Die Blockchain-Strategie der Bundesregierung zeigt dabei ein recht enges Verständnis der Technologie, indem sie die Anwendungsgebiete hauptsächlich in Finanzindustrie und Handel sieht (Mahn 2019). Darüber hinaus werden aber auch ausdrücklich der Energiesektor, deutlich weniger prominent die Verifikation von Hochschulbildungszertifikaten, Logistik, Verbraucherschutz und digitale Identitäten erwähnt (BMWi und BMF 2019). Die Blockchain-Strategie bietet aber auch den Ausblick auf Fördermittel für verschiedene Projekte wie Reallabore, Pilotprojekte usw., was bei der Verankerung der Blockchain-Technologie in NRW durchaus helfen kann. Auch die Maßnahmentabelle im Anhang der Strategie bietet einen guten Überblick über die geplanten Aktivitäten der Bundesregierung. Hier Synergien mit der regionalen Ebene zu schaffen ist sicher kein Nachteil.

Weitergehende und spezialisierte Initiativen wie die „Initiative Blockchain in der Verwaltung Deutschland (BViD)“ haben möglicherweise größeres Potenzial als die relativ abstrakte Blockchain-Strategie. Letztere bietet einen groben Handlungsrahmen, aber

anwendungsnahe Initiativen wie BViD können konkret Produkte liefern, Synergien schaffen und bei der Vermeidung von Dopplungen helfen (MWIDE NRW 2020). Das Land NRW ist in dieser Initiative bereits aktiv, was beispielsweise auch bei der Standardisierung helfen kann. So können Ergebnisse aus BViD durch das Reallabor nach unten durchgegeben werden, gleichzeitig können Ergebnisse aus dem Reallabor nach oben gespielt werden und so auch auf Bundesebene Gehör finden.

Eine Verwendung der Technologie ist aber auch in anderen Branchen bzw. Anwendungsgebieten als in der Blockchain-Strategie genannt denkbar. Bei den Branchen werden Internet der Dinge (IoT), Smart Grid bzw. Energieverteilung insgesamt, Einkauf, Supply Chain Management, Medizin und der öffentliche Sektor / Verwaltung genannt. Bei Anwendungsgebieten stechen Herkunftsnachweise, Buchhaltung, Rechtemanagement, Verschlüsselung und Übertragung sensibler Daten, sowie (möglicherweise rechtssichere) Validierung von Transaktionen heraus. (Schütte et al. 2017; World Economic Forum 2019; Nascimento und Pólvora 2019).

Ein weiteres potentielles Anwendungsgebiet der Blockchain-Technologie sind die *Smart Cities* der Zukunft. In diversen Pilotprojekten in China, den Vereinigten Arabischen Emiraten, Kambodscha und Taiwan werden derzeit Möglichkeiten ausgelotet, wie städtische Infrastrukturen mithilfe von Blockchains unterstützt oder gänzlich getragen werden können. Dabei geht es beispielsweise um Bildung, Verkehrsmanagement (von ÖPNV bis zu Verkehrsflüssen), Nachhaltigkeit oder Gesundheitswesen (Cant 2019). Wichtige Themen für die chinesische Regierung sind dabei die Interaktion von Infrastruktur bzw. Städten und Daten, sowie Identifikation und Datenaustausch in den einzelnen Anwendungsgebieten dar (Perez 2019; Cant 2019). Dies reicht von Blockchain-basierter Rechnungsstellung in der Provinz Yunnan bis hin zu einer Kombination von Gesichtserkennung und Blockchain zur automatischen Schuldenüberprüfung in der Gemeinde Guangzhou (Perez 2019). Dies deutet darauf hin, dass China fehlende staatliche Infrastruktur direkt durch Blockchain-basierte digitale Prozesse aufbauen möchte – ohne den Umweg über herkömmliche Infrastruktur zu gehen (Perez 2019). In den USA kündigte die Katastrophenschutzbehörde FEMA an, sich mit Blockchain als Mittel zur Harmonisierung und Beschleunigung von Hilfszahlungen und Versicherungsleistungen im Katastrophenfall zu beschäftigen. Gerade bei Naturkatastrophen verlieren Betroffene häufig sämtliches Hab und Gut, darunter auch Versicherungsunterlagen (PYMNTS 2019). Das Gesundheitswesen sowie Energie- und Versorgungsunternehmen, von denen viele in kommunaler Hand sind, sind in der staatlichen Daseinsvorsorge eines der größten Anwendungsgebiete der Blockchain-Technologie (J.P.Morgan 2019; Lyons et al. 2018b).

Hier gilt es, durch einen politischen Rahmen, etwa eine erweiterte oder gar lokale Blockchain-Strategie, und geeignete politische Instrumente Anreize zu schaffen, sich dieser verschiedenen Themen anzunehmen. Die Verankerung des Blockchain-Reallabors in der regionalen Wirtschaft und die Ausstattung mit ausreichenden Mitteln ist ein guter erster Schritt, diesen Weg zu gehen. Ein weiterer ist aber die klare Benennung von strategischen Zielen. Das Land Bayern hat mit seiner eigenen Blockchain-Strategie ein Beispiel vorgelegt, wie dies aussehen kann. Ob dies für Nordrhein-Westfalen ein erstrebenswerter Schritt ist, oder ob die Förderung der Blockchain Teil der Implementierung der eigenen Digitalstrategie sein kann, muss geprüft werden. So oder so müssen die Fördermaßnahmen und die zugrunde liegenden Ziele aber genau definiert und tatkräftig umgesetzt werden.

Bei allen Digitalisierungsvorhaben gilt: die öffentliche Verwaltung ist zu jedem Zeitpunkt den Bürger*innen gegenüber verpflichtet, transparent, nachvollziehbar und kosteneffizient zu arbeiten. Die Blockchain-Technologie bietet hier großes Potenzial, als Teil der Digitalisierung von staatlichen Aufgaben (eGovernance) und Prozessen (eGovernment) bei der Verifizierung, Prüfung, Konsolidierung und Nachvollziehbarkeit von Daten(-sammlung) und Eintragungen durch Behörden Kosten zu sparen. Dies betrifft etwa Geburts- und Sterbeurkunden, und Identitätsnachweise für Individuen, Organisationen, Verbände, sowie zunehmend Maschinen und autonome Akteure. Aber auch die digitale Registrierung von Eigentumsverhältnissen und Grundbucheinträgen ist ein potentielles Anwendungsgebiet. Dies lässt sich auch auf andere Registrierungen wie Eintragungen um Handelsregister und Kfz-Anmeldungen oder Zertifizierung, wie von Bildungsabschlüssen, ausweiten (Lyons et al. 2018b). Dabei ist es wichtig die Integrität der gespeicherten Daten zu gewährleisten. In Estland wird Blockchain-Technologie etwa dazu genutzt, einen zusätzlichen Schutz von medizinischen Daten zu gewährleisten. So werden nicht die medizinischen Daten selbst in der Blockchain gespeichert, sondern die Logfiles dazu. Diese zeichnen manipulationssicher alle Änderungen an und Zugriffe auf die gespeicherten Daten auf (Einaste 2018; Lyons et al. 2018b).

5 RECHTLICHE RAHMENBEDINGUNGEN

Kernaussagen und Rahmenbedingungen	
RK1	Aufgrund des disruptiven Charakters der DLT stellt sich oftmals die Frage, ob die jeweiligen Blockchain-basierten Anwendungen in den entsprechenden Rechtsrahmen (de lege lata) passen oder ob die Besonderheiten der Blockchain-Technik eine rechtliche Anpassung (de lege ferenda) notwendig machen. (Kapitel 5a, 5c)
RK2	In den meisten Bereichen erlaubt das jeweils anzuwendende Recht zwar schon de lege lata eine rechtliche Einordnung. (Kapitel 5a, 5a-ii)
RK3	Besonders im Bereich des Datenschutz- und des Kapitalmarktrechts bestehen aber besonders drängende Rechtsprobleme, die eine weitere wirtschaftliche Implementierung der jeweiligen Blockchain-basierten Anwendungen gefährden. (Kapitel 5a, 5a-ii, 5b)
RK4	Des Weiteren stellt sich die grundlegende Frage, ob die rechtliche Einordnung den jeweiligen Anwender*innen und Aufsichtsbehörden, der Judikative oder letztlich dem Gesetzgeber überlassen werden sollte. (Kapitel 5a-ii)
RK5	Nicht zuletzt besteht bei den meisten Anwendungen die Notwendigkeit einer genauen Beobachtung der jeweiligen technischen Entwicklung und wirtschaftlichen Implementierung, da bisher noch theoretisch vorhandene Rechtsprobleme, wie beispielsweise die Anspruchsdurchsetzung oder die Gewährleistung eines adäquaten Verbraucherschutzniveaus, erst bei steigender Verbreitung/Anerkennung auch praktischen Charakter erlangen. (Kapitel 5a-iii, 5c)
RK6	Die Blockchain-Technologie kann Chancen bieten, bestehende Rechtsinstitute zu digitalisieren, was zu Effizienzgewinnen führen kann. Es muss aber stets eine genaue Prüfung erfolgen, ob die erhofften Vorteile gegenüber Risiken und Schwierigkeiten bei der Implementierung tatsächlich überwiegen. (Kapitel 5d)

Handlungsempfehlungen

RH1	Eine grundlegende Entscheidung, ob auch bislang nicht verkehrsfähige Rechtspositionen durch Tokenisierung dem Kapitalmarktrecht unterworfen werden können, sollte so schnell wie möglich getroffen werden. (Kapitel 5a-ii)
RH2	Aus datenschutzrechtlicher Sicht sind stets Modelle vorzuziehen, bei denen keine personenbezogenen Daten in die Blockchain geschrieben werden. (Kapitel 5b)
RH3	Technische Möglichkeiten für die zuverlässige Anonymisierung personenbezogener Daten sollten weiter erforscht werden. (Kapitel 5b)
RH4	Aus rechtspolitischer Sicht sollte genau geprüft werden, ob eine vollständige Anonymisierung erstrebenswert ist. Ist dies nicht der Fall und stellt die Anonymisierung die einzige Möglichkeit dar, einen Anwendungsfall datenschutzrechtskonform zu gestalten, so ist die Blockchain keine geeignete Lösung. (Kapitel 5b)
RH5	Eine gesetzgeberische Grundsatzentscheidung über die kapitalmarktrechtliche Behandlung der jeweiligen Arten von Token aus Gesichtspunkten der Rechtssicherheit wäre begrüßenswert. (Kapitel 5a-ii)
RH6	Aus Sicht des Anlegerschutzes ist eine Ausarbeitung von einheitlichen Definitionen und Abgrenzungskriterien für die verschiedenen Token-Arten wünschenswert, da diese bisher lediglich von der Rechtsliteratur und der zuständigen Aufsichtsbehörde (BaFin) ausgearbeitet wurden und sich schon in ihrer Namensgebung unterscheiden. (Kapitel 5a-ii)
RH7	Insoweit bestimmte Arten von bei ICOs verwendeten Token nicht der Prospektpflicht unterfallen, ist es aus Sicht eines umfassenden Anlegerschutzes wünschenswert, dass zumindest grundlegende Informationspflichten durch die diesen Token zugrundeliegenden White Paper erfüllt werden sollten. In diesem Zusammenhang sollte das weitere Vorgehen der ESMA beobachtet werden, um auch frühzeitig auf gesetzgeberische Entwicklungen auf EU-Ebene reagieren zu können. (Kapitel 5a-ii)
RH8	Auch im Bereich des Datenschutzrechts stellt die fehlende Rechtssicherheit ein erhebliches Innovationshindernis dar. Im Rahmen der anstehenden Überprüfung der DSGVO sollte auf Klarstellungen sowohl im Allgemeinen als auch im Hinblick auf die Besonderheiten der Blockchain-Technologie hingewirkt werden.

	Für Anwender*innen der Technologie sollten Auslegungshilfen und Leitlinien geschaffen werden, die sich explizit mit der Blockchain-Technologie auseinandersetzen. (Kapitel 5b)
RH9	Zertifizierungsverfahren und Codes of Conduct können sinnvolle Mittel der Selbstregulierung im Bereich des Datenschutzrechts darstellen und sollten gefördert werden. (Kapitel 5b)
RH10	Notwendig ist eine genaue Beobachtung der entstehenden Geschäftsmodelle und Tendenzen, um potenzielle neuartige Risiken für Verbraucherinteressen frühzeitig zu erkennen. Hier kann sich gesetzlicher Anpassungsbedarf ergeben, um effektiven Verbraucherschutz zu gewährleisten. (Kapitel 5c)
RH11	Vorhandene Informationspflichten sollten auf ihre Eignung überprüft werden, Verbraucher*innen ausreichend darüber aufzuklären, welche Konsequenzen der Einsatz der Blockchain-Technologie für ihre Rechtspositionen haben kann. (Kapitel 5c)
RH12	Eine genaue Beobachtung der Verkehrsfähigkeit und Handelbarkeit von Token ist notwendig, um frühzeitig den Wandel von derzeit theoretischen zu dann praktischen Rechtsproblemen zu erkennen. (Kapitel 5a-ii)
RH13	Zertifizierungsverfahren und Prüfsiegel können wirksame Mittel darstellen, um die technische Sicherheit von Smart Contracts zuverlässig zu bewerten. Daher empfiehlt sich die Schaffung solcher Instrumente und die Förderung ihres Einsatzes. (Kapitel 5c)
RH14	Verschiedene Blockchain-basierte Lösungen können zur Vereinfachung bestehender Prozesse in Erwägung gezogen werden. Häufig ist dafür eine Anerkennung durch den Gesetzgeber nötig. Wird die Ergänzung oder der Ersatz eines vorhandenen Instruments durch eine Blockchain-Lösung in Erwägung gezogen, muss stets eine eingehende Prüfung durchgeführt werden, inwiefern dies aus rechtspolitischer Sicht wünschenswert und sinnvoll ist. (Kapitel 5d)
RH15	Die grundsätzliche rechtliche Diskussion zur Einordnung von virtuellen Gütern als absolute Rechte sollte beobachtet werden. (Kapitel 5a-i)

5.1 Abbau von Rechtsunsicherheit

Bestehende Rechtssicherheit ist ein wesentlicher Faktor für den Aufbau und die gesellschaftliche Implementierung neuer Wirtschaftszweige. Besonders bei neuen, wandlungsfähigen und disruptiven Technologien wie der Blockchain-Technologie ist die Entwicklung der rechtlichen Rahmenbedingungen für die wirtschaftliche Betätigung jedoch problematisch. Denn bei der Entwicklung dieser rechtlichen Rahmenbedingungen müssen neben der Standardisierung der Anwendungsmöglichkeiten nicht nur die wirtschaftlichen Interessen von Unternehmen, sondern auch die schutzwürdigen Interessen der jeweiligen Anwender*innen und Verbraucher*innen beachtet werden. Unter der Beachtung dieses Spannungsfeldes ist der Abbau der Rechtsunsicherheit zu betreiben. Hierzu müssen zunächst Rechtsunsicherheiten erkannt und in einem nächsten Schritt nach rechtlichen Lösungswegen untersucht werden.

5.1.1 Rechtliche Qualifikation von Token im Privatrecht

Die Frage nach der Rechtsnatur von Token war bisher mehrfach Gegenstand der juristischen Forschung, wobei der Schwerpunkt dabei vor allem bei Currency-Token (Kryptowährungen) liegt (bspw. Beck 2015, 580ff.; Boehm und Pesch 2014, 75ff.; Engelhardt und Klein 2014, 355ff.; Kaulartz 2016, 474ff.; Omlor 2018, 85ff.; Spindler und Bille 2014, 135ff.). Die meisten Autor*innen kommen zu der Erkenntnis, dass sich Currency-Token rechtlich nicht eindeutig einordnen lassen. Jedoch wurde bisher nicht hinreichend erörtert, wie eine Einordnung de lege lata stattzufinden hat. Die Rechtsprechung liefert bisher wenige Urteile, welche sich nur limitiert mit dieser Frage auseinandersetzen (bspw. KG Berlin 2018, 2015). Überwiegende Einigkeit besteht, dass (Currency-)Token weder Sachen nach § 90 BGB noch urheberrechtlich geschützte Immaterialgüter nach § 2 Abs. 2 UrhG darstellen (Boehm und Pesch 2014, S. 78). (Currency-)Token stellen weiterhin nach übereinstimmender Auffassung weder Bargeld, Buchgeld noch E-Geld dar (Schlund und Pongratz 2018, 599f.). Aufgrund der weitreichenden juristischen Folgen einer rechtlichen Qualifikation von Token ist es empfehlenswert, diese juristische Diskussion und die gesetzgeberische Entwicklung hierzu genau zu verfolgen.

Trotz der bisher unklaren rechtlichen Einordnung können die verschiedenen Arten von Token Gegenstand schuldrechtlicher Beziehungen sein (etwa Spindler und Bille 2014, 1357ff.; Kaulartz 2016, 474ff.; Schrey und Thalhofer 2017, 1431ff.; Omlor 2018, 85ff.). Die Pflicht zur Verschaffung von Token wird unabhängig davon, wie diese konkret erfolgt, als (Gegen-)Leistung aufgrund der §§ 311, 241 BGB grundsätzlich zulässig sein (Schroeder 2014, Abs. 27). Zwar ist die jeweilige schuldrechtliche Einordnung der vertraglichen Beziehungen sowie die Haftungsverteilung prima facie unklar und obliegt daher einer Betrachtung des Einzelfalls

(beispielsweise zur schuldrechtlichen Einordnung des Eintausches Bitcoins gegen Waren Boehm und Pesch 2014, S. 78; zur Haftung und Risikoverteilung bei der Verschaffung von Bitcoins und Alt-Coins Pesch 2017, 129ff.). Insoweit kann bei der vertraglichen Einordnung im Zusammenhang mit der Verschaffung von (Currency-)Token je nach Einzelfall die Klassifizierung als Kauf-, Tausch-, Werk- oder Dienstvertrag erfolgen (Pesch 2017, 129ff.). Nach übereinstimmender Auffassung in der Rechtsliteratur können Token aber zumeist als sonstige Gegenstände gemäß § 453 Abs. 1 Var. 2 BGB angesehen werden und daher Gegenstand kaufrechtlicher Beziehungen sein (Schroeder 2014, Abs. 51; Spindler und Bille 2014, S. 1362). Da alle Gegenstände, die Objekt eines Kaufs sein können, auch aus rechtlicher Sicht taugliche Tauschobjekte darstellen, bestehen auch innerhalb eines Tauschs nach § 480 BGB keine rechtlichen Barrieren (Pesch 2017, S. 134). Zuletzt ist der Begriff der Vergütung bei Werk- oder Dienstverträgen nicht auf Geldzahlungen beschränkt, wonach einer Vereinbarung der Vergütung in (Currency-)Token der Annahme eines Werkvertrags nach § 631 BGB oder eines Dienstvertrags nach § 611 BGB nichts entgegensteht (Pesch 2017, S. 135 mwN). Die Qualifikation als ein im BGB geregelter Vertragstyp hat insoweit Bedeutung, wenn innerhalb der jeweiligen schuldrechtlichen Beziehung Leistungsstörungen auftreten (Hanten und Sacarcelik 2019, S. 126). Denn insoweit bestimmt sich das jeweilige Haftungsregime nach den jeweiligen spezialrechtlichen Regelungen.

Aus Sicht des Bereicherungsrechts kommt bei einer unbefugten Übertragung von (Currency-)Token ein Anspruch aus Eingriffskondiktion nach § 812 Abs. 1 S. 1 BGB in Betracht (Martiny 2018, S. 564). Insoweit wird in der Rechtsliteratur auch angenommen, dass die zu (Currency-)Token gehörigen privaten Schlüssel durch ein Recht am eigenen Datenbestand als "sonstiges Recht" nach § 823 Abs. 1 BGB deliktsrechtlich geschützt werden (Spindler und Bille 2014, S. 1363). Auch ein Schutz nach § 823 Abs. 2 BGB i.V.m. § 303a StGB soll sich ergeben (Kaulartz 2016, S. 479).

Des Weiteren bestehen zwar verschiedene Auffassungen, wie die verschiedenen Arten von Token rechtlich übertragen werden. So wird einerseits zuweilen vertreten, dass sie nach §§ 873, 925 ff. BGB analog übereignet werden (Ammann 2018, 382ff.). Andererseits wird vereinzelt vertreten, dass Token der Übereignung nach §§ 929 ff. BGB unterliegen (Koch 2018, 362ff.). Die Übertragbarkeit nach §§ 413, 398 ff. BGB wird hingegen bisher abgelehnt (Ammann 2018, S. 382). Auch wird die Übertragung teilweise lediglich als reiner Realakt angesehen, der keine Einigung der Parteien verlangt (Engelhardt und Klein 2014, S. 358; Kaulartz 2016, S. 478). Insoweit man einer (sachen-)rechtlichen Einordnung folgt, ist schon zum einen nicht ersichtlich, inwiefern diese divergierenden rechtstheoretischen Auffassungen Auswirkungen auf die Praxis haben, da beide Übereignungsformen den gutgläubigen Erwerb kennen und

sich somit nur die Rechtsscheinträger (Besitz/Grundbucheintragung) unterscheiden. Zum anderen sind die jeweiligen gesetzlichen Regelungen und Grenzen in allen Fällen gesetzlich vorgegeben (Koch 2018, S. 362). Wenn aber von einem reinen Realakt ausgegangen wird, hat dies praktische Konsequenzen, da keine Gutglaubensvorschriften existieren. Letzteres ist aber wohl zu erwarten da die analoge Anwendung sachenrechtlicher Normen schon aufgrund des Numerus-Clausus-Prinzips des Sachenrechts fragwürdig erscheint (Shmatenko und Möllenkamp 2018, S. 497). Denn das Numerus-Clausus-Prinzip legt fest, dass alle dinglichen Rechte abschließend im Sachenrecht geregelt sind. Zu beachten gilt aber auch, dass zwar im Rahmen der rechtlichen Einführung elektronischer Wertpapiere diskutiert wird, ob diese durch eine gesetzliche Fiktion zu Sachen erklärt werden könnten (BMF und BMJV 2019, S. 2). Hierdurch würden die Vorschriften zum Schutz von Sachen gelten, sodass auch die sachenrechtlichen Regelungen des gutgläubigen Erwerbs gelten würden. Als Alternative wird jedoch auch eine Einordnung von elektronischen Wertpapieren als neues Recht sui generis gehandelt, demzufolge eigene Schutzbestimmungen geschaffen werden, die auch einen Gutglaubensschutz regeln würden (BMF und BMJV 2019, S. 3). Die Beobachtung dieser rechtlichen Entwicklung ist vor allem im Hinblick auf Security-Token geboten.

Es zeigt sich zum einen, dass die rechtliche Qualifikation gerade von der konkreten Art des Tokens und dem jeweiligen zugrundeliegenden Sachverhalt abhängig ist. Zum anderen ist die Frage der rechtlichen Einordnung von Token auch von der übergeordneten Frage, ob Rechte an virtuellen Gütern bestehen, betroffen (Boehm und Pesch 2014, S. 78).

Im Ergebnis ist es daher ratsam, die rechtliche und tatsächliche Entwicklung zu beobachten, um frühzeitig Rückschlüsse für die Praxis (v. a. für das jeweilige Haftungsregime) ziehen zu können. Vor allem sollte auch ein Augenmerk auf der grundsätzlichen Frage nach der Rechtsqualität von virtuellen Wirtschaftsgütern liegen.

Hinsichtlich sog. Utility- und (vor allem) Security-Token (nähere Erläuterungen unter a) ii)) sieht die deutsche Rechtslage bislang nicht vor, dass zivilrechtliche Wertpapiere auf einer Blockchain begeben werden können, da es für ihre Entstehung einer Verkörperung des jeweiligen Rechts auf einer körperlichen Urkunde bedarf (Kleinert und Mayer 2019, S. 859). Solche Token können lediglich kraft vertraglicher Vereinbarung Ansprüche, Forderungen oder Rechte abbilden (Kleinert und Mayer 2019, S. 859). Da besondere rechtliche Vorschriften für die Übertragung dieser Token fehlen, kann der Fall eintreten, dass ein von dem jeweiligen Token repräsentiertes Recht oder Forderung abgetreten, eine Änderung der Berechtigung in der Blockchain jedoch nicht vorgenommen wird (Kleinert und Mayer 2019, S. 859). Insoweit ist die Blockchain dann fehlerhaft, da sie die wahre Rechtslage nicht mehr abbilden kann.

Solange rechtliche Regelungen hierzu fehlen, muss durch Vertragsgestaltung dafür gesorgt werden, dass der jeweilige Token an sich und das durch ihn repräsentierte Recht nicht auseinanderfallen, mithin die tatsächliche rechtliche Berechtigung nicht von der aus der Blockchain ersichtlichen Rechtslage abweicht (Siedler, in: Möslein und Omlor 2019, § 5, Rn. 21). Insoweit ist es dringend erforderlich, dass die rechtliche Entwicklung für die regulatorische Behandlung von elektronischen Wertpapieren und Token genau verfolgt wird. Das Bundesministerium für Finanzen und das Bundesministerium der Justiz und für Verbraucherschutz haben hierzu bereits im März 2019 ein erstes Eckpunktepapier veröffentlicht (BMF und BMJV 2019).

Aufgrund der besonderen (aufsichts-)rechtlichen Komplexität von solchen Token, die im Rahmen von sog. ICOs emittiert werden, werden diese im folgenden Kapitel gesondert betrachtet.

5.1.2 ICOs

Initial Coin Offerings (ICOs)[2] als neuartige Form der Unternehmensfinanzierung haben in kurzer Zeit eine beachtliche wirtschaftliche Bedeutung erlangt (van Aubel, in: Habersack et al. 2019, § 20, Rn. 20.1). Betrug das Volumen von ICO-Finanzierungsrunden im Jahr 2016 insgesamt 256,4 Millionen US-Dollar, ist dieses im Jahr 2018 bereits auf 16,7 Milliarden US-Dollar gewachsen (Brandt 2019). Auch die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) hat bereits im Jahr 2017 einen rasanten Anstieg von Initial Coin Offerings verzeichnet und zugleich vor den bestehenden rechtlichen Risiken gewarnt (ESMA 13.11.2017).

Der Definition der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) folgend versteht sich ein ICO als Methode, mittels sog. „Tokens" Kapital aufzunehmen (BaFin 2017). Ähnlich wie bei einem Initial Public Offering (IPO) bezweckt ein ICO demnach die Kapitalbeschaffung für ein Unternehmen. Der wesentliche Unterschied ist, dass bei einem ICO nicht wie bei einem IPO die Aktien des Unternehmens, sondern die „Token" interessierten Anleger*innen erstmals zum Kauf angeboten werden (van Aubel, in: Habersack et al. 2019, § 20, Rn. 20.3). Die Besonderheit von ICOs ist demzufolge, dass „Token" anstatt von herkömmlichen Aktien als Finanzierungsinstrument verwendet werden. Dabei ist festzustellen, dass die bei einem ICO angebotenen Token keine standardisierte Form aufweisen, sondern eine Vielzahl von Rechten, Werten oder Zugangsberechtigungen verkörpern können (Klöhn et al. 2018, S. 92). Es besteht hierbei keine einheitliche Begriffsverwendung für die verschiedenen Arten von

[2] Im Folgenden wird der Begriff ICO als Oberbegriff für Initial Coin Offerings (ICOs), Initial Token Offerings (ITOs), Security Token Offerings (STOs) und Token Sales verwendet.

Token, da auch selbst der Begriff "Token" nicht gesetzgeberisch definiert ist (Kleinert und Mayer 2019, S. 859). Im Wesentlichen haben sich aber drei verschiedene Formen von Token herausgebildet (anlehnend an Hacker und Thomale 2017, 12f.). Currency-Token sollen eine neue Kryptowährung erschaffen und somit ein neues Zahlungsmittel darstellen, während Utility-Token dem*der Erwerber*in die Nutzung oder den Zutritt zu bestimmten Produkten oder Dienstleistungen ermöglichen sollen. Zuletzt können die Erwerber*innen durch den Erwerb von Investment-Token (auch Security-Token oder Equity-Token genannt) aktieninhaberähnliche Rechte wie Stimmrechte oder Zahlungsansprüche erhalten. Dabei ist eine eindeutige Einordnung der meisten am Markt befindlichen Token regelmäßig nicht möglich, weil sie häufig Mischformen darstellen – in diesem Fall ist der funktionale Schwerpunkt des jeweiligen Tokens maßgeblich für die Einordnung (BaFin 2019, S. 6).

Trotz der erheblich wachsenden wirtschaftlichen Präsenz bestehen jedoch noch offene Rechtsfragen. Die wohl wichtigste rechtliche Frage ist hierbei, inwiefern die gesetzlichen Regelungen für Transparenz und Anlegerschutz auch für ICOs gelten. Hintergrund ist zum einen, dass im Rahmen der Vorbereitung und Bewerbung eines ICOs sog. White Paper veröffentlicht werden, welche den Anleger*innen Informationen über das geplante ICO geben, die jeweils angebotenen Token beschreiben und zugleich diese bewerben sollen. Regelmäßig entsprechen diese White Paper aber nicht den Vorschriften für Wertpapier- oder Vermögensanlageprospekte und bieten den Anleger*innen daher keinen hinreichenden Schutz (BaFin 2019, S. 1). Zum anderen ist oftmals unklar, inwiefern die jeweils angebotenen Token einer Erlaubnispflicht unterliegen, was die zahlreichen Anfragen bei der BaFin hierzu praxisnah belegen (BaFin 2019, S. 1).

Für die Kapitalbeschaffung durch ein ICO besteht bei den betroffenen Unternehmen somit oftmals keine hinreichende Rechtssicherheit und Planbarkeit. Ein Negativbeispiel hierfür ist das gescheiterte ICO von Munchee-Inc. Das im US-Bundesstaat Kalifornien ansässige Unternehmen wollte durch den Verkauf von Token Kapital für einen geplanten Blockchain-basierten Restaurantbewertungsservice einsammeln, musste den ICO nach einer Unterlassungsverfügung der zuständigen Aufsichtsbehörde (SEC) jedoch abbrechen und den Anleger*innen ihr bereits investiertes Geld sofort zurückerstatten (U.S. Securities and Exchange Commission 11.12.2017), da nach Ansicht der SEC Registrierungspflichten nicht eingehalten wurden (Zaslowsky 2018). Obwohl sich dieses Beispiel auf das US-amerikanische Recht bezieht, zeigt es doch anschaulich, welchen finanziellen und ideellen Schaden die grundsätzlich nicht vorhandene Rechtssicherheit und folglich auch fehlende Planbarkeit bei den emittierenden Unternehmen und betroffenen Anleger*innen im Bereich der ICOs verursachen kann.

Aufgrund der eingangs beschriebenen Ähnlichkeit von IPOs und ICOs stellt sich daher vor allem die grundlegende Frage, ob letztlich auch bei einem ICO Wertpapiere nach § 2 Nr. 1 WpPG i.V.m. nach Art. 2 lit. a) Verordnung (EU) 2017/1129 (ProspektVO) angeboten werden (für die Definition des Begriffs „Wertpapier" nach beiden Normen ist letztlich Art. 4 Abs. 1 Nr. 44 RL 2014/65/EU (MiFID II) maßgeblich (Zickgraf 2018, S. 299)), sodass eine Prospektpflicht gemäß Art. 3 Abs. 1 ProspektVO (zuvor § 3 Abs. 1 WpPG a. F.) für diese besteht (Zickgraf 2018, 298f.). Weiterhin können die jeweiligen Token auch ein Finanzinstrument im Sinne des § 2 Abs. 4 WpHG bzw. nach Anhang 1 Abschnitt C der RL 2014/65/EU (MiFID II), also je nach Ausgestaltung entweder Vermögensanlagen nach § 1 Abs. 2 VermAnlG, Anteile an einem Investmentvermögen nach § 1 Abs. 1 KAGB bzw. Anhang I Abschnitt C (3) MiFID II oder Wertpapiere nach § 2 Abs. 1 WpHG darstellen (BaFin 2017, 2f.). Auch bei einer Qualifizierung als Finanzinstrument nach dem WpHG und der MiFID II kann der volle Anwendungsbereich der jeweiligen aufsichtsrechtlichen Vorgaben in Betracht kommen (Romba und Patz 2019, S. 301).

Des Weiteren können je nach der jeweiligen Ausgestaltung des Token bestimmte Erlaubnispflichten bestehen, wenn die jeweiligen Voraussetzungen nach KWG, ZAG oder KAGB erfüllt werden (BaFin 2017, 4f.). Vor allem bei Security-Token führt beispielsweise eine (wohl regelmäßige) Einordnung als Wertpapier auch zur Einordnung als Finanzinstrument nach § 1 Abs. 11 S. 1 Nr. 1 bis 5 KWG, wonach die Anlageberatung und Anlagevermittlung (§§ 1 Abs. 1 lit. a S. 2 Nr. 1, 1 lit. a KWG, § 2 Abs. 8 S. 1 Nrn. 4, 10 WpHG) gemäß § 32 Abs. 1 KWG der vorherigen Erlaubnis der BaFin bedarf (Weitnauer 2018, S. 234). Aufgrund der jüngsten Änderung des KWG durch die Umsetzung der 5. EU-Geldwäscherichtlinie sind nun "Kryptowerte" als Finanzinstrumente nach § 1 Abs. 11 S. 1 Nr. 10 KWG ausdrücklich geregelt. § 1 Abs. 11 S. 4 KWG definiert "Kryptowerte" nun wie folgt:

"*Kryptowerte im Sinne dieses Gesetzes sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.*"

Die Definition geht über den in der 5. EU-Geldwäscherichtlinie verwendeten Begriff der "virtuellen Währung" hinaus und ist als Auffangtatbestand für solche Token konzipiert, die nicht bereits unter eine andere Unterkategorie nach § 1 Abs. 11 KWG fallen (Kleinert und Mayer 2019, S. 862). Insoweit das KG Berlin entgegen der Ansicht der BaFin (BaFin 2011) bisher bei

Currency-Token (namentlich Bitcoin) davon ausgegangen ist, dass diese kein Finanzinstrument nach dem KWG darstellen (KG Berlin 2018, 2015), wird dies nun explizit gesetzlich festgehalten. Security-Token sind hingegen nur dann von der neuen Definition der "Kryptowerte" erfasst, soweit sie nicht bereits als Schuldtitel, Vermögensanlage oder Investmentvermögen nach § 1 Abs. 11 S. 1 Nrn. 2, 3 oder 5 KWG einzustufen sind. Ob Utility-Token davon umfasst sind, ist unklar, wobei jedoch zumindest bei solchen Utility-Token, die auch Anlagezwecken dienen, eine Einordnung in Betracht kommen könnte (Kleinert und Mayer 2019, S. 861).

Jeweils maßgeblich für eine Einordnung eines Tokens ist – nicht zuletzt auch aufgrund der Vielseitigkeit der verschiedenen Token – stets die jeweils verwendete Art (v. a. Security-, Utility- oder Currency-Token) von Token und somit letztlich das Recht, welches vom jeweiligen Token verkörpert wird (Zickgraf 2018, S. 295 mwN). Aus diesem Grund ist eine klare Katalogisierung der verschiedenen Arten von Token evident, um diese voneinander abgrenzen zu können. Aus Sicht der Rechtsliteratur besteht dabei wohl weitestgehende Einigkeit darüber, dass Security-Token regelmäßig Wertpapiere darstellen, Currency-Token hingegen nicht und Utility-Token je nach deren konkreter Ausgestaltung Wertpapiere sein können (Chatard und Mann 2019, S. 572).

Dabei besteht auf europäischer und deutscher Ebene aber gerade keine deutliche Positionierung der zuständigen Aufsichtsbehörden. Die ESMA geht davon aus, dass Token abhängig von ihrer Struktur unter die Regelungen des europäischen (und ggf. nationalen) Kapitalmarktrechts fallen können, nennt hierfür jedoch keine Abgrenzungskriterien für die Marktteilnehmer*innen (ESMA 2017). Die ESMA geht jedoch in ihrer Handlungsempfehlung vom 9. Januar 2019 aufgrund der besonderen Herausforderungen durch "Krypto-Assets" an die Regulierungsbehörden und Marktteilnehmer*innen von einer möglichen Regulierungsbedürftigkeit aus (ESMA 2019, S. 4). Auch die BaFin geht von einer erforderlichen Einzelfallprüfung des jeweiligen Token aus und fordert die Marktteilnehmer*innen dazu auf zu prüfen, ob ein reguliertes Instrument wie beispielsweise ein Finanzinstrument oder ein Wertpapier vorliegt, um etwaige gesetzliche Regelungen erfüllen zu können (BaFin 2017). Dabei nennt sie die Voraussetzungen der jeweiligen für die Einordnung relevanten Rechtsnormen und zeigt die grundsätzliche Möglichkeit der Einordnung von Token unter diese Rechtsnormen auf. Von einem Wertpapier nach Art. 4 Abs. 1 Nr. 44 RL 2014/65/EU (MiFID II) ist gemäß dem ersten Hinweisschreiben der BaFin vom 20.2.2018 bei einem Token beispielsweise dann auszugehen, wenn der jeweilige Token übertragbar, an den Finanz- oder Kapitalmärkten handelbar ist, Beteiligungs- oder schuldrechtliche Vermögensrechte verkörpert und zugleich kein reines Zahlungsmittel darstellt (Zusammenfassend Romba und

Patz 2019, S. 301; ausführlich BaFin 2017, 3f.). Auch zu der Möglichkeit, dass bestimmte Token verschiedenen Erlaubnispflichten unterliegen können, äußert sich die BaFin im Merkblatt vom 19. August 2019 ausführlich (BaFin 2019, 9ff.). Festzuhalten ist daher zunächst, dass es zu den (kapitalmarkt-)rechtlichen Anforderungen von ICOs ausführliche Äußerungen seitens der zuständigen nationalen Aufsichtsbehörde gibt.

Zum einen ist aber zweifelhaft, ob die Einschätzungen der Aufsichtsbehörden, vor allem die auf den ersten Blick praktikable Einschätzung der BaFin, eine ausreichend weite Aussagekraft zukommt, um Rechtssicherheit zu schaffen. Denn es ist grundsätzlich nicht die Aufgabe von Bundesbehörden, rechtsgestaltend tätig zu sein (KG Berlin 2018, 2017). Insoweit kommt einem Merkblatt der BaFin kein rechtsgestaltender Charakter zu (KG Berlin 2018, 2017). Die Befolgung der aufsichtsbehördlichen Einordnungen schützt somit zwar vor einem möglichen Einschreiten durch die Aufsichtsbehörde, garantiert aber nicht, dass bei möglichen gerichtlichen Auseinandersetzungen diesen Einschätzungen gefolgt wird. Gerade bei der Entwicklung neuer wirtschaftlicher Produkte ist es aber von zentraler Bedeutung, dass das jeweilige innovative Unternehmen rechtssicher beurteilen kann, ob und unter welchen Voraussetzungen eine Haftung infrage kommt. Ist das nicht der Fall, so wird die Innovationsfähigkeit gehemmt.

Zum anderen bestehen noch weitere offene Rechtsprobleme. Für die Voraussetzung der Handelbarkeit im Rahmen der Einordnung von Token als Wertpapier ist beispielsweise umstritten, inwiefern die Möglichkeit eines gutgläubigen Erwerbs für die Bejahung dieser Voraussetzung notwendig ist (Zickgraf 2018, S. 301 mwN). Da Token keine Sachen nach § 90 BGB darstellen (so für Currency-Token Fritzsche, in: Bamberger/Roth/Hau/Poseck 2020, § 90 BGB, Rn. 7), ist die direkte Anwendung der sachenrechtlichen Regelungen des gutgläubigen Erwerbs unklar und umstritten (zum gutgläubigen Erwerb von Token im Einzelnen Kap. a) i)). Bejaht man also die Möglichkeit eines gutgläubigen Erwerbs als Voraussetzung für die Handelbarkeit, kann die Einordnung von Token als Wertpapier demzufolge ausscheiden (ausführlich Zickgraf 2018, S. 301). Des Weiteren wird für die Einordnung als Wertpapier im kapitalmarktrechtlichen Sinn auch die funktionale Vergleichbarkeit mit den gesetzlich geregelten Regelbeispielen nach Art. 4 Abs. 1 Nr. 44 lit. a)-c) MiFID II und § 2 Nr. 1 lit. a)-c) WpPG gefordert (Koch 2018, S. 366; Zickgraf 2018, S. 302). Gerade aufgrund der Vielzahl der aufkommenden Formen von Token (vor allem bei sog. Hybrid-Token, welche Mischformen darstellen) ist eine solche funktionelle Vergleichbarkeit wiederum nur nach einer aufwendigen Einzelfallprüfung möglich (ausführlich hierzu Zickgraf 2018, 302ff.), die einerseits sicherlich gerade die

Leistungsfähigkeit von Start-Ups überschreitet und andererseits den Prüfungsaufwand bei der zuständigen Aufsichtsbehörde wachsen lässt.

Da vor allem die Tokenisierung von gesellschaftsrechtlichen Rechtspositionen vermehrt Gegenstand von ICOs ist (von „Equity-Tokens“ und somit von ETOs sprechend Hahn und Wilkens 2019, S. 10), welche Wertpapieren gleichen (sollen), besteht weiterhin die bislang nicht geklärte Frage, welche Rolle dem sog. Abspaltungsverbot nach § 717 BGB zukommt, welches besagt, dass keine neuen gesellschaftsrechtlichen Rechtspositionen geschaffen werden sollen (Klöhn et al. 2018, S. 93). Denn viele solcher Token, die in den vergangenen Jahren den Anleger*innen angeboten wurden, verkörperten verschiedene, rechtlich nicht anerkannte gesellschaftsrechtliche Rechtspositionen (Klöhn et al. 2018, S. 93; Koch 2018, S. 364; Weitnauer 2018, S. 232).

Um an ICOs interessierten Unternehmen, vor allem Start-Ups, und Anleger*innen einen geeigneten Wirtschaftsraum schaffen zu können, ist das Bestehen von Rechtssicherheit von hoher Bedeutung. Für Unternehmen ist es evident wichtig mit hoher Rechtssicherheit einordnen zu können, ob eine Haftung für fehlende oder mangelhafte Prospekte (beispielsweise nach §§ 21, 22, 24 WpPG) oder gar eine Straftat nach § 54 Abs. 1 Nr. 2 KWG aufgrund fehlender Erlaubnis zur Erbringung von Finanzdienstleistungen nach § 32 Abs. 1 S. 1 KWG bei einem geplanten ICO bestehen kann, während Anleger*innen von einem wirkungsvollen Anlegerschutz profitieren wollen. Nicht zuletzt ist aufgrund der steigenden Zahl von ICOs die Gewährleistung der Allokationsfunktion notwendig (Zickgraf 2018, S. 293).

Im Steuerrecht bestehen hingegen keine Einordnungsprobleme. Aus steuerrechtlicher Sicht lassen sich getätigte Investitionen in Token unter § 15 Abs. 2 EStG einordnen, wonach Investitionen in sie von gewerblicher Natur sein können (Albrecht und John 2018, S. 406). Die durch die Rechtsprechung des BFH entwickelten Grundsätze zum Wertpapierhandel sind auf den An- und Verkauf von Token zu übertragen (Albrecht und John 2018, 401ff.; allgemein hier auch Weitnauer 2018, S. 235).

Die zuvor aufgeführten Punkte legen jedoch dennoch den Rückschluss nahe, dass eine gesetzgeberische Grundsatzentscheidung über die aufsichtsrechtliche Behandlung der jeweiligen Arten von Token aus Gesichtspunkten der Rechtssicherheit begrüßenswert wäre. Darüber hinaus ist die Ausarbeitung von einheitlichen Definitionen und Abgrenzungskriterien für die verschiedenen Token-Arten wünschenswert, da diese bisher lediglich von der Rechtsliteratur (bspw. in Romba und Patz 2019, S. 302) und der BaFin (2019, 5f.) ausgearbeitet wurden und sich schon in ihrer Namensgebung unterscheiden. Exemplarisch hierfür sei die Verwendung der Wörter „Security-Token“, „Equity-Token“, „Asset-Token“ oder „Investment-

Token“ (angelehnt an die Begriffsverwendung aus der Tabelle von Romba und Partz 2019, S. 302; beispielsweise Hahn und Wilkens 2019, S. 10 ff. sprechen wiederum nur von Equity-Token; statt „Currency-Token“ von „Kryptowährungs-Token“ sprechend etwa Koch 2018, S. 361), welche letztendlich alle die besonders relevanten wertpapierähnlichen Token beschreiben sollen. Aus Gesichtspunkten des (privaten) Anlegerschutzes ist eine einheitliche Verwendung der Bezeichnungen wünschenswert, um eine eindeutige Klassifizierung der Token bei den jeweiligen interessierten Anleger*innen zu erreichen.

Auch besteht durch die Tokenisierung erstmals die Möglichkeit, bislang nicht verkehrsfähige Rechtspositionen dem Kapitalmarktrecht zu unterwerfen (Koch 2018, S. 366, der die grundsätzliche Möglichkeit hierzu gerade sog. Hybrid-Tokens bescheinigt). Insoweit sollte diese Entscheidung vom Gesetzgeber getroffen werden, um diesen Effekt nicht den emittierenden Unternehmen und letztlich auch den Aufsichtsbehörden zu überlassen. Des Weiteren stehen die rechtlichen Schranken des Gesellschaftsrechts im Widerspruch mit einer solchen Vorgehensweise, weshalb der Gesetzgeber aktiv werden müsste, wenn er sich für solch weitreichende Möglichkeiten durch die Blockchain-basierte Übertragung von Gesellschaftsanteilen entscheiden will (Hahn und Wilkens 2019, 14f.), um Unternehmen neue Handlungsmöglichkeiten zu gewähren.

Zuletzt kann die Frage gestellt werden, ob neben der Annahme einer wertpapierrechtlichen Prospektpflicht bei lediglich bestimmten Arten von Token (meist bei Investment-Token) nicht ein grundsätzliches (v. a. verbraucherschutzrechtliches) Interesse an einer allgemeingültigen rechtlichen Regelung der grundlegenden Informationspflichten für die einen Token bewerbenden White Paper besteht. Denn auch Utility- und Currency-Token weisen eine Investitionskomponente auf, da diese Arten von Token wiederum auf Sekundärmärkten mit Gewinnerzielungsabsicht gehandelt werden können (Hacker und Thomale 2017, S. 13). Insoweit kann auch hier eine vergleichbare Schutzwürdigkeit der Erwerber*innen solcher Token angenommen werden. Es ist jedoch generell zu beobachten, dass White Paper regelmäßig keinen hinreichenden Schutz für Anleger*innen schaffen (BaFin 2019, S. 1). Es besteht aber de lege lata keine rechtliche Verpflichtung oder ein rechtlicher Rahmen für die Veröffentlichung eines Prospektes oder qualifizierten Informationspapiers für Utility- oder Currency-Token (BMWi und BMF 2019, S. 6). Dennoch wird in der bisherigen juristischen Literatur - soweit ersichtlich - keine generelle rechtliche Regulierung dieser White Paper thematisiert. Eine Notwendigkeit für die Schaffung angemessener Risikoaufklärungspflichten durch die politischen Entscheidungsträger der EU wird jedoch von der ESMA angenommen (ESMA 2019, S. 40). Daher liegt die Annahme nahe, dass die juristische Diskussion dieser noch offenen Frage beobachtet werden sollte.

5.1.3 Möglichkeit der Anspruchsdurchsetzung

Die wachsende Verbreitung und wirtschaftliche Bedeutung von Blockchain-basierten Token und Smart Contracts drängt auch notwendigerweise die Frage auf, nach welchen Voraussetzungen die verschiedenen Arten praktikabel vollstreckt werden können.

(a) Token

Aus rechtlicher Sicht ist einerseits fraglich, ob die Zivilprozessordnung (ZPO) und Insolvenzordnung (InsO) de lege lata überhaupt die umfassende Vollstreckung von Token ermöglichen und andererseits, ob das Verfahren der Vollstreckung effektiv ausgestaltet werden kann.

Innerhalb der Einzelvollstreckung nach der ZPO muss grundsätzlich zwischen der Vollstreckung in Token-Guthaben wegen einer Geldforderung, der Vollstreckung in Ansprüche auf Übertragung von Token und der Vollstreckung von Ansprüchen auf Übertragung von Token unterschieden werden (Effer-Uhe 2018, S. 513).

Bei der Vollstreckung in Token-Guthaben wegen einer Geldforderung kommt lediglich die Vollstreckung in andere Vermögensrechte nach §§ 857, 828 ff. ZPO (analog) in Betracht (Effer-Uhe 2018, S. 518; Kütük und Sorge 2014, S. 644). Teilweise wird hier lediglich die Möglichkeit gesehen, dass auf vertraglichen Beziehungen beruhende Herausgabeansprüche von Token gegen Dritte pfändbar sind (Kütük und Sorge 2014, S. 644). Jedoch wird auch vertreten, dass sich die Token des Zwangsvollstreckungsschuldners dann direkt pfänden lassen, wenn es sich bei der Inhaberschaft von Token um ein „anderes Vermögensrecht“ nach § 857 Abs. 1 ZPO handelt, was jedoch als höchst problematisch angesehen wird (Boehm und Pesch 2014, S. 79; Effer-Uhe 2018, 517ff., wonach der faktischen Verfügungsgewalt über den jeweiligen Token Rechtsqualität zukommen müsste). Teilweise wird eine Anwendung des § 857 Abs. 1 ZPO auch gänzlich deshalb abgelehnt, da dieser aufgrund seines klaren Wortlauts und seines systematischen Verweises auf die Vorschriften der Forderungspfändung das Bestehen eines “Rechts” beim Vollstreckungsschuldner voraussetzt (Rückert 2016, S. 297). Es erscheint daher evident, dass die grundsätzliche Diskussion um die Frage, ob virtuelle Güter (absolute) Rechte darstellen können, aufmerksam verfolgt wird. Denn insoweit Token als rein virtuell existierenden (Wirtschafts-)Gütern eine rechtliche Stellung als (absolutes) Recht zukommt, lassen sie sich folglich auch als “Vermögensrecht” gem. § 857 Abs. 1 ZPO zuordnen.

Als unproblematisch werden die Fallgestaltungen angesehen, bei denen die Vollstreckung in Ansprüche auf Übertragung von Token erfolgen soll – diese lassen sich wie schon erwähnt problemlos über § 857 Abs. 1 ZPO pfänden.

Andererseits wird vereinzelt eine Anwendung der Vorschriften über die Sachpfändung nach § 808 ff. ZPO analog vertreten, soweit eine Speicherung des privaten Schlüssels auf einem Datenträger vorliegt (so zumindest für die Sicherung von Currency-Token (hier Bitcoins) im Ermittlungsverfahren durch dinglichen Arrest Rückert 2016, S. 297).

Unklar ist jedoch wiederum, ob die Vollstreckung von Ansprüchen auf die Übertragung von Token als vertretbare Handlung nach § 887 Abs. 1 ZPO oder als unvertretbare Handlung nach § 888 Abs. 1 ZPO erfolgen kann (für eine Einordnung als vertretbare Handlung Effer-Uhe 2018, S. 529; a. A. Bausch und Heetkamp 2018, 9f.; Kütük und Sorge 2014, S. 645; Schroeder 2014, Abs. 114). Praktische Auswirkungen hat diese Rechtsfrage vor allem für die korrekte Titulierung des Vollstreckungstitels. Auch insoweit der private Schlüssel lokal in einer Datei oder (was weitaus geläufiger ist) bei einem Anbieter eines Online-Wallets gespeichert ist, kommt zudem in Betracht, die Herausgabe der Datei oder die Übertragung des Herausgabeanspruchs zu verlangen (Rückert 2016, S. 299).

Doch selbst wenn man de lege lata von einer umfassenden Möglichkeit der Vollstreckung von Token ausgeht, stellen die Besonderheiten von Blockchain-basierten virtuellen Token das anschließende Verfahren vor Probleme. Hierbei ist es schon fraglich, ob die Normen der ZPO die Überweisung der jeweiligen Token auf einen Behördenschlüssel überhaupt hergeben – nur durch eine solche Überweisung wären die Token vor einer Einwirkungsmöglichkeit des Vollstreckungsschuldners geschützt (zu diesem Problem bei §§ 857 Abs. 1, 2, 828 ff. ZPO Effer-Uhe 2018, S. 525). Zuletzt haben Blockchain-basierte Token gemeinsam, dass es ihnen an einem Intermediär fehlt, den man zur Überweisung der vom jeweiligen Anspruch umfassten Token beauftragen kann. Der*die Vollstreckungsschuldner*in kann somit faktisch nur durch Zwangsgeld oder Zwangshaft (beispielsweise im Falle des § 888 Abs. 1 S. 1 ZPO) zu einer Transferierung der Token bewogen werden, wenn diese*r sich weigert (Kütük und Sorge 2014, S. 645). Doch selbst wenn die Überweisung auf einen Behördenschlüssel erfolgen würde, könnte jede Person, die Kenntnis von dem dazugehörigen privaten Schlüssel erlangt, die Token anonym transferieren (Effer-Uhe 2018, S. 525).

Im Rahmen der Gesamtvollstreckung lassen sich Token auf den ersten Blick nach § 35 Abs. 1 InsO in die Insolvenzmasse einordnen. Eine ausführliche rechtliche Analyse dessen steht jedoch bisher aus (Effer-Uhe 2018, S. 525; Kütük und Sorge 2014, S. 645).

Insoweit stellen sich aber auch im Rahmen der Gesamtvollstreckung die praktischen Probleme des Ablaufs des Vollstreckungsverfahrens.

Vor allem die Ausgestaltung des Verfahrens der Vollstreckung von Blockchain-basierten Token ist de lege lata folglich noch als nicht effektiv und ungeklärt zu betrachten. Insoweit ist aber bisher nicht festzustellen, dass hierdurch ein Hindernis besteht, da die bislang fehlenden gerichtlichen Entscheidungen zu derart gelagerten Fällen zeigen, dass es sich bisher noch um ein Randproblem handeln sollte. Soweit die Verkehrsfähigkeit von Token jedoch steigen sollte, erhält dieses Problem wiederum steigende Bedeutung.

(b) Smart Contracts

Die Frage nach einer wirksamen Durchsetzung von Ansprüchen ist im Kontext von Smart Contracts, hier verstanden als Mechanismus der Vertragsausführung (vgl. Kaulartz und Heckmann 2016, S. 621), besonders relevant. Im Allgemeinen bieten die bestehenden zivilrechtlichen Regelungen ausreichend Flexibilität, um Fragen im Zusammenhang mit Blockchain-basierten Smart Contracts zufriedenstellend zu lösen (Paulus und Matzke 2018). Dringender Anpassungsbedarf ist insofern nicht erkennbar. In praktischer Hinsicht kann sich die Durchsetzung von Ansprüchen, die mit Hilfe einer Blockchain-Transaktion zu erfüllen sind, aus den oben beschriebenen Gründen schwierig gestalten. Auch wenn rechtliche Konflikte, die im Zusammenhang mit Smart Contracts entstehen, unzweifelhaft vor staatlichen Gerichten verhandelt werden können (Kaulartz 2019, Rn. 12) bleiben die aufgezeigten Probleme angesichts der Vollstreckung ungelöst.

5.1.4 Konfliktlösungsmechanismen

Angesichts der soeben beschriebenen Schwierigkeiten bei der Anspruchsdurchsetzung ist über effektive Konfliktlösungsmechanismen nachzudenken. Teilweise werden in diesem Zuge Smart Contract-Schnittstellen zu staatlichen Gerichten gefordert (Bertram 2018, S. 1420; Simmchen 2017, S. 164). Bei entsprechender Ausgestaltung könnten die Gerichte dann eingreifen und geschuldete Transaktionen ohne Zutun des Schuldners auslösen. Eine tiefergehende Auseinandersetzung mit der konkreten Umsetzung solcher Lösungen ist bisher allerdings nicht ersichtlich. Vollkommen offen ist zum Beispiel, welche Änderungen der ZPO notwendig wären und wie die notwendige Infrastruktur geschaffen werden könnte. Zu beobachten ist eher eine Diskussion über alternative, technische Konfliktlösungsmechanismen, die im Ergebnis vielfach auf eine private Rechtsdurchsetzung hinauslaufen.

Für Fälle, die den Transfer von Werten auf der Blockchain betreffen, kommt eine Drei-Personen-Lösung (Werbach 2018, S. 546) in Betracht. Eine solche kann z.B. dort zum Einsatz kommen, wo ein durch einen Smart Contract übertragener Wert zurückgewährt werden soll. Alle Parteien und eine neutrale Stelle halten einen Private Key. Um die Transaktion auszulösen, muss diese mit zwei von drei Schlüsseln signiert werden. Sind sich die Parteien uneinig, kann die neutrale Stelle die Transaktion entweder freigeben oder verweigern. Smart Contracts könnten außerdem so gestaltet werden, dass ihr Ablauf durch zwei von drei Schlüsselinhaber*innen verhindert werden kann.

In eine ähnliche Richtung gehen Vorschläge, die spezielle Schiedsgerichte vorsehen (Smart Contract Dispute Resolution): Diesen Stellen könnten Einflussmöglichkeiten auf den weiteren Ablauf des Smart Contracts eingeräumt werden, z.B. in Form von standardisierten Programmbibliotheken (Kaulartz 2019, S. 78). Soweit die Schiedsstelle auch Transaktionen innerhalb des Smart Contracts kontrollieren kann, entfällt das Bedürfnis nach einer Zwangsvollstreckung, jedenfalls solange die Ansprüche ihrer Höhe oder ihrem Inhalt nach nicht außerhalb des Smart Contracts liegen (Kaulartz 2019, S. 79). Notwendig wäre eine wirksame Schiedsvereinbarung, §§ 1029 ff. ZPO. Sind Verbraucher*innen beteiligt, begrenzt § 1031 Abs. 5 ZPO (insbesondere das Schriftformerfordernis nach S. 1, aber auch die Begrenzung des Inhalts des Dokuments nach S. 3) die Freiheit, eine Schiedsvereinbarung zu treffen. Gem. § 1031 Abs. 6 ZPO besteht aber eine Heilungsmöglichkeit für unwirksame Schiedsvereinbarungen, wenn sich die Parteien auf die schiedsgerichtliche Verhandlung einlassen (Kaulartz 2019, 76f.).

Als besonders ausgereifte Lösung käme die Einbindung eines Konfliktlösungsmoduls für Smart Contracts über eine Programmierschnittstelle (API) in Betracht, welches verschiedene Formen der Konfliktlösung (abhängig von der jeweiligen "Eskalationsstufe") bereithält, angefangen bei einer automatisierten, regelbasierten Konfliktlösung bis hin zur gerichtlichen Klärung (so vorgeschlagen von Erbguth 2016, 294ff.).

5.2 Datenschutzrecht

Das Datenschutzrecht stellt eine der größten Herausforderungen für den Einsatz der Blockchain-Technologie dar (siehe auch Gentemann 2019, S. 40). Teilweise werden zwar die Chancen der Technologie für die Gewährleistung von Datensouveränität aufgezeigt. Insbesondere soll es vielversprechende Modelle für das Identitätsmanagement geben (Bechtolf und Vogt 2018, S. 71). Eine Unabhängigkeit von Intermediären wird als Chance gesehen, dem*der Einzelnen mehr Kontrolle über die eigenen Daten zu geben, ein Ziel, das auch die DSGVO verfolgt, siehe Erwägungsgrund 7 S. 2 (ausführlich Finck 2019a, 92ff.).

Dennoch gibt es erhebliche Spannungen zwischen einigen Grundideen von Blockchain und den Bestimmungen der DSGVO. Für Anwender*innen besteht die Aufgabe darin, eine rechtskonforme Gestaltung zu wählen. Diesbezüglich herrscht viel Unsicherheit, was auch Angst vor der Eingehung von Haftungsrisiken (insbesondere in Form von Bußgeldern für Datenschutzverstöße) auslösen kann (Vgl. z.B. Blockchain Bundesverband 2018, S. 2).

Eine abschließende datenschutzrechtliche Beurteilung setzt stets eine individuelle Betrachtung des konkreten Anwendungsfalls voraus. An dieser Stelle sollen zentrale Blockchain-spezifische Fragestellungen behandelt und die wichtigsten datenschutzrechtlichen Hindernisse identifiziert werden.

5.2.1 Anwendbarkeit der DSGVO

Die DSGVO regelt die Verarbeitung personenbezogener Daten. Der Begriff der Verarbeitung (Art. 4 Nr. 2 DSGVO) ist weit zu verstehen und umfasst jeglichen Umgang mit personenbezogenen Daten (Gola in: Gola, Art. 4 DSGVO Rn. 30). Im Kontext von Blockchain-Anwendungen fallen daher beispielsweise das Einpflegen personenbezogener Daten, ihre Speicherung und jede weitere Verwendung, u.a. auch zur Konsensfindung innerhalb des Netzwerks, unter den Begriff der Verarbeitung (Finck 2019a, S. 10).

In räumlicher Hinsicht ist die DSGVO zum einen dann anwendbar, wenn der für die Datenverarbeitung Verantwortliche oder ein Auftragsverarbeiter seine Niederlassung in der Europäischen Union hat. Zum anderen findet die DSGVO auch Anwendung, wenn personenbezogene Daten betroffener Personen verarbeitet werden, die sich in der Europäischen Union befinden und denen Waren oder Dienstleistungen innerhalb der Union angeboten werden oder deren Verhalten beobachtet wird (Art. 3 Abs. 1, 2 DSGVO).

Geschützt werden nur natürliche Personen. Daten, die allein juristische Personen betreffen, fallen nicht in den Anwendungsbereich der DSGVO. Zu beachten ist allerdings, dass auch Daten über juristische Personen Rückschlüsse auf natürliche Personen zulassen können und der Anwendungsbereich des Datenschutzrechts dann wieder eröffnet ist.

Zentrale Bedeutung hat der Begriff der personenbezogenen Daten, deren genaue Definition gewisse Schwierigkeiten bereitet. Ergibt sich die Identität nicht unmittelbar aus den verwendeten Daten (wie z.B. bei Verwendung des Klarnamens), kommt es maßgeblich auf die Identifizierbarkeit der hinter den Daten stehenden natürlichen Person an, vgl. Art. 4 Nr. 1 DSGVO. Nach Erwägungsgrund 26 der DSGVO sind alle Mittel zu berücksichtigen, „*die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu*

identifizieren". Hierzu hat der EuGH präzisiert, dass nicht alle zur Identifizierung notwendigen Informationen bei einer Person vorhanden sein müssen. Vielmehr kann der Personenbezug schon bejaht werden, wenn eine Person über rechtliche Mittel verfügt, entsprechende Informationen zu erhalten (EuGH, Urteil vom 19.10.2016 – C-582/14 (Patrick Breyer), Rn. 43, 49). Im Kontext von Blockchain-Anwendungen bedeutet dies konkret, dass Public Keys und Transaktionsdaten (Daten im Zusammenhang mit Transaktionen, die aber keine Public Keys sind) personenbezogene Daten sein können (Finck 2019a, S. 28). Da im Zusammenhang mit Blockchain-Transaktionen verschiedenste Arten von Daten übermittelt werden können, ist das für Transaktionsdaten leicht nachzuvollziehen (Finck 2019a, 28f.). Public Keys lassen dagegen die dahinterstehende Person nicht ohne weiteres erkennen, da es sich lediglich um eine Reihe von Zahlen und Buchstaben handelt. Hier kann aber mit Hilfe einer Gesamtschau mit zusätzlichen Informationen durch verschiedene Verfahren eine Verbindung zu einer natürlichen Person hergestellt werden (Finck 2018, S. 24; Lyons et al. 2018a, S. 20). Eine solche Nutzung ist auch ausreichend wahrscheinlich, da Public Keys bereits von staatlicher Seite, durch kommerzielle Anbieter*innen und durch die Wissenschaft zur Identifikation genutzt wurden (Finck 2018, S. 24 mwN; BSI 2019, S. 39 mwN). Auf die Personenbeziehbarkeit von Blockchain-Daten und ihre Beseitigung wird in Abschnitt iii) näher eingegangen, wenn die rechtskonforme Gestaltung von Anwendungen diskutiert wird.

5.2.2 Verantwortlichkeit

Verantwortlich im Sinne der DSGVO ist, wer „*allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet*", Art. 4 Nr. 7 DSGVO.

Die Frage nach dem Verantwortlichen ist äußerst relevant, weil dieser der Adressat datenschutzrechtlicher Pflichten ist. Kann/können der/die Verantwortlichen nicht identifiziert werden, so ist für Betroffene und Behörden kein Verpflichteter greifbar (vgl. Lyons et al. 2018a, 24f.). Auch für die Anwender*innen ist die Frage von erheblicher Bedeutung, da sie sich bei Nichterfüllung der datenschutzrechtlichen Pflichten Haftungsrisiken aussetzen. Diverse Pflichten treffen den Verantwortlichen schon vor Beginn der eigentlichen Datenverarbeitung (Finck 2019a, S. 51). Zentral ist außerdem, dass ein Verantwortlicher i.S.d. DSGVO einer Rechtfertigungsgrundlage (Art. 6 DSGVO) für jede Datenverarbeitung bedarf.

Für die Beantwortung der Frage nach dem Verantwortlichen ist die Unterscheidung zwischen den verschiedenen Arten der Blockchain von Bedeutung. In öffentlichen Blockchains steht die Teilnahme und die Einsicht in die gespeicherten Informationen einem beliebigen Personenkreis offen. In privaten Blockchains entscheidet dagegen eine zentrale Instanz über

die Aufnahme von Teilnehmer*innen in das System. Ferner unterteilt man nach dem Grad der Zugriffsberechtigung in sog. “permissioned” (zulassungsbeschränkte) und “permissionsless” (zulassungsfreie) Blockchains. Während in letzteren jede*r Teilnehmer*in alle Aktionen ausführen kann, sind in ersteren bestimmte Handlungen (z. B. die Teilnahme an der Konsensfindung) einzelnen Akteuren vorbehalten.

In privaten Blockchains, wo eine zentrale Stelle existiert, kann diese regelmäßig als Verantwortlicher identifiziert werden (Finck 2019a, S. 43). Obliegt die Governance des Systems einem Konsortium, ist an eine gemeinsame Verantwortlichkeit der Mitglieder i.S.v. Art. 26 DSGVO zu denken (Martini und Weinzierl 2017, S. 1254). Nodes und Miner werden regelmäßig lediglich als Auftragsdatenverarbeiter (Art. 28 DSGVO) tätig, die im Interesse der zentralen Instanz und nach deren Weisungen handeln und selbst nicht als Verantwortliche anzusehen sind (Martini und Weinzierl 2017, S. 1254).

Deutlich komplexer gestaltet sich die Bestimmung des Verantwortlichen in öffentlichen zulassungsfreien Blockchains. Die DSGVO basiert auf der Grundannahme, dass Datensammlung und -verarbeitung zentralisiert erfolgen und zielt auf die Regulierung solcher Zentralstellen ab. Dies steht in Konflikt mit den Prinzipien auf Dezentralität angelegter offener Blockchain-Systeme (Ibáñez et al. 2018, S. 5; Lyons 2018, S. 16). Eine oder mehrere steuernde Instanzen lassen sich kaum ausmachen. Verschiedene Akteure spielen eine Rolle, nicht alle sind aber als Verantwortliche anzusehen. So stellen die Entwickler*innen einer Blockchain-Architektur anderen lediglich eine Infrastruktur zur Verfügung und beeinflussen konkrete Datenverarbeitungsvorgänge nicht. Sie werden deshalb in aller Regel nicht als Verantwortliche anzusehen sein (Lyons et al. 2018a, S. 18; Finck 2019a, S. 46; Martini und Weinzierl 2017, S. 1253). Nutzer*innen, die Transaktionen in das Netzwerk einstellen, können als Verantwortliche angesehen werden, wenn es sich um andere als ihre eigenen personenbezogenen Daten handelt (Lyons et al. 2018a, S. 18; Finck 2019a, S. 48).

Schwieriger zu beurteilen ist die Stellung der einzelnen Nodes. Während deren Stellung als Verantwortlicher teilweise abgelehnt wird (Lyons et al. 2018a, S. 18; Blockchain Bundesverband 2018, S. 6 mit Hinweis auf Einordnung als Infrastruktur), lässt sich auch feststellen, dass sie keinen Weisungen unterliegen, eigene Entscheidungen über die Art und Weise ihrer Teilnahme am System treffen und eigene Zwecke verfolgen (Martini und Weinzierl 2017, S. 1253; Finck 2018, S. 26). Jeder Node verfügt frei über die in seiner Kopie der Blockchain eingetragenen Daten (Martini und Weinzierl 2017, S. 1254). In öffentlichen Systemen ist eine gemeinsame Verantwortlichkeit der Nodes i.S.v. Art. 26 DSGVO eher abzulehnen, da jeder von

ihnen unabhängig über die Art und Weise seiner Teilnahme am System entscheidet und eine gemeinsame Entscheidung über die Zwecke und Mittel der Datenverarbeitung nicht erkennbar ist (Böhme und Pesch 2017, S. 479; Finck 2018, S. 26). Die einzelnen Nodes beeinflussen auch die Datenverarbeitungen der anderen nicht (Martini und Weinzierl 2017, S. 1254). Zum Teil wird eine zusätzliche Unterscheidung zwischen Minern und Nodes vorgeschlagen. Miner, die nur neue Blöcke errechnen und deren Inhalt nicht beeinflussen, sollen demnach nicht für die Datenverarbeitung verantwortlich sein (Martini und Weinzierl 2017, S. 1253).

Stuft man jeden einzelnen Node als Verantwortlichen ein, bereitet dies in praktischer Hinsicht erhebliche Probleme. Die potenziell unüberschaubare Menge an Verantwortlichen schließt eine effektive Durchsetzung von Rechten und Pflichten durch Betroffene und Behörden faktisch aus (Martini und Weinzierl 2017, S. 1255). Zusätzlich werden die einzelnen Nodes in einem Großteil der Fälle aufgrund der Architektur des Netzwerks nicht in der Lage sein, datenschutzrechtlichen Verpflichtungen nachzukommen (Bechtolf und Vogt 2018, S. 69; Finck 2018, S. 26).

5.2.3 Betroffenenrechte: Recht auf Berichtigung und Recht auf Löschung

Verschiedene Betroffenenrechte nach der DSGVO können mit den technischen Besonderheiten Blockchain-Technologie in Konflikt geraten (BSI 2019, 62 ff.). Von besonderem Interesse sind die Rechte auf Berichtigung (Art. 16 DSGVO) und Löschung (Art. 17 DSGVO). Zentrales Charakteristikum der Technologie ist nämlich gerade die grundsätzliche Unveränderlichkeit der gespeicherten Daten, sodass ein erhebliches Spannungsverhältnis mit diesen Betroffenenrechten entsteht (Finck 2018, S. 29).

Hard Forking, also eine Spaltung der Blockchain durch die Einführung neuer Software-Regeln, die nicht mit den ursprünglichen kompatibel sind, ist nicht geeignet, um den entsprechenden Pflichten nachzukommen, da die ursprünglichen Blöcke mit den enthaltenen Daten bestehen bleiben (Bechtolf und Vogt 2018, S. 70; Finck 2018, S. 31).

Bei privaten Blockchains erscheint es noch denkbar, dass die Zentralstelle die einzelnen Nodes anweisen kann, einen neuen Konsens zu bilden und so Blöcke auch rückwirkend zu verändern, um der Pflicht zur Berichtigung oder Löschung nachzukommen. Hierfür muss das System so angelegt sein, dass die Zentralstelle rechtlich befugt ist, die beteiligten Nodes zu beeinflussen (Martini und Weinzierl 2017, S. 1255). Möglich ist auch, einzelnen Knoten das

Recht einzuräumen[3], Blöcke nachträglich zu ändern (BSI 2019, S. 63). In öffentlichen zulassungsfreien Systemen kann die Konsensfindung dagegen nicht entsprechend beeinflusst werden. Auch die Zuteilung privilegierter Rollen im System verträgt sich nicht mit dem Konzept der zulassungsfreien Blockchain.

Ein anderer Ansatz ist die Schaffung veränderlicher Blockchains. Durch den Einbau sog. Chameleon Hashes wird der nachträgliche Austausch einzelner Daten ermöglicht (Ateniese et al. 2017). Für solche Verfahren wird allerdings in aller Regel eine vertrauenswürdige Instanz benötigt, die die für die Änderung nötig Schlüssel verwahrt (BSI 2019, S. 63). Technisch können zwar auch Systeme ohne Zentralinstanz als veränderliche Blockchain ausgestaltet werden (Ateniese et al. 2017, S. 12 ff.). In praktischer Hinsicht wird eine nachträgliche Änderung von Blöcken in Systemen mit unkontrollierter Konsensfindung allerdings kaum in effektiver Weise zu erreichen sein (Marnau 2017, S. 1031).

Im Allgemeinen widersprechen Ansätze, die die nachträgliche Löschung oder Änderung von Daten erlauben, der Grundidee der Blockchain-Technologie und können neuen Angriffs- und Missbrauchspotenziale zur Folge haben (BSI 2019, S. 64). Vorzugswürdig sind daher Gestaltungen, bei denen keinerlei personenbezogene Daten[4] in die Blockchain geschrieben werden. Dabei ist zwischen Transaktionsdaten und Public Keys zu unterscheiden.

Soweit möglich sollten Daten vollständig außerhalb der Blockchain (off-chain) gespeichert werden, während die Blockchain nur einen Beweis enthält, dass die Daten existieren und nicht manipuliert wurden (Hash-Pointer; zu den Anforderungen, um den Personenbezug des Hash-Pointers auszuschließen, siehe unten) (Lyons et al. 2018a, S. 29; Finck 2018, 23, 29). Sind die Daten in einer Datenbank enthalten, die ihre Änderung und Löschung zulässt, kann den Pflichten aus der DSGVO in dieser Form nachgekommen werden (Finck 2018, S. 30). Bei Transaktionsdaten besteht diese Möglichkeit. Public Keys können dagegen nicht aus der Blockchain entfernt werden, da sie dauerhaft für die Verifikation von Transaktionen benötigt werden. Für diese muss erwogen werden, ob sie sich zuverlässig anonymisieren lassen.

[3] So bietet beispielsweise das Unternehmen Bonebits GmbH eine Lösung mit privilegierten Knoten an, die über entsprechende Befugnisse verfügen.

[4] Dies gilt auch in Bezug auf die Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) als Rechtfertigungsgrundlage für die Datenverarbeitung. Da die Einwilligung frei widerruflich ist (Art. 7 Abs. 3 DSGVO), müssten die Daten nach einem Widerruf aus der Blockchain entfernt werden, ansonsten würden sie bei jeder Transaktion erneut verarbeitet. Zusätzlich ist fraglich, ob angesichts der Charakteristika einer Datenverarbeitung auf der Blockchain (dezentrale und unveränderliche Speicherung) wirksam in eine solche eingewilligt werden kann. Voraussetzung ist nämlich, dass die betroffene Person die Tragweite der Datenverarbeitung ausreichend einschätzen kann. Dies dürfte regelmäßig zu verneinen sein, siehe Quiel 2018, S. 571; Finck 2019a, 61f.

Prinzipiell wird in Erwägungsgrund 26 der DSGVO anerkannt, dass personenbezogene Daten auf eine Art und Weise verarbeitet werden können, dass eine Identifizierung nach allgemeinem Ermessen nicht wahrscheinlich ist (Finck 2019a, S. 19). Anonymisierte Daten stellen keine personenbezogenen Daten mehr dar und fallen nicht in den Anwendungsbereich der DSGVO. Erwägungsgrund 26 der DSGVO stellt allerdings auch klar, dass pseudonymisierte Daten weiterhin als personenbezogene Daten anzusehen sind. Die Beantwortung der Frage, wann die Identifizierbarkeit einer Person in ausreichendem Maße ausgeschlossen ist, sodass von anonymisierten Daten i.S.d. DSGVO ausgegangen werden kann, weist einige Schwierigkeiten auf. Die Artikel-29-Datenschutzgruppe stellt insgesamt hohe Anforderungen an die getroffenen Maßnahmen (Artikel-29-Datenschutzgruppe 2014). Die Identifizierung soll unter Berücksichtigung der Mittel, die vernünftigerweise eingesetzt werden könnten, unumkehrbar unmöglich gemacht werden, sie muss „vernünftigerweise unmöglich geworden" sein (Artikel-29-Datenschutzgruppe 2014, 6, 9).

Allgemein sind bei der Prüfung potenzieller Anonymisierungstechniken zwei Risiken zu prüfen. Einerseits das Risiko der Umkehrung, also der Ermittlung der ursprünglichen Daten aus dem neuen Datensatz und andererseits das Risiko der Verknüpfung. Dabei geht es um die Frage, ob die veränderten Daten aufgrund von erkennbaren Mustern oder durch eine Verbindung mit anderen Informationen Rückschlüsse auf Personen erlauben (Lyons et al. 2018a, S. 19).

Verschlüsselte Daten stellen in aller Regel pseudonymisierte und keine anonymisierten Daten dar, solange die Schlüssel für ihr Auslesen existieren (Lyons et al. 2018a, S. 21; Finck 2019a, S. 29; Artikel-29-Datenschutzgruppe 2014, S. 24). Beim Einsatz von Verschlüsselungstechniken ist zu beachten, dass heutzutage sichere Verschlüsselungen in Zukunft möglicherweise aufgebrochen werden können (Lyons et al. 2018a, S. 21). Aufgrund der besonderen Eigenschaften der Blockchain-Technologie ist daher die neuartige, erhebliche Gefahr entstanden, dass Daten in einem solchen Fall lesbar und unveränderlich in der Blockchain gespeichert sind. Der Aspekt der Langzeitsicherheit fällt bei Blockchains deshalb besonders ins Gewicht (BSI 2019, S. 35).

Die Bewertung gehashter personenbezogener Daten fällt nicht eindeutig aus. Durch den Einsatz einer kryptografischen Hashfunktion lässt sich aus beliebigen Ausgangsdaten ein Hashwert berechnen, der einzigartig für diesen Datensatz ist. Eine weitere Besonderheit ist, dass sich die Ausgangsdaten nicht aus dem Hashwert berechnen lassen (Erbguth 2019, S. 655). Die Artikel-29-Datenschutzgruppe sieht Hashing als Pseudonymisierungstechnik an, weil die Bestimmung des Ausgangswertes durch Ausprobieren möglicher Ausgangswerte

(Brute-Force-Attacke) möglich[5] ist (Artikel-29-Datenschutzgruppe 2014, S. 24). Ließe sich die Menge der Ausgangswerte ausreichend groß und unvorhersehbar gestalten, wobei die steigende Rechenleistung und die sinkenden Rechenkosten zu berücksichtigen sind, könnte man wohl von einer Anonymisierung ausgehen (Finck 2019a, S. 30; vgl. Adam et al. 2017, S. 25). Ausschlaggebend ist die sog. Entropie des Ausgangsdatensatzes, also seine Variabilität, die das Erraten durch Ausprobieren erschwert. Gescannte Daten weisen beispielsweise eine hohe Entropie auf, während sich kurze Textdaten häufig schnell ermitteln lassen (Erbguth 2019, S. 655). Eine mögliche Technik, um die Entropie zu erhöhen, könnte im „salting" oder „peppering" liegen, wodurch der Datensatz durch zusätzliche Informationen so vergrößert wird, dass eine Umkehrung durch Brute Force unwahrscheinlich gemacht wird (Lyons et al. 2018a, S. 22; zweifelnd zum "Salting" Artikel-29-Datenschutzgruppe 2014, 24f.)

Bei mehrfacher Verwendung von Hashes ist eine Gesamtschau möglich. Sind Hashes allerdings für jede Transaktion einzigartig (möglicherweise auch unter Hinzufügung zufälliger Informationen), ist es für Dritte kaum möglich, hieraus personenbezogene Daten abzuleiten (Lyons et al. 2018a, S. 22).

Auch Aggregationstechniken könnten als Anonymisierungsverfahren vielversprechend sein (Lyons et al. 2018a, 23f.). Ferner kann die Beifügung von "noise" (stochastische Überlagerung), also die Gruppierung mehrerer Transaktionen, sodass von außen nicht erkennbar ist, wer jeweils Absender*in und Empfänger*in einzelner Transaktionen ist, in Erwägung gezogen werden (Finck 2018, S. 25). Hierzu führt die Artikel-29-Datenschutzgruppe an, dass dies in Kombination mit anderen Techniken die Identifizierung deutlich erschweren oder sogar ausschließen kann (Artikel-29-Datenschutzgruppe 2014, 14f.).

Kryptografische Anonymisierungstechniken wie Mixing, Ring-Signaturen oder Zero-Knowledge-Verfahren weisen einerseits Probleme bei der praktischen Anwendbarkeit auf, zum anderen bestehen bereits Zweifel an der Zuverlässigkeit der erreichbaren Anonymisierung (BSI 2019, S. 39 f.). Insgesamt lässt sich nur schwer vorhersagen, ob eine der aktuell diskutierten Techniken zur Anonymisierung von Public Keys taugt und weitere Beobachtung und Auseinandersetzung mit der Frage ist notwendig (Finck 2018, S. 26). Das gilt zum einen für technische Entwicklungen und Erkenntnisse, zum anderen aber auch für die rechtswissenschaftliche Diskussion. Bisher fehlt es insbesondere an einschlägiger Rechtsprechung, aus der sich mit ausreichender Sicherheit ableiten lässt, wann Daten als

[5] Bezüglich schlüsselabhängiger kryptologischer Hashfunktionen, deterministischer Verschlüsselung oder schlüsselloser kryptologischer Hashfunktionen erkennt sie allerdings an, dass ein Angreifer für eine solche Attacke unverhältnismäßig hohen Einwand eingehen bzw. eine enorme Rechenleistung aufbringen müsste, Artikel-29-Datenschutzgruppe 2014, 25.

anonymisiert anzusehen sind. Aus rechtspolitischer Sicht ist zu beachten, dass die Gewährleistung von Anonymität nicht in allen Anwendungsfällen erstrebenswert ist (Finck 2019a, 35f.). Würde beispielsweise eine staatliche Stelle ein System mit Zero-Knowledge-Proof nutzen, hätte sie ab dem Zeitpunkt der Transaktion keinen Einblick mehr in die Daten (Martini und Weinzierl 2017, S. 1255).

Perspektivisch sei noch auf mögliche Auslegungsarten der Betroffenenrechte hingewiesen, die deren Umsetzung erleichtern könnten. Inwiefern diese Auslegung rechtlich Bestand haben kann, ist allerdings bisher ungeklärt.

Was das Recht auf Berichtigung angeht, ließe sich an Art. 16 Satz 2 anknüpfen, der die Berichtigung durch eine ergänzende Erklärung erwähnt. Offen ist, ob eine solche Ergänzung ohne Veränderung der ursprünglichen Daten dem Berichtigungserfordernis genügt (Finck 2018, S. 29). Der Wortlaut der Regelung, die sich auf die Ergänzung unvollständiger, aber nicht auf die Änderung fehlerhafter Informationen bezieht, spricht dagegen.

Der Begriff der Löschung ist in der DSGVO nicht definiert, was zumindest in der Theorie eine Interpretation unterhalb der vollständigen Zerstörung der Daten zulässt und damit eine an die Besonderheiten einer Technologie angepasste Lösungen erlauben könnte. § 35 BDSG 2018 erlaubt es beispielsweise, die Löschung durch eine Begrenzung der Verarbeitung zu ersetzen, wenn sie aufgrund der technischen Gegebenheiten unmöglich ist. Setzt man voraus, dass § 35 BDSG 2018 unionsrechtskonform ist[6], ist dennoch unklar, ob dies auf die Blockchain-Technologie anwendbar ist. Public Keys werden nämlich grundsätzlich bei der Erschaffung von jedem neuen Block verarbeitet (Finck 2018, S. 30). Zumindest deutet die Regelung aber darauf hin, dass auch Alternativen zur vollständigen Entfernung der Daten in Betracht kommen könnten, wenn die Rechte der Betroffenen dadurch gewahrt werden (Finck 2018, S. 31; vgl. Blockchain Bundesverband 2018, S. 8).

5.2.4 Ausblick

Die Bundesregierung sieht aktuell keinen Änderungsbedarf bei der DSGVO. Am 30. Januar 2020 wurde aber ein Round Table zu datenschutzrechtlichen Fragen der Blockchain-Technologie durchgeführt, um Unsicherheiten von Entwickler*innen und Anwender*innen zu erörtern (vgl. BMWi und BMF 2019, S. 13). Eine der größten Herausforderungen stellt die generelle Unsicherheit bezüglich der Auslegung diverser Begriffe der DSGVO dar. Hilfreich wären insoweit beispielsweise Leitlinien für die Anwendung der DSGVO auf Blockchain-

[6] Zweifel bestehen, da es in Art. 23 DSGVO an einer einschlägigen Öffnungsklausel fehlt, siehe Peuker, in: Peuker, in: Sydow 2020, § 35 BDSG Rn. 6 ff.Sydow 2020, § 35 BDSG Rn. 6 ff.

Anwendungen (vorzugsweise auf europäischer Ebene; die Koordination könnte über das European Data Protection Board stattfinden) (Finck 2019a, S. 97). Die Bundesregierung strebt eine Zusammenarbeit mit den Datenschutzaufsichtsbehörden an, um Auslegungsschwierigkeiten möglichst auszuräumen und eventuell zusätzliche Leitlinien für die Praxis zu erarbeiten (BMWi und BMF 2019, S. 13). Ferner könnten die allgemeineren Dokumente der Artikel-29-Datenschutzgruppe überarbeitet werden, um mehr Rechtsklarheit zu schaffen (Finck 2019a, S. 97). Auf Grundlage der Art. 40 und 42 DSGVO könnten Codes of Conduct (nach dem Vorbild des EU Cloud Computing Code of Conduct) und Zertifizierungsmechanismen (hierzu BMWi und BMF 2019, S. 13) als Formen der Selbstregulierung geschaffen werden (Finck 2019a, 98f.).

In praktischer Hinsicht ist angesichts der aktuellen Rechtslage äußerst zweifelhaft, ob sich öffentliche zulassungsfreie Systeme für erfolgreiche Use Cases[7] eignen. Die Gestaltung einer rechtskonformen Lösung stellt eine erhebliche Herausforderung dar und die aufgezeigten Konflikte zwischen Datenschutzrecht und Grundideen der Technologie erscheinen nur schwer überwindbar (vgl. auch BSI 2019, S. 65).

Eine erhebliche Lockerung des Datenschutzniveaus ist nicht zu erwarten und auch nicht unbedingt wünschenswert. Aufgrund der Charakteristika der Blockchain-Technologie können sich tatsächlich erhebliche Belastungen für Datenschutzsubjekte ergeben. Dennoch könnte darauf hingewirkt werden, die technologischen Besonderheiten der Blockchain-Technologie stärker zu berücksichtigen. Es könnte beispielsweise überprüft werden, ob die Ziele der DSGVO auch mit anderen Mitteln, als ursprünglich vorgestellt, erreicht werden können (Finck 2018, S. 18). Eine Überprüfung der DSGVO steht im Jahr 2020 an. Auf regulatorische Klarstellungen (z.B. beim Konzept der Anonymisierung) sollte hingewirkt werden.

Weitere ungeklärte Fragen verdienen in Zukunft Beachtung. Wenig diskutiert ist bisher die Vereinbarkeit von Smart Contracts mit Art. 22 DSGVO, der die Möglichkeit automatisierter Einzelfallentscheidungen beschränkt. Hält man Art. 22 DSGVO in diesem Kontext für anwendbar, erscheint eine rechtskonforme Gestaltung zwar grundsätzlich möglich, stellt aber wiederum eine Herausforderung für Anwender*innen der Technologie dar (Finck 2019b). Die praktische Umsetzung erfordert daher weiterer vertiefter Auseinandersetzung. Eine weitere, bisher wenig beleuchtete Herausforderung stellt die Übertragung von Daten in Drittstaaten dar, Art. 44 DSGVO. Probleme bereiten zulassungsfreie Systeme oder solche zulassungsbeschränkte Blockchains, die global betrieben werden (Lyons et al. 2018a, S. 26).

[7] Zu den praktischen Schwierigkeiten bei der Umsetzung auf der Ethereum Blockchain vgl. Unterweger et al. 2018.

Für letztere kommt eventuell eine Einwilligung in die Übertragung in Betracht, Art. 49 Abs. 1 lit. a) DSGVO, für erstere ist dies wiederum schwer vorstellbar (Finck 2018, S. 28).

5.3 Verbraucherschutz

Das Thema Verbraucherschutz ist eine Querschnittsmaterie, die bereits in einigen der behandelten Themen anklingt, so z.B. bei der Frage nach Prospektpflichten im Rahmen von ICOs oder nach effektiven Konfliktlösungsmechanismen. Festzuhalten ist zunächst, dass alle de lege lata existenten Verbraucherschutznormen auch im Fall von Geschäftsmodellen, die die Blockchain-Technologie und insbesondere Smart Contracts einsetzen, anwendbar sind. Welche Vorschriften konkret einschlägig sind, richtet sich nach dem jeweiligen Einsatzszenario und dem zugrundeliegenden Vertrag (Spindler und Wöbbeking 2019, Rn. 11). In Betracht kommen vor allem Informationspflichten und Widerrufsrechte sowie die Kontrolle allgemeiner Geschäftsbedingungen (Spindler und Wöbbeking 2019, Rn. 8).

Bei der Blockchain handelt es sich um eine Technologie, die einige besondere und bisher unbekannte Charakteristika aufweist. Inwiefern hier auch neuartige Risiken für die Interessen der Verbraucher*innen auftreten können, lässt sich aktuell nicht mit Sicherheit sagen. Es bietet sich daher an, die entstehenden Märkte genau zu beobachten um zu beurteilen, ob die vorhandenen Regelungen für effektiven Verbraucherschutz in diesem Bereich ausreichen oder ob Anpassungen nötig sind (BMWi und BMF 2019, S. 12). So stellt sich beispielsweise die Frage, ob Verbraucher*innen durch die bestehenden Informationspflichten die Risiken von Programmierfehlern und die möglichen Schwierigkeiten bei der Durchsetzung von Ansprüchen wirksam vor Augen geführt werden oder ob sich ein Bedürfnis nach speziellen Informationspflichten auftut (Spindler und Wöbbeking 2019, Rn. 26).

Im Fall von Smart Contracts wird beiden Seiten durch Automatisierung die Leistung der anderen Partei garantiert, wovon grundsätzlich auch Verbraucher*innen profitieren (Spindler und Wöbbeking 2019, Rn. 33). Gleichzeitig wird die Freiheit bei der Vertragsdurchführung dadurch eingeschränkt, dass ein Smart Contract auch bei unwirksamen Vereinbarungen o.ä. zunächst einmal abläuft (Spindler und Wöbbeking 2019, Rn. 33). Risiken können sich auch aus dem Abbau von Intermediären, die vertrauensstiftend wirken und im Konfliktfall eingreifen können, ergeben.

Relevante Faktoren bei der Bewertung des Verbraucherschutzniveaus können der Umfang des Einsatzes der Technologie, die wirtschaftliche Bedeutung der jeweiligen Geschäfte und die konkrete Ausgestaltung der Geschäftsmodelle sein.

Von zentraler Bedeutung ist die Sicherstellung der technischen Sicherheit des Codes und seine Freiheit von Programmierfehlern sowie die korrekte Umsetzung getroffener Vereinbarungen auf der technischen Ebene. Sinnvoll könnte hier die Einführung freiwilliger Sicherheitsprüfungen und Prüfsiegel sein (Spindler und Wöbbeking 2019, Rn. 38). Die Bundesregierung will beispielsweise die Einführung freiwilliger Zertifizierungsverfahren prüfen, die bestätigen, dass die jeweiligen Smart Contracts technisch die zugesicherten Inhalte abbilden (BMWi und BMF 2019, S. 15).

5.4 Anerkennung von Blockchain-Lösungen

Zukünftig könnte die Blockchain-Technologie die Chance bieten, bestehende Prozesse zu vereinfachen. Eigenschaften der Technologie wie ihre Manipulationssicherheit könnten fruchtbar gemacht werden, um bestimmte Instrumente durch digitale Versionen zu ergänzen. Häufig wäre dafür eine gesetzliche Anerkennung entsprechender Verfahren nötig. Im Allgemeinen muss dann eingehend geprüft werden, inwiefern dies aus rechtspolitischer Sicht wünschenswert ist.

5.4.1 Elektronische Öffnungsklauseln

Als positives Beispiel und mögliches Vorbild lassen sich die elektronischen Öffnungsklauseln für Traditionspapiere im Handelsgesetzbuch (HGB) anführen. §§ 443 Abs. 3, 475c Abs. 4 und 516 Abs. 2, 3 HGB erlauben es, Traditionspapiere, die zuvor zwingend papiergestützt waren, durch ein digitales Äquivalent zu ersetzen, wenn dieses alle Funktionen des Originals erfüllt. Schon heute erlauben diese Normen den Einsatz der Blockchain-Technologie in diesem Bereich (Fridgen et al. 2019, S. 183). Daraus ergibt sich ein erhebliches Vereinfachungspotenzial für die Logistikbranche. Solche technologieneutralen Regelungen, die digitale Äquivalente für ursprünglich analoge Prozesse zulassen, könnten auch in anderen Gebieten geschaffen werden.

In eine ähnliche Richtung gehen die aktuellen Pläne der Bundesregierung zur Schaffung elektronischer Wertpapiere (BMWi und BMF 2019, S. 6). Bisher bedarf es für eine Einordnung als Wertpapier im zivilrechtlichen Sinne zwingend einer Verbriefung des jeweiligen Rechts in einer Papierurkunde. Für den Fall von Schuldverschreibungen soll eine technologieneutrale Öffnung für elektronische Versionen erfolgen, in einem nächsten Schritt wird die Schaffung elektronischer Aktien und Investmentfondsanteile geprüft. Bisher existiert lediglich ein Eckpunktepapier (BMF und BMJV 2019), ein Gesetzentwurf liegt noch nicht vor.

5.4.2 Blockchain-basierte Register

Ein weiterer möglicher Anwendungsfall ist die Nutzung der Blockchain im Rahmen der Registerführung.

Einerseits könnte der Blockchain eine lediglich absichernde und unterstützende Funktion zukommen, indem Hash-Werte von weiterhin off-chain geführten Registereinträgen gespeichert werden, um nachträgliche Manipulationen erkennbar zu machen (Knaier und Wolff 2018, S. 2258). Deutlich weiter gingen Modelle, bei denen der Registerinhalt (bestehender oder neuer Register) in die Blockchain geschrieben wird (siehe z.B. Knaier und Wolff 2018, S. 2257; Danninger et al. 2019, S. 7). Neben Fragen des Datenschutzrechts (s.o.) wäre hier zu klären, wer Informationen in die Blockchain einstellen kann (Knaier und Wolff 2018, S. 2257). Zulassungsfreie Systeme werden sich insofern höchstwahrscheinlich nicht eignen, da die Legitimität der eingestellten Informationen von einer vertrauenswürdigen Stelle geprüft werden sollte. Hier erfüllen die mit der Registerführung betrauten Stellen in ihrer Gatekeeper-Rolle eine wichtige Funktion (vgl. Boucher et al. 2017, S. 19; vgl. Heckelmann 2018, S. 509). Das Merkmal der Desintermediation ist also wenig förderlich. Deutlich wird dies auch in dem Zusammenhang, dass für Bürger*innen die für einen Registereintrag verantwortliche Stelle erkennbar sein muss (Danninger et al. 2019, S. 8).

Speziell zum Grundbuch wird zudem kritisch angemerkt, dass dieses Register mehr Funktionen erfülle, als die bloße Dokumentation. Diese seien nicht durch ein Blockchain-basiertes System zu ersetzen (Wilsch 2017; vgl. auch Püls und Gerlach 2019, 87f.). Dieser Gedanke ist generell einzubeziehen, wenn der Ersatz bestehender Instrumente durch Blockchain-Lösungen in Erwägung gezogen wird: Wird die neue Lösung den gleichen Bedürfnissen gerecht, wie die ursprüngliche? Eine verwandte Frage im Zusammenhang mit Registern ist, inwiefern dem Blockchain-Inhalt öffentlicher Glaube zukommen kann, wie es beispielsweise beim Grundbuch und beim Handelsregister der Fall ist (vgl. Knaier und Wolff 2018, S. 2258). Einige Vorschläge beschränken sich daher schon von vornherein auf Register ohne öffentlichen Glauben (NExT/BiVD 2019, S. 7).

Auch die Bundesregierung hält es nicht für sinnvoll, öffentliche Register, die auch der inhaltlich rechtlichen Prüfung durch staatliche Stellen dienen (wie Grundbuch, Handelsregister, Personenstandsregister) mit Hilfe der Blockchain-Technologie umzusetzen. Sie sieht dagegen die Bereiche Fahrzeughaltung und Dokumentenverifikation als vielversprechende Anwendungsszenarien an (BMWi und BMF 2019, S. 19). In jedem Fall müsste eine Ausgestaltung gewählt werden, durch die Grundrechte und andere verfassungsrechtliche Garantien gewahrt werden (NExT/BiVD 2019, S. 8).

5.4.3 Beweisführung im Zivilprozess

Was die Beweisführung im Zivilprozess angeht, kommt dem Blockchain-Inhalt kein besonderer Beweiswert zu. Elektronische Dokumente sind gem. § 371 Abs. 1 S. 2 ZPO dem Augenscheinsbeweis zugeordnet und unterliegen der freien richterlichen Beweiswürdigung gem. § 286 Abs. 1 ZPO. Nur soweit sie eine qualifizierte elektronische Signatur (siehe unter iv) enthalten, stehen sie gem. § 371a Abs. 1 S. 1 ZPO Urkunden gleich (Fries 2018, S. 89). Blockchain-Inhalte fallen aktuell unter den ersten der genannten Fälle. Die Bundesregierung prüft die Anerkennung diverser Elemente der Blockchain-Technologie im Rahmen der Beweisführung (BMWi und BMF 2019, S. 13).

5.4.4 Identitätsnachweise und qualifizierte elektronische Signaturen nach der eIDAS-Verordnung

Die eIDAS-VO[8] verfolgt das Ziel der Schaffung eines angemessenen Sicherheitsniveaus bei elektronischen Identifizierungsmitteln und Vertrauensdiensten, Art. 1 eIDAS-VO. Nach Erwägungsgrund 1 soll das Vertrauen in elektronische Transaktionen im europäischen Binnenmarkt gestärkt werden. Die Verordnung enthält Regelungen zur elektronischen Identifizierung und zu Vertrauensdiensten und schafft einen Rechtsrahmen für elektronische Signaturen sowie verwandte Instrumente. Die Blockchain-Technologie könnte in zwei Einsatzbereichen interessant sein.

Zum einen könnte die Technologie als Basis für ein elektronisches Identifizierungsmittel im Sinne der eIDAS-VO in Betracht gezogen werden. Für eine Anerkennung als solches Identifizierungsmittel wäre eine Notifizierung seitens eines Mitgliedsstaats der Europäischen Union nötig, Art. 9 eIDAS-VO. Die Voraussetzungen hierfür sind in Art. 7 eIDAS-VO festgelegt. Abstrakt gesehen sollten die Voraussetzungen, insbesondere die Einhaltung der vorgegebenen Sicherheitsniveaus, durch ein Blockchain-basiertes Identifizierungsmittel erfüllbar sein (Brisch/Brisch in: Hoeren et al. 2019, Teil 13.3 Rn. 134 f.). Im Zusammenhang mit dieser Thematik steht auch die Ankündigung der Bundesregierung, die Verknüpfung von Blockchain-Lösungen mit staatlichen digitalen Identitäten zu prüfen (BMWi und BMF 2019, 18f.).

Zum anderen stellt sich die Frage, ob im Blockchain-Kontext die Anforderungen an die qualifizierte elektronische Signatur erfüllt werden können. Dies ist insofern relevant, als dass die Schriftform nach § 126 BGB durch Blockchain-basierte Smart Contracts bisher nicht

[8] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

eingehalten werden kann und sich diese im Ergebnis nur für formfreie Rechtsgeschäfte eignen (Paulus und Matzke 2018, S. 457). Abgesehen von Ausnahmefällen kann die Schriftform aber durch die elektronische Form i.S.v. § 126a BGB ersetzt werden, § 126 Abs. 3 BGB. Voraussetzung hierfür ist das Anfügen einer qualifizierten elektronischen Signatur an die abgegebene Erklärung. Für einen Vertragsschluss ist nach § 126a Abs. 2 BGB notwendig, dass beide Parteien jeweils ein gleichlautendes Dokument mit einer qualifizierten elektronischen Signatur signieren.

Die qualifizierte elektronische Signatur ist in Artikel 3 Nr. 12 eIDAS-VO definiert. Danach handelt es sich um „*eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht*". Eine fortgeschrittene elektronische Signatur i.S.v. Art. 3 Nr. 11, Art. 26 eIDAS-VO erfüllt die folgenden Voraussetzungen: Sie kann dem Unterzeichner eindeutig zugeordnet werden und ermöglicht dessen Identifizierung. Sie wird mit Hilfe elektronischer Signaturerstellungsdaten erstellt, die der alleinigen Kontrolle des Unterzeichners unterliegen und ist mit den signierten Daten so verbunden, dass nachträgliche Veränderungen an diesen erkennbar sind. Das Gesetz formuliert also Anforderungen an die technische Ausgestaltung des Systems. Dass diese erfüllt werden ist nicht ausgeschlossen, angesichts der Strenge der Voraussetzungen ist die Umsetzung allerdings nicht trivial. Jedenfalls bisher ist typischerweise nicht davon auszugehen, dass die Anforderungen durch Blockchain-basierte Gestaltungen erfüllt werden (Möslein 2019, Rn. 13).

6 ORGANISATIONELLE RAHMENBEDINGUNGEN

Kernaussagen und Rahmenbedingungen	
OK1	Die Strategie einer Organisation leitet sich von der Wahl des Offenheitsgrads einer Blockchain ab. Das Geschäftsmodell wird von dieser unmittelbar determiniert und hat somit einen direkten Einfluss auf das Wertangebot, die Wertschöpfungsarchitektur und die Werteerfassung. Abgeleitet von diesen Geschäftsmodellelementen beschreiben die taktischen Mechanismen im Detail, wie Unternehmen/Organisationen mittels der Blockchain-Technologie Werte für Kunden schaffen und diese für sich monetarisieren. Bevor eine Blockchain realisiert wird, ist es daher erforderlich eine entsprechende Blockchain-Strategie auszuwählen. (Kapitel 6a)

OK2	Die Blockchain-Technologie bietet Potential neue Kundensegmente zu erschließen, deren Zugang bisher nicht möglich war. (Kapitel 6b-i)
OK3	Mehrwehrte, wie Vertrauen, Transparenz, etc., die mit der Blockchain-Technologie ermöglicht werden, können zu einer besseren und intensiveren Kundenbindung und Kundenzufriedenheit führen. (Kapitel 6b-i)
OK4	Die Blockchain-Technologie ermöglicht neue Organisationsstrukturen, wie Decentralized Autonoumos Organizations (DAO), wodurch sie neue Möglichkeiten in der Zusammenarbeit hinsichtlich der Wertegenerierung schafft, als auch neue Einnahmequellen hervorbringt. (Kapitel 6b-ii)
OK5	Mittels Blockchain kann u.a. ein hoher Grad an Transparenz in diversen Kontexten ermöglicht werden, wodurch ein hohes Vertrauen in das Unternehmen geschaffen werden kann. Das gewonnene Vertrauen kann wiederum zu einer besseren Kundenbeziehung und stärkeren Positionierung am Markt führen. (Kapitel 6b-i, 6b-ii)
OK6	Mit der Blockchain-Technologie können Serviceangebote generiert werden, die zum Ziel bspw. eine Effizienzsteigerung, Kostenreduzierung, Transparenz etc. umfassen. Neben den neuen Serviceangeboten, können aber auch bestehende Wertangebote mittels Blockchain optimiert werden und dadurch neue Kundensegmente erschlossen werden. (Kapitel 6b-i)
OK7	Intermediäre können über eine Blockchain-Lösung, wie Bitcoin, abgelöst werden. Für Unternehmen bedeutet dies, dass ein direkter Kontakt zu den Kunden aufgebaut und Verträge u.a. individuell und bei Wiederholung automatisiert werden können. Der direkte Kontakt zum Kunden über eine Blockchain kann folglich die Positionierung des Unternehmens am Markt verbessern. (Kapitel 6b-i, 6b-ii)
OK8	Mittels Smart Contracts kann eine hoher Automationsgrad (komplexer) Unternehmensprozesse erreicht werden. In den Smart Contracts ist das Regelwerk enthalten, in denen beschrieben ist, wie bei welchen Vorkommnissen zu handeln ist. Auf Basis dessen können die wiederkehrenden Prozesse effizient und kostensparend abgewickelt werden. Insbesondere bei einer Supply Chain bei denen mehrere Stakeholder beteiligt sind, bietet die Automatisierung der Prozesse einen enormen Mehrwert. (Kapitel 6b-ii)

OK9	Potentielle Ertragswege wie Pay-Per-Use, Service-Level Agreements oder Crowdfunding mittels Initial Coin Offering (IOC) stellen mögliche Ertragsformen in diversen Branchen dar, die zuvor nicht genutzt werden konnten, aber durch Blockchain nun nutzbar gemacht werden. (Kapitel 6b-iii)
OK10	Anstelle von Aktien ist es über eine Blockchain möglich Anteile eines Unternehmens in Form von Tokens Investoren zum Kauf anzubieten. Gegenüber dem umfassenden und restriktiven realen Prozess bietet Blockchain eine schnelle und unkomplizierte Lösung des Crowdfundings. (Kapitel 6b-iii)
OK11	Dem Kunden wird die Möglichkeit eröffnet, eine deutlich aktivere Rolle einzunehmen (C2B), als dies derzeit im Markt der Fall ist (B2C). Die Blockchain erzeugt neuartige Kundensegmente, welche sich als „Prosumers" charakterisieren lassen. (Kapitel 6b-i)
OK12	Die Implementierung einer Blockchain zieht Change Management Prozesse nach sich, wie bei anderen IKT-Anwendungen ebenfalls. (Kapitel 6c)
OK13	Die IT-Sicherheitsbetrachtung eines Blockchain-Systems unterscheidet sich im Kern nicht von anderen IT-Systemen. Blockchain-spezifische Standards und Empfehlungen existieren aktuell noch nicht, sind allerdings auf verschiedenen Ebenen in Arbeit. (Kapitel 6d)
OK14	Es können keine allgemeingültigen Aussagen über die Cyberrisiken von Blockchain-Systemen getroffen werden. Vielmehr ist eine Identifizierung der Gefährdungen und Bewertung je nach System und Use-Case notwendig. (Kapitel 6d)

Handlungsempfehlungen	
OH1	Im Rahmen der Einführung von Blockchain sollten personelle Ressourcen nicht außer Acht gelassen werden. Um langfristig Entwicklungspotential zu sichern, ist entsprechende Blockchain-Expertise aufzubauen bzw. zu schaffen. (Kapitel 6b-ii)
OH2	Mit der Implementierung einer Blockchain sind ausreichend informationstechnische Mittel (hinreichende Internetbandbreite; Rechenleistung, und Speicherplatz)

	sicherzustellen. Es ist daher zu prüfen, inwiefern Ressourcen anzuschaffen bzw. auszubauen sind. (Kapitel 6b-ii, 6b-iii)
OH3	Um bei einem möglichen Misserfolg nicht einen allzu hohen Verlust zu verzeichnen, ist zu empfehlen mit einer unternehmensinternen Blockchain-Lösung zu beginnen und sich dort auszuprobieren. (Kapitel 6b-iii)
OH4	Blockchain kann die Unternehmensprozesse und -aktivitäten enorm beeinflussen. Mit Hilfe der Technologie ist es bspw. möglich komplexe Prozesse zu optimieren, transparenter zu gestalten und dadurch gleichzeitig Kosten einzusparen. (Kapitel 6b-ii, 6b-iii)
OH5	Wartungs- und Instandhaltungskosten der Blockchain sollten mit bei der Kalkulation sowie bei der Konzeptualisierung berücksichtigt werden. (Kapitel 6b-iii)
OH6	Change Management und der frühe Einbezug der Mitarbeitenden hinsichtlich Nutzbarkeit und Aus-/Weiterbildung sollten frühzeitig im Implementierungsprozess berücksichtigt werden. (Kapitel 6c)
OH7	Kritikalitätskategorien von identifizierten Cyberrisiken müssen ermittelt werden um so eine Priorisierung der Cyberrisiken ableiten zu können (Kapitel 6d)

6.1 Blockchain-basierte Unternehmensorganisation und Strategie

Seitdem die Kryptowährung Bitcoin im Jahre 2009 am Markt eingeführt wurde, ist die Blockchain-Technologie, auf der die Kryptowährung basiert, mit eine der meistdiskutierten Innovationen des digitalen Zeitalters für Wirtschaft und Gesellschaft geworden (Kietzmann und Archer-Brown 2019; Swan 2015). Seither beschäftigen sich Wissenschaftler und Praktiker mit neuen, potenziellen Anwendungsmöglichkeiten, die mit dem Einsatz der Blockchain in Organisationen realisiert werden können (Meinel et al. 2018; Atzori 2015). Mittels der dezentralen Speicherung von Transaktionsdaten können neue organisationale Mehrwerte nutzbar gemacht werden, welche im Folgenden am Beispiel der Bitcoin-Technologie dargestellt wird.

In der Vergangenheit sind Bankkonten eines Finanzintermediäres eine zwingende Voraussetzung gewesen, um am bargeldlosen Zahlungsverkehr teilzunehmen (Jetzke und Richter 2017). Das Gehalt, Einkäufe aber auch monatliche Ausgaben werden darüber abgewickelt. Dadurch entsteht eine institutionalisierte Abhängigkeit der dahinterliegenden Bankeninfrastruktur, welche zentral organisiert ist. Mit der Bitcoin-Technologie wird diese

Abhängigkeit aufgebrochen. Die Finanzinfrastruktur wird über die Blockchain dezentral realisiert und somit kann ein gewisser Geldbetrag direkt von einer zur anderen Partei über ein „Peer-to-Peer-Netzwerk" transferiert und validiert werden, ohne dass weitere Intermediäre (bspw. Banken) involviert werden müssen. Aus dieser Neuorganisation ergeben sich entsprechende Mehrwerte für die Nutzer*innen der Bitcoin-Technologie. Vor allem können Transaktionskosten und Vermittlungsgebühren eingespart werden, die sonst von den Banken bspw. bei Auslandsüberweisungen in Rechnung gestellt werden (Kiviat 2015). Des Weiteren werden die Transaktionen in der Blockchain direkt sowie effizient verarbeitet bzw. verbucht und über einen Incentivierungsmechanismus des „Proof-of-Work" durch das Bitcoin-Schürfen dezentral validiert. Dadurch werden nicht nur Kosten eingespart, sondern auch Transaktionsprozesse effizienter und transparenter gestaltet. Weiterhin wird mit der redundanten und dezentralen Dokumentation sowie Verschlüsselung der Transaktionen eine Manipulations- und Datensicherheit geschaffen. Eine nachträgliche Veränderbarkeit oder Missbrauch der Transaktionsdaten vom Netzwerk wird somit ausgeschlossen (Gupta 2017b; Morabito 2016). Insgesamt werden mit der Blockchain-Technologie im Bankenkontext viele Mehrwerte wie Kosteneinsparungen, Prozessoptimierungen sowie Vertrauen und Sicherheit erzeugt (Gupta 2017a). Die Blockchain-Technologie ersetzt folglich die organisationale Rolle und disruptiert das Geschäftsmodell von diversen Intermediären, wie Banken als operativer Vertrauensgeber für die effiziente Verarbeitung von Transaktionen.

Der Einsatz der Blockchain-Technologie hat einen unmittelbaren Einfluss auf die Organisation und die Strategie eines Unternehmens, da sich mit der Einführung die organisationalen Rahmenbedingungen ändern (Gawer 2014; Zheng et al. 2018). Gemäß Gawer (2014) kann der organisationale Rahmen an den Dimensionen organisationales Design, digitale Schnittstellen, Ressourcen-/Kompetenzzugang und Koordinationsmechanismen festgelegt werden (siehe Abb. 1). Die Ausgestaltung dieser Dimensionen wird durch die Wahl der Blockchain-Technologie und ihrem Offenheitsgrad beeinflusst (Zheng et al. 2018).

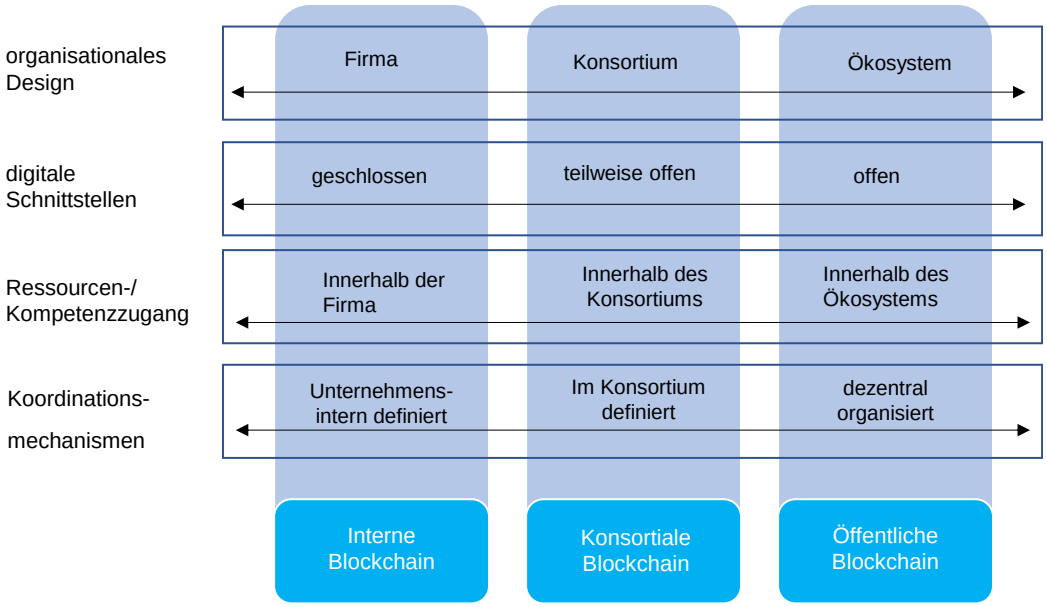

Abb. 1: Der Einfluss diverser Blockchain-Strategien auf die organisationalen Rahmenbedingungen, in Anlehnung an Gawer (2014)

Legt man den Fokus nun auf die Ausgestaltung des organisationalen Rahmens bezüglich der dezentralen Speicherungsmechanismen, können hierbei drei Offenheitsstrategien einer Blockchain-Umsetzungen unterschieden werden: (1) Interne Blockchain (2) Konsortial-Blockchain und (3) Öffentliche Blockchain (Chong et al. 2019; Iansiti und Lakhani 2017; Zheng et al. 2018; Morkunas et al. 2019).

Die erste Form der Blockchain-Umsetzung beschreibt die Nutzung einer unternehmensinternen Blockchain-Lösung, womit u.a. komplexe Unternehmensprozesse optimiert und transparenter realisiert werden können. Bei diesem organisationalen Design sind keinerlei Berührungspunkte bzw. digitale Schnittstellen zu Partnern oder anderen Institutionen zur Blockchain gegeben. Nur autorisierte Personen der Organisation und verbundenen Unterorganisationen, wie Tochtergesellschaften, können die Blockchain-Anwendungen nutzen. Für die organisationale Umsetzung der Blockchain bedeutet dies, dass das Blockchain-Protokoll mit den technischen Spezifikationen und die Schnittstellen zwischen den Applikationen und dem Blockchain-Protokoll intern entwickelt, aufgesetzt und gepflegt werden (Rossi et al. 2019). Es handelt sich dementsprechend um eine interne dezentrale Datenbank, wobei die Schnittstellen nicht nach außen, sondern zu den internen Untereinheiten geöffnet sind. Der organisationale Rahmen beschränkt die Umsetzung der Blockchain auf die internen Ressourcen und Kompetenzen, wobei diese für die Realisierung, innerhalb einer Organisation, ausreichend zur Verfügung stehen müssen. Ohne den Aufbau

von technologischen IT-Ressourcen und Blockchain-Expertise ist eine Umsetzung und Weiterentwicklung einer internen Blockchain-Lösung nicht möglich. Ein Szenario für eine interne Blockchain ist die Abbildung eines komplexen bereichsübergreifenden Produktionsprozesses. Die transparente und manipulationssichere Dokumentation von Daten einer Produktionslinie in der Blockchain kann u.a. den Aufwand für interne Audits/ Revisionen bzw. Qualitätsprüfungen reduzieren. Die Koordination eines internen Blockchain-Systems erfolgt hierbei durch interne „Governance"-Mechanismen, welche von der Organisation und der Führungsebene vorgeben wird.

Bei dem Design einer Konsortial-Blockchain schließen sich diverse Unternehmen, vornehmlich einer Branche, zusammen und betreiben gemeinsam eine Blockchain. In einer nach außen hin geschlossenen Blockchain können nur Mitglieder des Konsortiums partizipieren, wobei das zugrundeliegende Blockchain-Protokoll und die Applikationen im Verbund gestaltet werden. Die Schnittstellen der Blockchain unterliegen Spezifikationen, die für Konsortialpartner offen, aber für Außenstehende des Verbundes nicht zugänglich sind. Alle Teilnehmenden verfügen über gleiche oder ähnliche Stimmrechte bzw. die Entscheidungen hinsichtlich der Blockchain-Lösung (Blockchain-Protokoll und Applikationen) werden gemeinsam getroffen. Die Entscheidungsmacht kann auch nach den Anteilen (z.B. Investitionsanteil etc.) an einer Blockchain determiniert werden. Die Ressourcen & Kompetenzen dieser hybriden Blockchain-Lösung werden ebenfalls gemeinsam oder auch in diesem Fall, je nach Anteil, vom Konsortium bereitgestellt. Ein Beispiel für die Nutzung einer solcher Blockchain-Strategie ist der Zusammenschluss von Unternehmen, die entlang einer Wertschöpfungskette kooperieren. Hierbei bestehen vertragliche Beziehungen zwischen den Mitgliedorganisationen, welche im Verbund die Koordinationsmechanismen formalrechtlich festhalten (Gawer 2014).

An einer offenen Blockchain (Blockchain- Ökosystem) können jegliche Nutzer teilnehmen, wobei das Blockchain-Protokoll öffentlich zugänglich ist und Applikationen dazu frei entwickelt werden können. Zugriffsrechte, wie bei den vorherigen beiden Blockchain-Lösungen, sind offen gestaltet, sodass jegliche Parteien (multi-side-market) teilnehmen können. Solche Blockchains nennt man auch „permissonless", wobei die Transaktionen/Protokolle und die zugrundeliegenden Daten durch Kryptografie- und Validierungsmechanismen gesichert werden. Bei dieser Art der Blockchain steht insbesondere im Mittelpunkt, dass potenziell ein unbegrenzter Pool an externen Ressourcen, Fähigkeiten und Kompetenzen zur Verfügung steht und zur Weiterentwicklung einer solchen Blockchain-Lösung beiträgt (Gawer 2014). Die Weiterentwicklung durch Modifikationen der Blockchain ist bei Offenen-Design-Konzepten gewollt, um u.a. eine qualitativ hochwertige

Software zum Beispiel durch „Open Source Communities“ zu realisieren (Camilleri et al., 2018). Die bereits erwähnte Bitcoin-Blockchain stellt eine solch öffentliche und genehmigungsfreie Design-Lösung dar. Die Koordinationsmechanismen werden durch das Ökosystem gesamtheitlich festgelegt.

Eine Übersicht der Eigenschaften und Ausprägungen der drei Blockchain-Strategien auf die organisationalen Rahmenbedingungen sind in der Abb. 2 dargestellt.

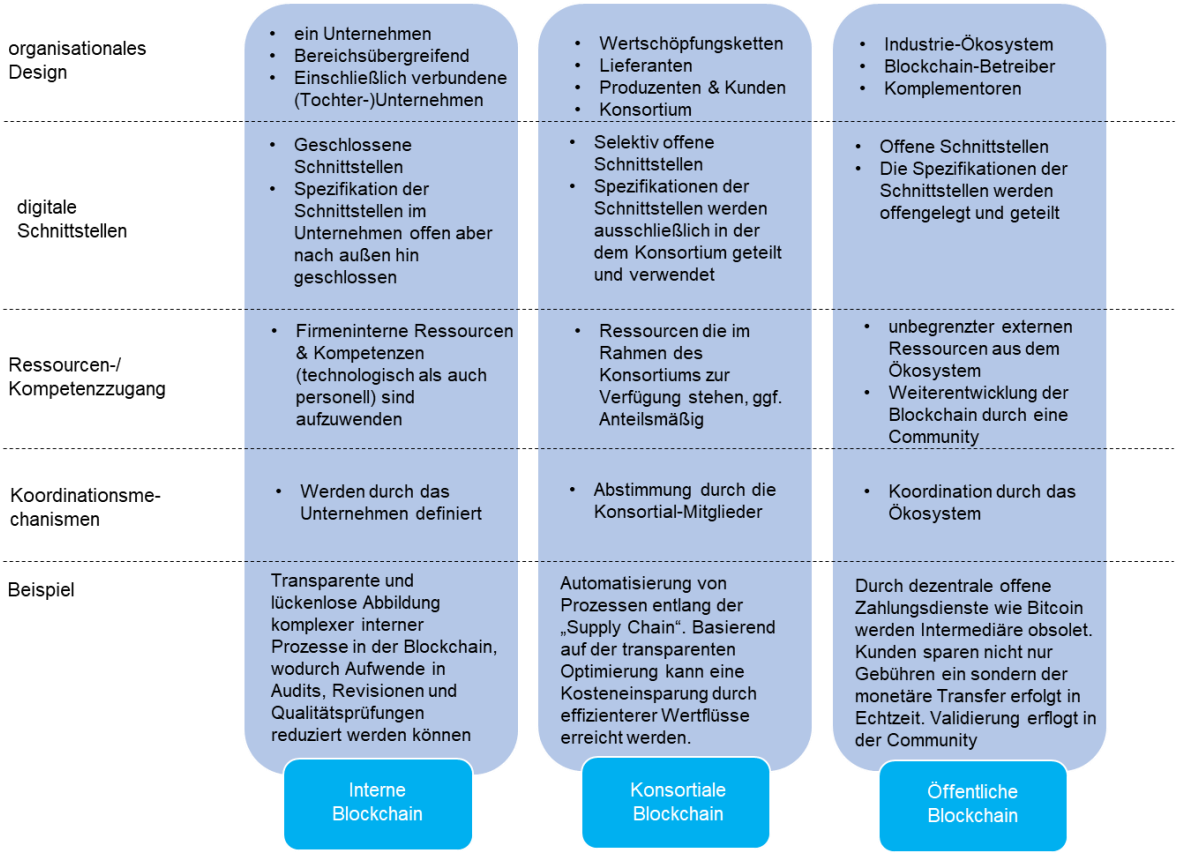

Abb. 2: Der Einfluss Blockchain-Strategien auf die organisationalen Rahmenbedingungen im Überblick,
in Anlehnung an Gawer (2014)

Die organisationalen Rahmenbedingungen der oben genannten Blockchain-Strategien spiegeln sich in dem Geschäftsmodell als operativer Rahmen wider (siehe Abb. 3). Die Wahl der Blockchain-Strategie (offene, konsortiale oder öffentliche Blockchain) determiniert das Design des Geschäftsmodells einer Organisation. Das Geschäftsmodell bildet folglich den operativen Rahmen, wie ein Unternehmen am Markt Werte schöpft und sich diese aneignet. Auf Basis des Geschäftsmodells werden die taktischen Mechanismen bestimmt, wie das Unternehmen/Organisation mittels der Blockchain-Technologie Werte für seine Kunden schafft und diese für sich monetarisiert (Casadesus-Masanell und Ricart 2010).

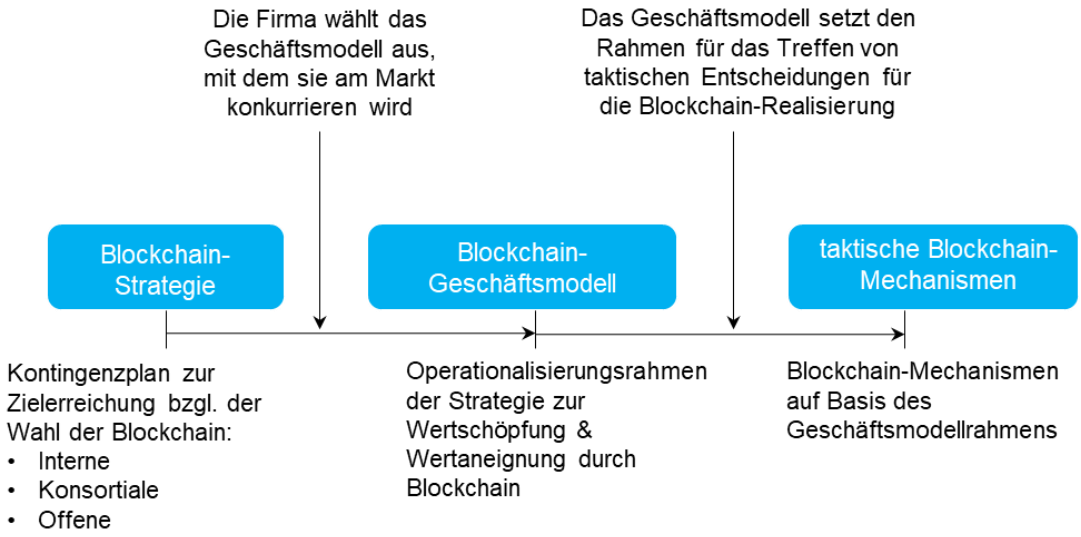

Abb. 3:Dreistufiges Realisierungsmodell einer Blockchain-Strategie, in Anlehnung Casadesus-Masanell,(2010)

Aufgrund des wechselseitigen Einflusses zwischen Strategie und Geschäftsmodell wird das Thema Geschäftsmodelle im Weiteren bezüglich des Einsatzes der Blockchain-Technologie näher beleuchtet. Dazu wird zunächst der Begriff des Geschäftsmodells im Detail näher betrachtet und grundlegend erörtert, um eine Grundverständnis aufzubauen. Anschließend werden die einzelnen Dimensionen und Elemente für die Innovation eines Geschäftsmodells in Bezug auf den Einfluss der Blockchain-Technologie erörtert. Einflussfaktoren der Blockchain-Technologie auf die jeweiligen Innovationsdimensionen eines Geschäftsmodells, sowie mögliche Auswirkungen werden dabei dargestellt und erklärt. Jeder Abschnitt fasst zudem die Rahmenbedingungen der Blockchain auf die jeweilige Dimension zusammen.

6.2 Blockchain-basierte Geschäftsmodellinnovation

Um das Fortbestehen und die Wettbewerbsfähigkeit eines Unternehmens zu sichern, reicht es heutzutage nicht mehr aus, innovative Produkte und Dienstleistungen am Markt anzubieten. Der Niedergang ehemals erfolgreicher Unternehmen wie Kodak, Brockhaus oder AEG haben dies deutlich gezeigt. Nicht das Fehlen neuartiger Produkte und Dienstleistungen alleine hat zu diesem Umstand beigetragen, sondern die fehlende Anpassung des Geschäftsmodells an die sich ändernden Rahmenbedingungen aus der zunehmenden Globalisierung und Digitalisierung haben dies versursacht (Casadesus-Masanell und Ricart 2010).

Dies zeigt das Unternehmensbeispiel Kodak deutlich. Kodak hatte in den 90er Jahren das Potential der digitalen Fotografie bereits früh erkannt und initiierte daraufhin eine Kooperation mit Microsoft, um das neue Geschäftsfeld zu erschließen. Die Entwicklung und

Umsetzung der Digitalfotografie stagnierten allerdings. Als die ersten Digitalkameras 1999 den Markt erreichten, schätze Kodak zur damaligen Zeit den Marktanteil für die kommenden zehn Jahre auf fünf Prozent. Zehn Jahre später zeigte sich jedoch eine andere Realität. Lediglich fünf Prozent des Markanteils verblieb für analoge Kameras. Als das Unternehmen diesen Wandel erkannte, war es bereits zu spät, das Unternehmen auf ein neues Geschäftsmodell umzustellen. Kodak verlor seine Marktführerschafft und konnte sich davon nicht mehr erholen, sodass das Traditionsunternehmen 2012 Insolvenz anmelden musste (Gassmann 2013). Dieses Beispiel zeigt, dass das Thema Geschäftsmodelle und dessen Innovation von hoher Bedeutung ist, um am Markt als Unternehmen langfristig bestehen zu können und um neue Technologien wie die Blockchain zu kommerzialisieren.

Die Blockchain-Technologie bietet viele Möglichkeiten neue Geschäftsfelder zu erschließen. Insbesondere Unternehmen mit Plattformgeschäftsmodellen, die auf Basis eines zentralen Vermittlers/Intermediäres zwischen zwei Transaktionsparten fungieren (bspw. im Bankensektor) stehen an einem Wendepunkt. Diese Organisationen müssen sich fragen, ob und wie sich die Blockchain-Technologie auf Ihr Geschäftsmodell auswirkt. Mittels Blockchain ist es nun einfacher möglich, Transparenz und Vertrauen, ohne die Involvierung von Intermediären herzustellen (Gassmann 2019).

Weiterhin zeigen Studien (Zott et al. 2011; Foss und Saebi 2017; Chong et al. 2019), dass das Thema Geschäftsmodellinnovation seit der letzten Dekade zunehmend an Präsenz gewonnen hat und häufig in spezifischen Themenfelder, wie z.B. Blockchain diskutiert wird. Eine allgemeingültige Definition des Begriffs „*Geschäftsmodell*" konnte seither nicht etabliert werden. Eine vielverwendete Definition von Geschäftsmodellen wurde von Amit und Zott beschrieben:

"A business model depicts the content, structure, and governance of transactions designed so as to create value through the exploitation of business opportunities. […] (2001, S. 493-520)"

Bei der Bestimmung der Begrifflichkeit des Geschäftsmodells wird hierbei der Fokus vornehmlich auf die Transkationen gelegt, die einen Wert für das Unternehmen generieren. Eine weitere Definition von Casadesus-Masanell und Ricart ist mehr holistisch und beschreibt den Begriff als eine operative Logik, welche ein zentraler Bestandteil der Strategie als Kontingenzplan zur Zielerreichung der Organisation ist. Sie definieren das Geschäftsmodell wie folgt:

„Business Model refers to the logic of the firm, the way it operates and how it creates value for its stakeholders."(2010, S. 201).

Eine der häufig genutzten Definition und Ontologie des Geschäftsmodells wurde von Osterwalder verfasst, der einen Rahmen zur Interpretation von Geschäftsmodellen darlegt. Osterwalder *(2004, S. 15)* beschreibt ein Geschäftsmodell als:

> *"(…) a conceptual tool that contains a set of elements and their relationships and allows expressing a company's logic of earning money. It is a description of the value a company offers to one or several segments of customers and the architecture of the firm and its network of partners for creating, marketing and delivering this value and relationship capital, in order to generate profitable and sustainable revenue streams."*

Demnach ist ein Geschäftsmodell ein konzeptioneller Rahmen, womit die Schlüsselfaktoren eines wertschöpfenden Unternehmens und deren Verbindungen zu einander betrachtet und analysiert werden. Das Geschäftsmodell stellt damit eine eigene Analyseebene dar. Um im Detail weitere Auswirkungen und Innovationsaspekte der Blockchain-Technologie auf das Geschäftsmodell strukturiert zu erörtern, wird der Business Model Canvas von Osterwalder und Pigneur (Osterwalder et al. 2013) als Basis herangezogen (s. Abb. 4). Der Business Model Canvas ist ein Framework zur Abbildung von Geschäftsmodelleigenschaften mit der Möglichkeit, Geschäftsmodellalternativen zu erstellen und diese mit einander vergleichbar zu machen. Dieses Analyse-Werkzeug besteht aus neun Geschäftsmodellelemente (1) Kundensegmente (Zielgruppe), (2) Kundenbeziehung (Marktpositionierung), (3) Wertversprechen (Produkt- und Serviceangebote), (4) Schlüsselressourcen (& Kompetenzen), (5) Schlüsselaktivitäten (interne Wertschöpfung), (6) Schlüsselpartnern (externe Wertschöpfung), (7) Vertriebskanäle, (8) Ertragslogik und (9) Kostenlogik.

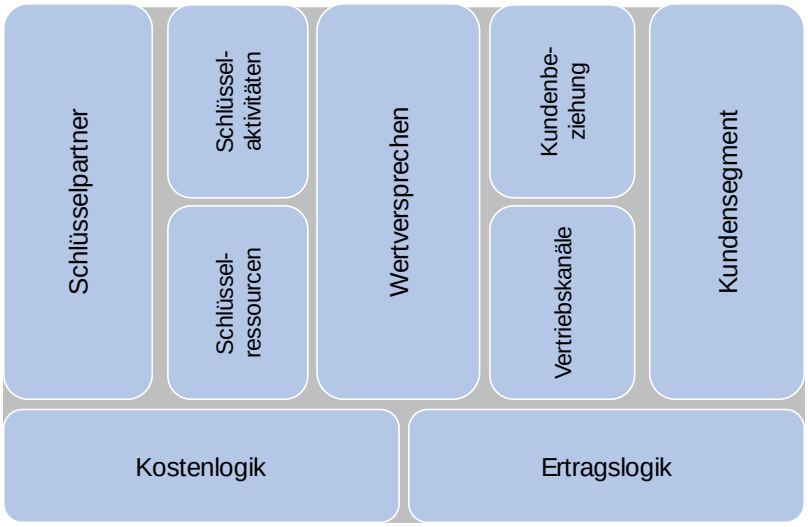

Abb. 4: Business Model Canvas
in Anlehnung an Osterwalder & Pigneur (2013, S.22f.)

Jede der oben genannten Definitionen legt einen anderen Schwerpunkt auf den Kern des Geschäftsmodells, beschreiben jedoch im Grunde, dass ein Geschäftsmodell als Analyseeinheit betrachtet werden kann, die erklären soll, wie das Unternehmen Werte schöpft und diese monetarisiert. Für den weiteren Verlauf wird auf die Geschäftsmodelldefinition von Osterwalder (2013) Bezug genommen, um die Auswirkungen sowie Rahmenbedingungen der Blockchain-Technologie auf ein Geschäftsmodell näher zu betrachten.

Für die Analyse der Potentiale für Geschäftsmodellinnovation durch die Blockchain-Technologie wird die Konzeptualisierung von Spieth und Schneider (2016) verwendet. Diese gliedern die neun Geschäftsmodellelemente in drei Hauptdimensionen für die Innovation des Geschäftsmodells bezüglich des Wertangebotes (Kundensegmente, Marktpositionierung sowie Produkt- und Serviceangebote), der Wertschöpfungsarchitektur (wie Kernkompetenzen und Ressourcen, interne und externe Wertschöpfung, Mechanismen, sowie Vertriebssysteme) und der Werterfassung (wie Ertrags- und Kostenlogik).

Zusätzlich zeigt die dreidimensionale Kategorisierung (s. Abb. 5) die Verbundenheit und Interdependenz der einzelnen Dimensionen untereinander. Eine Veränderung bspw. im Rahmen des Geschäftsmodells hinsichtlich der Zielgruppe in den Kundensegmenten hat einen unmittelbaren Einfluss auf die Marktpositionierung und auf das Produkt- und Serviceangebot. Eine Geschäftsmodellinnovation beinhaltet demnach die Änderung mindestens einer der drei Hauptdimensionen des Geschäftsmodelles (Spieth und Schneider 2016; Brenk et al. 2019).

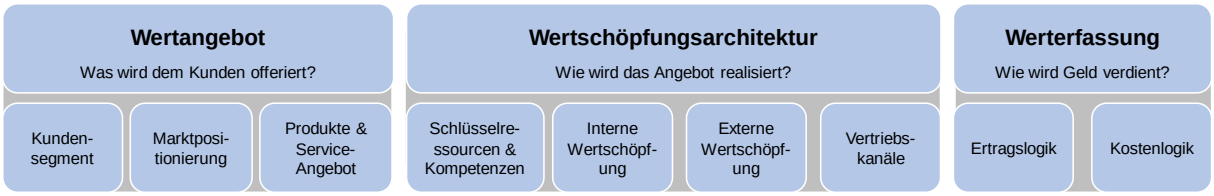

Abb. 5: Dimensionen und Elemente der Geschäftsmodellinnovation in Anlehnung an Spieth & Scheider (2016)

In diesem Sinne werden im Folgenden die einzelnen Dimensionen bezüglich des Einflusses von Blockchain-Technologie auf das Geschäftsmodell dargestellt. Dabei werden jede dieser drei Dimensionen sowie die neun zugehörigen Elemente für Geschäftsmodellinnovation in diesem Abschnitt näher betrachtet und die Auswirkung der Blockchain-Technologie auf diese erläutert. Rahmenbedingungen, die bei der Umsetzung einer der drei Blockchain-Strategien zu beachten sind, werden ebenfalls fokussiert. Mit Beispielen aus der Praxis werden die Effekte, die durch die Blockchain-Technologien resultieren, an den neun Elementen für Geschäftsmodellinnovation veranschaulicht. Die Beispiele stammen aus Interviews mit Unternehmensverantwortlichen, die Blockchain in ihren Unternehmen bereits nutzen, sowie aus einer Literaturrecherche (z.B. (Morkunas et al. 2019)).

6.2.1 Blockchain Wertangebot

Innerhalb dieser Innovationsdimension wird das Werteangebot betrachtet, welches ein Unternehmen am Markt anbietet und dadurch ein gewisses Kundenbedürfnis deckt und darüber den Kunden an sich bindet. Hierbei steht im Fokus die folgende Frage: „Was wird dem Kunden (an Produkte / Dienstleistungen etc.) offeriert?“ Die Geschäftsmodellinnovationselemente (1) Kundensegment, (2) Marktpositionierung und (3) Produkt- und Serviceangebote (s. Abb. 6) dienen dazu zu klären, welche Vorteile eine Organisation wem bietet und wie man sich dadurch von seinen Wettbewerbern abhebt. Jedes dieser Geschäftsmodellelemente beantwortet eine konkrete Frage in Bezug auf die Perspektive der Geschäftsmodellinnovation. Im Hinblick auf Blockchain befasst sich das Element Kundensegment mit der Frage: „Wen möchte ich mit meinem Blockchain-Angebot erreichen?“ Im Fokus des Elements Marktpositionierung steht die Frage: „Wie kann ich mich durch die Blockchain-Technologie von meinen Konkurrenten differenzieren.“ Das dritte Geschäftsmodellelement dieser Dimension „Produkt- & Serviceangebot“ analysiert: „Welche Produkte, Services und Kundenvorteile biete ich mit meiner Blockchain-Lösung?“ (Spieth und Schneider 2016). Im weiteren Verlauf werden die vorgestellten Geschäftsmodellelemente im Detail betrachtet und anhand von Beispielen die möglichen taktischen Blockchain-Mechanismen abgeleitet.

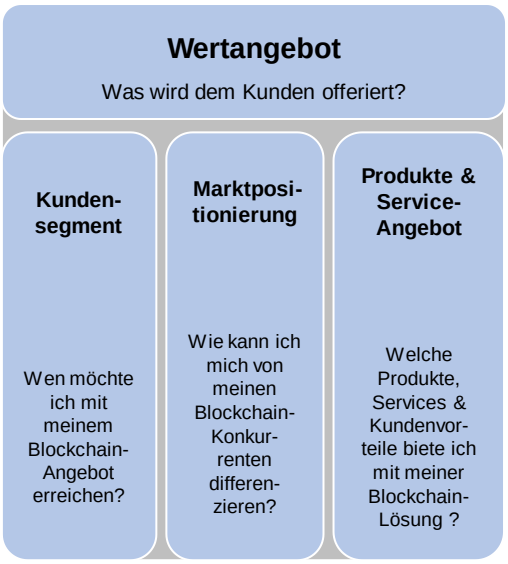

Abb. 6: Blockchain-Wertangebot

Kundensegmente

Zielgruppen werden durch die Kundensegmente determiniert, welche nach Osterwalder und Pigneur (2013) als diverse Personengruppen und Organisationen beschrieben werden, die ein Unternehmen mit Ihren Produkten und Services erreichen möchte. Diese Gruppen von Menschen und Organisationen werden i.d.R. in entsprechende Segmente kategorisiert, welche durch spezifische Eigenschaften charakterisiert sind. In Bezug auf Blockchain bedeutet dies die Feststellung, für welche Kunden die Blockchain einen Wert schafft.

Die Blockchain-Technologie besitzt das Potential, neue Segmente zu adressieren, welche aufgrund von Vertrauens- und Skalierungsproblemen zuvor nicht bedienbar waren. Mit der Blockchain können völlig neue Märkte und derer Kundensegmente erreicht werden, deren Zugang über eine zentralisierte Bewirtschaftung von Organisationen bisher nicht oder nur begrenzt möglich war (Larios-Hernández 2017). Etwa 2 Milliarden Menschen aus Entwicklungsländern wie Afrika, Asien oder Südamerika rücken nunmehr in den Fokus. Oftmals besitzen die Menschen in weit abgelegenen Dörfern dieser Länder keinen Zugang zu einer Bank und haben keine Möglichkeit, ihr Geld zu verwalten (Iansiti und Lakhani 2017). Mit Hilfe der Bitcoin Blockchain ändert sich diese Situation. Landesübergreifende Zahlungen bspw. an Freunde oder Familie sind mit dem Einsatz von Blockchain schnell und direkt möglich, ohne dafür hohe Gebühren zu entrichten, oder ein Bankkonto zu besitzen. Dadurch, dass die Transaktionsdetails verteilt und verschlüsselt im Netzwerk abgelegt werden, ist eine entsprechende Nachweisbarkeit gesichert und die Manipulation der Daten ausgeschlossen.

Somit wird gleichzeitig eine hohe Transparenz und Sicherheit bei reduzierten Kosten und gesteigerter Effizienz durch eine Skalierung von Transaktionen geschaffen.

In einer Blockchain, in der sich die einzelnen Stakeholder wie Kunden und Nutzer selbst und dezentral organisieren, können diese fortan selbst bestimmen, welche Rolle sie einnehmen. Sie können auf der einen Seite die klassische Rolle des Kunden einnehmen, in der sie einen Dienst der Blockchain nutzen. Auf der anderen Seite können die Nutzer auch als Anbieter agieren, indem sie Ihre persönlichen Daten bspw. zu Forschungszwecken verkaufen und weitergeben. In diesem Fall kann der Kunde nun auch als Lieferant z.B. für Daten agieren. Dem Kunden wird die Möglichkeit eröffnet, eine deutlich aktivere Rolle einzunehmen (C2B), als dies derzeit im Markt der Fall ist (B2C). Die Blockchain erzeugt neuartige Kundensegmente, welche sich als „Prosumers" charakterisieren lassen (Kenning 2018).

Marktpositionierung

Die Positionierung "beschreibt die Arten von Beziehungen, die ein Unternehmen zu bestimmten Kundensegmenten" eingehen möchte (Osterwalder et al. 2013, S. 27). Die Gestaltung der Kundenbeziehung basiert dabei nicht nur auf die entsprechende Zielgruppe, sondern wird auch von den Zielen des Unternehmens beeinflusst, wie bspw. Neukundegewinnung, Bestandskundenpflege, etc.. Um dies genauer zu erörtern helfen Fragen, wie:

- „Welche Erwartungshaltung haben die einzelnen Zielgruppen im Hinblick auf die Gestaltung der Beziehung?" oder
- „Wie wird die Beziehung zu den Kunden organisiert?" und vor allem
- „Welchen Beitrag kann die Blockchain liefern, um die Wertschöpfungsbeziehungen zu festigen?"

Wird das Ziel verfolgt, die Beziehung zu bestehenden Kunden zu intensivieren und diese langfristig an das Unternehmen zu binden, kann die Blockchain-Technologie einen wertvollen Beitrag dazu leisten. Denn mit dem Einsatz einer Blockchain ist es möglich Prozesse transparent abzubilden und dadurch die Vertrauensbasis zwischen dem Kunden und Unternehmen zu stärken (Gassmann 2019). Kunden, die ein hohes Vertrauen zu einem Unternehmen besitzen, binden sich langfristig und bleiben dem Unternehmen i.d.R. treu. Neukunden zu erreichen und an das Unternehmen zu binden, bedarf einem vielfach höheren Investitionseinsatz, anstatt die Beziehung zu bestehenden Kunden zu stärken. Die Transparenz, die mit der Blockchain geschaffen wird, kann Unternehmen dabei unterstützen ihre Positionierung am Markt zu stärken, indem sie die Erwartungen ihrer Kunden besser

erfüllen können. Vor allem beim Melden von Schadens- oder Unfallfälle ist es häufiger so, dass ab dem Zeitpunkt der Meldung i.d.R. sechs bis acht Wochen benötigt werden (oder sogar länger) bis ein Gutachter den Schaden bewertet und dieser im besten Fall reguliert wird (Teichner 2009). Dieser Prozess lässt sich mit Hilfe einer Blockchain auf der Basis von Smart Contracts soweit automatisieren, dass in diversen Bereichen anhand von historischen Schadensansprüchen entsprechende Gutachten erstellt werden können (Deloitte 2017). Aufgrund der schnelleren und leichteren Abwicklung des Prozesses ist davon auszugehen, dass die Kundenzufriedenheit gesteigert und die Position am Markt durch eine bessere Kundenbindung gesichert werden kann.

Wie bereits im vorherigen Kapitel beschrieben, ist es möglich durch die Blockchain Intermediäre abzulösen. Das bekannteste Beispiel hierfür ist die digitale Kryptowährung Bitcoin. Mit Hilfe von Blockchain erfolgt die Transaktion von sogenannten Bitcoins zwischen zwei Parteien, ohne dass weitere Intermediäre in dem Prozess involviert sind. Das traditionelle Geschäftsmodell der Banken beruht darauf, dass diese als Vermittler bei Geldangebot und -nachfrage auftreten und diverse Interessen ausgleichen und Vertrauen schaffen, welches die Kundenbeziehungen beeinflusst und steuert (Nakamoto; Iansiti und Lakhani 2017). Durch die Blockchain-Technologie wird die Kundenbeziehungen direkter und autonomer, wobei Plattformen oder Intermediäre für eine vertrauensvolle Kundenbeziehung nicht mehr relevant sind. Die Transaktionspartner sind dadurch in einem direkten Austausch, da das Vertrauen und die Sicherheit über die Blockchain-Technologie abgebildet werden und kein Intermediär die direkte Kundenbindung und dementsprechend die Marktpositionierung beeinflusst. Aufgrund der direkten Bindung der Nutzer ist es möglich gezielter auf die Bedürfnisse einzugehen und dadurch die Kundenbindung zu stärken. Mit Hilfe von Smart Contracts können bei regelmäßig wiederkehrenden Zahlungen automatisierte Prozesse vereinbart werden, wodurch die Transaktionsbeziehungen weiter intensiviert und selbstorganisiert werden.

Produkte- & Serviceangebot

Wie der Harvard Business School Professor Theodore Levitt (1974) einmal sagte: „Die Leute wollen keinen Bohrer kaufen, sie wollen ein Loch in Ihrer Wand." Mit anderen Worten, Kunden wollen nicht das Produkt kaufen, sondern eine Lösung, die mit dem Produkt erzielt werden kann, um eine wichtige Aufgabe zu erledigen, den sogenannten „Job-to-be-done". Alle Aktivitäten eines Unternehmens, die einen Mehrwert für die Kunden eines Unternehmens bietet, werden daher in dem „Produkte und Serviceangebot" zusammengefasst, welches das Wertversprechen darstellt (Osterwalder et al. 2013). Prinzipiell wird mit dem Einsatz einer

Blockchain ein digitales Serviceangebot generiert, welches zum Ziel hat, eine Effizienzsteigerung, Kostenreduzierung, Erhöhung der Flexibilität, Transparenz und Automatisierung von Transaktionen zu erzeugen. Das Wertversprechen baut bei der Blockchain-Technologie auf eine dezentrale und vertrauenswürdige Datendokumentation auf, welche durch Pseudonymisierung und Kryptographie vor Manipulation und Datenmissbrauch gesichert ist (Iansiti und Lakhani 2017; Nakamoto).

Am Beispiel einer digitalen Patientenakte werden zwei Mehrwerte mit dem Einsatz von Blockchain deutlich. Durch den unmittelbaren und universellen Zugriff auf die Patientenakte, können Mediziner sich in kürzester Zeit einen Überblick über die Krankheitshistorie des Patienten verschaffen (Yue et al. 2016). Dadurch ist es möglich, dass schneller und gezielter eine Diagnose gestellt und eine Behandlung vorgenommen werden kann. Die Transparenz und Zugänglichkeit, wodurch eine Prozessoptimierung erwirkt wird, sind Mehrwerte als Werteversprechen, die mit der Blockchain erreicht werden können. Neue Wertangebote können dadurch zugänglich gemacht werden.

Betrachtet man den Energiesektor stellt sich oftmals dort das Problem, dass es keine vertrauenswürdigen Mechanismen zur Verfolgung der erzeugten Energie aus erneuerbaren Quellen und ihrer Lieferung zum Endkunden existieren. Die Blockchain bietet an dieser Stelle einen Lösungsansatz, bei dem von der Erzeugung bis hin zur Lieferung an den Haushalt eine transparente Verfolgung geschaffen und dokumentiert wird. Die Transparenz erlaubt dem Energieunternehmen das Labeln von Ökostrom und der Überprüfung von echtem Ökostrom. Das bestehende Wertangebot von Unternehmen kann mithilfe der Blockchain-Technologie optimiert werden (Meinel et al. 2018).

6.2.2 Blockchain Wertschöpfungsarchitektur

Die Geschäftsmodellinnovationsdimension „Wertschöpfungsarchitektur“ bezieht sich darauf wie das Wertangebot operativ realisiert wird. Die Frage „Wie das Unternehmen das Angebot konkret umsetzt“ steht hierbei im Mittelpunkt. Um diese Frage konkret beantworten zu können, bedarf es einer Kombination aus vier Elementen: (4) Schlüsselressourcen, (5) Interne Wertschöpfung, (6) Externe Wertschöpfung und (7) Vertriebskanäle (s. Abb. 7). Jeder dieser Geschäftsmodellinnovationselemente betrachtet jeweils aus einer anderen Perspektive die übergreifende Frage. Somit steht bspw. bei den „Kernkompetenzen und Ressourcen“ im Hinblick auf das Thema Blockchain die folgenden Fragen im Fokus: „Welche Blockchain-Kernkompetenzen & -Ressourcen stehen mir zur Verfügung? Worauf basiert mein Blockchain-Angebot?“. Das Element „Vertrieb“ beschäftigt sich mit der Frage; „Wie möchte ich meine Zielgruppe erreichen und an mich binden (über welche Kanäle)?“ Und die

beiden Dimensionen „Interne & externe Wertschöpfung“ betrachten die Frage nach den Kernaktivitäten, die innerhalb und außerhalb der Organisation erbracht werden müssen, um das Blockchain-Wertangebot umsetzten und damit die Zielgruppe erreichen zu können (Spieth und Schneider 2016). Im weiteren Verlauf werden die vorgestellten Geschäftsmodellelemente im Detail betrachtet und anhand von Beispielen mögliche taktische Blockchain Mechanismen abgeleitet.

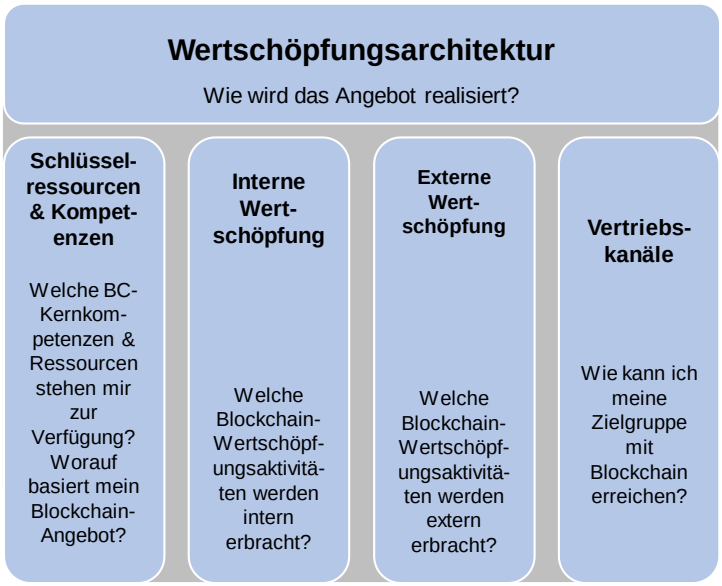

Abb. 7: Blockain-Wertschöpfungsarchitektur

Schlüsselressourcen

Schlüsselressourcen bilden den Grundstein für ein funktionsfähiges Geschäftsmodell (Osterwalder et al. 2013). Unternehmen sind darauf angewiesen Ressourcen zu nutzen, um mit Hilfe derer ein Werteangebot zu generieren, Märkte zu erreichen, Kundenbeziehungen aufzubauen und Umsätze zu erzielen. Ohne den Einsatz entsprechender Ressourcen wäre dies nicht möglich. Vor allem ausreichend liquide Mittel verhelfen Unternehmen oftmals zu (neuen) Möglichkeiten, um ein entsprechendes Wertangebot zu schaffen. Neben diesen finanziellen Mitteln sind allerdings auch menschliche, physische sowie interkulturelle Ressourcen von Bedeutung und spielen eine ebenso entscheidende Rolle.

Es stellt sich die Frage, welche Schlüsselressourcen notwendig sind, um die Blockchain-Technologie im eigenen Unternehmen zu implementieren. Zunächst müssen physische Ressourcen geschaffen werden. Möchte man als Unternehmen an einer Blockchain partizipieren oder diese implementieren, ist es notwendig, den Zugang zu dieser zu realisieren. Die Peer-2-Peer-Netzwerk-Infrastuktur, die das Kernstück einer Blockchain bildet, werden durch eine Verbindung über das Internet abgebildet. Mit jeder Transaktion, die

getätigt wird, wächst der Block einer Blockchain und die Internetverbindung wird zunehmend beansprucht. Um eine kontinuierliche Verbindung zum Netzwerk sicherzustellen, ist eine ausreichende und stabile Internetverbindung und IT notwendig.

Entscheidet sich ein Unternehmen eine konzerneigene Blockchain aufzusetzen ist zu beachten, dass auch hier die physischen Bedingungen zunächst zu prüfen sind. Unter anderem ist sicherzustellen dass ausreichend Speicherplatz für die Sicherung der Transaktionsblöcke, sowie genügend Rechenleistung, für die Mining-Prozesse zur Verfügung steht. Um diese technologischen Anforderungen zu realisieren, bedarf es zudem personelle Ressourcen. Fachlich ausgebildetes Personal ist dafür einzustellen, oder vorhandenes Personal über Lehrgänge oder Schulungen fortzubilden, somit kann langfristig eine interne Blockchain-Expertise aufgebaut werden.

Mit dem Einsatz einer Blockchain müssen Unternehmen ihre Ressourcen und deren Einsatz überdenken. Betrachtet man in diesem Zusammenhang den Immobiliensektor, wird deutlich, dass mittels der Technologie diverse Schlüsselressourcen abgelöst bzw. neu definiert werden. Mit Hilfe der anonymisierten, vergleichbaren Daten einer Blockchain ist es möglich Investitionen effizient zu bewerten. Die Erfahrung und das Wissen eines Immobilienbewerters bzw. Maklers könnte aufgrund der automatisierten und transparenten Bewertung obsolet werden, da dies über die Blockchain-Technologie abbildbar wird. Der Vorteil ist, dass nicht nur finanzielle Mittel wie Transaktionskosten eingespart werden, sondern auch Transparenz im Immobilienkauf geschaffen wird. Immobiliengesellschaften wären demzufolge nicht mehr auf die Ressource Immobilienmakler angewiesen.

Interne und externe Wertschöpfungsströme (Schlüsselaktivitäten)

Neben den Schlüsselressourcen sind die internen und externen Wertschöpfungsaktivitäten von elementarer Bedeutung. Innerhalb dieser Elemente des Geschäftsmodells werden die Schlüsselaktivitäten eines Unternehmens betrachtet, die maßgeblich zur Schaffung des Leistungsangebotes beitragen (Osterwalder et al. 2013, S. 34). Mit der Identifizierung dieser Schlüsselaktivitäten wird deutlich, welche Prozesse sich unmittelbar auf den Geschäftserfolg auswirken. An diesen Aktivitäten sind häufig diverse Stakeholder wie Partner, Lieferanten, sowie Mitarbeiter beteiligt, die einen direkten oder indirekten Einfluss auf diese Aktivitäten haben. Demzufolge ist bei der Betrachtung dieser Dimension wichtig zu hinterfragen, wer bzw. welche Personen(gruppen) an den Aktivitäten beteiligt sind. Die Elemente „Vertriebskanäle“ und „Ertragslogik“ stehen demnach unmittelbar mit den Schlüsselaktivitäten in Verbindung.

Bei der Betrachtung der Frage, welchen Mehrwehrt die Blockchain-Technologie im Hinblick auf die Schlüsselaktivitäten bewirkt, steht beispielsweise der Vorteil der Automatisierung der Supply Chain von produzierenden Unternehmen im Vordergrund. Mit Hilfe von Smart Contracts ist es möglich, Lieferketten zu optimieren. Auf Basis eines festgelegten Regelwerkes können automatisiert Entscheidungen getroffen werden. Langwierige, diffizile Preisverhandlungen oder Prozessschritte könnten in Zukunft dank der Blockchain-Technologie verschlankt und effizienter gestaltet werden (Morkunas et al. 2019). Für Unternehmen reduziert sich dadurch der Bearbeitungs- sowie Kostenaufwand bei regelmäßig wiederkehrenden Aufgaben.

Ein weiterer positiver Effekt der Blockchain im Hinblick auf wertschöpfende Prozesse ist, dass eine höchstmögliche Transparenz für jegliche Stakeholder geschaffen werden kann. Eine hohe Transparenz ist u.a. für die Rückverfolgung (Track & Trace) von Fleischprodukten zur Qualitätssicherung von Interesse. Denn oftmals können bisher nur einzelne Ausschnitte einer Wertschöpfungskette überprüft werden. Wodurch eine lückenlose und fälschungsfreie Rückverfolgung und die damit verbundene Ermittlung „schwarzer Schafe“ innerhalb der Produktionslinien erschwert wird (Dimitrov 2020). Durch Smart Contracts ändert sich diese Situation jedoch grundlegend. Über QR-Codes oder RFID-Chips lassen sich alle relevanten Daten über Tier, Haltung, Futter, Züchter, Schlachtung, Transport und Qualität des Fleisches weltweit erfassen und in einer für alle Beteiligten einsehbaren Blockchain lückenlos dokumentieren (Meinel et al. 2018). Im Smart Contract sind alle Richtlinien und Eventualitäten, sowie die Folgeschritte hinterlegt. Das System kann die nächsten Schritte automatisch auslösen, wenn eine Bedingung eingetreten ist (Dimitrov 2020)

Auf Basis der Blockchain-Technologie ist es zudem möglich sogenannte dezentrale autonome Organisationen (DAO) zu realisieren, dessen Ziel es ist gemeinsam neue Produkte und Werteangebote zu realisieren (Meinel et al. 2018). Diese Art der Organisation unterliegt keinen hierarchischen Strukturen bzw. hat keinen Geschäftsführer oder eine andere leitende Instanz. Gehandelt und entschieden wird anhand des Regelwerks (Smart Contracts, welches die Teilnehmenden gemeinsam, basieren auf dem Mehrheitsprinzip, aufgestellt haben (Meinel et al., 2018). Mittels einer DAO können neue Potentiale erreicht werden, um in einer Gemeinschaft von Wertschöpfungspartnern neue Produkte und Dienstleistungen zu entwickeln und zu vermarkten. Die erste DAO, die auf Basis einer Ethereum-Blockchain umgesetzt wurde, hatte keine Mitarbeiter, sondern agierte auf Basis von Smart Contracts. Das Wertangebot dieser DAO bestand darin Crowdfunding zu betreiben und finanzierte sich dadurch. Der Erlös, der im Rahmen einer DAO mit dem Verkauf der Leistungen erzielt wird, wird entweder reinvestiert oder an ihre Anteilseigner aufgeteilt. Die DAO stellt demnach eine

neue Organisationsform der Wertschöpfung dar, mit Hilfe derer im Verbund von Akteuren neue Opportunitäten & Wertangebote erzeugt werden können (Meinel et al., 2018).

Vertriebskanäle

Die Dimension Vertrieb beschreibt, wie ein Unternehmen mit seinen Kundensegmenten kommuniziert und diese erreicht, um ein Leistungsversprechen zu liefern (Osterwalder et al., 2013, S. 26). Die Kanäle gestalten sich divers. Sie können bspw. physisch vor Ort als lokale Geschäfte oder digital über Telefon, Mail Webseiten etc. organisiert sein.

Durch die Eliminierung von Intermediären mittels der Blockchain-Technologie, können Unternehmen eine direkte Verbindung zum Kunden aufbauen, wo es zuvor nicht möglich war und lediglich über den Intermediär organisiert wurde. Die Kunden werden direkt über die Blockchain mit dem Anbieter in Kontakt treten und Preise bzw. Verträge aushandeln. Gelingt dieser Schritt, können Vermittlungsplattformen wie UBER oder Airbnb abgelöst werden (Iansiti und Lakhani 2017). Ein weiterer Vorteil des direkten Kontaktes zum Kunden mittels der Blockchain ist der potentielle Zugriff auf entsprechende Kundendaten. Diese können für Echtzeitanalysen genutzt werden, um u.a. eine gezieltere und erfolgreichere Bedürfnisadressierung zu ermöglichen und folglich maßgeschneiderte Angebote zu offerieren (Seidel 2019).

Im Zuge der Digitalisierung gehören digitale Verträge in jeglichen Branchen mittlerweile zum täglichen Geschäft. Mit dem Einsatz von Smart Contracts können digitale Verträge zukünftig automatisch, basierend auf dem festgelegenen Regelwerk, und ohne eine zeitintensive menschliche Schnittstelle landesübergreifend abgewickelt werden, welche eine effizientere Distribution von Services über eine Blockchain ermöglicht. Aber auch neue Arten von Kanälen können mittels einer Blockchain innerhalb und außerhalb eines Unternehmens eingeführt werden, z.B. durch die gemeinsame Nutzung von einheitlichen Codes zur Stärkung einer Lieferkette (Montecchi et al. 2019).

6.2.3 Blockchain Wertfassung

Unternehmen entwickeln Wege, um Erträge zu generieren, Kosten zu managen und gleichzeitig die Kundenbedürfnisse zu befriedigen, welches innerhalb der Dimension Werterfassung betrachtet wird. Hierbei wird aus der gegebenen Wertschöpfungsarchitektur der höchstmögliche Gewinn versucht zu erzielen. Im Allgemeinen werden diese Vorhaben in den Elementen (8) Ertragslogik und (9) Kostenlogik erfasst (s. Abb. 8), um die folgende Frage zu beantworten: „Wie das Unternehmen Geld verdient?“. Innerhalb der Ertragslogik wird betrachtet, welche Verdienstmöglichkeiten mit der Blockchain generiert werden und was in

diesem Zusammenhang die Haupteinnahmequellen sind. Dahingegen betrachtet die Kostenlogik die Frage: „Wie die Blockchain-Kostenstruktur aussieht und was die primären Kostenblöcke sind?“ (Spieth und Schneider, 2016). Im weiteren Verlauf werden die vorgestellten Geschäftsmodellelemente im Detail betrachtet und anhand von Beispielen mögliche taktische Blockchain-Mechanismen abgeleitet.

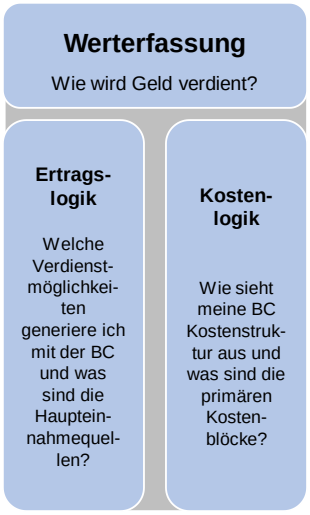

Abb. 8: Blockchain-Werterfassung

Ertragslogik

Das Element der „Ertragslogik“ in einem Geschäftsmodell stellt dar, wie und aus welchem Segment Umsatz generiert wird (Osterwalder et al., 2013, S. 30). Unterschieden werden zwei Arten von Einnahmeströmen: Die einmalige Zahlung und fortlaufenden Zahlungen (Kandolf 2015). In der Blockchain kann bspw. direkt und transparent der Stromverbrauch aller Haushalte erfasst und gespeichert werden. Ertragsmodelle, wie „Pay per Use“ (sogenannte Service-Modelle), bei dem der Kunde lediglich den tatsächlichen Verbrauch bezahlt, wären für Kunden denkbar, die eine zusätzliche Flexibilität schätzen (Schmück und Gassmann 2019). Energieproduzenten & -lieferanten könnten, nachdem ein Kunden Strom bezogen hat, umgehend den Betrag vom Konto des Kunden abbuchen. Die Kunden müssten nicht mehr einen ungefähren Betrag im Voraus bezahlen oder am Ende des Jahres mit einer Nachzahlung überrascht werden. Ebenfalls müsste der Energielieferant nicht mehr aufwändige Verbraucherabrechnungen erstellen, da die Bezüge bzw. Abrechnungen transparent in der Blockchain gespeichert werden. Mit der Optimierung des Abrechnungsprozesses würden zudem weitere Kosten eingespart werden (Gatteschi et al. 2018).

Mit dem Wegfall von Intermediären durch die Blockchain ist vor allem damit zu rechnen, dass sich auch die Margenverteilung für wertschöpfende Unternehmen positiv auswirken wird. Betrachtet man den Kauf einer Immobilie, wird schnell deutlich, dass neben Makler, Immobilienbewerter, Notare und diverse weitere Intermediäre beteiligt sind. Mit der Blockchain und der Nutzung von Smart Contracts, in denen u.a. der Verkaufsablauf geregelt ist, fallen all die verursachten Kosten/Umsätze der vermittelnden Parteien weg, welche dem System selbst zu gebucht werden kann. Abhängigkeiten von zwischenliegenden Parteien werden aufgelöst, sodass eine höhere Marge durch eine transparentere Preissetzung erzielt werden kann (Morkunas et al. 2019).

Eine weitere Möglichkeit Erträge über die Blockchain zu generieren ist die Nutzung von Initial Coin Offerings (ICOs) (siehe hierzu auch Kapitel Rechtliche Rahmenbedingungen). ICO ist ein Finanzierungsmittel, in dem Kunden reales Geld, wie Euro oder Dollar, in einen virtuellen Wert, Currency-Token genannt, tauschen können (Schmück und Gassmann 2019). Diese Methode wird oftmals von Startups genutzt, um den Kapitalbeschaffungsprozess zu umgehen. Mittels der Currency-Token, können Anteile der Startups, anstelle von Aktien, an Investoren verkauft werden. Je mehr Anteile ein Investor besitzt, desto höher ist sein Mitspracherecht. Neben dessen können die Currency-Token, wie Libra oder Bitcoin, auch als reine digitale Währung zur direkten Bezahlung von Produkten- und Dienstleistungen über die Blockchain genutzt werden (Iansiti und Lakhani, 2017). Alle Transaktionen werden in der Blockchain verifiziert und gespeichert.

Kostenlogik

Der letzte Baustein bezieht sich auf die Kostenstruktur eines Geschäftsmodells. Die Kostenlogik beschreibt alle anfallenden Kosten, die im Rahmen der Wertschöpfung eines Unternehmens entstehen (Osterwalder et a., 2013, S. 40). Ein wesentlicher Vorteil, der mit der Implementierung einer Blockchain erzielt werden kann, ist die Kostenreduzierung im Rahmen der Automatisierung von Prozessen. Mit dem Einsatz der Technologie kann u.a. ein Track & Trace in der Supply Chain erzielt werden. Mit Track & Trace, im Logistiksektor auch als Sendungsverfolgung bekannt, ist mittels der Rückverfolgung ein vereinfachtes Dokumentenmanagement entlang der Lieferkette realisierbar. Ursprungszeugnisse für den Zoll, Nachweispapiere wie FIATA-Dokumente und Ladescheine für den Wassertransport sind nicht weiter aufwendig zu erstellen, da die Authentifizierung über die Blockchain abgebildet werden kann. Jeder beteiligte dieser Supply Chain kann auf die Daten des Transportes digital zugreifen und entsprechend prüfen und verifizieren. Prozesse können dadurch optimiert, eine

Kostensenkung realisiert und im besten Fall eventuell sogar eine Gewinnerhöhung erreicht werden (Meinel et al. 2018).

Demgegenüber sollten jedoch nicht die Implementierungskosten für die Blockchain-Technologie vernachlässigt werden. Um nicht allzu hohe Investitionskosten aufzuwenden, empfiehlt es sich zunächst eine private Unternehmens-Blockchain aufzusetzen, in der im geschützten Umfeld die Technologie ausprobiert werden kann (Iansiti und Lakhani, 2017). Speicherplatz, sowie ausreichend Rechenkapazität werden u.a. für das Speichern der Transaktionen in der Blockchain als auch zum Verarbeiten der Mining-Prozesse benötigt, welche sich in Form von Transaktionskosten bei einer Öffnung der Blockchain wiederspiegeln.

Nachdem die Technologie aufgesetzt und in den Betrieb genommen wurde, passiert es oftmals, dass bei der Initiierung des Projektes nicht die Folgekosten beachtet wurden. Wartungs- sowie weitere Entwicklungskosten zur Instandhaltung der Blockchain sollten demnach großzügig vorgesehen werden. Hierbei sind auch die Personalkosten wie die Blockchain-Pflege zu berücksichtigen (Gassmann 2019). Im Zeitalter der Digitalisierung wird die Halbwertszeit des Wissens stetig kürzer. Das Wissen veraltet zunehmend schneller. Es ist zu erwarten, dass auch die Blockchain-Technologie sich weiterhin stetig entwickeln wird. Für Mitarbeiter, die verantwortlich für diese Technologie sind, bedeutet dies, sich stetig auf dem neusten Stand zu halten, um den Anschluss am Markt nicht zu verlieren. Dies äußert sich in erhöhten Weiterbildungskosten für Mitarbeiter bezüglich der komplexen Blockchain-Technologie (Gassmann 2019).

6.3 Organisationswandel

Eine Blockchain im Unternehmen zu implementieren wird häufig in den Kontext von Change Management gesetzt, da zwangsläufig mitunter große Veränderungen in einem Unternehmen notwendig werden (Fujitsu und CXP Group 2017). Die Literatur zu Organisationswandel betont immer wieder die Tendenz vieler Organisationen Veränderungen langsam zu übernehmen, oder teilweise resistent gegenüber Veränderungen zu sein. Die Gründe reichen dabei von (fest-) gewachsenen Strukturen, dem Vertrauen auf feste und reproduzierbare Routinen bis zu „strukturellem Erstarren“ durch innere (z.B. Kosten, Willen) oder äußere Faktoren (z.B. rechtliche Hürden) (Hannan und Freeman 1984; Boettke et al. 2008).

Daher werden angemessenes Budget, gut ausgebildetes Personal und die Unterstützung des Managements als notwendige Erfolgsfaktoren gesehen (Fujitsu und CXP Group 2017). Ein weiterer Erfolgsfaktor sei der Einsatz interdisziplinärer Teams unter Einbeziehung

verschiedener, auch externer Experten in ko-kreativen Verfahren. Dies betrifft von der Identifizierung von Anwendungsgebieten, über technische Integration bis zur Prozessanpassung alle Teile eines Implementierungsprozesses (Fujitsu und CXP Group 2017). Dabei müssen die Belange, Sorgen und Wünsche der Belegschaft von vorne herein berücksichtigt werden (Piderit 2000).

Blockchain-Technologie kann unternehmensinterne Prozesse maßgeblich verändern. So besteht etwa die Möglichkeit, die Arbeit von Aufsichtsräten durch eine Blockchain redundant zu machen, da etwa Finanzen oder Compliance automatisiert und in Echtzeit überprüft und Berichtspflichten so erfüllt werden könnten. Auch Jahreshauptversammlungen könnten durch sichere, dezentrale Abstimmungen ein Ding der Vergangenheit sein (Jesuthasan und Ganu 2019). Dies bedarf natürlich einer noch zu schaffenden rechtlichen Grundlage.

Ein maßgebliches Kriterium für erfolgreiche Innovationen ist deren nachhaltige Verankerung in einer Organisation. Gerade bei Technologien stellt sich dabei die Frage, ob die Nutzer*innen in der Lage sind, sie angemessen zu verwenden. Eine Blockchain-basierte Anwendung wird daher die gleichen Standards an das Design des User Interfaces erfüllen müssen, wie andere Anwendungen auch (Shneiderman et al. 2018).

6.4 Cyberrisiken

Die Cyberrisiken in Bezug auf Blockchain-Systeme unterscheiden sich nicht grundlegend von denen anderer IT-Systeme. Es ist allerdings eine gesonderte Risikobewertung vorzunehmen. Hierbei ist zu beachten, dass keine allgemeingültigen Aussagen zu Blockchain-Systemen getroffen werden können, da diese Risiken je nach Anwendungsfall, Systemkontext und eingesetzter Technologie grundsätzlich anders bewerten werden müssen. Trotzdem lohnt sich eine Betrachtung der Risiken, da so die Dimensionen des Lösungs- und Gefahrenraums besser eingeschätzt werden können.

Konkrete Handlungsempfehlungen

Tabelle 1: (BSI 2012, S. 33–61; ESMA 2017, S. 21–24)

Offene Herausforderungen	Perspektivische Handlungsempfehlungen
Spezielle Informationssicherheitsstandards in Bezug auf Blockchain-Systeme: ▪ Vertraulichkeit von Daten ▪ Löschen oder sperren des Zugriffs auf Daten in der Blockchain	Anpassung gesetzlicher Anforderungen, wie z.B. DSGVO und branchenspezifischer und lokaler Vorschriften, an technische Rahmenbedingungen, bzw. Anpassung der Technologie an gesetzlichen Rahmen. Darüber hinaus Identifizierung oder Entwicklung von Standardmethoden für die Entfernung von Daten (mit der besonderen Herausforderung, dass dies technisch in regulären Blockchain-Systemen unmöglich ist) aus Blockchain-Systemen, bzw. Filterung von Ein- und Ausgabedaten entsprechend der rechtlichen Anforderungen.
Überwachung illegaler Aktivitäten und Fraud Detection	Anpassung existierender Fraud Detection Mechanismen an technische Gegebenheiten von Blockchain-Systemen.
Interoperabilität zwischen verschiedenen Blockchain-Systemen	Betrachtung existierender Blockchain-Interoperabilitätsframeworks, Implementierung klassischer Enterprise Application Integration Lösungen.
Konsequenzen von Quantencomputern	Erforschung und Entwicklung von Post-Quantum-Algorithmen für die asymmetrische Kryptographie. Gleichzeitig müssen die Konsequenzen in Hinblick auf die Kryptoagilität von bestehenden Blockchain-Systemen bewertet werden. Anforderungen an die Kryptoagilität sind Use Case spezifisch.

Datenschutz im Kontext von Smart Contracts	Spezielle Anforderungen in Hinblick auf die Entwicklung von datenschutzkonformen Smart Contracts und Smart Contract Laufzeitumgebungen müssen überprüft werden (Unterweger et al. 2018).
Regierungskontrollen	Mechanismen zur Ergänzung von existierenden Sicherheits- und Governance-Kontrollen müssen etabliert werden.
Wallet Management	Etablierung von Standards für Wallet-Management-Software, speziell in Hinblick auf Interoperabilität mit verschiedenen Blockchain-Systemen. Darüber Untersuchung von technischen Möglichkeiten zur sicheren Erstellung und Interaktion mit Schlüsselmaterial, sowie Erarbeitung von Lösungen und Empfehlungen zum Umgang von Verlust und Diebstahl von Schlüsselmaterial.

Risikobewertung

Mögliche Risiken müssen im Vorfeld identifiziert werden, um geeignete Maßnahmen frühzeitig einleiten zu können. Mit welcher Intensität und Dringlichkeit Risiken und Angriffen behandelt werden können und sollten, kann anhand einer Grafik beispielhaft quantifiziert und in verschiedene Risikokategorien einsortiert werden.

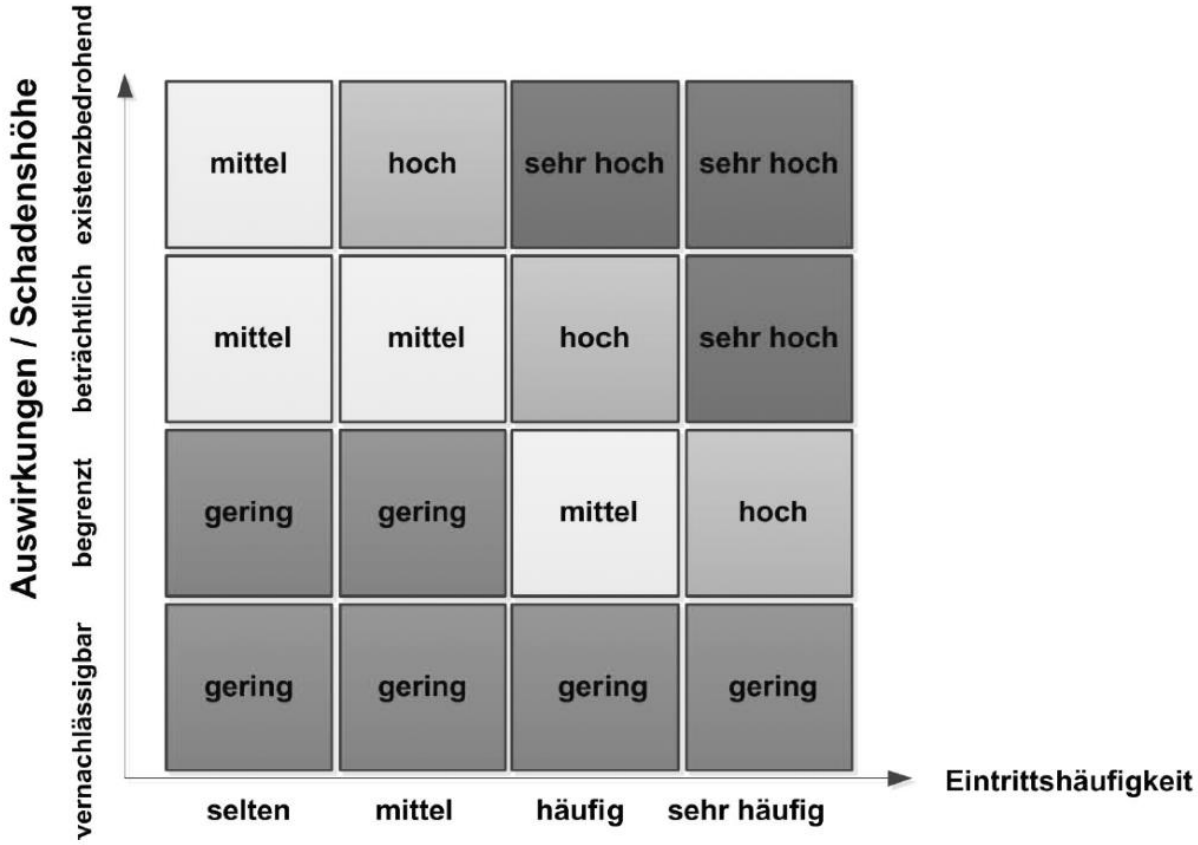

Abbildung 1: Matrix zur Einstufung von Risiken (Bundesamt für Sicherheit in der Informationstechnik 2017)

Tabelle 2: Definition der Risikokategorien (BSI 2017)

Risikokategorien	
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Gefährdungen können entsprechend der Cyber-Sicherheitsbedürfnisse in Anlehnung an die CIA-Triad identifiziert werden (BSI 2012, S. 14; Pohlmann 2019, S. 32):

- Vertraulichkeit (C): Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
- Verfügbarkeit (A): Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.
- Integrität (I): Übertragene und gespeicherte Information sind vollständig und unverändert.

Gefährdung	**Grund werte**	**Wirkung**	**Kommentar**	**Vorsichtsmaßnahmen**	**Handlungsempfehlung bei einem Notfall**
G0.1(a) Schlüsselverlust	A	Direkt	Schlüssel können lesenden Zugriff auf die Informationen innerhalb der Transaktionen ermöglichen. Bei Verlust eines Schlüssels kann der Zugriff auf die Informationen unwiederbringlich verloren gehen.	Verwendung von Wiederherstellungsschlüsseln und Backups.	Sperrung/Blockierung des Schlüssels vornehmen. Neuen Schlüssel generieren und autorisieren.
G0.1(b) Schlüsseldiebstahl	C, A, I	Direkt	Unautorisierter lesender Zugriff und Fälschung von eingehenden Daten möglich.	Sichere Speicherung von Schlüsselmaterial	Sperrung/Blockierung des Schlüssels vornehmen. Invalidierung geschriebener Blöcke seit Diebstahl. Neuen Schlüssel generieren und autorisieren.
G0.2 Kryptografie	C, I	Indirekt	Schlüsselmaterial muss entsprechend Industriestandards generiert und mit	Korrekte kryptographische	Schlüssel neu generieren und Kryptografie

			Ablaufdatum versehen werden.	Parameter verwenden. Standardsoftware zur Erstellung verwenden. Verschiedene Schlüssel für unterschiedliche Anwendungsfälle	auf Korrektheit überprüfen. Falls nötig Krytpoagilitäts maßnahmen anwenden.
G.03 Privatsphäre / Unbefugter Zugriff auf Daten	C	Direkt	Wenn Transaktionsdaten unverschlüsselt gespeichert sind, könnten Personen/Unternehmen unbefugten Zugriff erhalten.	Datenzugriffsmöglichkeiten auf ein Minimum reduzieren. (Need-to-know-Prinzip) Kriterien zur Berechtigungserteilung definieren. **Einsatz von Audit-Mechanismen für Zugriff.**	Zugriffsberechtigungen überprüfen und unbefugten Personen/Unternehmen Berechtigungen entziehen, falls unerlaubter Besitz vorliegt.
G0.4 Softwareintegrität	C, A, I	Indirekt	Die Korrektheit eines Blockchain-Systems kann bei unzureichender Codeüberprüfung nicht garantiert werden.	Sicherheitsrichtlinien und –Anforderungen zu regelmäßigen Code-Audits definieren.	Sicherheitsrichtlinien überarbeiten und dokumentierpflichtige Kontrollen nach vorgegebenen Intervallen durchführen.
G0.5 Betrügerische	I	Direkt	Eine unübliche Auslastung der Rechnerleistung könnte	Überwachen, ob einer der Knoten die Rechnerleistu	Transaktionen neu zuordnen oder einem Knoten das

Transaktionen			auf eine betrügerische Transaktion hinweisen.	ng erhöht oder eine größere Anzahl von Transaktionen ausführt.	Ausführen von einer großen Anzahl von Transaktionen erschweren.
G0.6 Identitätsdiebstahl.	C, I	Indirekt	Smart Contracts berechtigen bestimmte Entitäten zur Ausführung festgelegter Aktionen. Durch missbräuchliche Nutzung einer fremden oder falschen Identität kann ein Angreifer unberechtigt Zugriff auf diese Aktionen erhalten.	Teilnehmende Entitäten müssen validiert werden. Verantwortlichkeiten müssen klar definiert sein. Interne Identifizierung von natürlichen Personen über organisatorische Verfahren.	Entität kontaktieren und Verantwortlichkeiten überprüfen.
G0.7 Softwareintegrität von eingesetzten Smart Contracts	C, A, I	Direkt	Smart Contracts können als Bibliotheken zur Verfügung gestellt und eingebunden werden. Schadhafter Smart Contract Code kann daher potentiell die Integrität des gesamten Systems kompromittieren.	Siehe G0.4	Siehe G0.4

Tabelle 2: Ermittlung elementarer Gefährdungen und entsprechenden Sicherheitsmaßnahmen sowie Handlungsempfehlungen (vgl. BSI 2017, S. 27).

Identifizierte Gefährdungen müssen daraufhin auf ein konkretes System abgebildet werden, wobei anhand der resultierenden Kritikalitätskategorien eine Priorisierung vorgenommen werden kann. Die Kritikalitätskategorien spannen den Bereich von *unkritisch* bis *hoch kritisch* auf, wobei die Kritikalitätskategorie als Produkt verschiedener Parameter wie Wiederanlaufzeit bei Ausfall, maximal tolerierbare Ausfallzeit und Gesamtschaden nach Zeit X modelliert werden kann.

Eine einfache zweidimensionale Betrachtung der Gefährdungen eines spezifischen Blockchain-Systems in Hinblick auf die Kritikalitätskategorien ermöglicht die Darstellung innerhalb eines Koordinatensystems:

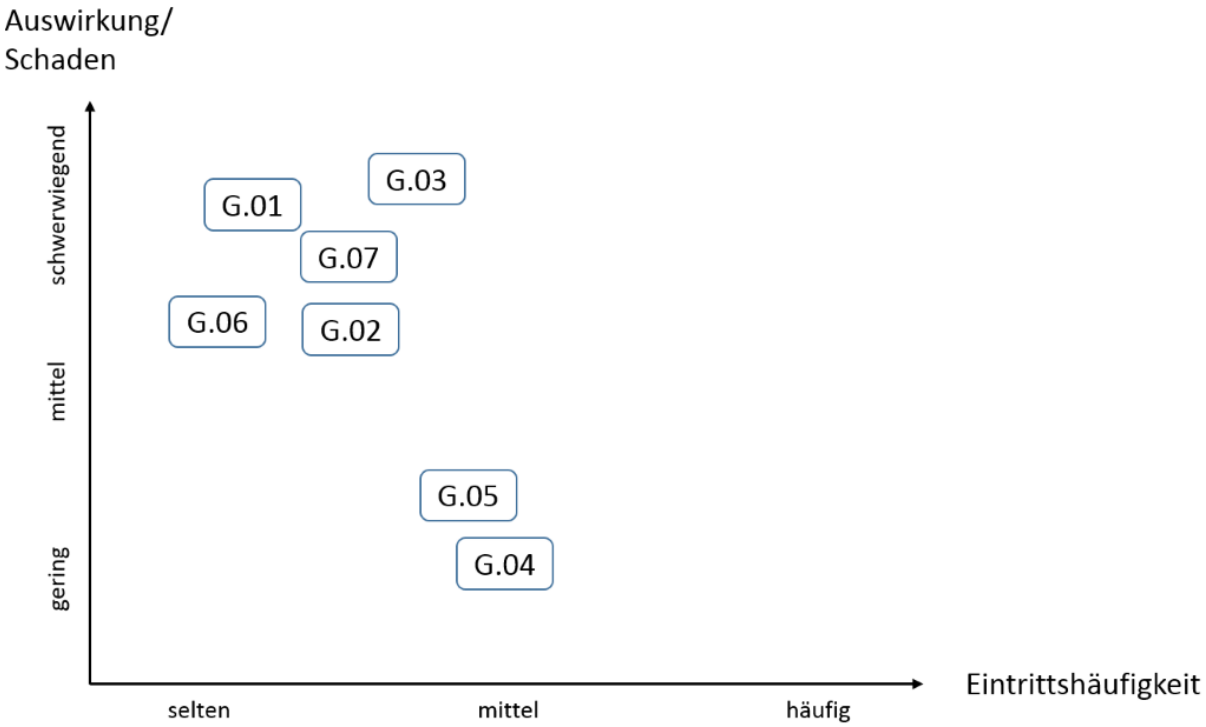

Abbildung 2: Beispielhafte Einstufung von Risiken (vgl. BSI 2017, S. 27)

Zusammenfassung

Zusammenfassend lässt sich sagen, dass aktuell keine offiziellen Standards und Handlungsempfehlungen zur Umsetzung und dem Betrieb von Blockchain-Systemen existieren. Da es sich bei einem Blockchain-System allerdings implizit um ein IT-System handelt, können diese bestehenden Leitfäden und Standards entsprechend auf Blockchain-Systeme angewendet werden, wobei allerdings eine Priorisierung und Gewichtung je nach Einzelfall notwendig ist. Betrachten wir z.B. G0.1(a) (Schlüsselverlust), so bedeutet dies im Fall einer Blockchain-basierten Kryptowährung in einem öffentlichen Netzwerk den unwiederbringlichen Verlust des eigenen Guthabens. Betrachten wir allerdings ein konsortiumgeführtes Blockchain-System zur Signierung von Daten, so kann bei Schlüsselverlust ein neuer Schlüssel durch das Konsortium autorisiert werden, die Kritikalität ist hier also niedriger als beim Währungsbeispiel.

7 Literaturverzeichnis

Adam, Katarina; Ben Naceur, Med Ridha; Kaulartz, Markus; Kunde, Elke; Kunz, Matthias; Liban, Samater et al. (2017): Faktenpapier Blockchain und Datenschutz. Bitkom e.V. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf, zuletzt geprüft am 12.02.2020.

Albrecht, Julian; John, David (2018): Die einkommenssteuerliche Abgrenzung zwischen Gewerbebetrieb und Vermögensverwaltung bei Investitionen in Kryptotoken. In: *Finanzrundschau* (Band 101, Heft 9), S. 393–407.

Ammann, Thorsten (2018): Bitcoin als Zahlungsmittel im Internet. In: *Computer und Recht* (6), S. 379–386.

Artikel-29-Datenschutzgruppe (2014): Stellungnahme 5/2014 zu Anonymisierungstechniken (WP216, 0829/14/DE).

Ateniese, Giuseppe; Magri, Bernardo; Venturi, Daniele; Andrade, Ewerton (2017): Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. In: IEEE Communications Society (Hg.): 2017 IEEE European Symposium on Security and Privacy (EuroS&P). Paris, S. 111–126.

Atzori, Marcella (2015): Blockchain Technology and Decentralized Governance: Is the State Still Necessary? In: *SSRN Journal*. DOI: 10.2139/ssrn.2709713.

BaFin (2011): Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 5 KWG. Bundesanstalt für Finanzdienstleistungsaufsicht. Online verfügbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html, zuletzt geprüft am 21.01.2020.

BaFin (2017): Hinweisschreiben (WA) – WA 11-QB 4100-2017/0010, Aufsichtsrechtliche Einordnung von sog. Initial Coin Offerings (ICOs) zugrundeliegenden Token bzw. Kryptowährungen als Finanzinstrumente im Bereich der Wertpapieraufsicht. Bundesanstalt für Finanzdienstleistungsaufsicht. Online verfügbar unter https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/, zuletzt geprüft am 13.01.2020.

BaFin (2019): Merkblatt (WA) – WA 51-Wp 7100-2019/0011, Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token. Bundesanstalt für Finanzdienstleistungsaufsicht. Online verfügbar unter

https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_wa_merkblatt_ICOs.html, zuletzt geprüft am 13.01.2020.

Bamberger, Heinz Georg; Roth, Herbert; Hau, Wolfgang; Poseck, Roman (2020): BeckOK BGB. 53. Aufl.

Bausch, Stephan; Heetkamp, Simon (2018): Wie kommt der „Kuckuck" auf den Bitcoin? Im Blickpunkt: Zwangsvollstreckung in Kryptowährungen. In: *Dispute Resolution* (1), S. 7–10.

Bechtolf, Hans; Vogt, Niklas (2018): Datenschutz in der Blockchain – Eine Frage der Technik. Technologische Hürden und konzeptionelle Chancen. In: *Zeitschrift für Datenschutz* 9 (2), S. 66–71.

Beck, Benjamin (2015): Bitcoins als Geld im Rechtssinne. In: *Neue juristische Wochenschrift : NJW* 68 (9), S. 580–586.

Berger, Daniel (2019): Brave 1.0: Browser blockiert Werbung und Tracker. Heise. Online verfügbar unter https://www.heise.de/newsticker/meldung/Brave-1-0-Browser-blockiert-Werbung-und-Tracker-4586145.html, zuletzt aktualisiert am 14.11.2019, zuletzt geprüft am 17.12.2019.

Bertram, Ute (2018): Smart Contracts. Praxisrelevante Fragen zu Vertragsabschluss, Leistungsstörungen und Auslegung. In: *Monatsschrift für Deutsches Recht* (23), S. 1416–1421.

Blockchain Bundesverband (2018): Blockchain, data protection, and the GDPR. Online verfügbar unter https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf, zuletzt geprüft am 20.01.2020.

BMF; BMJV (2019): Eckpunkte für die regulatorische Behandlung von elektronischen Wertpapieren und Krypto-Token. Bundesministerium der Finanzen; Bundesministerium der Justiz und für Verbraucherschutz. Online verfügbar unter https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2019-03-07-Eckpunktepapier-Wertpapiere-Krypto-Token/2019-03-07-Eckpunktepapier-regulatorische-Behandlung-elektronische-Wertpapiere-Krypto-Token.pdf?__blob=publicationFile&v=7, zuletzt geprüft am 12.02.2020.

BMWi; BMF (2019): Blockchain-Strategie der Bundesregierung. Wir stellen die Weichen für die Token-Ökonomie. Bundesministerium für Wirtschaft und Energie; Bundesministerium der Finanzen. Online verfügbar unter

https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.html, zuletzt geprüft am 08.01.2020.

BNetzA (2019): Die Blockchain-Technologie. Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation. Bundesnetzagentur.

Boehm, Franziska; Pesch, Paulina (2014): Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung. In: *Multimedia und Recht* 17 (2), S. 75–79.

Boettke, Peter J.; Coyne, Christopher J.; Leeson, Peter T. (2008): Institutional Stickiness and the New Development Economics. In: *American Journal of Economics and Sociology* 67 (2), S. 331–358. DOI: 10.1111/j.1536-7150.2008.00573.x.

Böhme, Rainer; Pesch, Paulina (2017): Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. In: *Datenschutz Datensich* 41 (8), S. 473–481. DOI: 10.1007/s11623-017-0815-y.

Boucher, Philip; Nascimento, Susana; Kritikos, Mihalis (2017): How blockchain technology could change our lives. In-depth analysis. [Brussels]: [European Parliament] (In-depth analysis). Online verfügbar unter www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf.

Brandt, Mathias (2019): Anleger investieren Milliarden in neue Krypto-Coins. statista. Online verfügbar unter https://de.statista.com/infografik/11517/volumen-von-ico-finanzierungsrunden-pro-monat/, zuletzt geprüft am 03.03.2020.

Brenk, Sebastian; Lüttgens, Dirk; Diener, Kathleen; Piller, Frank (2019): Learning from failures in business model innovation: solving decision-making logic conflicts through intrapreneurial effectuation. In: *J Bus Econ* 89 (8-9), S. 1097–1147. DOI: 10.1007/s11573-019-00954-1.

BSI (2012): Leitfaden Informationssicherheit. Bundesamt für Sicherheit in der Informationstechnik.

BSI (2017): BSI-Standard 200-3. Bundesamt für Sicherheit in der Informationstechnik.

BSI (2019): Blockchain sicher gestalten. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5, zuletzt geprüft am 15.12.2019.

Bundesverband Blockchain (2020): Über uns. Online verfügbar unter https://bundesblock.de/de/about-us/, zuletzt geprüft am 15.01.2020.

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) (2018): Die zunehmende Eigendynamik von Kryptowährungen und ihre Folgen (22). Online verfügbar unter https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-022.pdf, zuletzt geprüft am 08.01.2020.

Cant, Joeri (2019): China Introduces Blockchain-Based Identification System for Cities. Cointelegraph. Online verfügbar unter https://cointelegraph.com/news/china-introduces-blockchain-based-identification-system-for-cities, zuletzt geprüft am 25.11.2019.

Casadesus-Masanell, Ramon; Ricart, Joan Enric (2010): From Strategy to Business Models and onto Tactics. In: *Long Range Planning* 43 (2-3), S. 195–215. DOI: 10.1016/j.lrp.2010.01.004.

Chatard, Yannick; Mann, Maximilian (2019): Initial Coin Offerings und Token-Handel im funktionalen Rechtsvergleich. Entwicklung deutscher Leitlinien auf Grundlage des Diskussionsstands in der Schweiz, Frankreich und Deutschland.

Chong, Alain Yee Loong; Lim, Eric T. K.; Hua, Xiuping; Zheng, Shuning; Tan, Chee-Wee (2019): Business on Chain: A Comparative Case Study of Five Blockchain-Inspired Business Models. In: *JAIS*, S. 1308–1337. DOI: 10.17705/1jais.00568.

Danninger, Nadja; Glatz, Florian; Nehrenheim, Helmut; Papp, Laszlo; Rieger, Alexander; Wagner, Kai (2019): Blockchain in der Verwaltung. Anwendungsbereiche und Herausforderungen. Online verfügbar unter http://bivd-initiative.de/wp-content/uploads/2019/09/Blockchain_in_der_Verwaltung_Teil_1_2019-09-06.pdf, zuletzt geprüft am 01.02.2020.

Davis, Fred D.; Bagozzi, Richard P.; Warshaw, Paul R.: User acceptance of computer technology - a comparison of two theoretical models. In: *Management Science* 1989 (35), S. 982–1003.

Deloitte (2017): Die Blockchain (R)evolution. Die Schweizer Perspektive. Online verfügbar unter https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-de-innovation-blockchain-revolution.pdf, zuletzt geprüft am 17.02.2020.

Di Fabio, Udo (2019): Die Verwandlung der westlichen Demokratien. In: *FAZ*, 22.07.2019. Online verfügbar unter https://www.faz.net/aktuell/politik/inland/demokratien-im-westen-auf-der-suche-nach-europaeischer-identitaet-16295717.html, zuletzt geprüft am 07.01.2020.

Dimitrov, Biser (2020): How Walmart And Others Are Riding A Blockchain Wave To Supply Chain Paradise. Online verfügbar unter https://www.forbes.com/sites/biserdimitrov/2019/12/05/how-walmart-and-others-are-riding-a-blockchain-wave-to-supply-chain-paradise/#1c815fb57791, zuletzt geprüft am 16.01.2020.

Effer-Uhe, Daniel (2018): Kryptowährungen in Zwangsvollstreckung und Insolvenz am Beispiel des Bitcoin. In: *Zeitschrift für Zivilprozess* 131 (4), S. 513–532. DOI: 10.1515/zzp-2018-1310405.

Einaste, Taavi (2018): Blockchain and healthcare: the Estonian experience. Nortal. February 21, 2018. Online verfügbar unter https://nortal.com/blog/blockchain-healthcare-estonia/, zuletzt geprüft am 25.11.2019.

Engelhardt, Christian; Klein, Sascha (2014): Bitcoins – Geschäfte mit Geld, das keines ist – Technische Grundlagen und zivilrechtliche Betrachtung. In: *Multimedia und Recht* 17 (6), S. 355–360.

Erbguth, Jörn (2016): Konfliktlösung auf der Blockchain. In: Samuel van Oostrom und Stephan Weth (Hg.): Festschrift für Maximilian Herberger, S. 285–296.

Erbguth, Jörn (2019): Datenschutzkonforme Verwendung von Hashwerten auf Blockchains. Wann sind kryptografische Hashwerte von personenbezogenen Daten selbst wieder personenbezogene Daten? In: *Multimedia und Recht* 22 (10), S. 654–660.

ESMA (2017): Distributed Ledger Technology & Cybersecurity. Europäische Wertpapier- und Marktaufsichtsbehörde.

ESMA (13.11.2017): ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements. Online verfügbar unter https://www.esma.europa.eu/, zuletzt geprüft am 12.01.2020.

ESMA (2019): Advice to the European Union (EU) Institutions. Europäische Wertpapier- und Marktaufsichtsbehörde. Online verfügbar unter https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection, zuletzt geprüft am 03.03.2020.

Finck, Michèle (2019a): Blockchain and the general data protection regulation. Can distributed ledgers be squared with European data protection law? [Luxembourg]: Publications Office of the European Union. Online verfügbar unter www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

Finck, Michèle (2019b): Smart Contracts as a Form of Solely Automated Processing Under the GDPR. In: *SSRN Journal*. DOI: 10.2139/ssrn.3311370.

Finck, Michhle (2018): Blockchains and Data Protection in the European Union. In: *SSRN Journal*. DOI: 10.2139/ssrn.3080322.

Foss, Nicolai J.; Saebi, Tina (2017): Fifteen Years of Research on Business Model Innovation. In: *Journal of Management* 43 (1), S. 200–227. DOI: 10.1177/0149206316675927.

Francisco, Kristoffer; Swanson, David (2018): The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. In: *Logistics* 2 (1), S. 2. DOI: 10.3390/logistics2010002.

Fridgen, Gilbert; Guggenberger, Nikolas; Hoeren, Thomas; Prinz, Wolfgang; Urbach, Nils; Baur, Johannes et al. (2019): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. Fraunhofer-Institut für Angewandte Informationstechnik FIT. Online verfügbar unter https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile, zuletzt geprüft am 15.12.2019.

Fries, Martin (2018): Smart Contracts: Brauchen schlaue Verträge noch Anwälte? In: *Anwaltsblatt* 68 (2), S. 86–90.

Fujitsu; CXP Group (2017): Blockchain - the opportunity beyond the hype, zuletzt geprüft am 17.12.2019.

Gassmann, Oliver (2013): Geschaftsmodelle entwickeln. 55 innovative konzepte mit dem st. galler business model. [Place of publication not identified]: Carl Hanser Verlag Gmbh &.

Gassmann, Oliver (2019): Digitale Transformation gestalten, zuletzt geprüft am 16.01.2020.

Gatteschi, Valentina; Lamberti, Fabrizio; Demartini, Claudio; Pranteda, Chiara; Santamaria, Victor (2018): To Blockchain or Not to Blockchain: That Is the Question. In: *IT Prof.* 20 (2), S. 62–74. DOI: 10.1109/MITP.2018.021921652.

Gawer, Annabelle (2014): Bridging differing perspectives on technological platforms: Toward an integrative framework. In: *Research Policy* 43 (7), S. 1239–1249. DOI: 10.1016/j.respol.2014.03.006.

Gentemann, Lukas (2019): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Studienbericht. Bitkom e.V. Online verfügbar unter https://www.bitkom.org/sites/default/files/2019-06/190613_bitkom_studie_blockchain_2019_0.pdf, zuletzt geprüft am 10.02.2020.

Gola, Peter (Hg.): Datenschutz-Grundverordnung. Kommentar. 2. Aufl. München: C.H. Beck.

Gupta, Manav (2017a): Blockchain For Dummies®, limitierte Auflage von IBM. Online verfügbar unter https://www.ibm.com/downloads/cas/D8O9VBAK, zuletzt geprüft am 14.02.2020.

Gupta, Manav (2017b): Blockchain For Dummies®, limitierte Auflage von IBM. Online verfügbar unter https://www.ibm.com/downloads/cas/D8O9VBAK, zuletzt geprüft am 14.02.2020.

Habersack, Mathias; Mülbert, Peter; Schlitt, Michael (2019): Unternehmensfinanzierung am Kapitalmarkt. 4. Aufl.

Hacker, Philipp; Thomale, Chris (2017): Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. In: *SSRN Journal*. DOI: 10.2139/ssrn.3075820.

Hahn, Christopher; Wilkens, Robert (2019): ICO vs. IPO – Prospektrechtliche Anforderungen bei Equity Token Offerings. In: *Zeitschrift für Bankrecht und Bankwirtschaft* 31 (1), S. 10–26. DOI: 10.15375/zbb-2019-0104.

Hannan, Michael; Freeman, John (1984): Structural Inertia and Organizational Change. In: *American Sociological Review* 49 (2), S. 149–164.

Hanten, Mathias; Sacarcelik, Osman (2019): Zivilrechtliche Einordnung von Kryptowährungen und ICO-Token und ihre Folgen. In: *Recht der Finanzinstrumente* (3), S. 124–131.

Heckelmann, Martin (2018): Zulässigkeit und Handhabung von Smart Contracts. In: *Neue juristische Wochenschrift : NJW* 71 (8), S. 504–510.

Higginson, Matt; Nadeau, Marie-Claude; Rajgopal, Kausik (2018): Blockchain's Occam problem. McKinsey. Online verfügbar unter https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem, zuletzt aktualisiert am October 2018, zuletzt geprüft am 13.01.2020.

Hoeren, Thomas; Sieber, Ulrich; Holznagel, Bernd (Hg.) (2019): Handbuch Multimedia-Recht. München: C.H. Beck.

Iansiti, Marco; Lakhani, Karim R. (2017): Truth About Blockchain.

Ibáñez, Luis-Daniel; O'Hara, Kieron; Simperl, Elena (2018): On Blockchains and the General Data Protection Regulation. EU Blockchain Forum. Online verfügbar unter https://www.eublockchainforum.eu/knowledge?page=1, zuletzt geprüft am 05.01.2020.

J.P.Morgan (2019): The Next Step for Blockchain. What are the barriers and opportunities for the evolving blockchain ecosystem? Online verfügbar unter https://www.jpmorgan.com/global/research/blockchain-next-steps, zuletzt aktualisiert am 06.05.2019, zuletzt geprüft am 17.12.2019.

Jesuthasan, Ravin; Ganu, Shai (2019): Can a Board Member's Job Be Automated? Harvard Business Review. Online verfügbar unter https://hbr.org/2019/10/can-a-board-members-job-be-automated, zuletzt geprüft am 02.10.2019.

Jetzke, Tobias; Richter, Stephan (2017): Welt ohne Bargeld – Veränderung der klassischen Bezahl- und Bankensystemene. Hg. v. tab-beim-bundestag.de. Online verfügbar unter https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-016.pdf, zuletzt aktualisiert am 26.02.2020, zuletzt geprüft am 26.02.2020.

Kandolf, Thomas (2015): Systematische Geschäftsmodellentwicklung: Der Weg zum marktfähigen Geschäftsmodell. [Place of publication not identified]: Diplomica Verlag GmbH.

Kaulartz, Markus (2016): Die Blockchain-Technologie – Hintergründe zur Distributed Ledger Technology und zu Blockchains. In: *Computer und Recht* (Band 32, Heft 7), S. 474–480.

Kaulartz, Markus (2019): Smart Contract Dispute Resolution. In: Martin Fries und Boris P. Paal (Hg.): Smart Contracts. Tübingen: Mohr-Siebeck, S. 73–83.

Kaulartz, Markus; Heckmann, Jörn (2016): Smart Contracts – Anwendungen der Blockchain-Technologie. In: *Computer und Recht* 32 (9). DOI: 10.9785/cr-2016-0923.

Kenning, Peter (2018): Entgrenzungen des Konsums: Springer Fachmedien Wiesbaden.

Kietzmann, Jan; Archer-Brown, Chris (2019): From hype to reality: Blockchain grows up. In: *Business Horizons* 62 (3), S. 269–271. DOI: 10.1016/j.bushor.2019.01.001.

Kiviat, Trevor I. (2015): Beyond Bitcoin: Issues in Regulating Blockchain Transactions, zuletzt geprüft am 26.02.2020.

Kleinert, Ursula; Mayer, Volker (2019): Elektronische Wertpapiere und Krypto-Token. Aktuelle Rechtslage und die Blockchain-Strategie der Bundesregierung vom 18.9.2019.

Klöhn, Lars; Parhofer, Nicolas; Resas, Daniel (2018): Initial Coin Offerings (ICOs) – Markt, Ökonomik und Regulierung. In: *Zeitschrift für Bankrecht und Bankwirtschaft*, S. 89–106.

Knaier, Ralf; Wolff, Lothar (2018): Die Blockchain-Technologie als Entwicklungsoption für das Handelsregister? In: *Betriebs-Berater* 73 (39), S. 2253–2260.

Koch, Philipp (2018): Die „Tokenisierung" von Rechtspositionen als digitale Verbriefung. In: *Zeitschrift für Bankrecht und Bankwirtschaft* 30 (6), S. 359–368. DOI: 10.15375/zbb-2018-0604.

Kollmann, Tobias (1998): Akzeptanz innovativer Nutzungsgüter und -systeme. Konsequenzen für die Einführung von Telekommunikations- und Multimediasystemen. Wiesbaden: Springer.

Kütük, Erdem; Sorge, Christoph (2014): Bitcoin im deutschen Vollstreckungsrecht - Von der „Tulpenmanie" zur „Bitcoinmanie". In: *Multimedia und Recht* 17 (10), S. 643–646.

Larios-Hernández, Guillermo Jesús (2017): Blockchain entrepreneurship opportunity in the practices of the unbanked. Online verfügbar unter https://www.sciencedirect.com/science/article/pii/S0007681317301209?via%3Dihub, zuletzt geprüft am 16.01.2020.

Lyons, Tom (2018): Blockchain Innovation in Europe. A thematic report prepared by the European Union Blockchain Observatory & Forum. European Union Blockchain Observatory & Forum. European Union Blockchain Observatory & Forum. Online verfügbar unter https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf, zuletzt geprüft am 05.01.2020.

Lyons, Tom; Courcelas, Ludovic; Timsit, Ken (2018a): Blockchain and the GDPR. A thematic report prepared by the European Union Blockchain Observatory & Forum. European Union Blockchain Observatory & Forum. European Union Blockchain Observatory & Forum. Online verfügbar unter https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, zuletzt geprüft am 05.01.2020.

Lyons, Tom; Courcelas, Ludovic; Timsit, Ken (2018b): Blockchain for Government and Public Services. A thematic report prepared by the European Union Blockchain Observatory &

Forum. European Union Blockchain Observatory & Forum. Online verfügbar unter https://www.eublockchainforum.eu/reports.

Lyons, Tom; Courcelas, Ludovic; Timsit, Ken (2019): Blockchain and Digital Identity. A thematic report prepared by the European Union Blockchain Observatory & Forum. European Union Blockchain Observatory & Forum. Online verfügbar unter https://www.eublockchainforum.eu/reports.

Mahn, Jan (2019): Blockchain-Technik jenseits von Kryptogeld. c't. Online verfügbar unter https://www.heise.de/ct/artikel/Blockchain-Technik-jenseits-von-Kryptogeld-4564147.html, zuletzt aktualisiert am 28.10.2019, zuletzt geprüft am 17.12.2019.

Marnau, Ninja (2017): Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung. In: Maximilian Eibl und Martin Gaedke (Hg.): Informatik 2017. Bonn: Gesellschaft für Informatik, S. 1025–1036.

Martini, Mario; Weinzierl, Quirin (2017): Die Blockchain-Technologie und das Recht auf Vergessenwerden. Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen. In: *Neue Zeitschrift für Verwaltungsrecht : NVwZ : vereinigt mit Verwaltungsrechtsprechung* 36 (17), S. 1251–1259.

Martiny, Dieter (2018): Virtuelle Währungen, insbesondere Bitcoins, im Internationalen Privat- und Zivilverfahrensrecht. In: *IPRax : Praxis des internationalen Privat- und Verfahrensrechts*.

Meinel, Christoph; Gayvoronskaya, Tatiana; Schnjakin, Maxim (2018): Blockchain - Hype oder Innovation. Potsdam: Universitätsverlag Potsdam (Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam).

Montecchi, Matteo; Plangger, Kirk; Etter, Michael (2019): It's real, trust me! Establishing supply chain provenance using blockchain. In: *Business Horizons* 62 (3), S. 283–293. DOI: 10.1016/j.bushor.2019.01.008.

Morabito, Vincenzo (2016): The Future of Digital Business Innovation [recurso electrónico]. Trends and Practices. First edition 2016. Cham.

Morkunas, Vida J.; Paschen, Jeannette; Boon, Edward (2019): How blockchain technologies impact your business model. In: *Business Horizons* 62 (3), S. 295–306. DOI: 10.1016/j.bushor.2019.01.009.

Möslein, Florian (2019): Rechtsgeschäftslehre und Smart Contracts. In: Tom Braegelmann und Markus Kaulartz (Hg.): Rechtshandbuch Smart Contracts. München: C.H. Beck; Vahlen, S. 81–98.

Möslein, Florian; Omlor, Sebastian (2019): FinTech-Handbuch. Digitalisierung, Recht, Finanzen. München: C.H. Beck.

Muth, Robert; Eisenhut, Kerstin; Rabe, Jochen; Tschorsch, Florian (2019): BBBlockchain: Blockchain-based Participation in Urban Development. Preliminary version of 24/06/2019.

MWIDE NRW (2020): Blockchain-Technologie in der Verwaltung. Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen. Online verfügbar unter https://www.wirtschaft.nrw/einsatz-der-blockchain-technologie-der-verwaltung, zuletzt geprüft am 15.01.2020.

Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. Online verfügbar unter https://bitcoin.org/bitcoin.pdf, zuletzt geprüft am 17.02.2020.

Nascimento, S.; Pólvora, A. (2019): Blockchain now and tomorrow. Assessing multidimensional impacts of distributed ledger technologies. Unter Mitarbeit von Nascimento S. (ed), Pólvora A. (ed), Anderberg A., Andonova E., Bellia M., Calès L., Inamorato. Hg. v. S. Nascimento und A. Pólvora. Publications Office of the European Union. Luxemburg (EUR 29813 EN). Online verfügbar unter https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow, zuletzt geprüft am 26.09.2019.

NExT/BiVD (2019): Ankündigung Whitepaper. Online verfügbar unter http://bivd-initiative.de/wp-content/uploads/2019/05/V3.2_BiVD-Whitepaper.pdf, zuletzt geprüft am 01.02.2020.

Omlor, Sebastian (2018): Blockchain-basierte Zahlungsmittel – Ein Arbeitsprogramm für Gesetzgeber und Rechtswissenschaf. In: *Zeitschrift für Rechtspolitik* 51 (3), S. 85–89.

Osterwalder, Alexander; Pigneur, Yves; Clark, Tim (2013): Business model generation. A handbook for visionaries, game changers, and challengers. Hoboken NJ: Wiley. Online verfügbar unter https://profesores.virtual.uniandes.edu.co/~isis1404/dokuwiki/lib/exe/fetch.php?media=bibliografia:9_business_model_generation.pdf, zuletzt geprüft am 16.01.2020.

Paulus, David; Matzke, Robin (2018): Smart Contracts und das BGB – Viel Lärm um nichts? In: *Zeitschrift für die gesamte Privatrechtswissenschaft* 4 (4), S. 431–465.

PayPal Government Relations (2019): Blockchain. Online verfügbar unter https://publicpolicy.paypal-corp.com/issues/blockchain, zuletzt aktualisiert am 17.12.2019.

Perez, Elena (2019): China's Dive Into Blockchain, Digital ID Spurs Rest of World to Action. Cointelegraph. Online verfügbar unter https://cointelegraph.com/news/chinas-dive-into-blockchain-digital-id-spurs-rest-of-world-to-action, zuletzt geprüft am 25.11.2019.

Pesch, Paulina Jo (2017): Cryptocoin-Schulden: Verlag C.H.BECK oHG.

Piderit, Sandy Kristin (2000): Rethinking Resistance and Recognizing Ambivalence. A Multidimensional View of Attitudes toward an Organizational Change. In: *The Academy of Management Review* 25 (4), S. 783. DOI: 10.2307/259206.

Pohlmann, Norbert (2019): Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung: Springer Vieweg.

Püls, Joachim; Gerlach, Christian (2019): Die eIDAS-VO - ein Update zu elektronischen Signaturen. In: *Zeitschrift für die notarielle Beratungs- und Beurkundungspraxis* (3), S. 81–89.

PYMNTS (2019): FEMA Looks At Blockchain To Aid Disaster Payouts, zuletzt aktualisiert am 20.11.2019, zuletzt geprüft am 17.12.2019.

Quiel, Philipp (2018): Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO. In: *Datenschutz Datensich* 42 (9), S. 566–573. DOI: 10.1007/s11623-018-1000-7.

Romba, Eric; Patz, Anika (2019): Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe von Krypto-Token. In: *Recht der Finanzinstrumente* (298-305).

Rossi, Matti; Mueller-Bloch, Christoph; Thatcher, Jason Bennett; Beck, Roman (2019): Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda. In: *JAIS* 20 (9), S. 14.

Rückert, Christian (2016): Vermögensabschöpfung und Sicherstellung bei Bitcoins - Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten. In: *Multimedia und Recht* 19 (5), S. 295–300.

Schäfer, Martina; Keppler, Dorothee (2013): Modelle der technikorientierten Akzeptanzforschung : Überblick und Reflexion am Beispiel eines Forschungsprojekts zur

Implementierung innovativer technischer Energieeffizienz-Maßnahmen. Online verfügbar unter https://depositonce.tu-berlin.de/bitstream/11303/4758/1/schaefer_keppler.pdf, zuletzt geprüft am 09.01.2020.

Schlund, Albert; Pongratz, Hans (2018): Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung. In: *Deutsches Steuerrecht* 56 (12), S. 598–604.

Schmück, Kilian; Gassmann, Oliver (2019): DLT/Blockchain-basierte Geschäftsmodelle. In: Oliver Gassmann und Philipp Sutter (Hg.): Digitale Transformation gestalten. Geschäftsmodelle, Erfolgsfaktoren, Checklisten. 2., überarbeitete und erweiterte Auflage, S. 161–178.

Schneider, Johannes (2019): Das gereizte Jahrzehnt. In: *Zeit Online*, 23.12.2019. Online verfügbar unter https://www.zeit.de/kultur/2019-12/debattenkultur-digitalisierung-empoerung-moral-identitaet-afd-donald-trump, zuletzt geprüft am 07.01.2020.

Schrey, Joachim; Thalhofer, Thomas (2017): Rechtliche Aspekte der Blockchain. In: *Neue juristische Wochenschrift : NJW* 70 (20), S. 1431–1436.

Schroeder, Moritz (2014): Bitcoin: Virtuelle Währung – reelle Problemstellungen. In: *JurPC*, S. 9. DOI: 10.7328/jurpcb2014296103.

Schütte, Julian; Fridgen, Gilbert; Prinz, Wolfgang; Rose, Thomas; Urbach, Nils; Hoeren, Thomas et al. (2017): Blockchain und Smart Contracts. Technologien, Forschungsfragen und Anwendungen. Hg. v. Fraunhofer Gesellschaft. Online verfügbar unter https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf, zuletzt geprüft am 06.09.2019.

Seibel, Andrea (2019): „Viele diskutieren nicht, sondern stellen sich tot“. In: *Welt*, 20.06.2019. Online verfügbar unter https://www.welt.de/politik/deutschland/article195613345/Gedenken-an-Ralf-Dahrendorf-Das-deutsche-Fremdeln-mit-der-Freiheit.html, zuletzt geprüft am 07.01.2020.

Seidel (2019): Banking & Innovation 2018/2019: Springer Fachmedien Wiesbaden.

Shmatenko, Leonid; Möllenkamp, Stefan (2018): Digitale Zahlungsmittel in einer analog geprägten Rechtsordnung - A bit(coin) out of control - Rechtsnatur und schuldrechtliche Behandlung von Kryptowährungen. In: *Multimedia und Recht* 21 (8), S. 495–501.

Shneiderman, Ben; Plaisant, Catherine; Cohen, Maxine; Jacobs, Steven; Elmqvist, Niklas; Diakopolous, Nicholas (2018): Designing the user interface. Strategies for effective human-computer interaction. 6th ed. Pearson: Harlow.

Simmchen, Christoph (2017): Blockchain (R)Evolution. Verwendungsmöglichkeiten und Risiken. In: *Multimedia und Recht* 20 (3), S. 162–165.

Spieth, Patrick; Schneider, Sabrina (2016): Business model innovativeness: designing a formative measure for business model innovation. In: *J Bus Econ* 86 (6), S. 671–696. DOI: 10.1007/s11573-015-0794-0.

Spindler, Gerald; Bille, Martin (2014): Rechtsprobleme von Bitcoins als virtuelle Währung. In: *Zeitschrift für Wirtschafts- und Bankenrecht* 68 (29), S. 1357–1369.

Spindler, Gerald; Wöbbeking, Maren (2019): Smart Contracts und Verbraucherschutz. In: Tom Braegelmann und Markus Kaulartz (Hg.): Rechtshandbuch Smart Contracts. München: C.H. Beck; Vahlen, S. 135–145.

Swan, Melanie (2015): Bitcoin. A Blueprint for a New World Currency. 1. Aufl. Sebastopol: O'Reilly & Associates.

Sydow, Gernot (2020): Bundesdatenschutzgesetz. Handkommentar. Baden-Baden: Nomos.

Teichner, Matthias (2009): Was läuft falsch in der Schadensregulierung? In: Christel Bienstein und Andreas Spickhoff (Hg.): Arzthaftung - Mängel im Schadensausgleich? Berlin, Heidelberg: Springer Berlin Heidelberg (MedR Schriftenreihe Medizinrecht), S. 107–115.

Treat, David; Giordano, Giuseppe; Schiatti, Luca; Borne-Pons, Hugo (2018): Connecting Ecosystems: Blockchain Integration. Accenture.

U.S. Securities and Exchange Commission (11.12.2017): Company Halts ICO After SEC Raises Registration Concerns. Online verfügbar unter https://www.sec.gov/news/press-release/2017-227, zuletzt geprüft am 03.03.2020.

Unterweger, Andreas; Knirsch, Fabian; Leixnering, Christoph; Engel, Dominik (2018): Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum. In: IEEE Communications Society (Hg.): 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). Paris, S. 1–5.

Vries, Alex de (2018): Bitcoin's Growing Energy Problem. In: *Joule* 2 (5), S. 801–805. DOI: 10.1016/j.joule.2018.04.016.

WBGU - Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (2019): Unsere gemeinsame digitale Zukunft. Online verfügbar unter https://epic.awi.de/id/eprint/50474/1/WBGU_2019_HGD_UnsereGemeinsameDigitaleZukunft.pdf, zuletzt geprüft am 08.01.2020.

Weitnauer, Wolfgang (2018): Initial Coin Offerings (ICOs): Rechtliche Rahmenbedingungen und regulatorische Grenzen. In: *Zeitschrift für Bank- und Kapitalmarktrecht* 18 (6), S. 231–236.

Werbach, Kevin (2018): Trust, But Verify: Why the Blockchain Needs the Law. In: *Berkeley Technology Law Journal* 33 (2), S. 487–550.

Wilsch, Harald (2017): Die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts. In: *Deutsche Notar-Zeitschrift* 112 (10), S. 761–787.

World Economic Forum (2019): Strategic Intelligence: Blockchain. Online verfügbar unter https://intelligence.weforum.org/topics/a1Gb00000038qmPEAQ?tab=publications, zuletzt geprüft am 02.10.2019.

Yaga, Dylan; Mell, Peter; Roby, Nik; Scarfone, Karen (2018): Blockchain Technology Overview. U.S. Department of Commerce (NISTIR 8202).

Yue, Xiao; Wang, Huiju; Jin, Dawei; Li, Mingqiang; Jiang, Wei (2016): Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. In: *Journal of medical systems* 40 (10), S. 218. DOI: 10.1007/s10916-016-0574-6.

Zaslowsky, David (2018): SEC's First Cases Imposing Civil Penalties Solely for ICO Securities Offering Registration Violations. Baker McKenzie. Online verfügbar unter https://www.lexology.com/library/detail.aspx?g=3f8f341a-167c-4873-9010-2503fd5d33ec, zuletzt geprüft am 14.01.2020.

Zheng, Zibin; Xie, Shaoan; Dai, Hong Ning; Chen, Xiangping; Wang, Huaimin (2018): Blockchain challenges and opportunities: a survey. In: *IJWGS* 14 (4), S. 352. DOI: 10.1504/IJWGS.2018.095647.

Zickgraf, Peter (2018): Initial Coin Offerings – Ein Fall für das Kapitalmerktrecht? In: *Die Aktiengesellschaft* (9), S. 293–308.

Zott, Christoph; Amit, Raphael; Massa, Lorenzo (2011): The Business Model: Recent Developments and Future Research. In: *Journal of Management* 37 (4), S. 1019–1042. DOI: 10.1177/0149206311406265.