



ulm university universität
uulm

Blockchain-Technologie: Analyse ausgewählter Anwendungsfälle und Bewertung rechtlicher Aspekte

Anna Rasinski

Band 16

**Analysen und Berichte zum Wirtschafts- und Steuerrecht
Herausgegeben von Prof. Dr. iur. Heribert M. Anzinger**

Anna Rasinski

**Blockchain-Technologie: Analyse
ausgewählter Anwendungsfälle und
Bewertung rechtlicher Aspekte**

Schriftenreihe
Analysen und Berichte zum Wirtschafts- und
Steuerrecht

Herausgeber:
Prof. Dr. iur. Heribert M. Anzinger

Anna Rasinski

Blockchain-Technologie: Analyse ausgewählter Anwendungsfälle und Bewertung rechtlicher Aspekte

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

Dissertation/Magisterarbeit, Universität Ulm,
Fakultät für Mathematik und Wirtschaftswissenschaften,
Jahr 2017

Impressum

Universität Ulm
Institut für Rechnungswesen und Wirtschaftsprüfung
Prof. Dr. iur. Heribert M. Anzinger
Helmholtzstraße 22
89081 Ulm
<http://www.uni-ulm.de/index.php?id=43569>

Eine Übersicht über alle Bände der Schriftenreihe finden Sie unter
<http://www.uni-ulm.de/index.php?id=44832>

Diese Veröffentlichung ist im Internet auf dem institutionellen Repository der Universität Ulm (<https://oparu.uni-ulm.de>) verfügbar und dort unter der Lizenz CC BY-NC-ND 4.0 publiziert.

Details zur Lizenz sind unter
<https://creativecommons.org/licenses/by-nc-nd/4.0/> zu finden.



Zu dieser Reihe

In der Reihe Analysen und Berichte zum Wirtschafts- und Steuerrecht werden herausragende Abschlussarbeiten veröffentlicht, die einen Beitrag zum Erkenntnisgewinn insbesondere im Steuerrecht, im Bilanzrecht, im Unternehmensrecht, im Finanz-, Bank- und Kapitalmarktrecht und in angrenzenden Rechtsgebieten liefern wollen.

Anlass zur Begründung dieser Reihe war der Umstand, dass mir als Hochschullehrer immer wieder gute Arbeiten vorgelegt wurden, deren Gedanken und Erkenntnisse ich gerne einer breiteren Fachöffentlichkeit zugänglich gemacht hätte. Doch zu oft ließen vereinzelte methodologische Zweifel, kleinere formale Mängel oder schlicht der Umfang der Arbeiten den Weg zu einer wissenschaftlichen Zeitschriftenveröffentlichung als weit erscheinen. Und die studentischen Verfasser hatten zwar regelmäßig großes Interesse an einer Veröffentlichung, oft aber bereits bei Abgabe ihrer Arbeiten mit dem ersten Arbeitsvertrag ausgestattet, nicht mehr die Zeit zu den dafür notwendigen Kürzungen und Überarbeitungen.

Diese ausdrücklich als Forum für Abschlussarbeiten deklarierte Reihe ermöglicht es, weiterführende studentische Analysen und Berichte unredigiert herauszugeben.

Prof. Dr. iur. Heribert M. Anzinger, Professor für Wirtschafts- und Steuerrecht

Vorwort

Mit Blockchain-Technologie verbinden die einen neue Geschäftsmodelle und eine Revolution traditionsreicher Rechtsinstitute. Andere sehen darin eine überschätzte Hype. Die Wahrheit liegt in der Mitte. Die im Frühjahr 2017 abgeschlossene Arbeit von Anna Rasinski nähert sich Potential und Rechtsfragen der Blockchain-Technologie aus drei Richtungen. Sie behandelt die technischen Grundlagen mit ihren vielfältigen Verknüpfungen zu anderen Distributed Ledger-Technologien und zu Smart Contracts. Sie trägt Geschäftsmodelle zusammen und sie widmet sich im Zusammenhang damit den grundlegenden juristischen Fragen. Auf diese Weise gelingt ihr zum einen eine instruktive Abgrenzung zwischen automatisierten Handelssystemen und selbstvollziehenden Verträgen und zum anderen eine Perspektive auf zukunftsweisende Handlungs- und Organisationsformen.

Die Arbeit greift alle wesentlichen Entwicklungen auf, trägt das deutsche und englischsprachige Schrifttum zusammen und reflektiert eigenständig neue Rechtsfragen und Entwicklungen. Die Verfasserin verliert sich nicht in Details. Die Arbeit glänzt durch eine Fülle von Anwendungsfällen. Beeindruckend ist die Breite der aufgezeigten juristischen Themenfelder mit einem rechtsvergleichenden Einblick in das Vertragsrecht und einem ersten Überblick über die bilanz- und kapitalmarktrechtlichen Fragen.

Auch wenn Forschung und Entwicklung seit der Abgabe Anfang 2017 nicht stillgestanden haben, lohnt sich für den Einstieg in die Themen Blockchain und Smart Contracts noch ein Blick in die Arbeit.

Im Frühjahr 2018

Prof. Dr. Heribert M. Anzinger

Zusammenfassung / Abstract

Die anhaltenden Kursanstiege bei Bitcoins und vermehrten Rufen nach staatlicher Regulierung der Kryptowährungen rücken wieder die Blockchain als zugrundeliegende Technologie und ihr Potenzial in den Fokus der Öffentlichkeit. Zu klären ist dabei jedoch, welche Anwendungsmöglichkeiten für Wirtschaft und Gesellschaft über die Nutzung für Kryptowährungen hinaus bestehen. Mögliche Anwendungsfelder wiederum sind an die spezifische Ausgestaltung der Blockchain geknüpft, sodass ein genaues Verständnis der technischen Varianten und ihrer Auswirkungen auf das jeweilige Geschäftsmodell erforderlich ist. Gleichsam unterliegt die neue Technologie der Einhaltung der bestehenden Gesetzgebung, während sie zugleich eine neuartige, an die Blockchain angepasste Regulierung erforderlich macht. Folglich ist die Analyse möglicher Use Cases sowohl auf die inhärenten technologischen Eigenschaften der Blockchain auszurichten, als auch auf die bestehenden rechtlichen Herausforderungen auf Seiten des Gesetzgebers und der Anwendung selbst.

Bei der Blockchain handelt es sich um ein Buchungsregister, das elektronische Transaktionen dezentral in einem Netzwerk aus Rechnern hinsichtlich ihres Zeitpunktes und ihres Transaktionsinhalts speichert. Dieser Funktionsweise liegt ein Prozess zugrunde, der Transaktionsblöcken einen sogenannten Hash zuordnet und die Erweiterung der Transaktionskette an den Proof-of-Work knüpft.

Die wesentlichen Eigenschaften der Blockchain umfassen dabei insbesondere die Fälschungssicherheit sowie die Substitution vertrauensschaffender Intermediäre durch die dezentrale Transaktionsdokumentation. Während die ursprüngliche Blockchain keinerlei Zugangsbeschränkung bezüglich der Teilnahme und den Transaktionsdaten kennt, erfolgen Entwicklungsansätze für die Mehrzahl potentieller Anwendungsmöglichkeiten aufgrund von Datenschutzerfordernungen, sensibler Informationen für den Wettbewerb und die zu bewältigenden Transaktionsmengen im Bereich der zugangsbeschränkten Blockchains.

Aufgrund ihrer Funktionsweise eignet sich die Technologie besonders für Prozesse, in denen die Verarbeitung von Daten

im Fokus steht. Dies ist unter anderem im Finanzsektor der Fall, sodass hier mitunter die größten Potentiale bei all jenen Finanztransaktionen vorliegen, deren Anbieter außer der Sicherstellung der korrekten Durchführung keinen weiteren Mehrwert schaffen. Darüberhinaus ermöglicht die Blockchain als Verwaltungs- und Ausführungsplattform entscheidende Entwicklungsmöglichkeiten im Bereich des Smart Property und der Smart Contracts. In der Umsetzung von vertraglichen und Rechten dient die Blockchain hierbei als automatisierte und manipulationssichere Anwendungsplattform. Als umfassendes Transaktionsregister bietet die Technologie sogar Anwendungsmöglichkeiten für das Tätigkeitsfeld des Wirtschaftsprüfers.

Die wesentlichen technischen Hürden für eine flächenweite Umsetzbarkeit der Blockchain liegen derzeit in der begrenzten Skalierbarkeit, der Kompatibilität mit anderen Systemen und Datentypen, der Sicherstellung des Datenschutzes sowie der Ermöglichung von Fehlerberichtigungen.

Während die Regulierung der neuen Technologie im Finanzsektor mit seiner traditionell umfangreichen und auf häufige technologische und produktbezogene Neuerungen reagierende Regulierung als eine erfüllbare Aufgabe darstellt, benötigen Smart Property und Smart Contracts eine weitreichendere Diskussion bezüglich der Vereinbarkeit mit geltenden Rechtsgrundsätzen. So stellt sie insbesondere das geltende Verständnis bezüglich des Zustandekommens von Verträgen, deren Ausführung und Interpretation in Frage. Ebenso auf dem Prüfstand steht somit die Gewährung von Besitz und Eigentum über die Blockchain.

Weiterhin ist trotz der geringen Bedeutung für den internationalen Zahlungsverkehr der Einsatz Kryptowährungen im Zusammenhang mit öffentlichen Blockchains als Zahlungsmittel und zur Gewährleistung der Funktionsweise hervorzuheben, sodass auch hier ein breiteres rechtliches Verständnis von Zahlungsmitteln erforderlich sein wird.

Inhaltsverzeichnis

ABBILDUNGSVERZEICHNIS	III
ABKÜRZUNGSVERZEICHNIS.....	IV
A. EINLEITUNG	1
B. GRUNDLAGEN DER BLOCKCHAIN-TECHNOLOGIE.....	4
I. FUNKTIONSWEISE DER BLOCKCHAIN-TECHNOLOGIE	4
II. SPEZIFIKATION UNTERSCHIEDLICHER BLOCKCHAIN-VARIANTEN	11
C. AKTUELLE ANWENDUNGSFELDER	15
I. DER MARKT FÜR BITCOINS UND WEITERE KRYPTOWÄHRUNGEN ...	15
1. <i>Entstehung und Marktkapitalisierung</i>	15
2. <i>Chancen und Risiken virtueller Währungen</i>	18
3. <i>Rechtliche Einordnung virtueller Währungen</i>	23
II. FRONTEND APPLIKATIONEN IN VERBINDUNG MIT KRYPTOWÄHRUNGEN	36
D. ZUKÜNFTIGE ANWENDUNGSFELDER IN DER DISKUSSION	41
I. SMART CONTRACTS	41
1. <i>Terminologie und Funktionsweise</i>	41
a) Smart Contract Codes	44
b) Smart Legal Contracts	46
2. <i>Eigenschaften von Smart Contracts</i>	49
3. <i>Ausgestaltung eines Smart Contracts:</i> <i>Datenorientierte Verträge</i>	55
4. <i>Use Cases für Smart Contracts</i>	60
a) Dezentrales Vergütungssystem für Musikkünstler.....	62
b) Verwaltung digitaler Identitäten.....	64
c) Dezentrale Plattform für Gesundheitsdaten.....	68
5. <i>Ausführung des Vertragsinhalts am Beispiel eines Kaufvertrags</i>	75
a) Ausführung unter Anwendung des Trennungs- und Abstraktionsprinzips	76
b) Ausführung unter Anwendung ausländischer Rechtsgrundsätze	80

c) Konsequenzen unterschiedlicher Rechtssysteme für Smart Contracts.....	83
6. Rechtliche Grenzen programmierbarer Verträge	85
II. SMART PROPERTY: FUNKTIONSWEISE DER KODIERUNG UND DER ÜBERTRAGUNG VON EIGENTUMSRECHTEN	90
III. TÄTIGKEITSFELDER VON FINANZINTERMEDIÄREN.....	98
1. <i>Funktion von Intermediären auf dem Finanzmarkt ..</i>	<i>98</i>
2. <i>Wertpapierhandel</i>	<i>103</i>
a) Das Clearing und Settlement System	103
b) Abwicklung: Mindestanforderungen an das Risikomanagement	109
c) Anmerkungen zur Umsetzbarkeit von IFRS 9.....	115
IV. ANWENDUNGEN IM RECHNUNGSWESEN UND IN DER WIRTSCHAFTSPRÜFUNG.....	120
1. <i>Vergleich der doppelten Buchführung mit Triple Entry Accounting.....</i>	<i>120</i>
2. <i>Prüfungshandlungen des Wirtschaftsprüfers.....</i>	<i>123</i>
E. TECHNISCHE VORAUSSETZUNGEN FÜR EINE ERFOLGREICHE UMSETZUNG	128
F. FAZIT UND AUSBLICK.....	133
LITERATURVERZEICHNIS	139

Abbildungsverzeichnis

Abb. 1: Transaktionsprozess auf der Blockchain	5
Abb. 2: Clearing und Settlement unter Nutzung einer Clearingstelle	60
Abb. 3: Clearing und Settlement unter Nutzung einer Blockchain.....	62

Abkürzungsverzeichnis

Abb.	Abbildung
Abl. EU Union	Amtsblatt der Europäischen Union
Abs.	Absatz
Art.	Artikel
BA	Bankenaufsicht
BaFin leistungsaufsicht	Bundesanstalt für Finanzdienst- leistungsaufsicht
BGB	Bürgerliches Gesetzbuch
Bspw.	Beispielsweise
ca.	circa
DLT	Distributed Ledger Technologie
ECU	European Currency Unit
EStG	Einkommenssteuergesetz
ESZB ralbanken	Europäisches System der Zent- ralbanken
et al.	et alia
EuGH	Europäischer Gerichtshof
EZB	Europäische Zentralbank
ff.	folgende
id.	idem
IKS	Internes Kontrollsystem
KWG	Kreditwesengesetz
Mio.	Million(en)
Mrd.	Milliarde(n)
n.F.	neue Fassung
Nr.	Nummer
Rn.	Randnummer
Rs.	Rechtssache
S.	Satz
SZR	Sonderziehungsrechte
Tz.	Teilziffer

u.	und
Ü.	Überschrift
U.a.	Unter anderem
Urt.	Urteil
v.	vom
Vgl.	Vergleiche
Vol.	Volumen

A. Einleitung

Mit der umfassenden Digitalisierung durch Technologien wie das Internet steht die Wirtschaft vor einem tiefgreifenden Strukturwandel. Neuartige Geschäftsmodelle und Optimierungspotenziale werden die Wirtschaft grundlegend verändern und zu einer intelligenten und automatisierten Verschmelzung der realen und virtuellen Welt führen.¹ Ganze Wertschöpfungsketten, aber auch die Nutzung von Konsumgütern, werden im Zuge dieser Entwicklung in digitalisierter Form und in Echtzeit erfasst werden. Dementsprechend haben Politik und Wirtschaft ein Interesse an der Erforschung möglicher Einsatzgebiete und innovationsfreundlichen Gesetzgebung, um dem globalen Strukturwandel in Deutschland frühzeitig zu begegnen. Die Digitalisierung der Wirtschaft kann dabei durch dezentral und automatisiert agierende Netzwerke unterstützt werden – die Blockchain-Technologie soll dies ermöglichen. Das bisher für Transaktionen mit Kryptowährungen bekannte Transaktionsregister wird seit einigen Jahren für eine Vielzahl von Anwendungen erprobt. Banken, Versicherungen, Telekommunikationsdienstleister, Automobiliensteleister und weitere Unternehmen testen bereits, wie sie von dem dezentralen Register für ihre Produkte und Prozesse profitieren können. Doch auch das Recht ist von der Blockchain-Technologie betroffen. So muss die Technologie auf die Einhaltung geltenden Rechts und von Regulierungen überprüft werden. Gleichzeitig ermöglicht die Blockchain jedoch eine automatisierte Ausübung von Recht und greift somit direkt in unser Rechtsverständnis ein, sodass nicht nur untersucht werden muss, wie sich Geschäftsprozesse durch die Blockchain verändern. Auch die Wechselwirkungen zwi-

¹ Ähnlich *Menn*, Wie Industrie 4.0 die Welt verändert, wiwo.de, Artikel v. 07.09.2016.

schen Recht und Technologie erfordern angesichts neuer technologischer Methoden im Bereich der Rechtsanwendung eine umfassende Erforschung.

Die Analyse ausgewählter Anwendungsfälle soll als erster Schwerpunkt dieser Ausarbeitung einen Überblick über die Vielzahl an Entwicklungen verschaffen, welche mit der Blockchain neue und optimierte Geschäftsprozesse verfolgen. Es soll untersucht werden, inwiefern die Anwendungsbeispiele, die sich zumeist in der Testphase befinden, bestehende Prozesse verändern oder verbessern. Darüber hinaus werden zu erwartende Problematiken technischer und prozessbezogener Natur, sowie mögliche Lösungsansätze aufgezeigt. Da die ursprüngliche Anwendung der Kryptowährungen sowohl als Zahlungsmittel an Bedeutung gewinnt, als auch in aktuelle Anwendungen integriert wird, bedarf es hier trotz der bereits mehrjährigen Anwendungsphase ebenfalls einer Analyse. Näher betrachtet werden neben der zugrundeliegenden Blockchain und der Kryptowährungen, die Implementierung von Smart Contracts und Smart Property. Sie bilden dabei die Grundlage für die ausgewählten Use Cases. Aufgrund der besonderen Eignung des Finanzsektors zur Prozessdigitalisierung und der vielversprechenden Konzepte für die Blockchain soll die Finanzbranche näher analysiert werden. Der zweite Schwerpunkt befasst sich mit den rechtlichen Implikationen der Blockchain. Zu diesem Zweck werden die Anwendungen auf eine Vereinbarkeit mit geltendem Recht und Regulierungen überprüft, sowie kritische Sachverhalte aufgezeigt. Ziel dieses Schwerpunkts ist es, rechtliche Grenzen der Blockchain-Technologie zu identifizieren und hieraus Empfehlungen für eine mögliche Regulierung abzuleiten. Die Vorschläge sollen hierbei sowohl die regulatorischen Bedürfnisse des Staates und der Verbraucher, als auch das Potenzial der Blockchain im Kontext der Digitalisierung der Wirtschaft berücksichtigen.

Im folgenden werden zunächst grundlegende Begriffe der Blockchain-Technologie, sowie deren Funktionsweise dargestellt. Hiernach erfolgt eine Einordnung der bereits etablierten Anwendung der Kryptowährungen. Die aktuell diskutierten Anwendungen umfassen Smart Contracts und Smart Property. Neben der Erläuterung der Funktionsweise und Vorstellung industrieübergreifender Use Cases werden rechtliche Grenzen bei der Durchführung und die Klassifizierung als Vertrag im Rechtssinne diskutiert. Als weitere Anwendungsmöglichkeit wird der Clearing und Settlement Prozess näher beleuchtet. Aufgrund des hohen Regulierungsgrads der Finanzbranche werden zudem die Auswirkungen der Blockchain auf einschlägige Vorschriften und Rechnungslegungsstandards untersucht. Als weitere Fallbeispiele werden mögliche Umsetzung im Rechnungswesen und Tätigkeitsfeld der Wirtschaftsprüfung diskutiert. Nach Einschätzung der zu nehmenden technischen Hürden werden abschließend die Entwicklungschancen der Blockchain-Technologie bewertet und wesentliche rechtliche Problemfelder identifiziert.

B. Grundlagen der Blockchain-Technologie

I. Funktionsweise der Blockchain-Technologie

Als Blockchain wird die ursprünglich der Kryptowährung Bitcoin zugrunde liegende Technologie bezeichnet, deren technische Konzeption im November 2008 unter dem Pseudonym Satoshi Sakamoto veröffentlicht wurde.² Bei der Blockchain handelt es sich um ein Distributed Ledger – ein dezentrales Buchungsregister. Informationen über elektronische Transaktionen werden im Gegensatz zu herkömmlichen Protokollen oder Büchern nicht zentral speichert, sondern dezentral in einem Netzwerk aus Teilnehmern archiviert.³ Der Transaktionsverlauf wird dabei unwiderruflich und damit revisions sicher abgebildet.⁴ Der Begriff der Blockchain bezeichnet somit ein Distributed Ledger, der speziell für das Bitcoinsystem kon-

² Vgl. *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

³ Vgl. *European Securities and Markets Authority*, The Distributed Ledger Technology, 2016, 8.

⁴ Hierzu *Finextra Research*, Banking on Blockchain, Whitepaper, 2016, 6.

zipiert wurde.⁵ Die grundlegende Funktion der Blockchain besteht in der dezentralen Protokollierung von getätigten Transaktionen zwischen den Netzwerkteilnehmern hinsichtlich ihres Zeitpunktes und deren korrekten Ausführung.⁶ Diese Funktion ermöglicht wiederum das primäre Ziel der Blockchain, Transaktionen zwischen zwei Vertragspartnern ohne die Existenz eines unabhängigen Dritten, der die Transaktion bestätigt.⁷

Zu diesem Zweck soll zunächst der Ablauf einer Transaktion unter Verwendung der Blockchain als elektronisches Zahlungssystem erläutert werden. Beginnend mit dem Handel einer elektronischen Münze, die eine Kette digitaler Signaturen der jeweiligen Besitzer zu bestimmten Zeitpunkten darstellt, soll diese von dem Verkäufer auf einen Käufer übertragen werden.⁸ Um die Transaktion zu tätigen, benötigen die Beteiligten sowohl einen privaten Schlüssel, als auch einen

⁵ Das Originalkonzept nach *Satoshi Nakamoto*, 2008, verwendet lediglich den Begriff der „Data blocks“ die miteinander verknüpft werden („chained“). Aufgrund der weit verbreiteten synonymen Verwendung von DLT und Blockchain, bspw. in Ausdrücken wie „Blockchain Economy“ und „Blockchain Revolution“, wird in dieser Arbeit in Anlehnung an *Matilla*, *The Blockchain Phenomenon*, ETLA Working Papers No. 38, 2016, 6, der Begriff der Blockchain gleichbedeutend zum Begriff des DLT verwendet. Gegensätzlich hierzu mit Beibehaltung der Bezeichnung des DLT: *European Securities and Markets Authority*, *The Distributed Ledger Technology*, 2016, 8.

⁶ Hierzu *Crosby, et al.*, *Blockchain technology: Beyond bitcoin*, *Applied Innovation Review* 2016, 6, 8.

⁷ Vgl. *Nakamoto*, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, 1.

⁸ Dazu *Nakamoto*, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, 2.

öffentlichen Schlüssel: Der private Schlüssel ist ein Datenstrang, der zur Verwendung von elektronischen Münzen von einem bestimmten Konto berechtigt.⁹ Folglich bedarf dieser Schlüssel der Geheimhaltung, da er den Zugang zu den erworbenen Münzen und deren Nutzung gewährleistet. Der öffentliche Schlüssel dagegen entsteht durch Verschlüsselung des privaten Schlüssels und ist für die Netzwerkteilnehmer der Blockchain sichtbar.¹⁰ Bei dem Verkauf ergeben sich Problemstellungen, die das Zustandekommen der Transaktion erschweren könnten. Da es sich bei der Münze um eine digitale Währung handelt, besteht beim Kauf das Risiko, dass die Einheit bereits für andere Transaktionen verwendet wurde und der Verkäufer keine Rechte mehr an ihr besitzt.¹¹ Dementsprechend wäre eine unabhängige dritte Instanz notwendig, die jegliche Transaktionen chronologisch protokolliert und somit nur diejenigen Transaktionen zur Ausführung verifiziert, die keine bereits ausgegebenen Münzen enthalten.¹² Eine zentrale, unabhängige Instanz existiert in der Blockchain jedoch nicht.

Um das fehlende Vertrauen zwischen den Teilnehmern zu kompensieren, werden daher alternative Verfahren eingesetzt. Wie in Abbildung 1 zu sehen, überträgt der Besitzer zunächst die Bitcoins an den Empfänger, indem er die vorherige Transaktion und den öffentlichen Schlüssel des Empfän-

⁹ Vgl. *Lee*, *New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market*, 12 *Hastings Bus. L.J.* 81 (2016) at 131.

¹⁰ *Id.*

¹¹ Vgl. *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 2.

¹² Hierzu *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 2.

gers digital signiert.¹³ Die Signatur entsteht, indem der private und öffentliche Schlüssel zusammen gehasht werden, sodass bewiesen ist, dass die Transaktion von dem Besitzer des privaten Schlüssels ausgeht.¹⁴ Zudem wird ein sogenannter Timestamp Server eingesetzt, der jeden hinzugefügten Datenblock mit einem Zeitstempel versieht und somit dessen Hinzufügung zur Blockchain zu einem spezifischen Zeitpunkt bestätigt.¹⁵ Für diesen Prozess spielen sogenannte Hashes und Hash-Funktionen unter Nutzung von Proof-of-Work eine entscheidende Rolle. Bei einem Hash handelt es sich um einen Output, der aus der Umwandlung eines Informationsinputs mithilfe eines mathematischen Algorithmus – der Hash-Funktion – entsteht.¹⁶ Da der Output einer Zufallsausgabe entspricht, ist es nahezu unmöglich, aus dem Hash den Input zu generieren oder die ursprüngliche Transaktionsinformation zu ändern, ohne den zugehörigen Hash zu zerstören.¹⁷ Der Hash stellt somit einen digitalen Fingerabdruck dar, der den vorherigen Block abbildet.

¹³ Vgl. *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 2.

¹⁴ Dazu *Lee*, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, 12 Hastings Bus. L.J. 81 (2016) at 131.

¹⁵ Vgl. *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 2.

¹⁶ Dazu *Pilkington*, Blockchain Technology: Principles and Applications, 2015, 7.

¹⁷ In Anlehnung an *Lee*, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, 12 Hastings Bus. L.J. 81 (2016) at 130.

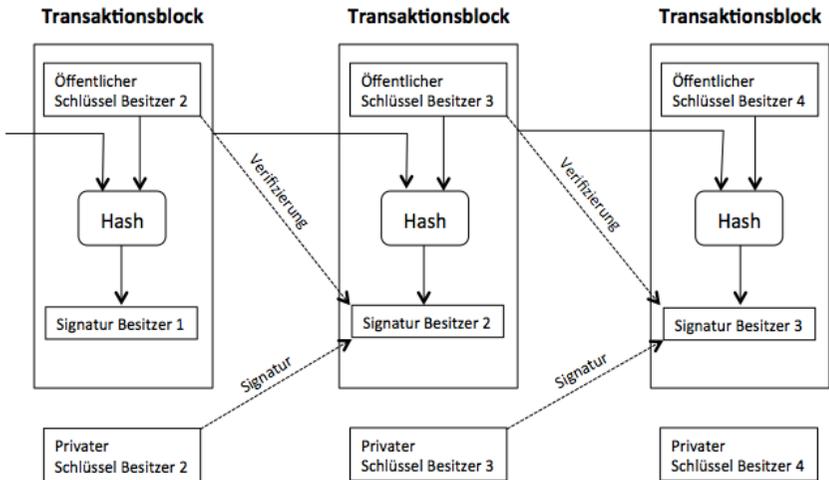


Abb. 1: Transaktionsprozess auf der Blockchain (Vgl. *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 2)

Damit jedoch ein Datenblock mit einem Hash versehen werden kann, der an die Blockchain angefügt wird, muss ein Proof-of-Work durch die Netzwerkteilnehmer geleistet werden.¹⁸ Dieser Prozess erfolgt durch dem Netzwerk angeschlossene Prozessoren, die neue Transaktionen in einem Block sammeln und nun komplexe Aufgaben lösen müssen.¹⁹ Der Prozessor, der den Proof-of-Work am schnellsten erbringt, sendet den Block an die übrigen Prozessoren, die wiederum ihre Bestätigung durch das Arbeiten an neuen Blocks unter Verwendung des Hashs des akzeptierten Blocks als Vor-

¹⁸ Vgl. *Pilkington*, Blockchain Technology: Principles and Applications, 2015, 7.

¹⁹ Hierzu *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 3.

gängerhash ausdrücken.²⁰ Der Prozess des Proof-of-Work wird als Mining bezeichnet, da durch die Lösung der kryptografischen Probleme neue Bitcoins als Belohnung für die Miner generiert werden.²¹ Sie sind somit ein Anreiz für die notwendige Verifizierung von Transaktionen, die Kosten in Form von Prozesszeit und Stromverbrauch verursacht.²² Der Schutz vor Manipulation der Datenblöcke wird durch den hohen Arbeitsaufwand zur Änderung einer bestätigten Transaktion sichergestellt, bei der ein Angreifer den Proof-of-Work für alle bereits nachfolgenden Blöcke wiederholen müsste und dessen Erfolgswahrscheinlichkeit mit steigender Blockanzahl in der Kette exponentiell sinkt.²³ Die Datenblöcke sind anders ausgedrückt miteinander verwoben und können daher nicht einzeln abgeändert werden, ohne folgende Blöcke zu ändern und somit eine Verifizierung durch die Mehrheit der Netzwerkteilnehmer zu erfordern.

Die Distributed Ledger Technologie der Blockchain weist eine Reihe von Eigenschaften auf, die sie insbesondere von anderen Technologien zur Transaktionspeicherung wie Datenbanken unterscheiden. Im Gegensatz zu einer dezentralen Datenbank ermöglicht eine Distributed Ledger eine simultane

²⁰ Vgl. *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 3.

²¹ Vgl. *Kaplanov*, Nerdy Money: The Private Digital Currency, and the Case Against its Regulation, 5 Loy. L. Consumer Rev. 111 (2012) at 119.

²² In Anlehnung an *Lee*, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, 12 Hastings Bus. L.J. 81 (2016) at 132.

²³ Hierzu *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 3.

Transaktionsausübung, die gleichzeitig eine mehrfache Ausgabe eines Betrags verhindert.²⁴ Eine doppelte Ausgabe eines Betrags würde durch die Blockchain nicht bestätigt und demnach auch nicht ausgeführt werden. Aus dem beschriebenen Transaktionsvorgang in der Blockchain sind die Charakteristika der Dezentralität des Netzwerks und des Ersatzes eines unabhängigen Dritten durch das Netzwerk als solches hervorzuheben. Die Blockchain sei daher nicht als Technologie ohne notwendiges Vertrauen zwischen den Transaktionspartnern anzusehen, da die unabhängige Instanz lediglich durch dezentrale und zusammenarbeitende Organisationen ersetzt werde.²⁵ Zudem ist der Einsatz von kryptografischen Methoden von entscheidender Bedeutung. Sie garantieren die Sicherheit der Transaktionsdaten, da hierdurch sowohl der Besitz des privaten Schlüssels, als auch die Existenz der Transaktion zu einem bestimmten Zeitpunkt bewiesen wird.²⁶ Diese Eigenschaften bieten die Grundlage für eine Vielzahl neuer Anwendungsgebiete, die über die ursprüngliche Verwendung für virtuelle Währungen hinausgehen.

²⁴ In Anlehnung an *Peters, et al.*, Understanding Modern Banking Ledgers through Blockchain Technologies, 2015, 9.

²⁵ Vgl. *Scott*, How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?, Working Paper 2016-1, 2016, 1.

²⁶ Hierzu *Lee*, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, 12 *Hastings Bus. L.J.* 81 (2016) at 97.

II. Spezifikation unterschiedlicher Blockchain-Varianten

Weitere Eigenschaften von Distributed Ledgers resultieren aus der Spezifikation unterschiedlicher Blockchain-Typen, die primär unterschiedliche Zugangsmöglichkeiten zur Blockchain oder zu den enthaltenen Daten anbieten. Hierfür wird zunächst zwischen „Permissionless“ und „Permissioned“ bezüglich des Zugangs zur Blockchain unterschieden.²⁷ „Permissionless“ bedeutet, dass ein unbeschränkter Zugang zur Blockchain existiert und die Teilnahme an den Validierungsprozessen gestattet wird.²⁸ Charakteristisch ist dabei die Notwendigkeit eines Anreizsystems, das die Entlohnung der zur Verfügung gestellten Rechenleistung für die Validierung der Blöcke sicherstellt.²⁹ Die bekannteste Distributed Ledger dieser Form ist die Bitcoin Blockchain, in der alle Transaktionen der hinzugefügten Blöcke öffentlich zugänglich sind.³⁰ Ein weiteres Beispiel ist das Ethereum Projekt, das eine Plattform für Smart Contract Applikationen bietet und unter anderem mit dem Schutz vor Betrug, Zensur und Einflussnahme Dritter wirbt.³¹ Permissionless Blockchains zeichnen sich insbesondere

²⁷ Da diese Unterteilung in den meisten Fällen dem Zugang zu den enthaltenen Daten entspreche, könne auf eine Kategorisierung der Datenfreigabe verzichtet werden. Vgl. *Peters, et al.*, *Understanding Modern Banking Ledgers through Blockchain Technologies*, 2015, 5.

²⁸ So auch *Biella, et al.*, *Blockchain Technology and Applications from a Financial Perspective*, Technical Report Version 1.0, Unicredit, 2016, 7.

²⁹ *Id.*

³⁰ Einsehbar unter: <https://blockchain.info>, Stand:15.08.2016.

³¹ Einsehbar unter: <https://www.ethereum.org>, Stand: 15.08.2016.

re durch ihre Fälschungssicherheit und den Schutz vor Zensur aus.³² Hierfür ist der Validierungsprozess verantwortlich, der mithilfe des dezentralen Netzwerks aus Teilnehmern Manipulationsversuche Einzelner nicht validiert, sofern die aggregierte Prozessorleistung der Mehrheit diejenige des Angreifers übersteigt.³³ Permissionless Blockchains sind jedoch aufgrund ihrer Arbeitsweise mit Nachteilen verbunden. Im Vergleich zu Permissioned Blockchains zeigen sich Defizite bei der Schnelligkeit der Transaktionen, der Energieeffizienz, sowie einer hohen Skalierbarkeit.³⁴

Die Permissioned Blockchain wird bezüglich der Einsehbarkeit des Codes und der Nutzungsmöglichkeit nur für ausgewählte Teilnehmer freigegeben und büßt somit an Transparenz und Dezentralität ein.³⁵ Diese Zugangsbeschränkung sei jedoch für Geschäftsmodelle, die eine Authentifizierung der Beteiligten und deren Rechner voraussetzen, zu bevorzugen.³⁶ Insbesondere spiele dabei für beteiligte Unternehmen der Schutz der eigenen Wertschöpfungskette vor neuen Wettbewerbern

³² Hierzu *Matilla*, The Blockchain Phenomenon, ETLA Working Papers No. 38, 2016, 8.

³³ Ähnlich *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 5.

³⁴ Hierzu *Matilla*, The Blockchain Phenomenon, ETLA Working Papers No. 38, 2016, 8. Näheres zu technischen Herausforderungen unter Gliederungspunkt E.

³⁵ Vgl. *Kaye Scholer*, An Introduction to Bitcoin and Blockchain Technology, 2016, 9.

³⁶ Dazu *Biella, et al.*, Blockchain Technology and Applications from a Financial Perspective, Technical Report Version 1.0, Unicredit, 2016, 7.

eine Rolle.³⁷ Ein Unterschied zur Permissionless Blockchain besteht darin, dass kein Anreizsystem für die Teilnehmer notwendig ist. Stattdessen stellen die autorisierten Teilnehmer oder eine privilegierte Teilmenge die korrekte Ausführung und die Aufstellung von Regeln sicher.³⁸ Dies führt einerseits dazu, dass der Schutz vor Zensur und die Unabhängigkeit von einer leitenden Instanz eingeschränkt wird. Andererseits erleichtert die begrenzte Anzahl an identifizierbaren Mitgliedern die Verhandlung von Regeln und weiteren Entscheidungen, wodurch der Prozess einer Vertragsverhandlung ähnelt.³⁹ Unerwünschte oder gar gesetzeswidrige Transaktionen können von der Durchführung ausgeschlossen werden, was bei einer öffentlichen und global vernetzten Blockchain mangels übergeordneter Instanz und Kontrollmöglichkeiten problematisch ist.

Als Kombination der Permissionless und Permissioned Blockchain wurde darüber hinaus das Konzept der Hybrid oder auch Consortium Blockchain entwickelt. Der Validierungsprozess wird durch eine vordefinierte Auswahl an Teilnehmern ausgeführt, wobei die Einsehbarkeit der Blockchain öffentlich oder auf die Beteiligten beschränkt sein kann.⁴⁰ Sie ist somit

³⁷ Hierzu *Morgan Stanley*, Global Insight: Blockchain in Banking: Disruptive Threat or Tool?, 2016, 6.

³⁸ Vgl. *Mainelli, et al.*, The Impact and Potential of Blockchain on The Securities Transaction Lifecycle, Swift Institute Working Paper No. 2015-007, 2016, 47.

³⁹ Ähnlich *Yermack*, Corporate Governance and Blockchains, National Bureau of Economic Research, Working Paper 21802, 2015, 47.

⁴⁰ Hierzu *Buterin*, On Public and Private Blockchains, Ethereum Blog, Blogeintrag v. 07.08.2015.

der Permissioned Blockchain im Hinblick auf die kryptografische Authentifizierung überlegen, ohne auf die Vorteile bezüglich der effizienten und schnellen Prozessausführung verzichten zu müssen.⁴¹ Abhängig von den Anforderungen an das Geschäftsmodell und die technischen Bedingungen kann folglich zwischen einer öffentlichen, privaten und hybriden Blockchain gewählt werden.

⁴¹ Id.

C. Aktuelle Anwendungsfelder

I. Der Markt für Bitcoins und weitere Kryptowährungen

1. Entstehung und Marktkapitalisierung

Bei der Bitcoin handelt es sich um eine virtuelle Währung, die auf dem kryptografischen Zahlungssystem der Blockchain basiert.⁴² Obwohl die Währung lediglich in digitaler Form vorliegt, stellt eine mehrfache Verwendung für Transaktionen – sogenanntes Double Spending – kein Risiko dar.⁴³ Die mit einem Zeitstempel, Signatur und öffentlichem Schlüssel versehenen Transaktionen ermöglichen die Nachverfolgung, ob die beteiligten Bitcoins im Besitz der Partei sind oder bereits ausgegeben wurden. Bitcoins werden durch das Netzwerk an Teilnehmern generiert, die für die Bereitstellung von Rechenleistung und der damit verbundenen Kosten Bitcoins auf ihr Konto gutgeschrieben bekommen.⁴⁴ Die Generierung der Währung untersteht damit keiner politisch legitimierten Institution, wie dies bei der Europäischen Zentralbank der Fall ist. Durch die Satzung des Systems der Europäischen Zentralbanken und der Europäischen Zentralbank steht es lediglich dem ESZB zu, die Geldpolitik der Mitgliedsländer zu bestimmen

⁴² Hierzu *Guadamuz/Marsden*, „Blockchains and Bitcoin: Regulatory responses to cryptocurrencies, First Monday 2015, Tz. 2.2.

⁴³ In Anlehnung an *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 2.

⁴⁴ Vgl. *Nakamoto*, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, 4.

und auszuführen.⁴⁵ Ihm obliegt somit die Kontrolle über die Erhöhung oder Reduzierung der Zentralbankgeldmenge.⁴⁶ Die Bitcoinausgabe wiederum folgt einem vorgegebenen Plan nach mathematischen Regeln, wonach die Erstellung neuer Münzen im Zeitverlauf exponentiell sinkt.⁴⁷ Die festgelegte Wachstumsrate bietet somit im Vergleich zu Zentralbankgeld Schutz vor politisch motivierter Geldmengenausweitung und damit einhergehender Geldentwertung. Mit der sinkenden Wachstumsrate sinkt jedoch auch die Rentabilität des Miningprozesses, sodass die Bereitstellung von Rechenleistung zunehmend von Mining Pools mit leistungsstarker Hardware betrieben wird.⁴⁸ Damit gehe allerdings das Risiko einher, dass ein Pool die Mehrheit der Berechnungen kontrolliere und folglich auch die Blockchain manipuliert werden könne.⁴⁹ Seit Einführung der virtuellen Währung im Jahr 2009 wurden circa 16 Mio. Bitcoins hergestellt.⁵⁰ Das programmierte Ge-

⁴⁵ Gemäß Art. 3.1 der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank, vgl. *Europäische Zentralbank*, Über die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank, Amtsblatt der Europäischen Union, C 326/230, 26.10.2012.

⁴⁶ Das vom ESZB geschaffene Zentralbankgeld, die sogenannte Geldbasis, umfasst Bargeld und Einlagen bei der Zentralbank. Hierzu *Deutsche Bundesbank*, Glossar: Zentralbankgeld, bundesbank.de. Stand: 30.12.2016.

⁴⁷ Hierzu *bitcoin.org*, FAQ Bitcoin, bitcoin.org, Stand: 22.08.2016.

⁴⁸ Dazu *Thoma*, Die Macht der Mining Pools, golem.de, Beitrag v. 25.03.2014.

⁴⁹ In Anlehnung an *Thoma, Jörg*, Die Macht der Mining Pools, golem.de, Beitrag vom 25.03.2014.

⁵⁰ Vgl. *Blockchain Info*, Gesamtzahl der Bitcoins im Umlauf, blockchain.info, Stand: 23.01.2017.

samtkontingent von knapp unter 21 Millionen werde voraussichtlich um das Jahr 2140 erreicht.⁵¹ Die derzeitige Marktkapitalisierung beträgt rund 14,9 Mrd. US-Dollar.⁵² Allerdings unterliegt der Marktwert massiven Schwankungen, was beispielsweise Ende 2013 zu einem Bewertungshoch von zeitweise über 1000 US-Dollar je Bitcoin und einem darauffolgenden Wertabfall führte.⁵³ Die starken Preisschwankungen als Folge des Mangels an währungspolitischen Maßnahmen zur Steuerung der Geldmenge seien Ursache dafür, dass sich die Währung nur eingeschränkt als Bezahlungsmittel für Waren und Dienstleistungen etablierte.⁵⁴ Sie dient somit eher Spekulationszwecken. Darüber hinaus existiert eine Reihe weiterer virtueller Währungen, die jedoch eine weitaus geringere Marktkapitalisierung aufweisen.⁵⁵ In diese Kategorie wird die Litecoin Währung eingeordnet, die auf einer modifizierten Blockchain nach Vorbild der Bitcoin basiert und über ihr Softwareprogramm, das Litecoin Protokoll, gesteuert wird.⁵⁶ Die Marktkapitalisierung beträgt ca. 181 Mio. US-Dollar.⁵⁷ Eine geringere Kapitalisierung in Höhe von ca. 7 Mio. US-Dollar

⁵¹ Hierzu *bitcoinwiki*, FAQ, bitcoin.it, Stand: 23.08.2016.

⁵² Dazu *Blockchain Info*, Marktkapitalisierung, blockchain.info, Stand: 23.01.2017.

⁵³ Vgl. *Finanzen.net*, Bitcoin – US-Dollar – Historische Kurse, finanzen.net, Stand: 23.08.2016

⁵⁴ In Anlehnung an *Guadamuz/Marsden*, Blockchains and Bitcoin: Regulatory responses to cryptocurrencies, *First Monday* 2015, Tz. 3.3.

⁵⁵ Eine Übersicht zu Kryptowährungen unter coinmarketcap.com, Stand: 29.03.2017.

⁵⁶ Hierzu *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 2.

⁵⁷ Vgl. *CoinGecko.com*, Litecoin/US-Dollar Marktkapitalisierung, coingecko.com, Stand: 23.08.2016.

besitzt XCP.⁵⁸ Sie besitzt zwar ein eigenes Protokoll zur Transaktionsabwicklung, wird jedoch über die Bitcoin Blockchain geführt.⁵⁹ Einen vergleichsweise hohen Gesamtwert in Höhe von über 900 Mio. US-Dollar weist die Kryptowährung Ether auf.⁶⁰ Sie wird für die Entwicklung von Applikationen und die Nutzung von Smart Contracts auf der Ethereum Plattform benötigt.⁶¹

2. Chancen und Risiken virtueller Währungen

Neben den aus der Blockchain resultierenden Vor- und Nachteilen, existieren spezifische Vorzüge und Problematiken virtueller Währungen, die im Folgenden genannt werden sollen.⁶² Einer der wesentlichen Gründe für die Nutzung der Bitcoin und vergleichbarer Coins sind die geringen Transaktions-

⁵⁸ Vgl. *CoinGecko.com*, Counterparty/US-Dollar

Marktkapitalisierung, *coingecko.com*, Stand: 23.08.2016.

⁵⁹ Hierzu *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 2.

⁶⁰ Vgl. *CoinGecko.com*, Ethereum/US-Dollar Marktkapitalisierung, *coingecko.com*, Stand: 25.01.2017.

⁶¹ Hierzu *Ethereum.org*, *FAQ: Who needs Ether?*, Stand: 24.08.2016.

⁶² Der Begriff der virtuellen Währungen und Kryptowährungen wird im Folgenden aufgrund der dominierenden Stellung letzterer unter den virtuellen Währungen synonym verwendet. Es kann jedoch zwischen zentralen virtuellen Währungen mit einem zentralen Aufbewahrungsort und Administrator als Intermediär, sowie dezentralen virtuellen Währungen ohne diese Komponenten unterschieden werden. In die zweite Kategorie fallen Kryptowährungen wie Bitcoin. Hierzu *Financial Crimes Enforcement Network*, Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury, 19.11.2013, 3.

aktionskosten. Sie fallen mit durchschnittlich 1% niedriger aus als bei Clearinghäusern.⁶³ Allerdings müsse mit einem Anstieg der Kosten in Form von Gebühren aufgrund des steigenden Miningaufwands gerechnet werden.⁶⁴ Andernfalls genügten die Anreize für Netzwerkteilnehmer nicht, um die Fälschungssicherheit des Systems zu garantieren.⁶⁵ Ebenfalls strittig sind der Grad der Anonymität und Transparenz. Einerseits können durch den Verzicht auf die Preisgabe der Identität zunächst die privaten Daten des Nutzers geschützt werden. Andererseits wird angemerkt, dass anhand von Netzwerkanalysen Aktivitäten öffentlicher Schlüssel geortet und insbesondere über Wallets und Tauschbörsen Nutzerdaten erlangt werden könnten.⁶⁶ Es kann daher eher von Pseudonymität statt Anonymität ausgegangen werden.⁶⁷ Zudem erstreckte sich die Transparenz nicht auf die Identitäten des oder der Gründer, die frühzeitig große Bitcoinmengen erlangten und im Verdacht stehen, den Marktpreis zu beeinflussen.⁶⁸ Dass das Bitcoinsystem lediglich Pseudonymität gewährleistet, sollte jedoch besonders im Hinblick auf die Bekämpfung illegaler Transaktionen wie beispielsweise Waffenhandel als positiv

⁶³ Dazu *Wu*, *Why We Accept Bitcoin*, forbes.com, Artikel vom 13.02.2014.

⁶⁴ Hierzu *Kaskaloglu*, *Near Zero Bitcoin Transaction Fees Cannot Last Forever*, *DigitalSec* 2014, 91, 96.

⁶⁵ Id.

⁶⁶ Hierzu *Reid/Ferrigan*, *An Analysis of Anonymity in the Bitcoin System*, in *Security and Privacy in Social Networks*, 2012, 197, 221.

⁶⁷ Dazu *Wright, et al.*, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015, 56.

⁶⁸ Dazu *Guadamuz/Marsden, Chris*, *Blockchains and Bitcoin: Regulatory responses to cryptocurrencies*, *First Monday* 2015, Tz. 3.1.

bewertet werden. Es gebe zwar illegale Aktivitäten, die über Bitcoins getätigt werden.⁶⁹ Dennoch ist es nicht weniger wahrscheinlich, dass diese unter der Nutzung von Bargeld erfolgen, bei welchem eine Verfolgung des Mittelflusses deutlich schwerer zu kontrollieren sein sollte. Die gewonnenen Daten seien letztendlich vorteilhaft für Behörden, um illegale Aktivitäten aufzudecken.⁷⁰ Grundsätzlich kann daher nicht davon ausgegangen werden, dass Bitcoins und andere Kryptowährungen in dieser Hinsicht schädlicher sein könnten als reguläre Banknoten. Schon der Vergleich zum Bargeldumlauf im Euro-Währungsgebiet in Höhe von über einer Billion Euro⁷¹ verdeutlicht dabei die relativ geringe Bedeutung von Kryptowährungen. Darüber hinaus gibt es Zweifel, ob beispielsweise die befürchtete Geldwäsche im großen Stil über virtuelle Währungen praktiziert wird. Schwierigkeiten wie die aufwendige anonyme Einspeisung des Bargelds in das Bitcoinsystem bei Meidung der Handelsbörsen oder Nutzung von risikoreichen Verschleierungssystemen sprechen dagegen.⁷² Somit ist Geldwäsche bei Kryptowährungen zwar ebenfalls eine ernstzunehmende Problematik, sollte jedoch angesichts der untergeordneten Bedeutung nicht als Rechtfertigung für ein Verbot der alternativen Zahlungsform missbraucht werden.

⁶⁹ Hierzu *Europol*, The Relentless Growth of Cybercrime, Pressemitteilung v. 27.09.2016.

⁷⁰ Hierzu *Schulz*, Die Spuren des Geldes, DIE ZEIT Nr. 3/2016, 14.01.2016.

⁷¹ Vgl. *Statista*, Bargeldumlauf im Euro-Währungsgebiet von 1999 bis zum 1. Halbjahr 2016 (in Milliarden Euro), Statista.com, Stand: 24.01.2017.

⁷² Hierzu *Bergmann*, Bitcoin und Geldwäsche – keine gute Idee, BitcoinBlog.de, Artikel v. 11.06.2014.

Ein nicht zu unterschätzendes Problem stellt dagegen die vorgegebene sinkende Wachstumsrate der Bitcoinmenge dar. Anders als bei Zentralbankgeld könne das Angebot nicht an eine steigende Nachfrage der Wirtschaft angepasst werden, wodurch die Kaufkraft automatisch steige und Bitcoins aufbewahrt statt ausgegeben würden.⁷³ Eine derartige deflationäre Entwicklung würde nicht nur die Nutzung als Transaktionsmittel, sondern auch die Glaubwürdigkeit der Blockchain gefährden, da weniger Teilnehmer am Verifizierungsprozess teilnehmen würden.⁷⁴ Eine deflationäre Währung birgt zudem die Gefahr einer Spirale aus geringerer Konsumnachfrage und sinkenden Preisen aufgrund der Aufbewahrung der wertgewinnenden Währung, was ohne die Möglichkeit einer expansiven Geldpolitik zu einer rezessiven Wirtschaftsentwicklung beitragen könnte.⁷⁵ Eine Verwendung an Stelle von zentralbankgesteuertem Geld ist daher nicht wünschenswert und wäre zudem beispielsweise im ESZB ebenso wenig vereinbar mit deren Ziel zur Preisstabilität im Euro-Währungsraum⁷⁶

⁷³ In Anlehnung an *Barber, et al.*, Bitter to Better – How to Make Bitcoin a Better Currency, in *Financial Cryptography and Data Security*, 2012, 399, 404.

⁷⁴ Id.

⁷⁵ In Anlehnung an *Burdekin/Siklos*, *Deflation – Current and Historical Perspectives*, Cambridge University Press, 2004, 6. Teilweise zustimmend *Boianovsky*, *Wicksell on Deflation in the Early 1920s*, *History of Political Economy* 30(2), 1998, 219, 267.

⁷⁶ Der EZB-Rat strebt eine Preissteigerungsrate von 2 % an und berücksichtigt dabei die Korrelation zwischen der Geldmenge und den Preisen. Hierzu *Europäische Zentralbank*, *Die geldpolitische Strategie der EZB*, 3. Auflage, 2011, 9.

und den statuierten Aufgaben des ESZB.⁷⁷ Angesichts des geringen Zahlungsvolumens, das mit Bitcoins und anderen virtuellen Währungen abgewickelt wird, stellt ein Szenario, in welchem diese lediglich ergänzend zu den gesetzlichen Zahlungsmitteln genutzt werden, keine Gefährdung der Preisstabilität dar. Nichtsdestotrotz habe die Bitcoin durch die neue Sichtweise auf alternative Transaktionsmittel und Finanzinstitutionen einen entscheidenden Beitrag für Innovationen im Finanzsektor geleistet.⁷⁸ Zudem bieten Kryptowährungen im Falle von politisch unsicheren Zeiten, die sich auf die Stabilität der heimischen Währung auswirken können, eine alternative Zahlungs- und Anlageform.⁷⁹ Als eine Erweiterung des bestehenden Angebots der staatlichen Zahlungsmittel und somit der Förderung des Wettbewerbs zwischen den Währungen sind virtuelle Währungen zu begrüßen. Trotz berechtigter Kritikpunkte sollten daher die Chancen für neue Anwendungen und Verbesserungspotentiale im gegenwärtigen Finanzsystem wahrgenommen werden.

⁷⁷ Die Aufgaben der ESZB sind in Art. 3.1 der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank beschrieben und umfassen u. a. die Gestaltung der Geldpolitik der Union. Vgl. Protokoll Nr. 4 Über die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank v. 26.10.2012, Abl. EU Nr. C 326/231 v. 26.10.2012.

⁷⁸ Hierzu *Guadamuz/Marsden, Chris*, Blockchains and Bitcoin: Regulatory responses to cryptocurrencies, *First Monday* 2015, Tz. 2.6.

⁷⁹ In Anlehnung an *Ogundeji*, World Markets in Selloff, Trump Presidency Spikes Bitcoin Price, *cointelegraph.com*, Artikel v. 09.11.2016; *Tuttle*, Bitcoin Prices Are Surging Again Amid Global Uncertainty, *time.com*, Artikel v. 28.12.2016.

3. Rechtliche Einordnung virtueller Währungen

Die Untersuchung virtueller Währungen verdeutlicht bereits die Schwierigkeit der juristischen Bewertung von neuartigen technologischen Anwendungen, bei welchen bis dato unbekannte Produkte und Geschäftsmodelle de lege lata rechtlich bewertet werden müssen und gegebenenfalls neue Gesetze und Regulierungen erforderlich sind. Hier zeigen sich länderübergreifend heterogene Bewertungen, die lediglich in der Verneinung des Status des gesetzlichen Zahlungsmittels zu einer gleichen Einschätzung gelangen.⁸⁰ Stattdessen liegen unterschiedliche Bewertungen unter anderem als Ware, dezentrale virtuelle Währung, elektronischer Service oder gar digitales Gut vor.⁸¹ Diese Einordnungen spielen jedoch eine entscheidende Rolle, um schuldrechtliche oder zivilrechtliche Konsequenzen für die Nutzer abschätzen zu können. Ebenso ist danach zu bestimmen, inwieweit eine Besteuerung vorzunehmen ist. Im Folgenden werden zunächst Einordnungen zum rechtlichen Status von virtuellen Währungen anhand der ausgewählten Beispiele der USA, der Europäischen Union, sowie im Speziellen Deutschlands näher beleuchtet. Darüber hinaus erfolgt eine kurze Darstellung bezüglich der Besteuerung beim Umtausch virtueller Währungen in gesetzliche Zahlungsmittel. Abschließend werden die Möglichkeiten für eine Regulierung virtueller Währungen diskutiert.

⁸⁰ Hierzu *Künnapas*, From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of *de lege ferenda?*, in: The Future of Law and eTechnologies, 2016, 111, 115.

⁸¹ Id., Table 1.

In Deutschland maßgeblich ist die Bewertung der BaFin.⁸² Die Aufsichtsbehörde definierte Bitcoins bereits 2011 als privat-rechtlich ausgegebene Komplementärwährung und ordnete diese als Rechnungseinheiten ein.⁸³ Sie gelten somit als Finanzinstrumente nach § 1 Abs. 11 Satz 1 Nr. 7 KWG. Die Beurteilung durch die BaFin sei rechtlich bindend, solange keine rechtskräftige Gerichtsentscheidung oder eine andere gesetzliche Regelung getroffen würde.⁸⁴ Die Auffassung der BaFin teilt ebenso das Bundesministerium der Finanzen.⁸⁵ Rechnungseinheiten seien vergleichbar mit den auf Fremdwährung lautenden ausländischen Zahlungsmitteln, den Devisen.⁸⁶ Dies gilt demnach ebenso für Bitcoins. Um jedoch wie Devisen als gesetzliche Zahlungsmittel zu gelten, müsste für Bitcoins analog zur Euro-Währung eine Verpflichtung zur An-

⁸² Nicht näher eingegangen wird auf die Diskussion in der Literatur bezüglich der abzulehnenden Einordnung von Bitcoins als Sache oder immaterielles Gut, sowie der schuldrechtlichen Frage, ob ein Tausch nach § 480 BGB oder ein Kaufvertrag vorliegt, wenn der Schuldner mit Bitcoins bezahlt. Näheres dazu u. a. *Engelhardt/Klein*, Bitcoins – Geschäfte mit Geld, das keines ist – Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355, 357; *Kaulartz*, Die Blockchain-Technologie – Hintergründe zur Distributed Ledger Technology und zu Blockchains, CR 2016, 474, 477.

⁸³ Vgl. *BaFin*, BaFin Merkblatt – Hinweise zu Finanzinstrumenten, 20.12.2011, geändert am 19.07.2013, Punkt 2. hh), bafin.de.

⁸⁴ Hierzu *Auffenberg*, Bitcoins als Rechnungseinheiten – Eine kritische Auseinandersetzung mit der aktuellen Verwaltungspraxis der BaFin, NVwZ 2015, 1184, 1184.

⁸⁵ Vgl. Antwortschreiben des BMF vom 07.08. 2013 auf eine Schriftliche Anfrage des MdB Frank Schäffler, frank-schaeffler.de, Stand: 28.01.2017.

⁸⁶ Vgl. *Kociok* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 27 Rn. 100.

nahme im Zahlungsverkehr bestehen, sodass sie zur Schuldbegleichung akzeptiert werden müssen.⁸⁷ Bitcoins, die keinen zentralen Emittenten in Form einer Zentralbank aufweisen, erfüllen diese Eigenschaft nicht. Trotz der Akzeptanz als Zahlungsmittel in einer wachsenden Anzahl an Geschäften,⁸⁸ gibt es darüber hinaus keine Verpflichtung zur Annahme. Sie stellen somit kein gesetzliches Zahlungsmittel dar. Resultierend aus der Einordnung als Finanzinstrument könnten nach § 32 Abs. 1 KWG gewerbsmäßige Bankgeschäfte und Finanzdienstleistungen im Inland ein Genehmigungsverfahren durch die BaFin erfordern, falls Bitcoins Bestandteil dieser Geschäfte oder Dienstleistungen sind.⁸⁹ Beispielhaft erfasst § 1 Abs. 1a, 2 Nr. 1 KWG die Vermittlung von Geschäften über die Anschaffung und die Veräußerung von Finanzinstrumenten. Tauschbörsen für Bitcoins benötigen demnach aufgrund der Anlagevermittlung eine schriftliche Erlaubnis der BaFin nach § 32 Abs. 1 KWG.

Die Einordnung als Rechnungseinheit und damit als Finanzinstrument wird durchaus kritisch betrachtet. So kennt das Gesetz als Rechnungseinheiten unter anderem die Sonderziehungsrechte des Internationalen Währungsfonds und die

⁸⁷ In Anlehnung an *Papapaschalis* in von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, AEUV Art. 128 Rn. 46.

⁸⁸ Eine Auswahl an Akzeptanzstellen unter *BTC-Echo*, Bitcoin Akzeptanzstellen, btc-echo.de, Stand: 28.01.2017.

⁸⁹ Hierzu *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung – Eine erste juristische Einordnung, MMR 2014, 75, 76.

European Currency Unit als Vorgänger des Euro.⁹⁰ Diese unterscheiden sich jedoch in ihrem Zweck von Bitcoins.⁹¹ Sie sind primär dazu gedacht, als Umrechnungswährung zu dienen, anstatt als reguläres Zahlungsmittel.⁹² Ebenso stellt die Einschätzung eine Herausforderung für die IFRS-Bilanzierung dar. Sie impliziere eine Bilanzierung als Zahlungsmitteläquivalent, was angesichts der enormen Preisausschläge, die zudem bei den Handelsplattformen sehr unterschiedlich erfasst werden, nicht mit der Vorgabe geringer Wertschwankungsrisiken nach IAS 7.6 und IAS 7.7 vereinbar sei.⁹³ Fraglich bleibt jedoch, ob bereits die Nutzung für Zahlungen für eine Qualifikation als Zahlungsmitteläquivalent genügen sollte. Die BaFin benennt ausdrücklich privatrechtlich ausgegebene Komple-

⁹⁰ Vgl. *Auffenberg*, Bitcoins als Rechnungseinheiten – Eine kritische Auseinandersetzung mit der aktuellen Verwaltungspraxis der BaFin, NVwZ 2015, 1184, 1185.

⁹¹ Die ECU war Bezugsgröße für das Europäische Wechselkurssystem und war als ein Währungskorb definiert. SZR sind vom Internationalen Währungsfonds geschaffenes Buchgeld, das aus einem Währungskorb der vier wichtigsten Währungen besteht und nur von wenigen Institutionen genutzt werden darf, u. a. dem IWF und den Mitgliedswährungsbehörden. Vgl. *Deutsche Bundesbank*, Glossar: European Currency Unit, Sonderziehungsrechte (SZR), bundesbank.de, Stand: 30.12.2016.

⁹² Zutreffend *Auffenberg*, Bitcoins als Rechnungseinheiten – Eine kritische Auseinandersetzung mit der aktuellen Verwaltungspraxis der BaFin, NVwZ 2015, 1184, 1186.

⁹³ Hierzu *Thurow*, Bitcoin in der IFRS-Bilanzierung, IRZ 2014, 197, 197. Sinnvoll sei vielmehr eine Bilanzierung als nicht abnutzbarer immaterieller Vermögensgegenstand. Vgl. *Thurow*, Bitcoin in der IFRS-Bilanzierung, IRZ 2014, 197, 198.

mentärwährungen.⁹⁴ Jedes ansatzweise anerkannte Tauschmittel müsste demnach wie Bitcoin behandelt werden.⁹⁵ Trotz berechtigter Kritik an der Kategorisierung als Rechnungseinheit ist die Aufsicht durch die BaFin zu begrüßen, da sie der zunehmenden Bedeutung von Kryptowährungen im Zahlungsverkehr Rechnung trägt und durch die einzuhaltenden Vorgaben zu einem besseren Verbraucherschutz für deren Nutzer beitragen kann.

In den USA zielt die Einordnung von virtuellen Währungen ebenfalls auf eine Ermöglichung der Regulierung ab. Das Finanzministerium der Vereinigten Staaten bezieht dabei zentralisierte virtuelle Währungen, die einen zentralen Aufbewahrungsort und einen einzigen Administrator besitzen, sowie dezentrale virtuelle Währungen wie die Kryptowährung Bitcoin, bei denen dies nicht der Fall ist, ein.⁹⁶ Das Ministerium ordnet diese als Finanzdienstleistungen und folglich deren Verwalter oder Handelsbörsen als Finanzinstitute ein.⁹⁷ Erfolgt der Gebrauch virtueller Währungen nicht für persönliche Transaktionen, müssen die Vorschriften des Bank Secrecy Act zur Verhinderung von Geldwäsche und Terrorismusfinanzie-

⁹⁴ Vgl. *BaFin*, BaFin Merkblatt – Hinweise zu Finanzinstrumenten, 20.12.2011, geändert am 19.07.2013, Punkt 2. hh), bafin.de.

⁹⁵ Zigaretten waren bspw. in der Nachkriegszeit in Deutschland ein beliebtes Zahlungsmittel. Hierzu *Sprenger/Herzog*, Währungsreform und soziale Marktwirtschaft, Konrad-Adenauer-Stiftung e.V., 2008, 10.

⁹⁶ Vgl. *Financial Crimes Enforcement Network*, Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury, 19.11.2013, 3.

⁹⁷ *Id.*, 10.

rung erfüllt werden.⁹⁸ Im Gegensatz zur bundesweit geltenden Vorgabe der BaFin in Deutschland unterscheiden sich die Bundesstaaten bezüglich des Stands der Regulierungsvorgaben. Lediglich New York besitzt seit 2015 eine umfangreiche Regulierung für Virtual Currency Unternehmen vergleichbar mit derjenigen für andere Finanzinstrumente.⁹⁹ Demnach wird der Erwerb einer Lizenz zum Zweck des Handelns mit virtuellen Währungen vorausgesetzt.¹⁰⁰ Lizenzinhaber müssen ein umfangreiches Regelwerk einhalten. So ist ein Compliance Officer zur Überwachung der Regel- und Gesetzeseinhaltung erforderlich,¹⁰¹ sowie eine detaillierte Aufklärung der Kunden über die hohen Risiken virtueller Währungen einschließlich vorgegebener Aussagen zu den Gefahren.¹⁰² Zusätzlich besteht die Pflicht, quartalsweise die Bilanz der Aufsichtsbehörde zur Verfügung zu stellen und den Jahresabschluss zu veröffentlichen.¹⁰³ Die Regulierung des Bundesstaates New York stellt ein hohes Maß an Rechtssicherheit für den Handel mit virtuellen Währungen her. Dennoch ist anzumerken, dass diese Regulierung lediglich in einem Bundestaat greift, auch wenn der New Yorker Handelsplatz der wichtigste in den Vereinigten Staaten ist und auch weltweit eine immense Bedeu-

⁹⁸ Id., 9.

⁹⁹ Hierzu *de la Merced*, Bitcoin Rules Completed by New York Regulator, *nytimes.com*, Artikel v. 03.06.2015.

¹⁰⁰ Vgl. New York Codes, Rules and Regulations, Title 23.

Department of Financial Services, Chapter 1. Regulations of the Superintendent of Financial Services, Part 200. Virtual Currencies, Section 200.3.

¹⁰¹ Id., Section 200.7 b).

¹⁰² Id., Section 200.19.

¹⁰³ Id., Section 200.14.

tung für den internationalen Finanzhandel aufweist. Somit ist damit zu rechnen, dass betroffene Unternehmen die hohen, kostspieligen Hürden meiden und auf anderen, noch nicht regulierten Märkten in den USA aktiv werden.

Für die europäische Union existiert derzeit noch keine Regulierung, was eine Herausforderung der Mitgliedsstaaten bei der Bekämpfung der illegalen Aktivitäten im Zusammenhang mit virtuellen Währungen darstelle.¹⁰⁴ Die EZB definiert diese als nicht reguliertes digitales Geld, dessen Ausgabe durch seine Entwickler kontrolliert wird und in bestimmten virtuellen Kreisen zu Zahlungszwecken akzeptiert wird.¹⁰⁵ Gleichzeitig weist es in Teilen Charakteristika eines Ponzi-Schemas auf.¹⁰⁶ Dies liegt daran, dass Emittenten, bei dem die Forderung äquivalent zu gesetzlichen Zahlungsmitteln eingelöst werden kann, bei den dezentralen Währungen wie Bitcoin nicht existieren. Bitcoin-Besitzer sind daher darauf angewiesen, dass eine andere Person den Bitcoins einen Wert beimisst und sie erwirbt. Zudem wird die Einordnung in die bestehenden EU-Richtlinien der Electronic Money Directive (2009/110/EC) und der Payment Service Directive (2007/64/EC) verneint.¹⁰⁷ Letztere gilt für Zahlungsdienste,

¹⁰⁴ Hierzu *Europäische Zentralbank*, Virtual Currency Schemes, 2012, 45.

¹⁰⁵ Vgl. *Europäische Zentralbank*, Virtual Currency Schemes, 2012, 13.

¹⁰⁶ Dazu *Europäische Zentralbank*, Virtual Currency Schemes, 2012, 27.

¹⁰⁷ Hierzu *Europäische Zentralbank*, Virtual Currency Schemes, 2012, 47.

unter anderem für Kreditinstitute und E-Geld-Institute.¹⁰⁸ Bei den Zahlungsdiensten müsse es sich um juristische Personen handeln, sodass dezentrale, virtuelle Währungen grundsätzlich nicht in Frage kommen.¹⁰⁹ Um wiederum unter die Richtlinie für E-Geld-Institute zu fallen, müssten nach Art. 2 Nr. 2 virtuelle Währungen in elektronischer Speicherung vorliegen, von anderen als dem Emittenten als Zahlungsmittel angenommen werden, sowie eine Forderung gegenüber dem Emittenten, die gegen Zahlung eines Geldbetrags ausgestellt wird, darstellen.¹¹⁰ Virtuelle Währungen wie Bitcoins liegen ausschließlich in elektronischer Form vor.¹¹¹ Ebenso sind sie zu einem gewissen Grad als Zahlungsmittel auch außerhalb von Online Communitys akzeptiert. Allerdings entsteht keine Forderung gegenüber einem Emittenten. Im Fall von Bitcoins werden diese dezentral durch den Mining-Prozess generiert. Demnach sind die Bedingungen nicht erfüllt, auch wenn Bit-

¹⁰⁸ Hierzu *Shcherbak*, How should Bitcoin be regulated?, Eur. J. Legal Stud. Vol. 7:1, 2014, 41, 60.

¹⁰⁹ In Anlehnung an *Shcherbak*, How should Bitcoin be regulated?, Eur. J. Legal Stud. Vol. 7:1, 2014, 41, 60.

¹¹⁰ Vgl. Art. 2 Nr. 2 der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates v. 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, Abl. EU Nr. L 267/11 v. 10.10.2009.

¹¹¹ Es gibt zwar Anbieter von Bitcoin Münzen, wie das Unternehmen Lealana (Lealana.com). Jedoch ist kaum sicherzustellen, dass nur die Münzen den privaten Schlüssel enthalten und keine Kopien dieser beim Hersteller vorliegen.

coins und andere virtuelle Währungen Ähnlichkeiten zu E-Geld aufweisen.¹¹²

Angesichts der bestehenden Rechtsunsicherheit und fehlenden Regulierung bedarf es einer Ausweitung der bestehenden Regelungen auf virtuelle Währungen oder einer zusätzlichen neuen Gesetzgebung innerhalb der EU. Diese Auffassung teilt auch das EU-Parlament. Laut der Entschließung solle die EU-Kommission eine Task Force bilden, die Empfehlungen für eine Regulierung gegen illegale Aktivitäten erarbeiten soll, ohne jedoch den positiven Nutzen technologischer Innovationen für die Bevölkerung zu mindern.¹¹³ Die EU-Kommission arbeitet bereits an einer Einbeziehung von Tauschbörsen für virtuelle Währungen in die Richtlinie zur Bekämpfung der Geldwäsche.¹¹⁴ Das Ziel der Regulierung ist letztendlich, die Anonymität der Tauscher mithilfe von verpflichtenden Sorgfaltsprüfungen der Plattformen aufzuheben.¹¹⁵ Die EZB unterstützt dabei den Einbezug virtueller Währungen in die überarbeitete Richtlinie.¹¹⁶ Sie mahnt jedoch an, dass der Gesetz-

¹¹² Zutreffend *Künnapas*, From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of *de lege ferenda?*, in: The Future of Law and eTechnologies, 2016, 111, 116.

¹¹³ Vgl. Entschließung des Europäischen Parlaments v. 26.05.2016 zu virtuellen Währungen (2016/2007(INI)), P8_TA(2016)0228, Rn. 14.

¹¹⁴ Id., Rn. 19.

¹¹⁵ Id., Rn. 19.

¹¹⁶ Vgl. Stellungnahme der Europäischen Zentralbank v. 12.10.2016 zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG (CON/2016/49), Abl. EU C 459/3 v. 09.12.2016.

geber die Nutzung privat ausgegebener, digitaler Währungen nicht befördern sollte, da sie nicht Währungen im rechtlichen Sinne oder gesetzliche Zahlungsmittel seien.¹¹⁷ Das Vorgehen der europäischen Institutionen zeigt, dass aufgrund der befürchteten Gefahren durch illegale Aktivitäten der Fokus der Regulierung auf die Verhinderung krimineller Transaktionen gelegt wird. Eine breite Akzeptanz virtueller Währungen als Ergänzung zu gesetzlichen Zahlungsmitteln wird durch das derzeitige Regulierungsvorhaben nicht angestrebt. Hierfür müsste zusätzlich der Verbraucherschutz für die neue Währungsart an das Schutzniveau anderer Finanzdienstleistungen angepasst werden und eine eindeutige rechtliche Einordnung stattfinden, um die Nutzersicherheit zu verbessern und die Akzeptanz im Zahlungsverkehr zu steigern.

Dass hierbei innerhalb der Europäischen Union durchaus Meinungsverschiedenheiten herrschen, zeigt die Betrachtung steuerlicher Aspekte in Verbindung mit virtuellen Währungen. Im Oktober 2015 entschied der Europäische Gerichtshof, dass Umsätze aus dem Umtausch von virtuellen Währungen in konventionelle Währungen und umgekehrt nicht mehrwertsteuerpflichtig seien.¹¹⁸ Dem Urteil vorausgegangen war ein Rechtsstreit in Schweden, bei dem die Umsatzsteuerpflicht bei Tauschgeschäften zwischen Bitcoins und konventionellen Währungen in Frage gestellt wurde.¹¹⁹ Zunächst konstatierte das Gericht, dass es sich bei Bitcoins nicht um Ge-

¹¹⁷ Id., C 459/4.

¹¹⁸ EuGH, Urt. v. 22.10.2015, Rs. C-264/14, ECLI:EU:C:2015:718, Rn. 32.

¹¹⁹ EuGH, Urt. v. 22.10.2015, Rs. C-264/14, ECLI:EU:C:2015:718, Rn. 2.

genstände im Sinne von Art. 14 der Mehrwertsteuerrichtlinie handele, sondern eine Nutzung als Zahlungsmittel vorliege.¹²⁰ Zudem ließe sich aus dem betreffenden Art. 135 Abs. 1 e) der Mehrwertsteuerrichtlinie aufgrund der unterschiedlichen Sprachfassungen nicht eindeutig ableiten, dass lediglich Umsätze mit konventionellen Währungen unter die steuerbefreiten Umsätze der Richtlinie fielen.¹²¹ Folglich stellten auch Umsätze, die sich auf virtuelle Währungen beziehen, steuerbefreite Umsätze nach Art. 135 Abs. 1 e) dar.¹²² Die Anerkennung von Bitcoins als Zahlungsmittel durch den EuGH und deren Gleichbehandlung bezüglich der Steuerfreiheit für Tätigkeiten nach Art. 135 Abs. 1 e) ist begrüßenswert im Hinblick auf die bereits gängige Praxis einer wachsenden Bevölkerungsgruppe, Bitcoins als Zahlungsmittel zu nutzen. Kritisch zu sehen ist jedoch, dass der Art. 135 Abs. 1 e) explizit gesetzliche Zahlungsmittel als Bestandteil der Steuerbefreiung nennt. Das deutsche Umsetzung der Mehrwertsteuerrichtlinie erfasst in § 4 Nr. 8 b) UStG analog zur Richtlinie ebenfalls nur die Umsätze mit gesetzlichen Zahlungsmittel für die Steuerbefreiung und schließt Zahlungsmittel aus, die wegen ihres Sammlerwerts oder des Metallgehalts umgesetzt werden.¹²³ Die Begründung in den Schlussanträgen, dass die unterschiedlichen Sprachfassungen einen eindeutigen Ausschluss nicht

¹²⁰ EuGH, Urt. v. 22.10.2015, Rs. C-264/14, ECLI:EU:C:2015:718, Rn. 24.

¹²¹ EuGH, Urt. v. 22.10.2015, Rs. C-264/14, ECLI:EU:C:2015:718, Rn. 46.

¹²² EuGH, Urt. v. 22.10.2015, Rs. C-264/14, ECLI:EU:C:2015:718, Rn. 58.

¹²³ Ebenso *Wäger* in Sölch/Ringleb, UStG, § 4 Nr. 8 Rn. 120.

gesetzlicher Zahlungsmittel nicht zulässt,¹²⁴ ist zu kritisieren.¹²⁵ Es stellt sich vielmehr die Frage, warum derart gravierende sprachliche Unterschiede zustande gekommen sind, welche eine sprachenabhängige Auslegung zur Folge haben.

Die Untersuchung der vielfältigen rechtlichen Einordnungen bezüglich der Definition sowie die unterschiedlichen Regulierungsbestrebungen verdeutlicht die Unsicherheit, die bei virtuellen Währungen existiert. Die Subsumption unter bestehendes Recht wird vielfach dadurch erschwert, dass dieses bei monetären Begriffen keine Dezentralität kennt oder zulässt, wie sie bei Bitcoins unabdingbar ist. Ausgangspunkt vieler Regelungen bleibt stattdessen die zentralisierte Ausgabe der gesetzlichen Zahlungsmittel. Es sollte daher zunächst eine gültige Definition für virtuelle Währungen geschaffen und in bestehende Regelungen eingefügt werden, da sie zwar Gemeinsamkeiten zu anderen Finanzinstrumenten und Zahlungsmitteln aufweisen, in der Dezentralität ihres Entstehens jedoch von ihnen abweichen. Dies könnte besonders bei Steuerungsfragen und der Erlaubnispflicht für Geschäftstätigkeiten mit Bezug zu virtuellen Währungen für mehr Rechtssicherheit sorgen. Sinnvoll erscheint angesichts der internationalen Zahlungsströme eine supranationale Regulierung. Eine EU-weite Regelung ließe sich beispielsweise in das Europäische Finanzaufsichtssystem integrieren. Ebenso sollte akzeptiert werden, dass eine staatliche Kontrolle über die dezentralen Netzwerke nicht realistisch erscheint. Hierfür müsste die Mehrheit der wechselnden Nutzer den Bestimmungen zu-

¹²⁴ EuGH, Urt. v. 22.10.2015, Rs. C-264/14, ECLI:EU:C:2015:718, Rn. 46.

¹²⁵ Zustimmend *Wäger* in Sölch/Ringleb, UStG, § 4 Nr. 8 Rn. 121.

stimmen, um sie beispielsweise im System zu implementieren. Dagegen sprechen sowohl praktische Gründe, als auch die Überzeugung der Community von einer staatlich unabhängigen Währung.¹²⁶ Regulierungen sollten daher auf die Bereiche abzielen, die effektiv beaufsichtigt werden können. Dies sind zum einen die Tauschbörsen und Walletbetreiber,¹²⁷ die als Finanzdienstleistungsinstitute klassifiziert und damit bereits unter geltendem Recht reguliert werden könnten.¹²⁸ So könnten die Nutzer von einem höheren Verbraucherschutzniveau profitieren und gleichzeitig illegale Aktivitäten erschwert werden. Zum anderen könnten auch Unternehmen, die Bitcoins als Zahlungsmittel akzeptieren, Auflagen zum Schutz gegen Geldwäsche und Steuerhinterziehung auferlegt werden. Die getroffenen Maßnahmen sollten eine effiziente und kontrollierbare Regulierung im Interesse der Nutzer, involvierten Dienstleister und der Gesellschaft ermöglichen, ohne die dezentrale Funktionsweise virtueller Währungen zu behindern. Das dezentrale Netzwerk muss angesichts ineffizienter Kontrollmöglichkeit ohne Regulierung bleiben,¹²⁹ auch wenn dies zur Folge hat, dass Nutzern bei Transaktionen innerhalb des Netzwerks kein besonderer Schutz gewährt werden kann. Angesichts des voraussichtlich langwierigen Prozesses zur Erarbeitung eines Regelwerks ist anzumerken,

¹²⁶ Hierzu *Sixt*, *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie*, 2017, 125.

¹²⁷ Näheres zu Walletbetreibern unter Gliederungspunkt C.II.

¹²⁸ Der Begriff der Finanzdienstleistungsinstitute wird unter § 1a KWG spezifiziert.

¹²⁹ In Anlehnung an *Sixt*, *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie*, 2017, 125.

dass bis zum Zeitpunkt des Inkrafttretens nicht von einem rechtfreien Raum für vom Gesetzgeber nicht explizit geregelte Anwendungen wie Bitcoin gesprochen werden kann. Vielmehr erfolgten frühzeitig erste, wenngleich heterogene rechtliche Bewertungen, die Aktivitäten im Zusammenhang mit virtuellen Währungen bereits zum derzeitigen Zeitpunkt unter geltendes Recht subsumieren.¹³⁰

II. Frontend Applikationen in Verbindung mit Kryptowährungen

Neben virtuellen Währungen existieren Anwendungen, die sich im Zusammenhang mit den Kryptowährungen etabliert haben. Derzeit dominieren diejenigen Angebote, die zur Verwaltung der Währungen genutzt werden, sogenannte Frontend Applikationen.¹³¹ Dabei handelt es sich um eine Benutzeroberfläche auf einem Bildschirm, über die der Nutzer Be-

¹³⁰ Beispielhaft zu nennen sind die Antworten des Bundesministeriums der Finanzen, die bereits 2013 die Besteuerung von Bitcoins thematisierten. So ist die Veräußerung von Bitcoins innerhalb eines Jahres nach dem Erwerb als privates Veräußerungsgeschäft im Sinne des § 23 I S. 1 Nr. 2 EStG einzuordnen. Erwerbswirtschaftliches Mining führt wiederum zu einkommenssteuerpflichtigen Einkünften, wenn es einer Einkommensart des EStG entspricht. Vgl. Antwortschreiben des BMF vom 07.08.2013 auf eine Schriftliche Anfrage des MdB Frank Schäffler, frank-schaeffler.de, Stand: 28.01.2017; Antwortschreiben des BMF vom 20.06.2013 auf eine Schriftliche Anfrage des MdB Frank Schäffler, frank-schaeffler.de, Stand: 28.01.2017.

¹³¹ Hierzu *Swan*, Blockchain – Blueprint for a New Economy, 2015, xiii.

fehle zur Steuerung der Software oder Website eingibt.¹³² Der Nutzer benötigt demnach keinen Zugriff auf die zugrundeliegende Programmierung der Blockchain, um Transaktionen auszuführen und den privaten Schlüssel zu verwalten. Die Angebote dienen somit in erster Linie als benutzerfreundlicher Zugang zur Blockchain und der darauf getätigten Transaktionen. Eine solche Frontend Applikation sind Online Wallets – Onlinegeldbörsen – die eine von mehreren Möglichkeiten zur Speicherung und zum Transfer von virtuellen Währungen darstellen.¹³³ Ebenfalls besteht die Möglichkeit eine digitale Geldbörse auf dem Computer anzulegen. Diese muss jedoch vor Viren, dem Verlust der Walletdatei und physischen Schäden geschützt werden, da verlorene Bitcoins nicht wieder hergestellt werden können.¹³⁴ Für die Transaktionsabwicklung über Smartphones wiederum werden applikationsbasierte Anwendungen angeboten, die angesichts des limitierten Speicherplatzes lediglich auf einen kleinen Ausschnitt der Blockchain zurückgreifen.¹³⁵ Die Online Wallet wird dagegen über die Webseite eines Anbieters verwaltet.¹³⁶ Diese Variante bietet mehr Sicherheit bei Verlust in Folge von phy-

¹³² Vgl. *Business Dictionary.com*, front end application, Stand: 26.08.2016.

¹³³ Dazu *J. P.*, Virtual Currency: Bits and bob, THE ECONOMIST, Artikel vom 13.06.2011.

¹³⁴ Hierzu *J. P.*, Virtual Currency: Bits and bob, THE ECONOMIST, Artikel vom 13.06.2011.

¹³⁵ Dazu *BTC-Echo*, Bitcoin Wallet: Bitcoins sicher aufbewahren, btc-echo.de, Stand: 15.01.2017.

¹³⁶ Siehe *bitcoinwiki*, Browser based wallet, bitcoin.it, Stand: 30.08.2016.

sischen Schäden oder versehentlicher Datenlöschung.¹³⁷ Gleichzeitig sind jedoch sowohl Wallets, als auch Handelsbörsen Ziel von Hackerattacken, im Zuge derer Bitcoins gestohlen werden.¹³⁸ Während die Blockchain als sicher gilt, ist die Gefährdung bei den zugehörigen Aufbewahrungssystemen und Tauschbörsen zu verorten. Die Sicherheitsrisiken haben jedoch zur Folge, dass potenzielle Nutzer aufgrund von Sicherheitsbedenken die Währung mangels vergleichbarer Regulierung und Schutzmaßnahmen wie bei klassischen Bankdienstleistungen meiden.¹³⁹ Beispielsweise haben Verbraucher in Deutschland nach § 675u S. 1 u. 2 BGB Anspruch auf Erstattung nicht autorisierter Zahlungsvorgänge durch den Zahlungsdienstleister. Ein weiteres Beispiel für Verbraucherschutz bei Finanzdienstleistungen stellt der britische Consumer Credit Act von 1974 dar, der Verbraucher im Falle von Kreditkartenmissbrauch schützt.¹⁴⁰ Diese Vorkehrungen schützen nicht nur vor finanziellen Schäden, sondern fördern zugleich das Vertrauen in die Zahlungsmethode. Im Falle der Blockchain, wie sie bei der Bitcoin vorliegt, lässt sich keine

¹³⁷ Ähnlich *Guadamuz/Marsden*, Blockchains and Bitcoin: Regulatory responses to cryptocurrencies, First Monday 2015, Tz. 3.4.

¹³⁸ Hackerangriffe ereigneten sich bspw. bei der Handelsbörse Bitfinex („65 Millionen Bitcoins gestohlen“, 03.08.2016, Handelsblatt.com), u. der virtuellen Bitcoin-Sparkasse Instawallet („Virtuelle Währung, Hack-Attacken bremsen Bitcoin Rallye“, 04.04.2013, Spiegel.de.).

¹³⁹ In Anlehnung an *Guadamuz/Marsden*, „Blockchains and Bitcoin: Regulatory responses to cryptocurrencies, First Monday 2015, Tz. 3.6.

¹⁴⁰ Bspw. Abschnitte 75, 83 und 84 des Consumer Credit Act 1974, unter: legislation.gov.uk, Stand: 20.08.2016.

natürliche oder juristische Person identifizieren, die für eventuelle Schäden haften könnte. Eine Übertragung auf die Blockchain ist daher angesichts der dezentralen Verwaltung durch die hohe Anzahl an Rechnern und des öffentlichen Zugangs problematisch. Anders ist die Bewertung der Anbieter von Wallets und Handelsbörsen vorzunehmen. Hier sollte eine Identifizierung der Betreiber möglich sein. Notwendig wäre eine Regulierung ähnlich derer für Finanzdienstleister, bei der eine Haftungsregelung für die Zahlungsdienstleister das Risiko der Nutzer im Falle des Diebstahls des privaten Schlüssels minimieren könnte. Mangels einer solchen Regulierung haben sich weitere Verwahrungsmethoden zur Sicherung des privaten Schlüssels entwickelt. Hierzu gehören Hardware Wallets, welche die Wallet auf einem separaten Speichermedium verwahren, sowie die Erstellung der Zugangsdaten auf Papier.¹⁴¹ Beide Varianten schützen zwar gegen Hackerangriffe, bergen jedoch die Gefahr, mit der beschädigten oder verloren gegangenen Wallet auch unwiderruflich die verwalteten Kryptowährungen zu verlieren. Insgesamt bieten die Angebote im Bereich der Frontend Applikationen keinen Schutz der Verbraucher vor finanziellen Schäden. Die vergleichsweise hohen Risiken der Wallets gegenüber herkömmlichen Konten könnten dementsprechend zu der niedrigen Anzahl von Blockchain Wallet Benutzern beitragen:

¹⁴¹ Hierzu *BTC-Echo*, Bitcoin Wallet: Bitcoins sicher aufbewahren, btc-echo.de, Stand: 15.01.2017.

Lediglich 11,5 Mio. Wallets existieren,¹⁴² was die derzeit noch geringe Bedeutung der virtuellen Geldbörsen im Zusammenhang mit Kryptowährungen verdeutlicht. Ebenso bleibt festzuhalten, dass die Frontend Applikationen im Gegensatz zu innovativen Anwendungsmöglichkeiten der Blockchain-Technologie wie den Kryptowährungen oder Smart Contracts keine neuartigen Geschäftsmodelle darstellen. Stattdessen handelt es sich bei den Angeboten um eine Umsetzung von Produkten zur Konten- und Transaktionsverwaltung, die den herkömmlichen Applikationen und der Onlinekontenführung etablierter Finanzdienstleister stark ähneln. Sie unterscheiden sich dabei hauptsächlich bezüglich des gewährten Verbraucherschutzniveaus. Es handelt sich somit weder um eine Prozessinnovation, noch um eine Produktinnovation.¹⁴³

¹⁴² Vgl. *Blockchain Info*, Blockchain Wallet Benutzer, blockchain.info, Stand: 20.01.2017. Zum Vergleich: Das Online-Bezahlsystem Paypal weist im 3. Quartal 2016 192 Mio. aktive Accounts aus. Vgl. *Statista*, Anzahl der aktiven Accounts bei Paypal, statista.com, Stand: 20.01.2017.

¹⁴³ Definition von Innovation nach *Herrmann/Huber*, Produktmanagement: Grundlagen – Methoden – Beispiele, 2013, 124.

D. Zukünftige Anwendungsfelder in der Diskussion

I. Smart Contracts

1. Terminologie und Funktionsweise

Eine Anwendung der Blockchain mit einer Reihe von potenziellen Nutzungsmöglichkeiten stellen Smart Contracts dar, die eine neuartige Vertragsgestaltung sowie deren Ausführung ermöglichen sollen, und bereits von Unternehmen getestet werden.¹⁴⁴ Von der Abwicklung von Derivaten bis hin zu Versicherungsleistungen und digitalen Identitäten ist eine Vielzahl von Use Cases für Smart Contracts vorstellbar. Insbesondere in der Finanzbranche könnten die blockchainbasierten Anwendungen zukünftig eine hohe Bedeutung erlangen. Die erste Konzeption eines Smart Contracts wurde bereits Anfang der Neunziger Jahre von Nick Szabo vorgestellt.¹⁴⁵ Er definierte hierfür ein Protokoll, das auf Computerbasis gespeichert wird und der Ausführung von Vertragsbedingungen eines Vertrags dient.¹⁴⁶ Doch erst mit der Entwicklung der Distributed Ledger Technologie existiert eine technische Grundlage,

¹⁴⁴ Bspw. hat die Allianz ein erfolgreiches Pilotprojekt mit Katastrophen-Swaps und –anleihen mithilfe von Smart Contracts realisiert. Vgl. *Allianz*, Erfolgreiches Pilotprojekt: Allianz Risk Transfer und Nephila realisieren Katastrophen-Swap mit Blockchain-Technologie, Pressemeldung v. 15.06.2016, allianz.com.

¹⁴⁵ Hierzu Szabo, Smart Contracts, 1995, szabo.best.vwh.net, Stand: 20.05.2016.

¹⁴⁶ Vgl. Szabo, Smart Contracts, 1995, szabo.best.vwh.net, Stand: 20.05.2016.

um den innovativen Vertragstypus in der Realität umzusetzen. Im Folgenden sollen sowohl terminologische Unterschiede als auch die allgemeine Funktionsweise von Smart Contracts erläutert werden.

Bei einem Smart Contract handelt es sich um einen Vertrag, bei dem etwaige Rechte und Verpflichtungen von Vertragsparteien in einen Code programmiert werden.¹⁴⁷ In Abhängigkeit vom wissenschaftlichen Blickwinkel liegen unterschiedliche Verständnisse des Begriffs vor. Während IT-Spezialisten Smart Contracts als automatisierte Vereinbarungen außerhalb der Gerichtsbarkeit definieren, betrachten Juristen dies anders.¹⁴⁸ Die Anwendung werde zwar auch als automatisierte Vereinbarung angesehen, die jedoch nur in Verbindung mit einem rechtlichen Vertrag existiere, da die Gerichtsbarkeit nicht ausgeschlossen werden könne.¹⁴⁹ Basierend auf dem Code, der in der Blockchain angelegt und gespeichert wird, wird innerhalb des dezentralen Netzwerks durch die Verifizierung die Ausführung des programmierten Vertragsinhalts ausgelöst.¹⁵⁰ Hierbei bestätigen die dezentral organisierten Netzwerkteilnehmer der Blockchain den Smart Contract in seiner hochgeladenen Form. Der Vorgang entspricht dabei dem Mechanismus, der ebenfalls bei der Transaktion von

¹⁴⁷ Ähnlich Szabo, *Formalizing and Securing Relationships on Public Networks*, First Monday 1997, Ü. „Contracts Embedded in the World“.

¹⁴⁸ Hierzu Kölvart, *et al.*, *Smart Contracts*, in: *The Future of Law and eTechnologies*, 2016, 133, 136.

¹⁴⁹ Hierzu Kölvart, *et al.*, *Smart Contracts*, in: *The Future of Law and eTechnologies*, 2016, 133, 136.

¹⁵⁰ In Anlehnung an Swan, *Blockchain – Blueprint for a New Economy*, 2015, 16.

Bitcoins verwendet wird.¹⁵¹ Der Inhalt des Smart Contract wird folglich durch den Code dargestellt und zugleich ausgeführt. Da der programmierte Vertrag dezentral abgespeichert wird, gibt es für eine einzelne Vertragspartei keine Möglichkeit, den Vertragsinhalt einseitig zu verändern und somit in den auszuführenden Inhalt einzugreifen. Somit sind zwei wesentliche Eigenschaften der Anwendung deren Automatisierung sowie Durchsetzbarkeit.¹⁵² Jedoch sei Automatisierung nicht zwingend gleichbedeutend mit einer Ausführung, die vollständig auf menschliche Mitwirkung verzichte.¹⁵³ Menschliche Beteiligung, beispielsweise durch das Bereitstellen des Smart Contracts in dem Netzwerk oder die Eingabe benötigter Informationen für die korrekte Funktionsweise, ist in vielen Fällen ein notwendiger Bestandteil der Ausführung. Die Notwendigkeit weiterer Informationen könnte beispielsweise im Falle eines Kaufvertrags über eine Ware auftreten. Würde eine mangelhafte Ware vorliegen, die nicht digital vernetzt ist, so wäre der Smart Contract auf einen manuellen Input diesbezüglich angewiesen, da er den Zustand der Ware nicht eigenständig überprüfen könnte.¹⁵⁴ Somit liegen vielfach Smart Contracts vor, die als teilautomatisiert bezeichnet werden können.

¹⁵¹ Die Funktionsweise gilt analog für andere blockchainbasierte Netzwerke wie bspw. Ethereum mit der Kryptowährung Ether, die speziell für die Ausführung von Smart Contracts entwickelt wurde.

¹⁵² Hierzu *Clack, et al.*, Smart Contract Templates: foundations, design landscapes and research directions, Barclays, 2016, 3.

¹⁵³ Id.

¹⁵⁴ Der Anwendungsfall von Smart Contracts in Verbindung mit vernetzten Gegenständen – sogenanntes Smart Property – wird unter Gliederungspunkt D.II betrachtet.

a) Smart Contract Codes

Für eine nähere Betrachtung und Bewertung von Smart Contracts sollte zunächst zwischen zwei verschiedenen Typen von Smart Contracts unterschieden werden, die sich in ihrem Komplexitätsgrad und ihrer Umsetzbarkeit unterscheiden. Im Hinblick auf die Beantwortung der Frage, ob es sich bei Smart Contracts wie der Name suggeriert auch um Verträge im rechtlichen Sinne handelt, ist eine Einordnung der unterschiedlichen Konzepte notwendig. Zu differenzieren ist hierbei zwischen Smart Contract Codes und Smart Legal Contracts, die ebenfalls im Hinblick auf ihren konzeptionellen Umsetzungsstand betrachtet werden sollen. Smart Contract Codes geben einen vergleichsweise unkompliziert gestalteten Vertrag in Form einer Programmierung wieder. Sie enthalten eine Reihe von Bedingungen und daraus resultierende Konsequenzen, die von einem Softwareprogramm automatisiert ausgeführt werden.¹⁵⁵ Beispielhaft kann ein Smart Contract Code gestaltet werden, der die Auszahlung eines Erbes an Bedingungen knüpft und bei deren Erfüllung die Auszahlung automatisch und ohne menschliche Intervention auslöst. Die Bedingungen könnten beispielsweise das Versterben des Erblassers sowie zusätzlich das Erreichen eines vorgegebenen Alters durch den Erbenden sein. Bei Erfüllung der Bedingungen löst der Code die Überweisung des Erbes aus. Der Betrag könnte sowohl fix, als auch variabel im Hinblick auf den zur Verfügung stehenden Betrag sein. Um den Vertragsinhalt

¹⁵⁵ In Anlehnung an *Clack, et al., Smart Contract Templates: foundations, design landscapes and research directions*, Barclays, 2016, 2.

ausführen zu können, benötigt der Smart Contract Code spezifische Informationen. So muss er auf zuverlässige Quellen zugreifen können, welche die Erfüllung der Bedingungen verifizieren. In diesem Fall ist das zum einen das Geburtsdatum des Erbenden, das als eine Bedingung in den Code eingesetzt werden könnte. Zum anderen muss das Ableben des Erblassers belegt werden. Dies könnte durch den Zugriff auf digitale Traueranzeigen oder Sterberegister erreicht werden. Ein unberechtigtes Auslösen der Zahlung wäre somit nicht möglich. Zusätzlich müssen die anzusprechenden Konten der beteiligten Personen im Code hinterlegt sein. Wie in dem Beispiel sind die Ergebnisse, die der Smart Contract Code erzeugt, von den erfüllten Bedingungen und den codierten Folgen abhängig. Nicht programmierte Bedingungen und Konsequenzen sind demnach nicht ausführbar. Ein weiterer Fall eines Smart Contract Codes ist deren Umsetzung für Aktienoptionen.¹⁵⁶ Da diese von den Inhabern nur unter bestimmten Bedingungen realisiert werden, wäre es möglich, über Handelsplattformen die notwendigen Informationen zu Preisentwicklungen dem Smart Contract Code in der Blockchain zur Verfügung zu stellen. Ausgehend von der Funktionsweise des Smart Contract Codes ist die Bezeichnung als „smart“ durchaus als irreführend zu bezeichnen. Der Code führt lediglich die festgelegten Aktivitäten in Abhängigkeit von den formulierten Bedingungen aus. Eine eigenständige und intelligente Form der Bewertung und Anpassung der Aktivitäten durch den Code selbst, wie der Begriff des Smart Contracts Codes suggeriert,

¹⁵⁶ Ebenso *Yermack*, Corporate Governance and Blockchains, National Bureau of Economic Research, Working Paper 21802, 2015, 1.

riert, liegt nicht vor. Zumeist handelt es sich bei den derzeit diskutierten und teilweise bereits realisierten Use Cases für Smart Contracts um die beschriebenen Smart Contract Codes.¹⁵⁷ Diese Anwendungsfälle bieten zwar Vorteile für eine Vielzahl von auszuführenden Vertragsbestandteilen, wie sich in dem beispielhaften Smart Contract zur automatisierten Übertragung eines Erbes gezeigt hat. Sie sind jedoch nicht „smart“ im Sinne der Fähigkeit, den Vertragsinhalt in seiner Bedeutung und Wirkung zu verstehen. Die Automatisierung von Aktivitäten wie der Veranlassung einer Überweisung über zuvor festgelegte Konten stellt keinesfalls eine Form von maschineller Intelligenz dar.

b) Smart Legal Contracts

Smart Legal Contracts stellen dagegen eine weitaus höher entwickelte Vertragsausführung dar, die über die simple Darstellung und Ausführung von Bedingungen und Folgen eines Smart Contract Codes hinausgeht. Es handelt sich dabei um komplexe juristische Verträge, die mithilfe eines Softwareprogramms nicht nur ausgeführt, sondern durch dieses zusätzlich selbstständig interpretiert werden sollen.¹⁵⁸ Dies setzt voraus, dass zur Erstellung des Smart Legal Contracts ein Pro-

¹⁵⁷ Da die im Zuge dieser Arbeit vorgestellten Use Cases von Smart Contracts in ihrer Gestaltung Smart Contract Codes entsprechen, bezeichnet im Folgenden der Begriff des Smart Contracts das Konzept des Smart Contract Codes, sofern nicht anderweitig spezifiziert.

¹⁵⁸ Hierzu *Clack*, Smart Contract Templates: foundations, design landscapes and research directions, Barclays, 2016, 2.

ogramm zur Verfügung steht, das über eine künstliche Intelligenz verfügt. Diese fortschrittliche Eigenschaft ist für die maschinelle Verarbeitung notwendig, um vielschichtige juristische Vereinbarungen in Textform anstatt in reiner Datenform zu verstehen und daraus Schlüsse zu ziehen. Es wäre somit für das Programm möglich Vertragsklauseln, die sich aus dem sprachlichen Kontext ergeben, umzusetzen, sowie mit unterschiedlichen juristischen Ausdrucksvarianten zu arbeiten. Smart Legal Contracts sollen Sprache nicht nur in Form von programmierbaren Bedingungen und Folgen umsetzen. Vielmehr rückt die Semantik, in diesem Fall also die juristische Bedeutung von Wörtern und Sätzen, in den Fokus. Das Verständnis von Sprache sollte dabei äquivalent zu derjenigen der Juristen und Beteiligten sein, die den Vertrag verfasst haben. Smart Legal Contracts agieren somit „smarter“ als einfache Smart Contract Codes. Eine Umsetzung dieser Idee erscheint jedoch innerhalb eines kurzen Zeithorizonts nicht realistisch, da noch einige technologische Hürden zu nehmen sind. Zunächst einmal ist die Entwicklung künstlicher Intelligenz im Bereich des maschinellen Sprachverständnisses noch nicht weit genug fortgeschritten, als dass ein Computer einen Vertragstext tatsächlich verstehen, geschweige denn interpretieren könnte.¹⁵⁹ Dies ist jedoch essenziell, um eine fehlerfreie Vertragsausführung zu garantieren und somit auf eine manuelle Überprüfung der Ergebnisse verzichten zu können. Zahlreiche internationale Projekte und Forschungseinrichtungen treiben jedoch technologische Entwicklungen für juristi-

¹⁵⁹ Zustimmend *Surden*, *Computable Contracts*, 46 U.C. Davis L. Rev. 629 (2012) at 639.

sche Anwendungsmöglichkeiten voran. Sie umfassen beispielsweise Themengebiete wie Expertensysteme, die Visualisierung und Maschinenlesbarkeit von Recht, sowie die Schaffung eines semantischen Internets.¹⁶⁰ Es ist davon auszugehen, dass auch die Idee der Smart Legal Contracts von diesen Erkenntnissen profitieren wird. Obwohl mit dem derzeitigen Entwicklungsstand fundamentale Eigenschaften der Vertragsauslegung von künstlicher Intelligenz noch nicht erbracht werden können, könnte sich dies mit dem Entwicklungsfortschritt in Zukunft ändern. So könnten durch intelligente Verträge aufwendige Arbeitsschritte bei der Umsetzung von Vertragsinhalten, die juristische Expertise erfordern, reduziert werden. Kürzere Bearbeitungszeiten und Kostenersparnisse wären die Folge. Allerdings sollte unabhängig von der technischen Realisierbarkeit ebenso berücksichtigt werden, ob und wie sich Smart Legal Contracts überhaupt in bestehende Rechtssysteme einbinden lassen. Aufgrund der Funktionsweise, dass das Programm den Vertrag nicht nur automatisch ausführt, sondern auch rechtlich interpretiert, würde die Technologie die Rechtsauslegung maßgeblich beeinflussen. Hier könnten die intelligenten, automatisierten Verträge auf Ablehnung stoßen, da sie letztendlich eine neue und von der Gesellschaft losgelöste Form der Rechtsauslegung bedeuten werden.

¹⁶⁰ Für die genannten Forschungsgebiete sind hier beispielhaft OpenLaws (unter: info.openlaws.com), OASIS LegalRuleML TC (unter: oasis-open.org), Hammurabi Project (unter: hammurabiproject.com) und DBPedia (unter: wiki.dbpedia.org) aufzuführen.

2. Eigenschaften von Smart Contracts

Auf Grundlage der terminologischen Einordnung werden die Vorzüge von Smart Contracts gegenüber klassischen Vertragsgestaltungen im Hinblick auf eine effiziente Vertragsausführung dargestellt, die aus deren spezifischen Eigenschaften resultieren. Zudem erfolgen gegebenenfalls Einschränkungen dieser Vorteile bei der Nutzung der Technologie.¹⁶¹ Smart Contracts in der Ausgestaltung von programmierten Bedingungen und Konsequenzen bieten gegenüber klassischen Vertragsgestaltungen eine Reihe von Vorzügen. Ein gewöhnlicher Vertrag stellt eine Vereinbarung zwischen zwei oder mehreren Parteien dar. Aus der Vereinbarung ergeben sich wiederum Pflichten nach § 241 I BGB für die Vertragspartner, gewisse Leistungen zu erbringen oder eine Leistung zu unterlassen. Charakteristisch für einen solchen Vertrag ist die Notwendigkeit von gegenseitigem Vertrauen zwischen den Vertragsparteien. Sie müssen darauf vertrauen, dass die vereinbarten Rechte und Pflichten gemäß dem Vertrag ausgeführt werden. Dabei besteht das Risiko, dass einzelne Vertragspartner von der Vereinbarung abweichen, sodass sich deren Verhalten zu Lasten der anderen Parteien auswirkt. Insbesondere bei Informationsasymmetrien zwischen den Vertragsparteien existieren Anreize, die eigene vorteilhafte Lage auszunutzen. Beispielsweise könnte trotz einer Verpflichtung zur Zahlung nach Erhalt einer Leistung die Bezahlung grundlos ausbleiben. Derjenige, der seine vereinbarte Leistung er-

¹⁶¹ Kritische Aspekte, welche die Rechtsproblematik betreffen, werden im Rahmen folgender Gliederungspunkte benannt, sodass hier zunächst von einer fehlerfreien und rechtlich unstrittigen Ausführung ausgegangen wird.

bracht oder in Vorleistung gegangen ist, müsste wiederum kosten- und zeitintensive Schritte einleiten, um das vertraglich Vereinbarte durchzusetzen. Folglich muss eine vertrauenswürdige dritte Instanz existieren, um unerwünschtes Verhalten durch Informationsasymmetrien zu unterbinden beziehungsweise bei Vertragsbruch die Rechte durchsetzen zu können. Diese Instanz bildet häufig der Rechtsweg ab. Ebenso können andere Intermediäre die Dienstleistung der Vertragsüberwachung gegen Entgelt anbieten.

Smart Contracts sind dagegen in der Lage, bestimmte Vertragsrisiken zu minimieren und die Vertragsausführung zusätzlich zu vereinfachen. Bei einem auf der Blockchain angelegten Smart Contract können die Vertragsparteien auf eine vertrauenswürdige dritte Instanz zur Überwachung der korrekten Vertragsausführung verzichten und diese durch den Consensus Mechanismus der Blockchain ersetzen.¹⁶² Dies bedeutet allerdings nicht, dass Smart Contracts keinerlei Vertrauen mehr benötigen. Vielmehr vertrauen die Beteiligten auf das dezentrale Netzwerk der Blockchain anstatt auf eine zentrale Instanz. Würde eine Vertragspartei von dem in der Blockchain bestätigten Smart Contract abweichen wollen, müsste sie dessen Code verändern. Eine einseitige Veränderung des Codes ist jedoch aufgrund der dezentralen Speicherung und der Erfordernis der Annahme durch die Mehrheit des Netzwerks nicht möglich. Beim Consensus Mechanismus erfolgt die Einigung über den Stand des Registers auf die

¹⁶² Ebenso *Kaulartz/Heckmann*, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, 618, 620.

längste Blockkette mit dem höchsten Proof-of-Work.¹⁶³ Sofern die Kontrolle des Netzwerks bei der Mehrheit der beteiligten Nodes liegt, die das Netzwerk nicht attackieren, kann der Smart Contract nicht manipuliert werden. Betrugsversuchen wird damit effektiv vorgebeugt. Folglich besteht ein deutlich geringeres Vertragsrisiko hinsichtlich eines Abweichens vom Vertragsinhalt. Die Schaffung dieser neuen Form von Vertrauen bedeutet ebenfalls, dass die Vertragsparteien sich nicht kennen müssen, um einen Smart Contract zu vereinbaren.. Somit bleibt die Pseudonymität – wie sie von Bitcointransaktionen bekannt ist – erhalten, falls dies gewünscht ist. Außerdem könne problemlos nachverfolgt werden, wie sich die Vertragspartner in vorangegangenen Aktivitäten verhalten haben.¹⁶⁴ Die Aktivitäten sind aufgrund der Speicherung in der Blockchain vor Manipulationen geschützt und tragen zur Transparenz des Prozesses bei.

Eine weitere wichtige Eigenschaft der Smart Contracts ist deren Autonomie, sobald sie hochgeladen und gestartet wurden.¹⁶⁵ Die Vertragsumsetzung erfordere keine weitere Interaktion zwischen den Vertragsparteien.¹⁶⁶ Eingeschränkt ist die Autonomie des Vertragscodes erst dann, wenn der Code auf Informationen außerhalb der digitalen Überprüfbarkeit Zugriff erhalten muss, um Aktivitäten ausführen zu können.¹⁶⁷ In

¹⁶³ Hierzu *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, 4.

¹⁶⁴ In Anlehnung an *Kölvart, et al.*, Smart Contracts, in: *The Future of Law and eTechnologies*, 2016, 133, 134.

¹⁶⁵ Vgl. *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 16.

¹⁶⁶ Vgl. *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 16.

¹⁶⁷ Hierzu *Kaulartz/Heckmann*, *Smart Contracts – Anwendungen der Blockchain-Technologie*, CR 2016, 618, 620.

diesem Fall sind manuelle Eingriffe über IT-Schnittstellen notwendig.¹⁶⁸ Sie ermöglichen eine Einspeisung der benötigten Daten in den Smart Contract. Eine Vielzahl von Informationen könnte hierunter fallen, wie beispielsweise Zustellbestätigungen für Waren oder lediglich postalisch vorliegende Dokumente. Die Transparenz der automatisch ausgeführten Vertragsbestandteile bedeutet damit auch, dass gegenseitig unerwünschte Überwachungen nicht mehr notwendig sind.¹⁶⁹ Insbesondere bei einer Ausgangslage mit Prinzipal-Agenten-Problem zwischen den Vertragspartnern ist dieser Aspekt von Bedeutung. Der Ausführungsmechanismus erübrigt eine Überwachung, sodass Kosten für das Monitoring, das unter anderem durch Intermediäre geleistet wird, eingespart werden können. Insgesamt profitieren die Nutzer von einer gestiegenen Rechtssicherheit, obwohl die programmierten Verträge auf eine Überwachung verzichten.¹⁷⁰ Weitere Kostensparnisse ergeben sich aus der Automatisierung, da zwangsläufig weniger menschliche Interventionen notwendig sind und weitestgehend auf Intermediäre verzichtet wird.¹⁷¹ Ebenfalls kostensenkend wirkt sich das geringere Fehlerrisiko aus, das häufig von manuellen Eingriffen ausgeht. Fehlerhaft eingegebene Daten wirken sich auf die Umsetzung aus, sodass falsche Prozessaktivitäten gestartet werden oder der Prozessablauf verzögert wird. Infolgedessen können beispielsweise

¹⁶⁸ Id.

¹⁶⁹ Ebenso *Juels, et al.*, *The Ring of Gyges: Using Smart Contracts for Crime*, arXiv 2015, 54, 55.

¹⁷⁰ Zustimmend *Kaulartz/Heckmann*, *Smart Contracts – Anwendungen der Blockchain-Technologie*, CR 2016, 618, 619.

¹⁷¹ Hierzu *Ream, et al.*, *Upgrading blockchains: Smart contract use cases in industry*, Deloitte University Press, 2016, 3.

Transaktionen über Bankkonten nicht ausgeführt werden, da bei der manuellen Eingabe der Kontodaten Fehler unterlaufen sind. Smart Contracts dagegen können diese Risiken effektiv minimieren und kostspielige Korrekturen vermeiden. Dies setzt allerdings voraus, dass bei der manuell ausgeführten Programmierung des zugrundeliegenden Codes keine Fehler unterlaufen. Auch diese würde der Smart Contract schließlich ausführen. Aus der geringen menschlichen Interaktion und Fehlerreduktion resultiert neben der Kostenreduktion ebenfalls ein Zeitersparnis für zahlreiche Geschäftsprozesse.¹⁷² Der Code des Smart Contracts leitet die gewünschten Prozesse ein, sobald er gestartet wurde und die vereinbarten Bedingungen erfüllt sind. Die Transaktionsabwicklung erfolgt mit weniger Intervention und wird somit beschleunigt. Resultierend aus den gesunkenen Transaktionskosten und der Prozessbeschleunigung bei der Vertragsausführung ergeben sich Chancen für neue Geschäftsmodelle.¹⁷³ Neben den bereits vorhandenen Prozessen, die durch die Automatisierung von Kosten- und Zeitersparnissen profitieren, können zuvor nicht umsetzbare oder unrentable Prozesskonzepte implementiert werden. Darunter fallen unter anderem Transaktionen, für welche ein schneller Leistungsaustausch benötigt wird. Ebenso können bestimmte Prozesse erst durch die Kostensenkung über Smart Contracts ein rentables Kosten-Nutzen-Verhältnis erzielen. Insofern profitieren die Nutzer nicht nur von der gestiegenen Rechtssicherheit durch die sichere, schnelle und günstige Vertragsausführung. Zusätzlich

¹⁷² Id.

¹⁷³ Id.

stehen ihnen neue Anwendungsmöglichkeiten zur Verfügung. Von den Vorzügen der Smart Contracts könnten allerdings auch Kriminelle profitieren, welche sich die positiv zu bewertende Rechtssicherheit für illegale Geschäfte zunutze machen. Die automatisierte Ausführung garantiere auch Kriminellen eine hohe Vertragssicherheit, sodass sie auf fragwürdige Reputation und potenziell von Ermittlern infiltrierte Vermittler verzichten könnten.¹⁷⁴ Die Möglichkeit der Pseudonymität im Blockchain-System und der Automatisierung verringere auch in diesem Fall die Interaktion zwischen den Vertragspartnern, was internationale Aktivitäten erleichtere und rechtsstaatliche Eingriffe erschwere.¹⁷⁵ Trotz der Gefahr des Missbrauchs zu illegalen Zwecken sollte der erhebliche Nutzen der Smart Contracts für die Gesellschaft im Vordergrund stehen. Zumal zahlreiche alltäglich genutzte Technologien nicht minder stark für betrügerische Zwecke genutzt werden. So gibt es bereits Cyberkriminalität, die jedoch ebenso wenig von der Nutzung des Internets für legale Anwendungen abschreckt. Folglich sollten angesichts der zahlreichen vielversprechenden Anwendungsmöglichkeiten diese Risiken ebenfalls nicht außer Acht gelassen werden. Nichtsdestotrotz versprechen Smart Contracts einen erheblichen Nutzensgewinn bei Vereinbarungen und Transaktionen.

¹⁷⁴ Hierzu *Juels, et al.*, *The Ring of Gyges: Using Smart Contracts for Crime*, arXiv 2015, 54, 55.

¹⁷⁵ Dazu *Juels, Ari, et al.*, *The Ring of Gyges: Using Smart Contracts for Crime*, arXiv 2015, 54, 55.

3. Ausgestaltung eines Smart Contracts: Datenorientierte Verträge

Smart Contracts basieren in ihrer Ausführung als Smart Contract Codes auf datenorientierten Verträgen. Sie werden als Verträge definiert, bei denen bestimmte oder alle Konditionen der Vereinbarung durch Computersysteme ausführbar sein sollen.¹⁷⁶ Im Folgenden werden technische Aspekte von programmierten Verträgen erläutert, um den Prozess näher zu beleuchten, der Smart Contracts zugrunde liegt. Zudem sollen Einschränkungen der Nutzungsmöglichkeiten beschrieben werden. Die hierbei gewonnenen Erkenntnisse sind entscheidend für eine rechtliche Bewertung von Smart Contracts und begründen die technischen Herausforderungen bei den diskutierten Anwendungsmöglichkeiten.

Wesentliche Bestandteile des Smart Contracts bilden die digital prüfbar Informationen und die rechtlich relevanten Handlungen, die der Smart Contract auf Basis der erhaltenen Informationen ausführt.¹⁷⁷ Um diese Handlungen ausführen zu können, muss ein Programm erstellt werden, das auf einer strukturierten Programmiersprache basiert und Computern die Verarbeitung von Informationen ermöglicht.¹⁷⁸ Dies bedeutet, dass präzise definierte Regeln bestimmen wie der Computer Daten extrahiert und welche Befehle ausgeführt

¹⁷⁶ Vgl. *Surden*, *Computable Contracts*, 46 U.C. Davis L. Rev. 629 (2012) at 639.

¹⁷⁷ Hierzu *Kaulartz/ Heckmann*, *Smart Contracts – Anwendungen der Blockchain-Technologie*, CR 2016, 618, 618.

¹⁷⁸ In Anlehnung an *Harper*, *Practical Foundations For Programming Languages*, Cambridge University Press, 2016, 100.

werden.¹⁷⁹ Die Vertragsbestandteile liegen somit nicht mehr in natürlicher Sprache, sondern als Code in strukturierten Daten vor. So wird sichergestellt, dass der Vertragstext maschinell lesbar ist. So beinhaltet der Code im Falle benötigter Zeitangaben nur ein genaues Datum anstelle von interpretierbaren textuellen Formulierungen. Nicht eindeutig umsetzbar für das Programm wären dagegen Zeitangaben, die von einer angemessenen Frist oder zeitnahen Ausführung sprechen.¹⁸⁰ Datenorientierte Verträge müssen gleichzeitig von den beteiligten Parteien und dem ausführenden System verstanden werden können.¹⁸¹ Smart Contracts sind demnach von elektronischen Verträgen zu unterscheiden, die lediglich den Vertragstext über digitale Kanäle übermitteln, da hierbei der Text nicht durch Computer verarbeitet werden kann.¹⁸² Darüber hinaus muss ein datenorientierter Vertrag nicht zwangsläufig eine Ausführung über ein dezentrales Netzwerk wie die Blockchain bedeuten. Vielmehr sind auch Konstruktionen mit vertrauenswürdigen Intermediären möglich.¹⁸³ Geeignet seien die datenorientierten Verträge jedoch nur für Vertragsszenarien, in denen ein geringes Maß an Unsicher-

¹⁷⁹ Ähnlich Stobart/Parsons, *Dynamic Web Application Development: Using PHP and MySQL*, Cengage Learning EMEA, 2008, 125-126.

¹⁸⁰ In Anlehnung an *Kaulartz/Heckmann*, *Smart Contracts – Anwendungen der Blockchain-Technologie*, CR 2016, 618, 620.

¹⁸¹ Hierzu *Surden*, *Computable Contracts*, 46 U.C. Davis L. Rev. 629 (2012) at 641.

¹⁸² Ähnlich *Surden*, *Computable Contracts*, 46 U.C. Davis L. Rev. 629 (2012) at 642.

¹⁸³ Vgl. *Szabo*, *Formalizing and Securing Relationships on Public Networks*, First Monday 1997, Ü. „Contracting Phases“.

heit, Komplexität und Abstraktion vorliegt.¹⁸⁴ Ausgeschlossen sind somit relationale Verträge, bei denen eine Reduktion relevanter Vertragsbestandteile auf konkret definierte Verpflichtungen nicht möglich ist.¹⁸⁵ Flexible Vereinbarungen, die der Unsicherheit geschuldet sind, müssen entweder mit zu überprüfbareren Daten zusätzlich aufwendig programmiert werden oder dürfen lediglich als textueller Vertragsbestandteil außerhalb des Codes bestehen bleiben, der im Fall unwahrscheinlicher Ereignisse anstelle des nicht ausführbaren Smart Contracts manuell veranlasst werden muss. Nur dann kann sichergestellt werden, dass die Intentionen der Vertragspartner korrekt als Code dargestellt und zu extrahierenden Informationen zur Vertragsausführung verarbeitet werden können. Hierfür muss von der sprachlichen Darstellung der Vereinbarungen auf deren Darstellung in Form von strukturierten Daten gewechselt werden. Gleichsam nutzt die Anwendung den Vertragstypen, die eng abgegrenzte Bedingungen und Folgen beinhalten und somit für die Vertragspartner routinierte Tätigkeiten ohne Gestaltungs- und Interpretationsspielraum darstellen. Dazu zählen beispielsweise Transaktionen über Derivate oder Swaps, bei denen die benötigten Finanzmarktdaten und Kontoinformationen problemlos digital erlangt werden können. Sie ermöglichen es den Vertragsparteien, genaue Kriterien festzulegen, die automatisch mit-

¹⁸⁴ Hierzu *Surden*, *Computable Contracts*, 46 U.C. Davis L. Rev. 629 (2012) at 637.

¹⁸⁵ In Anlehnung an *Goetz/Scott*, *Principles of Relational Contracts*, 67 Va. L. Rev. 1089 (1981) at 1091.

hilfe externer Datenquellen erfasst werden können.¹⁸⁶ Dabei ist nicht ausgeschlossen, dass auch in diesen Fällen zusätzlich ein Vertrag in textueller Form vorliegt.

Betrachtet man Smart Contracts auf der Blockchain, basieren diese auf kryptographisch gesicherten Protokollen. Sie schützen den Smart Contract sowohl vor Manipulationen der am Vertrag Beteiligten, als auch vor Eingriffen Dritter.¹⁸⁷ Das Protokoll selbst besteht aus Algorithmen, mit denen Sequenzen von Nachrichten zwischen Computern ausgeführt werden.¹⁸⁸ Dabei wird der Quellcode, der für die Beteiligten lesbar ist, in einen auf Netzwerken ausführbaren Computercode kompiliert.¹⁸⁹ Die Interaktionen zwischen den Computern sind für die Ausführung von Vertragsbedingungen zuständig. Beispielsweise erfolgen über die Nachrichten der Depotwechsel eines Wertpapiers und eine Abbuchung auf einem Girokonto als vereinbarte Gegenleistung. Nutzungsspezifische Blockchains wie die für Smart Contracts entwickelte Ethereum Blockchain unterscheiden sich dabei unter anderem im Hinblick auf den Nachrichtenfluss vom Bitcoin Netzwerk. Sowohl Bitcoin-Transaktionen, als auch Transaktionen über Ethereum können über externe Entitäten Nachrichten an andere Teilnehmer ausführen.¹⁹⁰ Die Bitcoin Blockchain könne zusätzlich

¹⁸⁶ In Anlehnung an *Surden*, *Computable Contracts*, 46 U.C. Davis L. Rev. 629 (2012) at 677.

¹⁸⁷ Hierzu *Szabo*, *Formalizing and Securing Relationships on Public Networks*, First Monday 1997, Ü. „Attacks against Smart Contracts“.

¹⁸⁸ Id., Ü. „Protocols“.

¹⁸⁹ Hierzu *von Haller Grønbaek*, *Blockchain 2.0, smart contracts and challenges*, Bird&Bird, twobirds.com, Artikel v. 16.06.2016.

¹⁹⁰ Dazu *Buterin*, *A Next Generation Smart Contract & Decentralized Application Plattform*, Ethereum White Paper, 2015, 14.

jedoch keine Nachrichten aus einem Vertrag generieren.¹⁹¹ Dies ist jedoch erforderlich, um Smart Contracts für Transaktionen nutzen zu können. Des Weiteren ist es in Ethereum möglich, Nachrichten um Daten zu ergänzen und erhaltene Nachrichten bei Vertragstransaktionen zu beantworten, so dass sie ebenfalls Funktionen einschließen könnten.¹⁹² Der Smart Contract wird durch den sogenannten Ethereum Virtual Machine Code dargestellt. Einzelne Bytes stellen dabei die Aktivitäten des Vertrags dar, welche auch in einer Endlosschleife ausgeführt werden könnten.¹⁹³ Plattformen wie Ethereum bieten somit auf die Ausführung von Smart Contracts ausgelegte Rahmenbedingungen, über welche die Bitcoin Blockchain aufgrund der fehlenden Integration von Daten und Smart Contracts in den Nachrichtenfluss nicht verfügt.

Ein weiterer wichtiger Bestandteil zur Ausgestaltung von datenorientierten Verträgen auf Grundlage der Blockchain liegt in der Verwendung von Oracles, auch Smart Oracles genannt, die eine Schnittstelle für eine vertrauenswürdige Datenversorgung aus der Umwelt zur Blockchain gewährleisten.¹⁹⁴ Sie fügen die jeweils für die Vertragsausführung notwendigen Signaturen in die Blockchain ein, sobald die aufgestellten Bedingungen eingetreten sind und in den Daten außerhalb

¹⁹¹ Id.

¹⁹² Id.

¹⁹³ Id., 17.

¹⁹⁴ Hierzu *Swanson*, *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*, 2015, 46.

der Blockchain bestätigt werden können.¹⁹⁵ Smart Oracles sind notwendig, da die Verträge auf der Blockchain lediglich über Transaktionen innerhalb des für andere Inputs unzugänglichen Systems der Blockchain funktionieren.¹⁹⁶ Um die benötigten Daten für den Smart Contract zur Verfügung zu stellen, erstellen die Oracles ebenfalls Transaktionen, die kryptografisch signiert sind und Umweltdaten in Codeform darstellen.¹⁹⁷ Sie agieren somit ähnlich zu den anderen Transaktionsbeteiligten. Von hoher Bedeutung für die korrekte Ausführung der Smart Contracts ist die Sicherstellung der Vertrauenswürdigkeit dieser Transaktionen.¹⁹⁸ Ein besonderes Augenmerk sollte daher auf der Qualität der Daten und deren Schutz vor Manipulation liegen.

4. Use Cases für Smart Contracts

Das gestiegene Interesse an der Blockchain-Technologie und Smart Contracts kommt in der Vielzahl an präsentierten Use Cases während der letzten zwei Jahre zum Ausdruck. Die diskutierten Anwendungsmöglichkeiten umfassen dabei unterschiedliche Branchen, unter anderem Finanzdienstleistungen,

¹⁹⁵ Hierzu *Thomas/Schwartz*, Smart Oracles: A Simple, Powerful Approach to Smart Contracts, github.com, Artikel v. 17.07.2014.

¹⁹⁶ In Anlehnung an *Buterin*, A Next Generation Smart Contract & Decentralized Application Plattform, Ethereum White Paper, 2015, 15.

¹⁹⁷ Hierzu *Thomas/Schwartz*, Smart Oracles: A Simple, Powerful Approach to Smart Contracts, github.com, Artikel v. 17.07.2014.

¹⁹⁸ In Anlehnung an *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, 46.

Telekommunikation, den Energiemarkt sowie den öffentlichen Sektor.¹⁹⁹ Eine Reihe von Unternehmensberatungen beteiligt sich an der Erstellung von Proof-of-Concepts, da Smart Contracts ein neues Geschäftsfeld darstellen. Daneben entwickeln Start-Ups Smart Contract Produkte und namhafte Unternehmen testen bereits erste Anwendungsfälle. So berichtete der Versicherungskonzern Allianz 2016 von einem erfolgreichen Pilotprojekt.²⁰⁰ Dabei wurden Katastrophen-Swaps und -anleihen in Form von Smart Contracts ausgegeben, sodass eine erhebliche Beschleunigung und Vereinfachung der Zahlungs- und Transaktionsprozesse zu beobachten sei.²⁰¹ Das Beispiel verdeutlicht, dass selbst hochentwickelte Prozesse wie der Handel mit Finanzinstrumenten und deren Abwicklung Verbesserungspotenziale für Smart Contracts bieten. Im Folgenden wird eine Auswahl von Use Cases für Smart Contracts für unterschiedliche Industriezweige analysiert und zu klärende Fragen für eine Umsetzung der spezifischen Anwendungen aufgeworfen. Die Auswahl soll einen Überblick über mögliche Anwendungsgebiete und das ökonomische Potential der Technologie schaffen.²⁰² Die folgenden Use Cases umfassen die Bereiche der Medientechnologie,

¹⁹⁹ Hierzu *Ream, et al.*, Upgrading blockchains: Smart contract use cases in industry, Deloitte University Press, 2016, 4.

²⁰⁰ Hierzu *Allianz*, Erfolgreiches Pilotprojekt: Allianz Risk Transfer und Nephila realisieren Katastrophen-Swap mit Blockchain-Technologie, Pressemeldung v. 15.06.2016, allianz.com.

²⁰¹ *Id.*

²⁰² Der Finanzsektor wird im weiteren Verlauf dieser Arbeit näher betrachtet, um der besonderen Bedeutung der Blockchain-Technologie für dessen Geschäftsprozesse gerecht zu werden.

der digitalen Identitätsverifizierung und der Gesundheitsbranche.

a) Dezentrales Vergütungssystem für Musikkünstler

Der erste vorgestellte Anwendungsfall aus dem Gebiet der Medientechnologie ist eine dezentrale Musikplattform, deren Vergütungssystem für die Künstler auf Intermediäre verzichtet und bereits als Testplattform in die Praxis umgesetzt wurde.²⁰³ Als Problematik wird angesehen, dass trotz der fortschreitenden globalen Digitalisierung und des digitalisierten Musikkonsums auf veraltete intermediäre Strukturen bezüglich der Vergütung aufgebaut werde.²⁰⁴ Zu diesen Intermediären gehören unter anderem Verwertungsgesellschaften sowie publizierende Administratoren.²⁰⁵ Als Teil der Wertschöpfungskette beanspruchen sie Anteile an den Erlösen von Musikstücken, sodass für die Künstler nach einem langwierigen Prozess geringere Umsatzanteile zur Verfügung stehen.²⁰⁶ Die dezentralisierte Plattform ermöglicht dagegen den Künstlern, ihre Werke als Teil eines Smart Contracts auf die Ethereum Blockchain zu stellen, der Bedingungen zu unterschiedlichen

²⁰³ Informationen über die Plattform unter ujomusic.com, Stand: 18.02.2017.

²⁰⁴ Hierzu *Ujo Music, The Problem*, theproblem.wtf, Stand: 18.02.2017.

²⁰⁵ Vgl. *Ujo Music, The Problem*, theproblem.wtf, Stand: 18.02.2017.

²⁰⁶ In Anlehnung an *Matilla, The Blockchain Phenomenon*, ETLA Working Papers No. 38, 2016, 15.

Nutzungsmöglichkeiten und der Gewinnverteilung enthält.²⁰⁷

Kauft ein Nutzer den Titel, erfolgt direkt die Bezahlung in Form der Ethereum Kryptowährung.

Die Smart Contracts ermöglichen eine kürzere Wertschöpfungskette, die zu Kostenersparnissen und höheren Erlösen für die Künstler führt. Dieser besitzt zudem eine bessere Kontrolle über sein künstlerisches Werk. Ebenso könnten die Gestaltung flexibler Kaufmöglichkeiten für einzelne Musikstücke im Smart Contract und die voraussichtlich niedrigeren Endpreise einen Beitrag zur Bekämpfung illegaler Downloads beitragen. Trotz der Prozessoptimierung sind kritische Aspekte zu berücksichtigen. Zunächst einmal wird die dezentralisierte Plattform nicht in das bestehende Verwertungssystem implementiert, sondern steht zu diesem im Wettbewerb. Wie auch bei anderen Plattformen wird jedoch für einen erfolgreichen Marktzugang eine kritische Nutzermenge benötigt, um sich dauerhaft am Markt behaupten zu können. Eine Vielzahl von technisch bereits integrierten Onlinestreaming-Diensten erschwert den Gewinn einer hohen Nutzerzahl. Sinnvoll wäre es daher, die dezentralisierte Plattform stattdessen als Zahlungsplattform der Streaming-Dienste umzusetzen. Darüber hinaus treten Intermediäre wie Plattenfirmen nicht nur als Vermittler auf. Neben der Vermarktung tragen sie bei unbekanntem Künstlern die finanziellen Risiken eines Misserfolgs. Hohe Umsatzanteile aus den Smart Contracts sind daher eher für diejenigen Künstler möglich, die bereits große Bekanntheit und einen hohen Marktwert aufweisen, und somit einen ge-

²⁰⁷ Hierzu *Matilla*, The Blockchain Phenomenon, ETLA Working Papers No. 38, 2016, 15.

ringen Anteil für die Plattenfirmen im Smart Contract erstreiten können. Fraglich ist vielmehr die Stellung der Verwertungsgesellschaften. Sie könnten aus dem Prozess von der Schaffung eines Musikwerks bis zur Nutzung durch Endkunden entfernt werden. Hierfür müssten jedoch für zahlreiche Nutzungsmöglichkeiten erst wieder die Urheberrechte zurückerlangt werden, die an Verwertungsgesellschaften übertragen wurden.²⁰⁸ Erst dann können die Smart Contracts weitreichende Nutzungsrechte verwalten. Es ist somit damit zu rechnen, dass vor einer tiefgreifenden Veränderung der Wertschöpfungskette ein langwieriger Übergangsprozess bei der Rechteübertragung und zur flächendeckenden Akzeptanz notwendig sein wird.

b) Verwaltung digitaler Identitäten

Ein weiterer Anwendungsfall befasst sich mit der Verwaltung von digitalen Identitäten auf der Blockchain. Derzeit werden Kundendaten bei der Eingabe für eine Kundenregistrierung umfangreich von den jeweiligen Unternehmen geprüft, bevor erstellte Aufträge des Individuums ausgeführt werden. Die Daten müssen aufgrund der Vielzahl an unterschiedlichen Kundenkonten von den Nutzern wiederholt eingegeben werden und bleiben bei den Unternehmen gespeichert. Die gegenwärtige Verfahrensweise führt jedoch zu Nachteilen für

²⁰⁸ Bspw. führt die deutsche Verwertungsgesellschaft GEMA in ihrem Berechtigungsvertrag die umfangreichen zu übertragenden Urheberrechte während der Vertragsdauer auf. Vgl. *GEMA*, Berechtigungsvertrag Fassung April 2016, § 1, gema.de, Stand: 20.02.2017.

beide Transaktionsseiten. Der Prozess erfordere eine kosten- und zeitintensive Datenüberprüfung durch das betroffene Unternehmen, um Betrug und Missbrauch zu unterbinden.²⁰⁹ Nicht sichergestellt ist dabei, ob falsche Daten tatsächlich erkannt werden. Zudem trage das Unternehmen die Verantwortung für den Schutz der zentral gespeicherten Daten vor Hackern, während der Kunde die Kontrolle über seine Daten verliere und auf die Sicherheit bei einem Dritten vertrauen müsse.²¹⁰

Das Konzept der digitalen Identität versucht diese Probleme zu lösen, indem sie vertrauenswürdige Online-Identitäten ermöglicht. Hierfür registriert der Nutzer eine Smart ID in Form eines Smart Contracts und ergänzt diesen mit Attributen zu seiner Identität.²¹¹ Dabei kann es sich beispielsweise um Reisepässe, Personalausweise, Führerscheine, Mitgliedsausweise, Kontodaten, aber auch Eigentumsbelege handeln. Zudem wird ausgewählt, welche Privatsphäreinstellungen eingerichtet werden sollen. So sind diese im Smart Contract grundsätzlich privat und daher nicht öffentlich einsehbar, können jedoch nach Wunsch für Berechtigte zur Einsicht freigegeben werden.²¹² Der Nutzer verfügt dabei analog zu anderen Transaktionen einen öffentlich zugänglichen und einen privaten Schlüssel. Damit die hochgeladenen Daten entsprechend verifiziert werden können, müssen diese jedoch von einer

²⁰⁹ Vgl. *Chamber of Digital Commerce*, Smart Contracts: 12 Use Cases for Business & Beyond, White Paper, 2016, 15.

²¹⁰ Id.

²¹¹ In Anlehnung an *Deloitte*, Smart ID, deloitte.co.uk, Stand: 24.02.2017.

²¹² Hierzu *Deloitte*, Smart ID, deloitte.co.uk, Stand: 24.02.2017.

vertrauenswürdigen dritten Instanz bezüglich ihrer Echtheit bestätigt werden, da lediglich deren Existenz auf der Blockchain keinen Beweis hierfür darstellt.²¹³ Hierfür geeignet wären beispielsweise staatliche Behörden, die bei der Ausgabe neuer Dokumente die Smart ID bestätigen. Ebenso geeignet sind Banken. Diese bieten bereits umfangreiche Digital Identity Überprüfungen an, die sie aufgrund von rechtlichen Anforderungen und wirtschaftlichen Interessen durchführen.²¹⁴ Möchte ein Kunde zum Beispiel Onlinedienste der Bank in Anspruch nehmen, muss er umfassende Auskünfte zu seiner Person abgeben. Eröffnet ein Kunde ein neues Konto oder schaltet das Online-Banking frei, bestätigt die Bank nach ihrer Identitätsprüfung diejenigen Identitätsattribute in der Blockchain, die sie überprüft hat.²¹⁵ Ähnlich gut geeignet sind Telekommunikationsanbieter. Sie könnten die Identitätsprüfung als Teil ihres Geschäftsmodells in Form einer Smartphone-App gestalten.²¹⁶ Tätige der Nutzer beispielsweise Käufe über sein Smartphone, könnte die App die Identität des Nutzers für den Verkäufer gegen Gebühr verifizieren.²¹⁷ Die Identifizierung bietet Vorteile sowohl für die Nutzer, als auch die beteiligten Unternehmen. Die Kunden profitieren durch die vollständige Kontrolle über ihre persönlichen Daten, die sie bedarfsabhängig für Unternehmen freigeben können, ohne wiederholte

²¹³ Hierzu *Deloitte*, Smart ID, deloitte.co.uk, Stand: 24.02.2017.

²¹⁴ Hierzu *Matilla*, The Blockchain Phenomenon, ETLA Working Papers No. 38, 2016, 13.

²¹⁵ Ähnlich *Deloitte*, Smart ID, deloitte.co.uk, Stand: 24.02.2017.

²¹⁶ Hierzu *Monitor Deloitte*, Blockchain @ Telco – How Blockchain can impact the telecommunication industry and its relevance to the C-suite, 2016, 12.

²¹⁷ Id.

Eingaben tätigen zu müssen.²¹⁸ Die beteiligten Unternehmen müssen wiederum keine kostenintensiven Sicherheitsvorkehrungen für die sichere Kundendatenspeicherung tragen, die durch die zentralen Speicherort Angriffspunkte für Hacker bietet.²¹⁹ Somit gewährleisten die flexibel erweiterbaren Smart Contracts die Kontrolle über die eigenen Daten und geringere Transaktionskosten durch Einsparungen bei der Eingabe personenbezogener Daten und deren Überprüfung. Für eine erfolgreiche Etablierung digitaler Identitäten für online getätigte Transaktionen sollten jedoch die folgenden Aspekte berücksichtigt werden. Zunächst müsste die Verifizierung der Daten in den Smart Contracts für die ausführenden Beteiligten ein profitables Geschäftsmodell darstellen. Verifiziert beispielweise eine Bank die Daten im Zuge einer Kontoeröffnung, wird sie Interesse daran haben, die Verifizierungsdienstleistung nicht kostenlos für Dritte zur Verfügung zu stellen. Vielmehr wird eine Gebühr nötig sein, die entweder der Identitätsinhaber bei der Verifizierung oder andere Unternehmen beim Zugriff auf die Bestätigung bezahlen müssen. Hierbei werde die Interoperabilität der verschiedenen Systeme zwischen den beteiligten Einheiten eine Herausforderung darstellen.²²⁰ Kritisch ist auch die Festlegung der vertrauenswürdigen Instanzen bezüglich der Eignung und wie sie als solche in das System integriert werden. Zuerst müsste eine Bestätigung der Unternehmen stattfinden, die zur Verifizierung berechtigt sein sollen. Ebenso sollte bedacht werden,

²¹⁸ Hierzu *Chamber of Digital Commerce*, Smart Contracts: 12 Use Cases for Business & Beyond, White Paper, 2016, 16.

²¹⁹ Id.

²²⁰ Id.

dass digitale Identitäten ähnlich wie die bestehenden Sicherheitsvorkehrungen Betrug nicht gänzlich ausschließen können. Die Schwachstelle liegt hierbei bei den privaten Schlüsseln, die gestohlen werden und zum Missbrauch der digitalen Identität führen könnten. Ein Ersatz von echten Dokumenten außerhalb digital durchgeführter Transaktionen oder anderer Vertragsabschlüssen ist somit nicht wünschenswert. Digitale Identitäten können jedoch den Prozess für online getätigte Transaktionen vereinfachen und stellen in diesem Bereich eine sinnvolle Anwendung dar.

c) Dezentrale Plattform für Gesundheitsdaten

Ein weiteres mögliches Einsatzgebiet für Smart Contracts bietet das Gesundheitswesen bezüglich der organisationsübergreifenden Verwaltung und des Austauschs von Patienteninformationen. Der derzeitige Datenaustausch zwischen verschiedenen Gesundheitsorganisationen gilt als ineffizient und wenig digitalisiert: Um Patientendaten speichern und verwenden zu dürfen, müsse über den Patienten eine schriftliche Einverständniserklärung erlangt werden; eine Prüfstelle entscheide daraufhin über die Datennutzung der einzelnen Fälle durch andere Organisationen wie Krankenhäuser oder zu Forschungszwecken.²²¹ Möchte eine Organisation auf die Daten zugreifen, muss sie diese direkt bei den jeweiligen Einheiten anfragen und übermitteln lassen. Der Prozess ist zeitintensiv und bürokratisch, was gravierende Folgen für die

²²¹ In Anlehnung an *Chamber of Digital Commerce, Smart Contracts: 12 Use Cases for Business & Beyond, White Paper, 2016, 36.*

Patienten und die Bevölkerung haben kann. Für die Patientenversorgung könnten die Zeitverzögerungen und Hürden unterschiedlicher Datensysteme zu verspäteten Reaktionen auf Epidemien und fehlenden Daten für exakte Nutzenanalysen von Therapien zur Folge haben.²²² Die Patienten sind dabei kaum in den weiteren Verlauf ihrer Daten eingebunden. Sie müssen vielmehr auf den Datenschutz bei den Organisationen und unbekanntem Dritten vertrauen, wobei der bürokratische Aufwand eine Rücknahme der Einverständniserklärung erschwert.²²³

Der Prozess kann jedoch mithilfe von Smart Contracts vereinfacht und auf der Blockchain abgebildet werden. Gesundheitsorganisationen wie Krankenhäuser dokumentieren die klinischen Daten zunächst in ihren eigenen IT-Systemen und leiten sie zusammen mit einer öffentlichen ID für den jeweiligen Patienten über Programmierschnittstellen an die Blockchain weiter.²²⁴ Die Schnittstellen ermöglichen dabei die weitere Nutzung der bestehenden Infrastrukturen der Organisationen. Smart Contracts verarbeiten die eingehenden Transaktionen auf Grundlage der Einverständniserklärung des Patienten und der öffentlichen Patienten ID, sodass sie auf der

²²² Id.

²²³ Die Gefahr des Datenmissbrauchs allein in den USA zeigt sich in 112 Mio. gehackten Gesundheitsdaten im Jahr 2015. Vgl. *U.S. Department of Health & Human Services – Office for Civil Rights, Breaches Affecting 500 or More Individuals*, ocrportal.hhs.gov, Stand: 24.02.2017.

²²⁴ Hierzu *Krawiec, et al., Blockchain: Opportunities for Health Care*, Deloitte, 2016, 5.

Blockchain gesichert werden können.²²⁵ Die anonymisierten Patientendaten können nun von dritten Gesundheitsorganisationen und Forschungsgruppen eingesehen und analysiert werden. Hierfür nutzen diese wiederum Programmierschnittstellen zur Datenbankabfrage.²²⁶ Der private Schlüssel, der die Identität der Patienten mit den Daten in der Blockchain verknüpft, verbleibt bei dem Patienten.²²⁷ Sie können ihre Identität nach Wunsch für andere Organisationen freigeben, indem sie den privaten Schlüssel zur Verfügung stellen. Sogenannte Identity Permission Layers innerhalb der Blockchain entstehen, welche den Datenzugriff des jeweiligen privaten Schlüssels abbilden.²²⁸ Beispielsweise könnten andere Ärzte somit einen umfassenden Einblick in die Kranken- und Behandlungsakte des Patienten erlangen, ohne auf Auskünfte vorheriger Ärzte angewiesen zu sein. Vorstellbar wäre auch die Freigabe gegen Gebühr an Dritte, welche die Daten für Forschungszwecke erwerben wollen. Aus dieser Möglichkeit ergebe sich das Potenzial für eine neue Form des anreizbasierten Datenhandels.²²⁹ Im Vergleich zum gegenwärtigen Modell sei eine beschleunigte und vereinfachte organisationsübergreifende Datenverfügbarkeit feststellbar. Diese könne sowohl im Ernstfall zu einem schnellen Informationsaustausch bei Epidemien genutzt werden, als auch Vorbereitungspro-

²²⁵ Ähnlich *Krawiec, et al.*, Blockchain: Opportunities for Health Care, Deloitte, 2016, 5.

²²⁶ Vgl. *Krawiec, et al.*, Blockchain: Opportunities for Health Care, Deloitte, 2016, 5.

²²⁷ Id.

²²⁸ Hierzu *Krawiec, et al.*, Blockchain: Opportunities for Health Care, Deloitte, 2016, 7.

²²⁹ Id., 36.

zesse für Behandlungen und Tests vereinheitlichen.²³⁰ Dabei profitieren die Beteiligten vom direkten Datenzugang und der automatisierten Erfassung und Verfolgung der Patienteneinwilligung. Zusätzlich ist es möglich, den Smart Contract um benutzerdefinierte Schreib- und Leseerlaubnisse bezüglich der Patientendaten zu erweitern.²³¹ Eine Annahme von Änderungen erfordert wiederum die Zustimmung der Mehrheit der Netzwerkteilnehmer, sodass manipulierte Daten sofort auffallen würden. Somit lässt sich sicherstellen, dass nur autorisierte Personen oder Institutionen Änderungen vornehmen oder Einsicht in die Patientendaten erlangen. Der Diebstahl von Daten zur Identifizierung wird wiederum durch die Notwendigkeit des privaten Schlüssels erschwert, da nicht ein zentraler Datenspeicher angreifbar wäre, sondern die einzelnen Schlüssel erlangt werden müssen. Folglich wird ein hohes Maß an Datenschutz und -sicherheit für die Patienten gewährleistet.²³² Darüber hinaus besitzt der Patient aufgrund des privaten Schlüssels und der automatisierten Einwilligung im Smart Contract eine weitaus bessere Kontrolle über die Verwendung seiner Daten. Er könnte anhand dessen auch selbst die umfangreiche Dateneinsicht nutzen und somit sein Recht auf Akteneinsicht besser durchsetzen.²³³ Die Erweite-

²³⁰ Id., 36.

²³¹ In Anlehnung an *EY*, *Blockchain in health – How distributed ledgers can improve provider data management and support interoperability*, 2016, 6.

²³² Ebenso *Chamber of Digital Commerce*, *Smart Contracts: 12 Use Cases for Business & Beyond*, White Paper, 2016, 36.

²³³ In Deutschland haben Patienten nach § 630g I BGB das Recht, auf Verlangen unverzüglich ihre vollständige Patientenakte einsehen zu dürfen.

rung der bestehenden IT-Infrastruktur um eine Blockchain als interoperables Datenlager zum effizienten institutionsübergreifenden Datenaustausch liefert einen Beitrag zu einer besseren Patientenversorgung sowie einen erleichterten Datenzugang zu Forschungszwecken. Patienten sind dabei stärker in den Prozess um die Nutzung ihrer Daten eingebunden.

Anzumerken ist jedoch, dass die genannten Vorteile in ihrem vollen Umfang nur dann realisiert werden können, wenn die Daten vollständig in der Blockchain gespeichert werden können. Demnach müssten speicherintensive Daten wie beispielsweise Tomographieaufnahmen oder Geninformationen ebenfalls in der Blockchain abgelegt werden, um direkte Datenabfragen zwischen Organisationen abzuschaffen. Dies hat jedoch aufgrund der zu verarbeitenden Datenmenge längere Verarbeitungszeiten für neue Blöcke in der Blockchain zur Folge, sodass die Skalierbarkeit des dezentralisierten Systems an Grenzen stoße.²³⁴ Als Lösung bieten sich kryptografisch gesicherte Verknüpfungen zu den zentral gespeicherten Daten an, da sie wenig Speicherplatz benötigen.²³⁵ Eine Speicherung außerhalb der Blockchain habe jedoch zur Folge, dass Daten nicht mehr direkt abrufbar wären, sondern der Zugriff über die innehabende Organisation und weitere integrierende Layers erfolgen müsste.²³⁶ Der Prozess würde somit wieder mehr Zeit in Anspruch nehmen und die Patientendaten an

²³⁴ Hierzu *EY*, Blockchain in health – How distributed ledgers can improve provider data management and support interoperability, 2016, 10.

²³⁵ Dazu *Krawiec, et al.*, Blockchain: Opportunities for Health Care, Deloitte, 2016, 6.

²³⁶ Hierzu *Krawiec, et al.*, Blockchain: Opportunities for Health Care, Deloitte, 2016, 6.

den zentralen Speicherorten beispielsweise nicht mehr vor Datenverlusten oder Missbrauch geschützt werden. Aus diesen Gründen wird vorgeschlagen, eine kombinierte Blockchainspeicherung zu nutzen, bei der standardisierte Daten in der Blockchain gesichert werden, während dazugehörige große Datenpakete lokal gespeichert und über Links bedarfsabhängig angefragt werden.²³⁷ Folglich könnte sichergestellt werden, dass medizinische Informationen in Notfällen schnell verfügbar wären und ein Großteil der Daten vor fremden Zugriffen in der Blockchain geschützt werden könnte.

Kritisch bleibt jedoch, dass standardisierte Daten, unter anderem Geschlecht, Alter, Kranken- und Behandlungshistorie über den Smart Contract öffentlich einsehbar sind, sofern nicht abschließende Zugriffsrechte programmiert wurden. Bei seltenen Krankheiten oder geografischen Gruppen von geringer Personenanzahl könnten unter Umständen mithilfe statistischer Methoden Rückschlüsse auf die Identität des Patienten erlangt werden. Ein adäquater Datenschutz wäre somit nicht möglich. Es ist daher sinnvoll, für Anwendungsfälle im Gesundheitswesen eine Permissioned Blockchain anzustreben, um den Zugriff von vornherein einzuschränken.²³⁸ So könnte der Zugang an bestimmte wissenschaftliche Qualitäts- und Datenschutzkriterien geknüpft werden. Als Mitglieder der geschlossenen Blockchain kommen dabei Kliniken, Arztpraxen, Gesundheitsbehörden und Forschungseinrichtungen in

²³⁷ Dazu *Krawiec, et al.*, Blockchain: Opportunities for Health Care, Deloitte, 2016, 6.

²³⁸ Zustimmung *EY*, Blockchain in health – How distributed ledgers can improve provider data management and support interoperability, 2016, 7.

Frage. Neben der Konzeption als zugangsbeschränkte Blockchain mit einer ausreichend großen Computerleistung zur Verarbeitung der Datenblöcke wird die Interoperabilität der Datensysteme eine große Herausforderung für den Anwendungsfall darstellen.²³⁹ Da verschiedene Systeme für den medizinischen Prozessablauf unabdingbar sind, müssen Teilnehmer die Bereitschaft zur Implementierung neuer Programmierstellen aufbringen. Zusätzlich muss eine effiziente Datenabfrage gewährleistet werden, welche die typischerweise multidimensionalen Anfragen und damit verbundenen Operationen auch aus der Blockchain heraus bewältigen muss.²⁴⁰ Smart Contracts für klinische Daten bieten dennoch unter Berücksichtigung der zu nehmenden Hürden wie bei den meisten Blockchainanwendungen ein hohes Potenzial für Kosten- und Zeitersparnisse bei der organisationsübergreifenden Datennutzung.

Insgesamt unterstreichen die drei vorgestellten Use Cases sowohl den potenziellen Nutzen für unterschiedliche Geschäftsprozesse, als auch die Hürden der Interoperabilität. Die Ermöglichung von Smart Contracts wird dabei entscheidend von der Umsetzung vertrauenswürdiger Schnittstellen abhängen, die den Smart Contract mit Informationen außerhalb der Blockchain versorgen.²⁴¹ Ebenso wird es in vielen Fällen sinnvoll sein, eine Permissioned Blockchain einzufüh-

²³⁹ Id., 10.

²⁴⁰ In Anlehnung an *Nguyen*, *Complex Data Warehousing and Knowledge Discovery for Advanced Retrieval Development: Innovative Methods and Applications*, 2010, 138.

²⁴¹ Ebenso *Ream, et al.*, *Upgrading blockchains: Smart contract use cases in industry*, Deloitte University Press, 2016, 6.

ren, um die Skalierbarkeit und den Schutz der Daten vor unerwünschtem Zugriff zu gewährleisten. Handelt es sich jedoch um tragfähige Geschäftsmodelle, die monetäre Anreize zur Bereitstellung und Nutzung der Smart Contracts schaffen, wird es sehr wahrscheinlich zu einer Umsetzung der dezentralen und weniger auf Intermediäre aufbauenden Prozesse kommen.

5. Ausführung des Vertragsinhalts am Beispiel eines Kaufvertrags

Im Kontext mit Smart Contracts wird diskutiert, ob und in welchen Fällen die Codes einem rechtlichen Vertrag gleichgestellt werden können. Es ist zu klären, ob der Aussage „Code is Law“²⁴² zugestimmt werden kann und welche Auswirkungen dies auf die tatsächliche Vertragspraxis haben könnte. Neben der Beantwortung dieser Fragen ist es jedoch sinnvoll, grundlegende Rechtsgrundsätze von typischen Verträgen auf ihre Übertragbarkeit für Smart Contracts zu untersuchen.²⁴³ Einen solchen gängigen Vertragsfall stellen Kaufverträge dar. Im Folgenden wird deren Umsetzung über Smart Contracts im Kontext des deutschen Trennungs- und Abstraktionsprinzips im Vergleich zu ausländischen Rechtsgrundsätzen simuliert. Zu klären ist hierbei, ob unter der Annahme der Vertragseigenschaft Smart Contracts einen adäquaten Ersatz für einen üblichen Kaufvertrag darstellen.

²⁴² Vgl. *Lessig, Code – Version 2, 2006, 5.*

²⁴³ In Anlehnung an *Lessig, Code – Version 2, 2006, 6.*

a) Ausführung unter Anwendung des Trennungs- und Abstraktionsprinzips

Bei der Schließung eines Kaufvertrags und der anschließenden Eigentumsübertragung stellen das im deutschen Recht praktizierte Abstraktionsprinzip und Trennungsprinzip wesentliche Grundsätze dar. Das Trennungsprinzip, das auf dem Traditionsprinzip beruht, besagt, dass zwischen dem Verpflichtungsgeschäft und dem Verfügungsgeschäft unterschieden werden muss.²⁴⁴ Sie stellen separat zu betrachtende Rechtsgeschäfte dar.²⁴⁵ Bei einem Kaufvertrag nach § 433 BGB handelt es sich um ein Verpflichtungsgeschäft. Hierbei verpflichtet sich der Verkäufer nach § 433 I BGB zur Übergabe und Übereignung der verkauften Sache, während sich der Käufer nach § 433 II BGB zur Abnahme der Sache und der Kaufpreiszahlung verpflichtet. Erst mit dem Verfügungsgeschäft, beispielsweise durch Einigung und Übergabe nach § 929 BGB, kommt eine Rechtsänderung zustande. Auf dem Trennungsprinzip baut das Abstraktionsprinzip auf, wonach Verpflichtungs- und Verfügungsgeschäft in ihrer Wirksamkeit unabhängig voneinander betrachtet werden müssen.²⁴⁶ Von besonderer Bedeutung ist diese Unabhängigkeit, wenn das Verpflichtungsgeschäft und dessen Erfüllung auseinanderfallen.²⁴⁷ Das Auseinanderfallen liegt typischerweise nicht bei alltäglichen Barkäufen ohne besondere Vertragsklauseln, sondern bei aufwendigeren Kaufverträgen vor. Das Abstrakti-

²⁴⁴ Hierzu *Oechsler* in MüKoBGB, § 929 Rn. 5.

²⁴⁵ Vgl. *Oechsler* in MüKoBGB, § 929 Rn. 5.

²⁴⁶ Hierzu *Oechsler* in MüKoBGB, § 929 Rn. 8.

²⁴⁷ In Anlehnung an *Oechsler* in MüKoBGB, § 929 Rn. 11.

onsprinzip fördert die Rechtssicherheit, da das Verfügungsgeschäft unabhängig von Mängeln des Verpflichtungsgeschäfts ist.²⁴⁸

Betrachtet man einen Kaufvertrag, der mithilfe eines Smart Contracts geschlossen wurde, müssten das Verpflichtungs- und das Verfügungsgeschäft nach den genannten Grundsätzen ebenfalls unterscheidbar und unabhängig voneinander wirksam sein. Ausgegangen wird hierfür zunächst, dass die Vertragsparteien einzig auf Grundlage eines Smart Contracts einen Kaufvertrag schließen. Technisch soll dabei die Möglichkeit bestehen, Zahlungs- und Versandprozesse weitestgehend automatisiert abzuwickeln. Beispielhaft handelt es sich um eine bewegliche Sache, die von dem Verkäufer an den Käufer versendet werden soll und die der Käufer per Überweisung bezahlen möchte, sodass es sich nicht um einen Handkauf handelt.²⁴⁹ Der Kaufvertrag besteht entsprechend aus codierten Bestandteilen und basiert nicht auf natürlicher Sprache wie ein schriftlich oder mündlich geschlossener Kaufvertrag. Die Vertragsparteien codieren in dem Smart Contract die zu zahlende Geldsumme einschließlich des Befehls zur Belastung des Kontos des Käufers und Überweisung auf das Konto des Verkäufers in Höhe des Betrags. Dieser Bestandteil des Codes stellt einen Teil der Verpflichtung des Käufers dar. Ein weiterer Code beinhaltet den Befehl zur Initiierung des Versands an die im Smart Contract angegebene Adresse des Käufers. Dies ist wiederum ein Teil der Verpflichtung des Verkäufers. Das dezentrale Netzwerk bestätigt den Smart

²⁴⁸ Ähnlich *Oechsler* in MüKoBGB, § 929 Rn. 11.

²⁴⁹ In Anlehnung an *Oechsler* in MüKoBGB, § 929 Rn. 11.

Contract in einem Datenblock auf der Blockchain und die abgebildeten Transaktionen werden automatisch ausgeführt. Der Smart Contract löst über Schnittstellen die Überweisung des Kaufpreises und den Versand der Sache aus. Mit der Ausführung erfolgt somit das Verfügungsgeschäft.

Zu klären ist nun, ob das Trennungsprinzip und das Abstraktionsprinzip im Smart Contract umgesetzt werden können. Die Einigung über die Rechte und Pflichten der Vertragspartner beim Kausalgeschäft auf Ebene des Smart Contracts basiert auf den identischen Codebestandteilen, die für das Verfügungsgeschäft genutzt werden. Da der Code Transaktionen durchführt und nicht lediglich schuldrechtliche Aspekte konstituiert, könnte der Code daher ebenso die Einigung und Übergabe des abstrakten Geschäfts wiedergeben. Erfasst man die automatische Ausführung des Codes als Verfügungsgeschäft, bleibt unklar, an welcher Stelle das Verpflichtungsgeschäft abzugrenzen ist. Es fehlt an einer anderen Form der schuldrechtlichen Vereinbarung außerhalb der Programmierung des Smart Contracts, die nicht automatisch die Ausführung auslöst. Ein Ansatzpunkt könnte die Zeitspanne zwischen dem Hochladen des signierten Smart Contracts in den Datenblock in der Blockchain und dem Start der Vertragsausführung sein. Bevor die Transaktionsdaten nicht durch das Netzwerk im Datenblock bestätigt wurden, erfolgt keine Durchführung der Transaktion. Somit kann bis zu diesem Zeitpunkt von einem Verpflichtungsgeschäft als Code ausgegangen werden. Die Trennung zwischen Kausalgeschäft und abstraktem Geschäft könnte folglich auch bei strikt automatisierten Smart Contracts auf einer Blockchain umsetzbar sein. Aus der Trennbarkeit der beiden Geschäfte lässt sich allerdings nicht

auf die Unabhängigkeit der beiden Rechtsgeschäfte schließen, da eine Unterscheidung auch möglich ist, falls bei der Wirksamkeit eine Abhängigkeit besteht.²⁵⁰ Eine solche Abhängigkeit könnte auf einen automatisierten Kaufvertrag zutreffen. Maßgeblich hierfür ist der Grad an Kontrolle, die der Consensus Mechanismus durch die Bestätigung der Transaktion erzeugt. Hierzu wird in dem besagten Fall überprüft, ob der Smart Contract ausgeführt werden kann. Dabei kann zum Beispiel validiert werden, dass genug Bitcoins zur Bezahlung vorhanden sind. Ist das Netzwerk zusätzlich in der Lage, die Verfügungsmacht des Verkäufers zu überprüfen, indem der Eigentumsverlauf auf der Blockchain zurückverfolgt wird, müsste auch diese Bedingung bestätigt werden, bevor der Datenblock mit dem Smart Contract entsteht und der Inhalt ausgeführt wird.²⁵¹ Liegt keine Verfügungsmacht des Verkäufers vor, kommt es zu unterschiedlichen Ergebnissen bezüglich der Wirksamkeit der Rechtsgeschäfte. Im Normalfall gilt dann, dass zwar das Verpflichtungsgeschäft unwirksam, aber das Verfügungsgeschäft dennoch wirksam sein kann. Der Smart Contract wird dagegen nicht akzeptiert, sodass kein Verfügungsgeschäft zustande kommt. Es liegt in diesem Fall eine Abhängigkeit bezüglich der Wirksamkeit vor. Hier schützt der Smart Contract über einen alternativen Mechanismus die Käufer wie der gegebene Verkehrsschutz von Zweiterwerbbern beim Abstraktionsprinzip.²⁵² Allerdings ist anzumerken, dass

²⁵⁰ In Anlehnung an *Oechsler* in MüKoBGB, § 929 Rn. 5.

²⁵¹ Hierbei muss es sich nicht zwingend um Objekte handeln, die durch Smart Contracts kontrolliert werden. Hierzu unter Gliederungspunkt D. II.

²⁵² In Anlehnung an *Oechsler* in MüKoBGB, § 929 Rn. 10.

die Abhängigkeit der Rechtsgeschäfte nur für einen Smart Contract mit besagten Kontrollfähigkeiten gilt. Andernfalls würde der Smart Contract das Eigentum erst bei der automatischen Bestätigung zum Erhalt der Ware übertragen und nicht bereits zu einem früheren Zeitpunkt.²⁵³ Wäre dies bei dem Kaufvertrag nicht der Fall, käme es zu einem zeitlichen Auseinanderfallen des tatsächlichen Zeitpunkts des Erwerbs des Eigentums und des Eigentümerwechsels auf der Blockchain. Kann die fehlerhafte Eigentumszuordnung nicht erfasst werden, dann bliebe trotz Unwirksamkeit des Verpflichtungsgeschäfts die Verfügung wirksam. Die ausgeführten Transaktionen des Smart Contracts und damit der Code hätten Bestand. Folglich sind andere Gründe für eine Unwirksamkeit des Verpflichtungsgeschäfts ebenso wenig durch den Smart Contract erfassbar. Ein solcher Grund könnte beispielsweise eine erfolgreiche Anfechtung nach § 142 I BGB sein. In diesen Fällen ist analog zu anderen Kaufverträgen außerhalb der Blockchain zwangsläufig vom Abstraktionsprinzip auszugehen, sodass Smart Contracts zumindest in Anbetracht dieses Aspekts kein Hindernis für eine rechtliche Trennung der Verpflichtung und Verfügung darstellen.

b) Ausführung unter Anwendung ausländischer Rechtsgrundsätze

²⁵³ Dies kann der Fall sein sowohl bei Sachen außerhalb der tatsächlichen Kontrolle von Smart Contracts, als auch Smart Property. Näheres dazu unter Gliederungspunkt D. II.

Den im deutschen Recht verankerten Grundsätzen steht das Konsensualprinzip, auch Einheitsprinzip genannt, entgegen.²⁵⁴ Dieses wird beispielsweise im französischen Recht und in anderen Staaten wie Portugal und Italien praktiziert, deren Recht auf den französischen Code Civil zurückgeht.²⁵⁵ Laut dem Einheitsprinzip im französischen Recht erlangt ein Käufer nach Art. 1583 Code Civil das Eigentum über eine Sache nicht erst bei Einigung und Übergabe, sondern bereits bei Abschluss des Kaufvertrags. Das Eigentum geht nach Art. 1583 Code Civil auch dann über, wenn der Kaufpreis noch nicht beglichen und die Sache noch übergeben werden muss. Nimmt man wieder einen Code an, der den Kaufvertrag mit den bereits beschriebenen, fortschrittlichen Eigenschaften darstellt, erfolgt der Eigentumsübergang bereits vor der eigentlichen Ausführung des Vertrags. Allerdings kann eine Zuordnung des Eigentums zum Käufer durch den Smart Contract erst bei dessen Ausführung erfolgen, indem die Sache auf den neuen Eigentümer im Rahmen des Smart Contracts codiert wird. In diesem Fall erfolgt die Eigentumsübertragung im Sinne des geltenden Rechts bevor die Logik des Systems zu dem Ergebnis käme. Würde nun beispielsweise die Transaktion aufgrund einer nicht durchführbaren Zahlung abgelehnt werden, wäre der Käufer trotzdem bereits Eigentümer. Die Blockchain könnte dies jedoch nicht als wahr bestätigen und somit nicht auf Grundlage dieser Information

²⁵⁴ Hierzu *Stagl*, Die Eigentumsübertragung beim Kauf beweglicher Sachen – Gedanken über die Methode der Rechtsvereinheitlichung am Beispiel der Study Group on a European Civil Code, *Jb.J.ZivRWiss.* 2005, 369, 371.

²⁵⁵ *Id.*

Transaktionen über die Sache ausführen. Nach deutschem Recht wäre zu diesem Zeitpunkt stattdessen nur das Verpflichtungsgeschäft gegeben. Folglich würde der Smart Contract im Fall des Einheitsprinzips bei der Ausführung ein zwischenzeitliches Ergebnis wiedergeben, das nicht den rechtlichen Tatsachen entspricht. Würde der Smart Contract jedoch tatsächlich bereits vor Erhalt der Sache zum Zeitpunkt des Ausführungsstarts eine Eigentumsübertragung dokumentieren und es käme nicht zu einer fehlenden Bestätigung der Transaktion, so käme man zu einem anderen Ergebnis. Die Zeitpunkte des rechtlichen und technischen Eigentumserwerbs würden deutlich näher beieinanderliegen als nach dem deutschen Trennungs- und Abstraktionsprinzip.

Zwischen den deutschen und den französisch geprägten Prinzipien existiert ein weiteres Prinzip, das unter anderem in Österreich praktiziert wird.²⁵⁶ Hier geht das Eigentum auf den Käufer über, sofern eine Übergabe stattfindet und zeitgleich ein wirksamer Kaufvertrag vorliegt.²⁵⁷ Die Übertragung des Eigentums ist zwar wie im Code Civil von einem wirksamen Kaufvertrag abhängig. Der Zeitpunkt des Eigentümerwechsels ähnelt jedoch dem deutschen Prinzip. Übertragen auf die Transaktion auf der Blockchain, wird das Eigentum erst zum Zeitpunkt der Beendigung der automatisiert ausgeführten Transaktionen übertragbar sein. Der Kaufvertrag wird auch in diesem Fall zuvor in Codedarstellung bestätigt, bevor eine Ausführung erfolgt. Die Befolgung der Lehre vom Modus et

²⁵⁶ Hierzu *Stagl*, Die Eigentumsübertragung beim Kauf beweglicher Sachen, Jb.J.ZivRWiss. 2005, 369, 372.

²⁵⁷ *Id.*

Titulus Adquirendi²⁵⁸ produziert in der Blockchain bezüglich des betrachteten Grundfalls keine unerwünschten Zustände, sodass hierbei zunächst kein Hindernis für eine Verwendung von Smart Contracts für den dargestellten Kaufvertrag entsteht. Problematisch wird in diesem Fall erst wieder eine vorzeitige Eigentumsübertragung auf der Blockchain, wie dies auch nach den deutschen Grundsätzen zu beobachten wäre. Auch hier fehlt es an der Übergabe.

c) Konsequenzen unterschiedlicher Rechtssysteme für Smart Contracts

Der Fall eines Warenkaufs, der lediglich über einen Smart Contract abgewickelt wird, hat gezeigt, dass die Anwendung nicht grundsätzlich ungeeignet ist, um Prinzipien wie das Trennungs-, Abstraktions- oder Einheitsprinzip unter bestimmten Bedingungen zu erfüllen. Im besagten Grundfall, bei dem Eigentümerwechsel nach Erhalt der Ware gespeichert wird, führte lediglich das Einheitsprinzip zu einem Widerspruch zwischen Recht und Technik. Hierfür muss jedoch unterschieden werden, ob die Übertragung noch auf herkömmlichem Weg zustande kommt oder ob die Smart Contracts zur Codierung von Eigentum und der Automatisierung des Versands technisch in der Lage sind. Ausgereifte Oracles und weitreichende Befugnisse des Smart Contracts auf externe Systeme werden vorausgesetzt. Erst in letzterem Fall ergeben sich für die Rechtsgrundsätze Abweichungen bei der automatischen Ausführung des Kaufvertrags, wie das Beispiel bereits

²⁵⁸ Hierzu *Oechsler* in *MüKoBGB*, § 929 Rn. 8.

gezeigt hat. Sollte die technische Überprüfung der Verfügungsmacht nicht möglich sein, besteht für Rechtssysteme ohne Abstraktionsprinzip ein höheres Risiko für ungültig ausgeführte Befehle des Codes. Davon unabhängig käme es auch zusätzlich aus anderen Gründen zu deren Unwirksamkeit, sodass eine Aufhebung der Smart Contracts nach dem Einheitsprinzip notwendig würde. Aus Effizienzsicht könnte daher das deutsche Trennungs- und Abstraktionsprinzip helfen, die Anzahl der zu berichtigten Transaktionen zu verringern. Unabhängig von den beschriebenen Rechtsgrundsätzen einzelner Gesetzgebungen ist das Prinzip der Wirksamkeit und Unwirksamkeit von Transaktionen eine Hürde für die Funktionsweise der Blockchain und die Verfechter der Idee „Code is Law“, da das Recht nicht als codiert gegeben angesehen werden kann, sondern eine Anfechtbarkeit weiterhin möglich sein muss. Dies widerspricht jedoch der Endgültigkeit der gespeicherten Transaktionen. Hier zeigen sich erste Anhaltspunkte für rechtliche Herausforderungen und Grenzen von Smart Contracts. Die Erweiterung des Grundfalls um eine durch den Smart Contract geregelte Eigentumszuordnung zeigt jedoch die Problematik der Eigentumsübertragung in den bestehenden Rechtssystemen auf. Unter Anwendung des deutschen und österreichischen Systems produziert die Blockchain möglicherweise vermehrt strittige Ergebnisse bezüglich der Eigentümereigenschaft. Daher könnte wiederum das Einheitsprinzip das vorteilhaftere System sein, da die beiden Zeitpunkte der technischen und rechtlichen Eigentumsübertragung in diesem Fall geringe Diskrepanzen aufweisen.

6. Rechtliche Grenzen programmierbarer Verträge

Die untersuchten Anwendungsfälle verdeutlichen, welchen Nutzen Smart Contracts bei der Automatisierung und Kontrolle von Vertragsbedingungen haben. Bestimmte Anwendungen wie der Kaufvertrag legen jedoch nahe, dass Smart Contracts sogar das eigentliche Rechtsgeschäft darstellen könnten.²⁵⁹ Hierzu muss zum einen ein ausdrückliches oder konkludentes Vertragsangebot vorliegen.²⁶⁰ Zum anderen muss das Angebot angenommen werden, damit ein Vertrag zustande kommt.²⁶¹ Transaktionen, die auf der Blockchain abgebildet und abgewickelt werden sollen, sind jedoch nicht nur in Form eines Codes abgebildet, sondern resultieren aus Angeboten und Annahmen, die beispielsweise auf einer Homepage ersichtlich sind oder mündlich kommuniziert werden. Die zugrundeliegende Programmierung des Vertrags entspreche dagegen für die meisten Nutzer, die keine Programmiersprache beherrschen, nicht dem objektiven Empfängerhorizont.²⁶² Willenserklärungen, welche die Transaktionspartner abgeben, beziehen sich somit nicht auf den Code, sondern auf die tatsächlich wahrgenommene Kommunikation des Vertrags. Damit stellt der Smart Contract in diesem Fall

²⁵⁹ Zutimmend *Bourque/Fung Ling Tsui*, A lawyer's introduction to Smart Contracts, *Scientia Nobilitat Reviewed Legal Studies*, 2014, 4, 10.

²⁶⁰ Hierzu *Busche* in *MüKoBGB*, § 145 Rn. 15.

²⁶¹ Hierzu *Eckert* in *BeckOK BGB*, § 146 Rn. 9.

²⁶² Dazu *Kaulartz/Heckmann*, *Smart Contracts – Anwendungen der Blockchain-Technologie*, CR 2016, 618, 618.

lediglich das Verfügungsgeschäft dar, da er nur das vertraglich Vereinbarte ausführt und somit unterstützend wirkt.²⁶³

Es besteht allerdings die Möglichkeit, dass der Smart Contract den Vertrag darstellt. Da bei individual verhandelten Verträgen keine rechtliche Vorgabe zur Sprachwahl und gleichzeitig Gestaltungs- und Formfreiheit bestehe,²⁶⁴ kann auch eine Programmiersprache in Betracht gezogen werden. Die Transaktionspartner müssen sich jedoch auf dieses Vorgehen verständigen, indem sie den Smart Contract zum Vertrag erklären oder keine Kommunikation außerhalb des Aktivierens des Smart Contracts auf der Blockchain vorliegt. In diesem speziellen Fall wäre es eindeutig, dass wirksame Willenserklärungen vorliegen, die dem objektiven Empfängerhorizont entsprechen. Doch auch diese tatsächlichen Verträge in Codeform sind nicht unabhängig vom geltenden Rechtsumfeld. Beispielsweise sei eine Anfechtung wegen einer anderen Vorstellung von der Wirkung des Codes weiterhin rechtlich durchsetzbar.²⁶⁵ Ebenso unterstehen nicht individuell vereinbarte Smart Contracts den Beschränkungen der Allgemeinen Geschäftsbedingungen.²⁶⁶ Folglich besteht kein rechtfreier Raum aufgrund der Nutzung von Smart Contracts und der Blockchain, sodass die Aussage „Code is Law“ nur eingeschränkt gelten dürfte.

Es gibt jedoch Fälle, in denen bei der Gestaltung des Smart Contracts dem Grundsatz des „Code is Law“ zum Vorbild genommen wurde und der Code als Vertrag galt. Welche massi-

²⁶³ Id., 623.

²⁶⁴ Id., 621.

²⁶⁵ Id., 622.

²⁶⁶ Id., 622.

ven Auswirkungen eine Einigung auf den programmierten Smart Contract als Vertragssprache haben kann, zeigte der DAO Hack im vergangenen Jahr. Bei der DAO handelt es sich um eine dezentrale autonome Organisation, die mithilfe von Smart Contracts unternehmerische Funktionen abbildet.²⁶⁷ Um über die Investitionsvorschläge der DAO abstimmen zu dürfen, müssen zuvor Ether – die Kryptowährung der Ethereum Blockchain – erworben und gegen DAO Token eingetauscht werden.²⁶⁸ Dem Angreifer gelang es, rund ein Drittel der Mittel in Höhe von 150 Mio. US-Dollar aus der DAO zu entwenden, indem eine Schwachstelle in der Programmierung ausgenutzt wurde.²⁶⁹ Eine Funktion, die einen Ausstieg und die Rückzahlung der Ether an den Besitzer ermöglichen sollte, erfasste dabei bereits ausgezahlte Beträge nicht, sodass dem Hacker eine wiederholte Ausgabe möglich war.²⁷⁰ Zwar wurden über eine radikale Lösung, bei der die Mehrheit der Teilnehmer für eine Aufspaltung der Blockchain stimmte, die entwendeten Mittel zurückerlangt.²⁷¹ Dennoch widerspricht der Eingriff der grundlegenden Überzeugung des „Code is Law“. Die fehlerhafte Funktion war schließlich ein angenommener Bestandteil des „Vertrags“, auch wenn es

²⁶⁷ Vgl. *Deloitte*, The DAO – Chronology of a daring heist and its resolution, 2016, 4.

²⁶⁸ Hierzu *Deloitte*, The DAO – Chronology of a daring heist and its resolution, 2016, 4.

²⁶⁹ Hierzu *Deloitte*, The DAO – Chronology of a daring heist and its resolution, 2016, 5.

²⁷⁰ Dazu *Deloitte*, The DAO – Chronology of a daring heist and its resolution, 2016, 5.

²⁷¹ Hierzu *Deloitte*, The DAO – Chronology of a daring heist and its resolution, 2016, 6.

sich um einen menschlichen Programmierfehler handelte. Zudem war der Eingriff ein Fall, in dem Smart Contract nicht mehr die Vertragsausführung garantierte, sodass die essenzielle Eigenschaft der automatisierten Ausführung auch für andere Fälle bei Erreichen von Netzwerkmehrheiten ausgeschaltet werden könnte.

Smart Contracts könnten, auch wenn sie nur die Vertragsausführung bezwecken, an weitere rechtliche Grenzen stoßen. Dies sind zunächst die bereits beschriebene Problematik von Programmierfehlern und vom Vertrag abweichenden Aktivitäten, die sich aus der Programmierung ergeben. In diesen Fällen entstehen berechnigte Ansprüche zur Korrektur des Smart Contracts, um das vertraglich Vereinbarte umzusetzen. Ein solcher Eingriff ist bisher jedoch bei Smart Contracts nicht vorgesehen, sodass eine Schnittstelle für Anfechtungen und zuvor legitimierte Korrekturen eingebaut werden müsste. Eine weitere Hürde für eine vollständige Abbildung des Vertragsinhalts als Code stellt die Vielzahl an Rechtsfolgen dar, die bereits bei der Implementierung des Smart Contracts berücksichtigt werden müssten.²⁷² Zudem scheitert der Code an unpräzisen Rechtsbegriffen und sich daraus ergebenden Rechtsfolgen, die nicht in Computersprache abgebildet werden können. Darüber hinaus könnten Smart Contracts, die auf der Blockchain unter Pseudonymen geschlossen werden und zunächst von dem durch die Dezentralität geschaffenen Vertrauen profitieren, bei den beschriebenen Fehlerquellen und Unzulänglichkeiten einen Nachteil entwickeln. Kommt es zu

²⁷² Ebenso *Kaulartz/Heckmann*, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, 618, 623.

einer Notwendigkeit der Rückabwicklung oder beispielsweise nachzubessernden Mängeln, ist die Durchsetzung der Rechte gegen eine unbekannte Person kaum möglich.²⁷³

Aus den rechtlichen Grenzen von Smart Contracts lässt sich schlussfolgern, dass aufgrund der erschwerten Reaktion auf nicht programmierte Bestandteile eher solche Verträge in Frage kommen, bei deren Abwicklung selten die beschriebenen Fälle auftreten. Dies könnten beispielsweise Derivate sein, da die Bedingungen eindeutig und vollständig formuliert werden können. Zum anderen ist klarzustellen, dass Smart Contracts trotz spezifischer rechtlicher Regelungen nicht im rechtsfreien Raum ausgeführt werden. Obwohl anonyme Transaktionspartner und Verträge auf Codebasis eine Herausforderung für die Durchsetzung von Rechten darstellen, ist nicht damit zu rechnen, dass diese beiden Spezialfälle die Norm darstellen werden. Die meisten Anwendungen wie die eines Kaufs unter Nutzung eines Smart Contracts basieren weiterhin auf den üblichen Vertragsabschlüssen mit Vertragstext und werden nicht mit anonymen Transaktionspartnern ausgeführt.

²⁷³ Id.

II. Smart Property: Funktionsweise der Kodierung und der Übertragung von Eigentumsrechten

Ein weiteres Anwendungsgebiet für die Blockchain bildet Smart Property. Hierbei handelt es sich um eine Nutzung von Smart Contracts, die eine automatische Kontrolle und Eigentumsübertragung von Objekten leisten.²⁷⁴ Smart Property ist somit häufig an eine Implementierung von Smart Contracts zu Steuerungszwecken geknüpft.²⁷⁵ Digital erfasst werden alle Pflichten und Rechte, die mit dem Eigentum einhergehen. Zu den Rechten gehören neben sowohl Besitz, als auch Nutzung und Beseitigung des Besitzes.²⁷⁶ Das Eigentum wird dabei über den Besitz des privaten kontrolliert, der über einen Smart Contract an einen Vertragspartner weitergegeben wird.²⁷⁷ Der private Schlüssel ist einem in der Blockchain codierten Objekt zugeordnet. Der in der Blockchain gespeicherte Smart Contract hält fest, wer aktuell über den privaten Schlüssel verfügt und somit dauerhaft als Eigentümer oder zeitlich begrenzt zur Nutzung berechtigt ist. Diese Informationen werden an das entsprechende Objekt übermittelt. Anders als ausschließlich elektronische Vermögenswerte benötigen

²⁷⁴ Hierzu *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, 47.

²⁷⁵ Ähnlich *Swan*, Blockchain – Blueprint for a New Economy, 2015, 14.

²⁷⁶ Vgl. *Kölvart, et al.*, Smart Contracts, in: The Future of Law and eTechnologies, 2016, 133, 137.

²⁷⁷ Hierzu *Swan*, Blockchain – Blueprint for a New Economy, 2015, 14.

physische Werte allerdings eine Methode zur digitalen Erfassbarkeit.²⁷⁸ Voraussetzung für Smart Property sei die Möglichkeit, Objekte über technische Systeme zu identifizieren und zu verfolgen.²⁷⁹ Im Zusammenhang mit dem „Internet of Things“ erfassen und verarbeiten die Objekte unter anderem über Sensoren, Softwarecodes und einen Internetzugang Informationen für die Smart Contracts beziehungsweise verarbeiten von diesen ausgehende Informationen.²⁸⁰ Diese Systeme ermöglichen die Eigentumsverfolgung, Lokalisierung und Sicherung von Objekten über digitale Protokolle, die über Smart Contracts verwaltet werden könnten.²⁸¹ Digitale Objekte benötigen hierfür keine speziellen technischen Einbauten, die in physischen Werten gegeben sein müssen. Die Herausforderung bei digitalen Assets wie elektronischen Büchern oder Bildern bildet vielmehr die unberechtigte Vervielfältigung, die zu einer ungenehmigten Nutzung durch Dritte führt. Die Verwaltung als Smart Property bietet jedoch auch für diese Werte Schutzmöglichkeiten. Smart Property geht somit über bereits existierende Formen von digital gesicherten Objekte hinaus, da die Kontrolle und der Schutz vor unberechtigter Nutzung effektiv umgesetzt werden können. Zu den verbesserungswürdigen Anwendungen gehören beispielsweise

²⁷⁸ Zustimmend *Kölvart, et al.*, Smart Contracts, in: *The Future of Law and eTechnologies*, 2016, 133, 138.

²⁷⁹ Vgl. *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, 47.

²⁸⁰ In Anlehnung an *Shrier, et al.*, *Blockchain & Transactions, Markets and Marketplaces*, MIT, 2016, 6; *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 14.

²⁸¹ Hierzu *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, 47.

Zugangskarten und Wegfahrsperrern, die ein hohes Risiko für Manipulation und Diebstahl aufweisen.²⁸² Erst die digitalen Kontrollmöglichkeiten über das Eigentum ermöglichen in zahlreichen Anwendungsfällen für Smart Contracts, dass die Aktivitäten von Vertragsparteien und die Erfüllung von Vertragsbedingungen beobachtet und verifiziert werden können.²⁸³ Auf diese Weise können unterschiedliche Vermögenswerte verwaltet werden. Sowohl physische Werte wie Automobile und Smartphones, als auch immaterielle Werte wie Wertpapiere oder Nutzungsrechte für digitale Produkte können als Smart Property verwaltet werden. Demnach beinhalten Anwendungsfälle für Smart Contracts, in denen nicht nur ein Eigentümerwechsel dokumentiert wird, sondern durch den Smart Contract selbst der Zugang und die Nutzung des Vermögenswerts als Folge von Transaktionen gesteuert wird, zwangsläufig Smart Property.

Neben den Objekten, die weitreichend von Smart Contracts kontrolliert werden, gibt es Anwendungsfälle mit einem geringeren Automatisierungsgrad. Zu unterscheiden ist Smart Property von Blockchainanwendungen, die vordergründig auf eine Dokumentation und Identifizierbarkeit von Vermögenswerten abzielen, jedoch trotz fehlender Kontrollmöglichkeiten bezüglich der Nutzungseinschränkung und Lokalisierung über Smart Contracts im Zusammenhang mit Smart Property genannt werden. Unter diese Kategorie ist die dezentrale Plattform Everledger einzuordnen, auf der Diamanten registriert und anhand ihrer einzigartigen Eigenschaften zurückver-

²⁸² Ähnlich *Kölvart et al.*, Smart Contracts, in: *The Future of Law and eTechnologies*, 2016, 133, 137.

²⁸³ *Id.*, 138.

folgt werden können.²⁸⁴ Die fälschungssichere Dokumentation des Diamanten auf einer Blockchain beinhaltet dabei seine Eigenschaften, Historie und Verkaufsgeschichte.²⁸⁵ Ziel der Plattform sei es, die Authentizität der Diamanten zu verifizieren und somit das Risiko für Betrug und Diebstahl zu senken. Bisher seien knapp eine Million Diamanten in Kooperation mit Partnern aus der Diamantindustrie registriert worden. Anstatt schriftlicher Dokumente werden für diesen Zweck die Eigenschaften und eine gelaserte ID auf dem Diamanten in einen digitalen Pass auf die Plattform geladen.²⁸⁶ In diesen werden die Herkunft und zugehörige Transaktionshistorie fälschungssicher abgespeichert. Zudem könnten auch Smart Contracts implementiert werden, um den Diamantenkauf bei der Ausführung der Finanzierung und Versicherungsbedingungen verstärkt zu automatisieren.²⁸⁷ Das Register ermöglicht es somit neben der höheren Sicherheit für Beteiligte, den illegalen Diamantenhandel sowie die Nutzung als Mittel zur Finanzierung illegaler Aktivitäten zu erschweren. Beteiligte Parteien, wie Händler, Versicherungen, Regierungen und Konsumenten könnten die Daten nutzen. Eine Kontrolle des Eigentums über den Diamanten erfolgt jedoch nicht in der Form, als dass die Nutzung analog zu anderem Smart Property eingeschränkt werden könnte.

²⁸⁴ So auch *Shrier, et al.*, *Blockchain & Transactions, Markets and Marketplaces*, MIT, 2016, 6.

²⁸⁵ Näheres dazu *Everledger*, *Everledger Media One-Pager*, media.everledger.io, Stand: 01.03.2017.

²⁸⁶ Hierzu *Government Office für Science*, *Distributed Ledger Technology: beyond block chain*, 2016, 56.

²⁸⁷ Ebenso *Government Office für Science*, *Distributed Ledger Technology: beyond block chain*, 2016, 56.

Smart Property ermöglicht neben der Nutzung in simpel gestalteten Kaufverträgen, bei denen der Eigentümerwechsel ausgeführt wird, eine Vielzahl von Anwendungen, welche die Problematik asymmetrischer Informationsverteilung zwischen Vertragspartner beheben. Ein häufig genanntes Beispiel ist der Autokauf, der über Raten finanziert wird.²⁸⁸ Hierbei wird ein Smart Contract konzipiert, der Funktionen über eine vertragliche Vereinbarung der Ratenzahlungen und der Sicherungsübereignung hinaus ausübt.²⁸⁹ Hierzu kann zunächst die durch den Smart Contract automatisierte Ratenzahlung gehören. Zusätzlich erfolgt über die Zuordnung des privaten Schlüssels die Freigabe zur Nutzung des Fahrzeugs durch den Berechtigten. Der Smart Contract enthält jedoch eine Programmierung, welche die Stilllegung über die mit der Blockchain verbundene Elektronik des Fahrzeugs unter Einhaltung von Sicherheitsvorkehrungen ermöglicht.²⁹⁰ Die Stilllegung wäre zum Beispiel an die Information gebunden, dass das Fahrzeug zu dem Zeitpunkt nicht im Betrieb ist und sich in einem bestimmten Radius befindet. Der Kreditgeber könnte von dieser Programmierung Gebrauch machen, wenn erhebliche Zahlungsrückstände registriert werden oder der Smart

²⁸⁸ Bspw. *Swanson*, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, 48; *Rath*, Smart Contracts und das Blockchain-Prinzip – Das Ende der Juristen?, Ito.de, Artikel v. 30.08.2015.

²⁸⁹ Die Sicherungsübereignung stellt für den Kreditgeber eine Absicherung seiner Forderung dar. Dem Sicherungsgeber wird dabei der Besitz und die Nutzung der Sache ermöglicht. Hierzu *Kindl* in BeckOK BGB, § 930 Rn. 12.

²⁹⁰ Hierzu *Rath*, Smart Contracts und das Blockchain-Prinzip – Das Ende der Juristen?, Ito.de, Artikel v. 30.08.2015.

Contract die Abbuchung mehrfach nicht vornehmen kann. Mit Eingang der Schlusszahlung würde diese Befehlsoption automatisch deaktiviert werden.²⁹¹ Die Deaktivierung entspricht folglich der endgültigen Eigentumsübertragung. Zudem ist es vorstellbar, die Fahrzeugdaten zum Fahrverhalten über einen weiteren Smart Contract mit der Fahrzeugversicherung zu verknüpfen, um risikoorientierte Prämien berechnen.

Ein weiteres Anwendungsbeispiel befasst sich mit dem Einsatz von Smart Property bei der Verwaltung von Sicherheiten. Derzeit entstünden den Banken für das ineffiziente Management von Sicherheiten jährliche Kosten in Milliardenhöhe, unter anderem durch über dem Optimum liegende Höhen der Sicherheiten.²⁹² Smart Property könnte dafür genutzt werden, die von Unternehmen hinterlegte Sicherheiten über Smart Contracts zu vernetzen und Informationen effizienter mit den Berechtigten zu teilen.²⁹³ Zuvor müssten die Parteien zuverlässige Datenquellen für den Smart Contract vereinbaren.²⁹⁴ Dies könnten beispielsweise Sensordaten und externe Makrodaten sein.²⁹⁵ Die Werte der Sicherheiten ließen sich dadurch dynamisch anpassen, sodass das Risiko- und Sicher-

²⁹¹ Id.

²⁹² Vgl. *Accenture/Clearstream, Collateral Management – Unlocking the Potential in Collateral*, 2011, 10.

²⁹³ In Anlehnung an *Shrier, et al., Blockchain & Transactions, Markets and Marketplaces*, MIT, 2016, 6.

²⁹⁴ Hierzu *Shrier, et al., Blockchain & Transactions, Markets and Marketplaces*, MIT, 2016, 6.

²⁹⁵ Ähnlich *Shrier, et al., Blockchain & Transactions, Markets and Marketplaces*, MIT, 2016, 6.

heitenmanagement optimiert werden könne.²⁹⁶ Die erfassten Daten nutzen sowohl Banken, als auch den Kreditnehmern, um korrekte und übereinstimmende Werte zu erlangen. Darüber hinaus könnten auch andere Gruppen von der Bereitstellung von Sicherheiten in Form von Smart Property profitieren. So wäre sogenanntes „Trustless Lending“ vorstellbar, bei dem die Kreditvergabe zwischen unbekanntem Vertragspartnern durch die Hinterlegung des Smart Property als Sicherheit im Smart Contract ermöglicht würde.²⁹⁷ Im Falle eines Zahlungsausfalls würde der Smart Contract den Vermögenswert auf den Kreditgeber codieren, sodass eine Kreditvergabe ohne einen hohen Informationsbedarf und Vertrauen zwischen den Parteien zustande kommen könnte. Hierdurch könnten Verbraucher auf dem Kreditmarkt sowohl von mehr Wettbewerb, als auch niedrigeren Kosten profitieren.²⁹⁸

Die Anwendungsbeispiele verdeutlichen, dass durch Smart Property bereits bestehende Prozesse, die zeit- und kostenintensive Arbeitsschritte von Menschenhand erfordern, aufgrund der Selbstaussführung und des dezentral aufgebauten Vertrauens effizienter gestaltet werden können. Die Ergebnisse, wie im Falle der Nutzungssperre beim Kraftfahrzeug, würden ebenso von Juristen und Gerichtsvollziehern erzielt werden, jedoch mit höheren Kosten und längerer Bearbeitungs-

²⁹⁶ Hierzu *Shrier, et al.*, *Blockchain & Transactions, Markets and Marketplaces*, MIT, 2016, 6.

²⁹⁷ Hierzu *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 15.

²⁹⁸ Ebenso *Swan*, *Blockchain – Blueprint for a New Economy*, 2015, 15.

dauer.²⁹⁹ Dies erfordert allerdings ein hohes Maß an differenzierten Bedingungen, die ein Smart Contract zur Verwaltung von Smart Property beinhalten muss, um nicht erfassbare Umstände gegebenenfalls auf dem Rechtsweg klären zu können. Im Falle des Fahrzeugs als Smart Property wird demnach ein regulärer Vertrag weiterhin benötigt, da der Smart Contract lediglich die Durchsetzung der Nutzungssperre automatisiert, sobald der Kreditgeber diese bei Erfüllung bestimmter Bedingungen manuell veranlasst. Ebenso sollte berücksichtigt werden, dass Smart Property zu einem erheblichen Datenaustausch führt, um die digitale Kontrolle zu ermöglichen. Insbesondere das Nutzungsverhalten und die Standortabfrage werden erfasst, was datenschutzrechtliche Fragen aufwirft. Zudem sind nicht alle Vermögensgegenstände gleichermaßen für eine Umwandlung in Smart Property geeignet. Technisch einfach umsetzbar sind diejenigen Objekte, die im Zusammenhang mit dem Internet of Things bereits vernetzt und mit Sensoren ausgestattet werden. Smart Property hat neue Formen der Eigentumsübertragung zur Folge, die das Eigentumsrecht vor Herausforderungen stellen, da das Eigentumseigenschaft direkt auf dem Eigentum codiert wird. Im Vordergrund steht jedoch, dass die Eigentumsübertragung in vielen Fällen deutlich vereinfacht werden könnte und daher als Möglichkeit für eine effizientere Eigentumsverwaltung gesehen werden sollte.

²⁹⁹ Ebenso *Rath*, Smart Contracts und das Blockchain-Prinzip – Das Ende der Juristen?, Ito.de, Artikel v. 30.08.2015.

III. Tätigkeitsfelder von Finanzintermediären

1. Funktion von Intermediären auf dem Finanzmarkt

Als eines der vielversprechendsten Anwendungsgebiete für die Blockchain steht der Finanzmarkt im Fokus des öffentlichen Interesses.³⁰⁰ Diskutiert wird zudem, ob die Blockchain sogar bestimmte Finanzintermediäre gänzlich ersetzen könnte.³⁰¹ Die Finanzindustrie gelte allgemein als eine Branche, die IT-Innovationen frühzeitig adaptiere und somit häufig erste Schritte in Richtung Digitalisierung gehe.³⁰² Durch rapide Entwicklungen in der Informationstechnologie seien unter anderem bereits Prozesse am Bankschalter durch das Online-Banking substituiert wurden, sodass massive Kosten- und Zeitersparnisse realisiert werden konnten. Gleichzeitig bietet das Bankengeschäft weitere Prozesse, die weiterhin stark auf intermediären Strukturen basieren und somit Potenzial für neue Finanzmarktinfrastrukturen aufweisen. Da nahezu das gesamte Bankengeschäft in elektronische Prozesse umge-

³⁰⁰ U. a. *Wetzel*, Im Fieber, Sueddeutsche.de, Artikel v. 16.03.2016; *Schmies*, Blockchain und Wertpapierabwicklung – Neue Technik bringt disruptive Veränderungen, Börsen-Zeitung, Artikel v. 01.12.2016.

³⁰¹ So auch *Riedl*, Derivate auf Knopfdruck, sueddeutsche.de, Artikel v. 23.09.2015; Dagegen *Nees*, Zukunft der Blockchain III: Banken vs. FinTechs – wer hat die Nase vorn?, finance-it-blog.de, Artikel v. 20.02.2017.

³⁰² Hierzu *Alt/Puschmann*, Digitalisierung der Finanzindustrie: Grundlagen der Fintech-Evolution, 2016, 217.

wandelt werden könne,³⁰³ ist es möglich, weite Teile der Wertschöpfungskette auf einer Blockchain abzubilden und auszuführen. Um jedoch zu analysieren, welche Prozesse sich für eine Implementierung eignen, sollen zuvor wesentliche Funktionen von Intermediären auf dem Finanzmarkt benannt werden. Es soll zudem geklärt werden, welche dieser Funktionen die Blockchain aufgrund ihrer Eigenschaften leisten kann und in welchen Fällen sie lediglich die zugrundeliegenden Prozesse optimieren kann.

Finanzinstitute bringen zunächst die Zeitpräferenzen von Haushalten als Nettosparer und Unternehmen als Nettoleiher in Einklang.³⁰⁴ Während Haushalte als Sparer kürzere Zeithorizonte präferieren, benötigen Unternehmen langfristige Kredite für langfristige Investitionen. Finanzinstitute bringen die Präferenzen in Einklang, indem sie die Einlagen für Kredite entsprechend bündeln. Andernfalls müssten Haushalte gemeinschaftlich handeln, um Kredite gewähren zu können. Bei der Nutzung von Finanzinstituten profitieren Investoren jedoch von deren Funktionen als Monitor und Bereitsteller von Informationen.³⁰⁵ Als Folge des Prinzipal-Agenten-Problems zwischen Verleihern und Leihenden benötigen die Prinzipale Informationen über die Agenten, sowie eine Beobachtungsmöglichkeit der Handlungen. Finanzinstitute haben dabei einen Vorteil bei der Bereitstellung von Informationen über

³⁰³ In Anlehnung an *Alt/Puschmann*, Digitalisierung der Finanzindustrie: Grundlagen der Fintech-Evolution, 2016, 217.

³⁰⁴ Hierzu *Saunders/Cornett*, Financial Institutions Management: A Risk Management Approach, 2014, 4.

³⁰⁵ Vgl. *Saunders/Cornett*, Financial Institutions Management: A Risk Management Approach, 2014, 6.

Kreditnehmer, die sie auf Risiken und Aktivitäten überprüfen. Die Bereitstellung von Informationen und das Monitoring erfolgt aufgrund der Skaleneffekte effizienter als bei einer separaten Durchführung durch die einzelnen Prinzipale.³⁰⁶ Des Weiteren transformieren Finanzintermediäre finanzielle Risiken,³⁰⁷ indem sie Finanzprodukte mit unterschiedlichen Laufzeiten und Risiken entwickeln und bündeln. Darüber hinaus bieten Finanzinstitute grundlegende Zahlungsdienste und die Funktion als Broker an, bei der sie Handelskosten durch Skaleneffekte bei der Bündelung von Transaktionen reduzieren können.

Prüft man die Funktionen auf eine Übertragbarkeit auf die Blockchain, zeigt sich, dass bestimmte Aufgaben durch eine dezentrale Plattform substituiert werden könnten, während andere Bereiche die Einbeziehung von Intermediären rechtfertigen. Die Kreditvergabe könnte durch eine Bündelung von Guthaben auf Smart Contracts ebenfalls ermöglicht werden. Allerdings wäre die Vereinheitlichung der Zeitpräferenzen eine Herausforderung für die Gestaltung des Smart Contracts. Ebenso stünden den Kreditgebern keine umfangreichen Analysen und Informationen über mögliche Kreditrisiken zur Verfügung, sodass diese von den einzelnen Kreditgebern erlangt werden müssten. Ebenfalls entfällt das Monitoring durch einen Intermediär. Allerdings hat das Beispiel des Trustless Lending gezeigt, dass durch Smart Property Kreditgebern Vermögenswerte als Sicherheit im Falle eines Kreditausfalls

³⁰⁶ In Anlehnung an *Saunders/Cornett*, *Financial Institutions Management: A Risk Management Approach*, 2014, 6.

³⁰⁷ Hierzu *Saunders/Cornett*, *Financial Institutions Management: A Risk Management Approach*, 2014, 5.

übertragen werden könnten. Somit würde die Blockchain das Risiko der Informationsasymmetrie senken und die korrekte Vertragsausführung sichern. Dennoch ist nicht auszuschließen, dass diese Möglichkeit zwangsläufig zu einer adversen Selektion führt, bei der überwiegend schlechte Risiken Trustless Lending nutzen und für die Kreditgeber unerwünscht hohe Ausfallraten mit einer Übertragung von Smart Property entstehen. Hier stellt sich wiederum die Frage, wie nicht teilbares Smart Property mehreren Kreditgebern zugeteilt und weiter verwertet werden kann. Trustless Lending und die Blockchain sind somit weniger für hohe Kreditvergaben mit komplexen Risiken geeignet, als für kurzfristigere private Kredittransaktionen zwischen wenigen Beteiligten mit einsetzbarem Smart Property. Finanzinstitute selbst können jedoch die Blockchain und Smart Contracts nutzen, um die Ausführung der Kreditvergabe zu automatisieren, was die Überweisung des Kredits und die Sicherstellung von Sicherheiten über Smart Property betrifft. Ähnlich könnten Transaktionen mit weiteren Finanzprodukten ohne intermediäre Interaktion über eine Blockchain abgewickelt werden, da hierbei keine spezifische Expertise benötigt wird.³⁰⁸ Die Transformation der Risiken würde damit weiterhin durch Finanzinstitute ausgeführt werden. Sie erfordert umfangreiche und fallabhängige Analysen, die nicht durch Funktionen der Blockchain substituiert werden können. Ebenfalls potenziell durch eine Blockchain ausführbar sind Überweisungsgeschäfte. Insbesondere Auslandstransaktionen seien für Peer-to-Peer Netzwerke

³⁰⁸ Ebenso *Finextra Research*, *Banking on Blockchain*, Whitepaper, 2016, 12.

geeignet, da sie gegenwärtig hohe Kosten und lange Ausführungsdauern verursachen.³⁰⁹ Sowohl eine Integration in bankinterne Prozesse, als auch neue Wettbewerber aus der FinTech-Industrie, die Peer-to-Peer Transaktionen anbieten, sind in diesem Geschäftsfeld möglich.³¹⁰ Gleiches gilt für Intermediäre, die Transaktionskosten durch hohe Handelsvolumen reduzieren oder Clearing und Settlement anbieten. Hier sind ebenfalls vertikale Integrationen, als auch neue externe Anbieter realisierbar. Es zeigt sich, dass insbesondere die Abwicklung von Transaktionen durch Finanzintermediäre aufgrund der zuverlässigen Durchführung der Transaktionen auf der Blockchain gefährdet ist. Finanzdienstleistungen, die ein komplexes Verständnis von Sachverhalten und Risiken erfordern, rechtfertigen jedoch die Existenz von Finanzintermediären auch in Zukunft, da hier nur ein geringer Automatisierungsgrad möglich ist. Es stellt sich somit die Frage, ob Intermediäre die neue Technologie selbst adaptieren oder neue Akteure die Plattformen für Finanzinstitute sowie Endkunden anbieten.³¹¹ Im folgenden soll daher eine Blockchainanwendung betrachtet werden, die Intermediäre im Wertpapierhandel substituieren.

³⁰⁹ Hierzu *Finextra Research*, *Banking on Blockchain*, Whitepaper, 2016, 13.

³¹⁰ In Anlehnung an *Dapp/Karollus*, *Blockchain – attack is probably the best form of defence*, Deutsche Bank Research, 2016, 1.

³¹¹ *Id.*

2. Wertpapierhandel

a) Das Clearing und Settlement System

Die Notwendigkeit einer Clearingstelle resultiert aus dem Double Spending Problem, bei dem eine Bank simultan Zahlungen an Gegenparteien veranlasst, ohne diese tatsächlich begleichen zu können.³¹² Der Wertpapierhandel und zugehörige Termingeschäfte zwischen Banken, die keine gegenseitigen Konten verfügen, bauen daher auf intermediären Banken oder Clearingstellen auf, wie in Abbildung 2 zu sehen ist.³¹³ Hierbei stellt das Clearinghouse vor einer Transaktionsdurchführung fest, welche Verbindlichkeiten, Forderungen und zu leistende Eigentumsübergaben zwischen den beteiligten Banken zu leisten sind.³¹⁴ Beim Settlement erfolgt wiederum die Durchführung der Transaktionen zum vereinbarten Zeitpunkt.³¹⁵ Bevor Clearingstellen die Ausführung der Transaktionen überwachen, prüfen sie die Bonität der Clearing-Mitglieder und fordern Sicherheiten von diesen ein.³¹⁶ Folglich garantiert die Clearingstelle, dass vereinbarte Transaktionen ordnungsgemäß ausgeführt werden. Im Falle eines Aus-

³¹² Hierzu *Kiviat*, „Smart“ Contract Markets: Trading Derivates Contracts on the Blockchain, 2015, 32.

³¹³ Hierzu *Biella/Zinetti*, Blockchain Technology and Applications from a Financial Perspective, Technical Report Version 1.0, Unicredit, 2016, 12.

³¹⁴ Ähnlich *Braechevelt*, Clearing, settlement and depository issues, BIS Papers No 30, 2006, 284, 286.

³¹⁵ Hierzu *Braechevelt*, Clearing, settlement and depository issues, BIS Papers No 30, 2006, 284, 286.

³¹⁶ Vgl. *Beike/Schlütz*, Finanznachrichten lesen – verstehen – nutzen, Handelsblatt Bücher, 2010, 506.

falls des Transaktionspartners muss der Intermediär die Erfüllung des Geschäfts verantworten. Die Transaktionspartner profitieren von der Absicherung der Ausfallrisiken durch die streng regulierten Clearingstellen.³¹⁷ Allerdings beansprucht das Clearing und Settlement mehrere Tage.³¹⁸ Zudem entstehen für den weltweiten Finanzhandel schätzungsweise Handelskosten in Höhe von 65 bis 89 Mrd. US-Dollar.³¹⁹ Es stellt sich somit die Frage, ob mithilfe einer Blockchain die Funktion der Intermediäre abgebildet und optimiert werden kann.

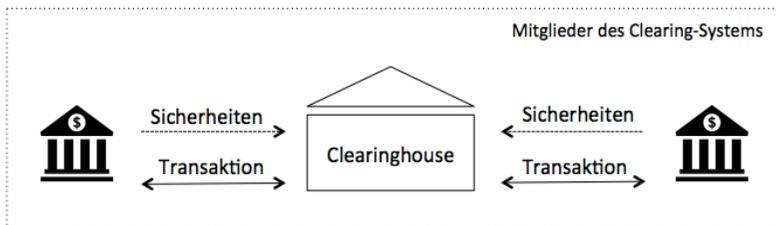


Abb. 2: Clearing und Settlement unter Nutzung einer Clearingstelle

Das Konzept beinhaltet eine Permissioned Blockchain, zu der sich die Finanzinstitute ähnlich zur Clearingstelle Zutritt verschaffen müssen.³²⁰ Die Zugangsbeschränkung dient dem Schutz vor einem Zugriff Dritter auf die in der Blockchain ge-

³¹⁷ Näheres zur Regulierung in Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates v. 04.07.2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, Abl. EU Nr. L 201/2 v. 27.07.2012.

³¹⁸ Vgl. *Peters/Panayi*, Understanding Modern Banking Ledgers through Blockchain Technologies, 2015, 26.

³¹⁹ Vgl. *Government Office für Science*, Distributed Ledger Technology: beyond block chain, 2016, 60.

³²⁰ Hierzu *Peters/Panayi*, Understanding Modern Banking Ledgers through Blockchain Technologies, 2015, 28.

speicherten Informationen. Anstatt über die Zuhilfenahme eines Intermediärs agieren die Transaktionspartner direkt miteinander, wie in Abbildung 3 zu sehen ist.³²¹ Transaktionen werden dabei auf der Blockchain auf ihre Validität überprüft, bevor sie durch die Netzwerkteilnehmer automatisch im Consensus Mechanismus bestätigt und somit kryptografisch gesichert einem Datenblock in der Blockchain hinzugefügt werden.³²² Die Buchung der Transaktionen auf den beteiligten Konten erfolgt ohne eine mehrtätige Prozessabwicklung durch Intermediäre. Die Transaktion erfolgt somit analog zu den Bitcoin-Transaktionen, die ebenfalls nur dann ausgeführt werden, wenn das Konto über die Bitcoins verfügt. Zudem lassen sich Smart Contracts implementieren, die beispielsweise derivative Transaktionen automatisch abwickeln und somit die Vertragsausführung sicherstellen.³²³ Zusätzlich wird ein verpflichtendes Reservekonto für die gesamten oder jeweils ein eigenes pro Transaktionspartner angelegt, um das Kontrahentenrisiko zu minimieren.³²⁴ Die Prüfung der gedeckten Reservekonten würde dann zusätzlich im Validierungsprozess durch das dezentrale Netzwerk ausgeführt werden. Das Konzept hat dabei eine Reihe von Vorteilen gegenüber dem be-

³²¹ Hierzu *Biella/Zinetti*, Blockchain Technology and Applications from a Financial Perspective, Technical Report Version 1.0, Unicredit, 2016, 13.

³²² In Anlehnung an *Government Office für Science*, Distributed Ledger Technology: beyond block chain, 2016, 60.

³²³ Ebenso *Van de Velde, et al.*, Blockchain in Capital Markets – The Prize and the Journey, Euroclear, u. Oliver Wyman, 2016, 10.

³²⁴ Hierzu *Biella/Zinetti*, Blockchain Technology and Applications from a Financial Perspective, Technical Report Version 1.0, Unicredit, 2016, 13-14.

stehenden intermediären System. Zunächst ermöglicht die Blockchain einen transparenten Handelsvorgang, da die Bedingungen für den Handel erfüllt sein müssen, um ausführbar zu sein. Das Matching und Settlement erfolgen in Echtzeit über das dezentrale Transaktionsregister.³²⁵ Die Abwicklung und typische Handelsrisiken wie Ausfälle oder fehlerhafte Transaktionen übernimmt nicht mehr die Clearingstelle gegen Leistung von Gebühren und Sicherheiten. Mit der schnelleren Ausführung sinken automatisch das Risiko der Transaktionen und damit einhergehende Kapitalerfordernisse.³²⁶ Folglich sei weniger Kapital als bei den Intermediären zur Absicherung von Risiken notwendig, sodass die Finanzmittel für anderweitige Bankgeschäfte genutzt werden könnten.³²⁷ Insgesamt erfolgt das Clearing und Settlement schneller und günstiger, ohne jedoch zu höheren Risiken zu führen.³²⁸ Das fälschungssichere und transparente Register kann zudem gezielt von Aufsichtsbehörden genutzt werden, um die Einhaltung der umfangreichen Vorschriften für Banken besser zu beaufsichti-

³²⁵ Ebenso *Van de Velde, et al.*, *Blockchain in Capital Markets – The Prize and the Journey*, Euroclear, u. Oliver Wyman, 2016, 12.

³²⁶ Allein die Reduktion der Settlementdauer von T+3 zu T+2 im derzeitigen Prozess führt zu einer Senkung der Sicherheiten bei der Clearingstelle um 15% bis 24% je nach Marktvolatilität. Dies verdeutlicht bereits das hohe Einsparpotenzial der Blockchain. Vgl. *BCG, Cost benefit analysis of shortening the settlement cycle*, 2012, 33.

³²⁷ Hierzu *Biella/Zinetti*, *Blockchain Technology and Applications from a Financial Perspective*, Technical Report Version 1.0, Unicredit, 2016, 14.

³²⁸ Ähnlich *Peters/Panayi*, *Understanding Modern Banking Ledgers through Blockchain Technologies*, 2015, 27.

gen und zu kontrollieren.³²⁹ Problematisch ist jedoch, dass alle Netzwerkteilnehmer die Transaktionsdaten der anderen Teilnehmer einsehen können. Hier sei der Schutz der Daten noch nicht gewährleistet.³³⁰ Es wäre somit notwendig, die Plattform in der Form zu gestalten, dass nur die beteiligten Transaktionsteilnehmer Zugriff auf die vollständigen Daten der jeweiligen Transaktion erhalten.³³¹ Allerdings verliert die Plattform dann eine wesentliche Eigenschaft der Blockchain, bei der alle Transaktionen transparent sind.

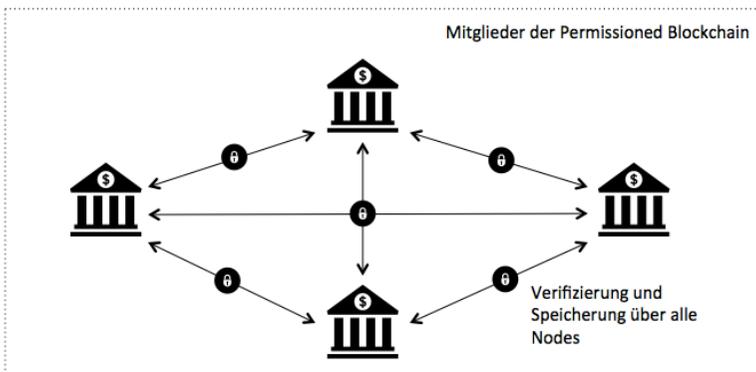


Abb. 3: Clearing und Settlement unter Nutzung einer Blockchain

³²⁹ Ebenso *Van de Velde, et al.*, *Blockchain in Capital Markets – The Prize and the Journey*, Euroclear, u. Oliver Wyman, 2016, 12.

³³⁰ Hierzu *Biella/Zinetti*, *Blockchain Technology and Applications from a Financial Perspective*, Technical Report Version 1.0, Unicredit, 2016, 13.

³³¹ Eine solche Plattform mit Schutz der Privatsphäre, die gleichzeitig skalierbar sein soll, stellt Enigma dar. Näheres dazu *Zyskind, et al.*, *Enigma: Decentralized Computation Platform with Guaranteed Privacy*, Whitepaper, 2015, 2.

Aufgrund der vielfältigen Vorteile, durch welche die Clearingstellen adäquat ersetzt werden könnten, ist es nachvollziehbar, dass ein breites Interesse an der Forschung und Entwicklung eines solchen Systems bei den Beteiligten besteht. Sowohl Start-Ups aus der Fintech-Branche, als auch Finanzinstitute und die Clearingstellen selbst arbeiten an einer Umsetzung der Blockchain für den Finanzsektor.³³² Unklar ist daher zum derzeitigen Zeitpunkt, welcher Akteur die notwendige IT-Struktur aufbauen und verwalten wird, sowie welche Netzwerke eine hinreichend große Teilnehmerzahl entwickeln werden. Zudem besteht die Möglichkeit, weitere Geschäftstätigkeiten der Finanzinstitute in die Blockchain zu integrieren, wie beispielsweise die Kreditvergabe. Hierdurch könnten weitere manuelle Prozesse automatisiert und beschleunigt werden. Darüber hinaus lassen sich umfangreiche Reportingpflichten sowie die Compliance effizienter erfüllen, da relevante Informationen auf der Blockchain abgebildet wären.³³³ Aufgrund der hohen Bedeutung der Regulierungsvorschriften und aussagekräftigen Bilanzierung für ein funktionierendes Finanzsystem sollte daher ebenfalls die Vereinbarkeit der

³³² Hierzu gehören u. a. die Fintech-Unternehmen Ripple und SETL, sowie das R3 Consortium, das aus ca. internationalen Finanzinstituten besteht. Ebenso engagiert sich das Clearinghouse Euroclear an der Erforschung von Einsatzmöglichkeiten. Näheres dazu *Ripple*, ripple.com, Stand: 10.03.2017; *SETL*, setl.io, Stand: 10.03.2017; *R3 Consortium*, r3cev.com, Stand: 10.03.2017; *Van de Velde, et al.*, Blockchain in Capital Markets – The Prize and the Journey, Euroclear, u. Oliver Wyman, 2016.

³³³ Ebenso *European Central Bank*, Distributed Ledger Technology, In Focus Issue 1, 2016, 4.

blockchainbasierten Prozesse mit den rechtlichen Vorgaben analysiert werden.

b) Abwicklung: Mindestanforderungen an das Risikomanagement

Die Mindestanforderungen an das Risikomanagement (BA) stellen für Banken die zentralen Verwaltungsanweisungen der BaFin dar, welche die Ausgestaltung des Risikomanagements regeln.³³⁴ Sie setzen die zweite Säule der Basel II/III-Regelungen zum bankaufsichtlichen Überprüfungsprozess der Adäquanz der Kapitalausstattung und des Risikomanagements um,³³⁵ und spezifizieren § 25a KWG. Die Vorgaben sind auf wesentliche Risiken anzuwenden, zu denen unter anderem Adressenausfallrisiken, Liquiditätsrisiken und operationelle Risiken zählen können.³³⁶ Die MaRisk geben dabei die durch das Risikomanagement zu erreichenden Ziele vor, spezifizieren jedoch nicht die konkrete Ausgestaltung der Maßnahmen.³³⁷ Somit ist ein Einbezug neuer Technologien nicht ausgeschlossen, sofern die Vorgaben erfüllt werden können. Unter Einsatz eines Finanzmarktmodells, bei dem Clearing und Settlement über die dezentrale Blockchain abgewickelt werden, ist somit zu klären, ob die Technologie die Steuerung

³³⁴ Vgl. *Grützner/Jakob* in *Grützner/Jakob*, Compliance von A-Z, MaRisk.

³³⁵ Vgl. *Conrad/Hupertz* in *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, § 33 Rn. 286.

³³⁶ Vgl. *Braun* in *Boos/Fischer/Schulte-Mattler*, KWG, § 25a Rn. 108.

³³⁷ Vgl. MaRisk²⁰¹² AT 4.3.2 Tz. 1-2.

der Risiken innerhalb der Risikosteuerungs- und -controllingprozesse beeinflussen könnte.³³⁸

Zunächst muss die Bank sicherstellen, dass das Risiko, dass ein Vertragspartner seine Verpflichtungen nicht oder verspätet erfüllt, oder für das Institut daraus eine Leistungsverpflichtung entsteht, minimiert wird.³³⁹ Für den Clearing und Settlement Prozess bedeutet dies, dass Prozesse zur Steuerung des Ausfallrisikos implementiert sein müssen. Zu diesem Zweck werden sowohl die Clearingstellen als auch weitere Vorkehrungen wie Kontrahentenlimite für Handelspartner vorgegeben,³⁴⁰ dessen Überschreiten weitere Kontrollen zur Risikotragfähigkeit erfordert. Die Transaktionsabwicklung über eine Blockchain in der beschriebenen Ausgestaltung ermöglicht jedoch eine zügige Überprüfung der Ausführbarkeit und eine Abwicklung nahezu in Echtzeit, sodass geringere Ausfallrisiken und damit niedrigere Kapitalerfordernisse für Sicherheiten für kürzere Zeitdauern bereitgestellt werden müssten. Zusätzlich verhindert der Einsatz von Smart Contracts ein vom Vertrag abweichendes Verhalten. Somit könnte die Anwendung die Einhaltung der MaRisk zur Absicherung von Ausfallrisiken unterstützen, indem das Risiko verringert wird. Allerdings ist anzumerken, dass Kassageschäfte, die innerhalb von zwei Handelstagen abgewickelt werden,

³³⁸ Hierzu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 129.

³³⁹ Hierzu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 260.

³⁴⁰ Dazu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 265.

häufig bereits ohne Sicherheiten durchgeführt werden.³⁴¹ Darüber hinaus benötigten derivative Transaktionen, bei denen die Verpflichtungen über die gesamte Vertragsdauer bestünden, weiterhin einen Austausch von Sicherheiten.³⁴² Das Ausfallrisiko könne hier nicht durch die Blockchain beseitigt werden.³⁴³ Trotz der eingeschränkten Auswirkungen auf bestimmte Transaktionsgruppen existieren jedoch genügend Finanzgeschäfte, die von der verkürzten Abwicklungsdauer profitieren, und somit zu einem geringeren Risiko eines Ausfalls führen.

Ähnlich können die Auswirkungen auf das Liquiditätsrisiko beurteilt werden. Das Finanzinstitut ist verpflichtet sicherzustellen, dass eine Erfüllbarkeit der Zahlungsverpflichtungen durch ausreichend Liquidität sichergestellt ist.³⁴⁴ Im Zuge der Finanzkrise, die 2007 begann, ist das Risiko eines Liquiditätsengpasses in den Vordergrund der Regulierung gerückt,³⁴⁵ sodass frühzeitig auf sich abzeichnende Risiken reagiert und mehr Liquidität vorgehalten werden muss. Die schnellere Abwicklung von Transaktionen und Überprüfung der Ausführbarkeit auf der Blockchain reduziert die Höhe des in Sicherheiten gebundenen Kapitals und noch nicht beglichener Forderungen. Somit könnte das Finanzinstitut die vorgeschriebenen Stresstests aufgrund der veränderten Bedingun-

³⁴¹ Hierzu *European Securities and Markets Authority*, *The Distributed Ledger Technology Applied to Securities Markets*, Discussion Paper, 2016, 12.

³⁴² *Id.*, 11.

³⁴³ *Id.*, 11.

³⁴⁴ Vgl. *Braun* in Boos/Fischer/Schulte-Mattler, *KWG*, § 25a Rn. 318.

³⁴⁵ Hierzu *Braun* in Boos/Fischer/Schulte-Mattler, *KWG*, § 25a Rn. 316.

gen bei der Prozessausführung besser erfüllen und etwaige Liquiditätsrisiken schneller erkennen.³⁴⁶ Doch auch hier gilt die Einschränkung, dass für derivative Transaktionen weiterhin Liquidität in Form von Sicherheiten bereitgestellt werden muss beziehungsweise Kassageschäfte kein besonders hohes Einsparpotenzial aufweisen könnten. Die Senkung des Liquiditätsrisikos hängt somit wie beim Ausfallrisiko von dem betrachteten Finanzinstrument ab. Eine weitaus größere Auswirkung auf die Kontrolle des Liquiditätsrisikos könnte die separate und chronologische Behandlung der Transaktionen in Echtzeit im Blockchainsystem haben. Das Clearing zwischen Transaktionspartnern verläuft über eine Saldierung der Transaktionswerte, sodass beim Settlement nur noch die Nettobeträge über Transaktionen ausgeführt werden, anstelle der einzelnen Transaktionen.³⁴⁷ Es müsste somit weitaus mehr Kapital bei dem Bruttoabrechnungssystem bereitstehen, um die einzeln ausgeführten Transaktionen auf der Blockchain erfüllen zu können. Sollte eine Anpassung der Funktionsweise auf ein Nettoabrechnungssystem nicht möglich sein, würde dies eine höhere Liquidität erfordern und somit die Einhaltung der MaRisk erschweren.³⁴⁸

Ein weiteres Risiko, das durch die MaRisk explizit überwacht werden muss, ist das operationelle Risiko, das von Verlusten durch fehlerhafte Systeme und internen Verfahren, sowie von

³⁴⁶ Hierzu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 331.

³⁴⁷ Ähnlich *Sinz* in Uhlenbruck, InsO, § 96 Rn. 73.

³⁴⁸ Ebenso *European Securities and Markets Authority*, The Distributed Ledger Technology Applied to Securities Markets, Discussion Paper, 2016, 15.

menschlichem Versagen und externen Faktoren ausgeht.³⁴⁹ Dabei kann es sich unter anderem um Geschäftsunterbrechungen und Systemausfälle, fehlerhafte Dateieingaben, fehlerhaftes Verhalten von Kontrahenten oder Schäden durch Computerhacker handeln.³⁵⁰ Operationelle Risiken weisen zudem eine hohe Korrelation zu Marktrisiken und Kreditrisiken auf.³⁵¹ Die MaRisk erfordern daher wirksame Maßnahmen zur Kontrolle operationeller Risiken im Rahmen der Risikosteuerung.³⁵² Ein dezentrales Transaktionsregister könnte sich positiv auf diese Risikokontrolle auswirken, da es die Gefahr von Systemausfällen oder Angriffen durch Dritte reduziert. Dies liegt daran, dass es keinen zentralen Angriffspunkt für Hacker gibt und die kryptografische Verschlüsselung und der Consensus Mechanismus das dezentral gespeicherte Register vor Manipulationen schützen. Zudem ist die Plattform zuverlässig und permanent verfügbar, da Ausfälle einzelner Netzwerkteilnehmer nicht die Funktionsunfähigkeit des Systems zur Folge haben. Clearingstellen könnten dagegen aufgrund ihrer zentralen Struktur eher von einem Systemausfall oder Angriffen betroffen sein. Eine Herausforderung im Hinblick auf operationelle Risiken aus fehlerhaften oder absichtlichen falschen Eingaben stellt die eigentlich positive Eigenschaft des Schutzes vor Änderungen dar. Kommt es jedoch zu fehlerhaften Eingaben, muss es für Berechtigte technisch möglich sein, die

³⁴⁹ Hierzu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 356.

³⁵⁰ Vgl. *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 358.

³⁵¹ Dazu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 371.

³⁵² Hierzu *Braun* in Boos/Fischer/Schulte-Mattler, KWG, § 25a Rn. 352.

Transaktion zu korrigieren oder aufzuheben. Die Möglichkeit einer zügigen Fehlerkorrektur sei insbesondere aufgrund des beschleunigten Clearing und Settlement Prozesses ein Problem, das zwingend gelöst werden müsse.³⁵³ Zudem könnte die Übergangsphase operationelle Risiken zusätzlich erhöhen, da vor einem endgültigen Systemwechsel zwei Systeme parallel notwendig sein werden und dabei mögliche Komplikationen noch nicht absehbar sind.³⁵⁴ Folglich muss das skizzierte Modell um einen solchen Mechanismus erweitert werden, wobei jedoch die fundamentale Fälschungssicherheit des dezentralen Registers angegriffen würde. Die erfolgreiche Kontrolle bestimmter operationeller Risiken könnte durchaus mit der Blockchain-Technologie erzielt werden. Dies setzt jedoch eine Weiterentwicklung insbesondere zur Implementierung von Korrekturmechanismen voraus.

Insgesamt lässt sich feststellen, dass die Verkürzung der Abwicklungsdauer zunächst einen Zugewinn für die Einhaltung der Mindestanforderungen an das Risikomanagement im Hinblick auf die Risikokontrolle darstellt. Der Effekt ist jedoch vom betrachteten Finanzinstrument abhängig und erfordert eine Modifizierung der Blockchain um Operationen zur Korrektur, um den Vorgaben der BaFin entsprechen zu können. Zwar stellt die Darstellung der Transaktionen in mit Signaturen und Hashs versehenen Datenblöcken zunächst eine Herausforderung für die weitere Datenanalyse dar, die sowohl das Risikomanagement als auch Aufsichtsbehörden betrifft.

³⁵³ Hierzu *European Securities and Markets Authority, The Distributed Ledger Technology Applied to Securities Markets, Discussion Paper, 2016, 15.*

³⁵⁴ *Id.*, 19.

Gleichzeitig ermöglicht der hohe Informationsgehalt aus einem einzigen Register einen schnelleren und direkten Zugriff auf relevante Daten für diese Gruppen. Folglich könnte das frühzeitige Erkennen von relevanten Risiken mithilfe der Blockchain erleichtert werden.

c) Anmerkungen zur Umsetzbarkeit von IFRS 9

Mit der Erstanwendung des neuen Standards IFRS 9 zum 1. Januar 2018³⁵⁵ treten erhebliche Veränderungen bei der Bilanzierung von Finanzinstrumenten im Vergleich zum IAS 39 auf. Da die Änderungen auf eine Vereinfachung der Rechnungslegung für Finanzinstrumente, sowie die Vergleichbarkeit der Abschlüsse abzielen, könnte die Integration der Blockchain in das Finanzsystem von besonderem Interesse sein. Zum einen könnte sie die Abbildung in der Rechnungslegung beispielsweise bei der Klassifikation oder Bewertung von Finanzinstrumenten schnell und transparent gestalten. Zum anderen erscheinen die vereinfachten Vorgaben vorteilhaft, um Finanzinstrumente korrekt in Smart Contracts abbilden zu können, sodass die IFRS 9 zu einer Umsetzbarkeit und Kompatibilität der Anwendung mit den rechtlichen Vorgaben beitragen könnten. Folglich sollen die wesentlichen Änderungen der IFRS 9 im Kontext der Blockchain für Finanzinstrumente betrachtet werden, welche die Klassifikation und Bewertung, Impairment sowie Hedge Accounting einschließen.

Die IFRS führen nach IFRS 9.4.1.1 eine Klassifikation von Finanzinstrumenten in drei Kategorien ein, nach der die Folge-

³⁵⁵ Vgl. *Hartenberger* in IFRS-Handbuch, § 3 Rn. 545.

bewertung zu fortgeführten Anschaffungskosten, erfolgsneutral zum beizulegenden Zeitwert im sonstigen Ergebnis oder erfolgswirksam zum beizulegenden Zeitwert nach bestimmten Kriterien erfolgt, sofern nicht die Fair Value Option freiwillig gewählt wird. Die Kategorisierung hängt zum einen von der Wahl des Geschäftsmodells für das jeweilige Finanzinstrument ab, also ob dieses zur Erzielung vertraglicher Zahlungsströme gehalten werden soll, eine Handelsabsicht besteht oder ein gemischtes Modell vorliegt.³⁵⁶ Zum anderen wird überprüft, ob die Zahlungsströme lediglich aus Zinszahlungen und Kapital bestehen.³⁵⁷ In Abhängigkeit des Geschäftsmodells und der Art der Zahlungsströme erfolgt die Klassifikation der Finanzinstrumente. Bezogen auf die Blockchain stellt die Erfassung aller vertraglichen Zahlungsströme wie auch im bestehenden System eine Herausforderung dar. Beide Systeme profitieren demnach von einem höheren Standardisierungsgrad bei geschlossenen Verträgen, um die relevanten Zahlungsströme zuverlässig und effizient ermitteln zu können. So wäre eine Einbindung der Finanzinstrumente in Smart Contracts, sowie eine automatisierte Übertragung zugehöriger Zahlungsströme beim Verkauf des Finanzinstruments im Einklang mit den IFRS 9 durchführbar. Unter der noch gültigen Regelung nach IAS 39 sei diese Automatisierung aufgrund der komplexen regelbasierten Anforderungen weit aus schwieriger.³⁵⁸ Eine prospektive Änderung des Ge-

³⁵⁶ Hierzu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 363.

³⁵⁷ Hierzu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 369.

³⁵⁸ Dazu *Peters/Panayi*, *Understanding Modern Banking Ledgers through Blockchain Technologies*, 2015, 25.

schäftsmodells und somit eine Reklassifizierung³⁵⁹ könnte ebenfalls als externe Information an den Smart Contract weitergeleitet und verarbeitet werden. Problematisch ist jedoch die Notwendigkeit einer Berichtigung bei einer fehlerhaften Klassifizierung während einer laufenden Berichtsperiode.³⁶⁰ Sie müsste retrospektiv wirksam werden.³⁶¹ Die Möglichkeit zur Veränderung bereits validierter Blöcke ist jedoch bei den diskutierten Blockchainmodellen nicht vorgesehen.³⁶² Die Bilanzierung des betroffenen Finanzinstruments würde sich dann von den Informationen in der Blockchain systematisch unterscheiden und somit die Informationsqualität in der Blockchain mindern. Die Funktionsweise stellt damit nicht nur ein Hindernis für eine wahrheitsgetreue Bilanzierung dar, sondern generell für einen fehlerfreien Prozessablauf, wenn falsche Transaktionen auf der Blockchain zu berichtigen sind. Da auch Kreditbeziehungen in Form von Smart Contracts diskutiert werden, spielt auch das neu eingeführte Expected Loss Impairment Model bei der Bewertung von Kreditrisiken eine Rolle. Hierbei muss der erwartete Verlust bereits mit Beginn der bilanziellen Erfassung ebenfalls erfasst werden.³⁶³ Beim Incurred Loss Model nach IAS 39 wurden Wertberichtigungen dagegen erst mit Eintreten von Verlustereignissen bilan-

³⁵⁹ Vgl. IFRS 9.4.4 ff.

³⁶⁰ Vgl. IAS 8.41.

³⁶¹ Hierzu IAS 8.41.

³⁶² Ebenso *Peters/Panayi*, *Understanding Modern Banking Ledgers through Blockchain Technologies*, 2015, 25.

³⁶³ Hierzu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 386.

ziert.³⁶⁴ In den Vordergrund rücken relative Veränderungen von Ausfallrisiken.³⁶⁵ Für Kredite, die nicht einem niedrigen Ausfallrisiko entsprechen, müssen die Risiken auf Basis der Restlaufzeit ermittelt werden.³⁶⁶ Die neue standardisierte Regelung steigere die Transparenz der Bilanzierung und reduziere teilweise die Komplexität der Regeln.³⁶⁷ Dies vereinfacht die Umsetzbarkeit von Smart Contracts für Kredite, da sie standardisierte Regelungen besser abbilden können.³⁶⁸ Da jedoch nicht alle Finanzinstrumente von der Neuregelung betroffen sind,³⁶⁹ könnte die Darstellung der komplexen alten Regelungen eine Hürde für Smart Contracts darstellen. Allerdings ist anzumerken, dass die automatisierte Aktualisierung zu einer zeitnahen Erfassung der zu erwarteten Verluste beiträgt.³⁷⁰ Dies ist insbesondere aufgrund des gestiegenen Analyseaufwands beim Impairment durch die Unterteilung in drei Risikostufen mit unterschiedlichem Bewertungshorizont von Bedeutung, um eine zügige Bilanzierung und Aktivitäten des Risikomanagements einzuleiten.

³⁶⁴ Dazu *Lopatta, et al.*, Kritischer Vergleich der Wertminderungsmodelle nach IAS 39 und IFRS 9 – eine Fallstudie, IRZ 2016, 499, 499.

³⁶⁵ Hierzu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 386.

³⁶⁶ Hierzu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 388-389.

³⁶⁷ Dazu *Lopatta, et al.*, Kritischer Vergleich der Wertminderungsmodelle nach IAS 39 und IFRS 9 – eine Fallstudie, IRZ 2016, 499, 505.

³⁶⁸ Ebenso *Peters/Panayi*, Understanding Modern Banking Ledgers through Blockchain Technologies, 2015, 25.

³⁶⁹ Hierzu *PwC*, Bilanzierung von Finanzinstrumenten bleibt komplex auch mit dem neuen IFRS 9, pwc.de, Stand: 14.03.2017.

³⁷⁰ Ebenso *Peters/Panayi*, Understanding Modern Banking Ledgers through Blockchain Technologies, 2015, 25.

Der dritte Änderungsbereich der IFRS 9 betrifft das Hedge Accounting. Neben der Ausweitung der zulässigen Sicherungs- und Grundgeschäfte ist ein wesentlicher Aspekt die Annäherung zwischen der Bilanzierung vom Hedge Accounting und des Risikomanagements des Unternehmens.³⁷¹ Dies soll eine transparente Information für Stakeholder über die Sicherungseffekte ermöglichen und geht mit einer umfangreichen Offenlegung über das Risikomanagement einher.³⁷² Angesichts eines Risikomanagements, bei dem die Blockchain zur Verringerung der wesentlichen Risiken beitragen soll und benötigte Daten und Veränderungen in Echtzeit für das Risikomanagement bereitstellen kann, könnte der Prozess vom Hedge Accounting bis zum Risikomanagement vereinheitlicht werden.³⁷³ Beide Bestandteile wären dann über die Blockchain als Register miteinander verknüpft, sodass Anpassungen aus dem jeweiligen Bereich automatisiert in den anderen Bereich übernommen werden könnten.

Die Anwendung einer Blockchain im Finanzsystem profitiert maßgeblich von dem hohen Standardisierungsgrad der IFRS 9 und ermöglicht somit eine der Rechnungslegung entsprechende Automatisierung in den meisten Fällen. Die schnelle Übersetzung von Informationen aus der Blockchain in die Rechnungslegung, beispielsweise bei Zahlungsausfällen, trägt somit dazu bei die Ziele der IFRS 9, die als Reaktion auf die Finanzkrise entwickelt wurden, zu unterstützen. Allerdings könnten bestimmte Finanzbeziehungen nach derzeitigem

³⁷¹ Hierzu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 523.

³⁷² Dazu *Hartenberger* in IFRS-Handbuch, § 3 Rn. 523.

³⁷³ Ebenso *Peters/Panayi*, *Understanding Modern Banking Ledgers through Blockchain Technologies*, 2015, 25.

Regelungsstand auch weiterhin nur schwer über Smart Contracts entsprechend der Bilanzierung dargestellt werden. Ebenso ist der Korrekturfall in der Bilanzierung, ob nun nach IFRS oder anderen rechtlichen Vorgaben, eine Hürde für die Blockchain, die es zu beseitigen gilt.

IV. Anwendungen im Rechnungswesen und in der Wirtschaftsprüfung

1. Vergleich der doppelten Buchführung mit Triple Entry Accounting

Unternehmen verwenden zumeist ein System der doppelten Buchführung an,³⁷⁴ das sich während der Renaissance aufgrund des länderübergreifenden Handels und neuer Unternehmensformen etablierte.³⁷⁵ Dabei erfolgt die Änderung und Erfassung der Vermögensgegenstände und Schulden auf Bestandskonten, während auf den Erfolgskonten die Erträge und Aufwendungen erfasst werden.³⁷⁶ Die doppelte Buchführung stellt dabei sicher, dass die Salden der Erfolgskonten der Veränderung des Eigenkapitals in der Bilanz entsprechen.³⁷⁷ Folglich ermöglicht das Verfahren eine Kontrolle über die Richtigkeit der Buchhaltung für das Unternehmen. Allerdings benö-

³⁷⁴ Vgl. *Winnefeld* in *Winnefeld*, Bilanz-Handbuch, Rn. 720.

³⁷⁵ In Anlehnung an *Deloitte*, Blockchain Technology – A game-changer in Accounting?, 2016, 2.

³⁷⁶ Vgl. *Ballwieser* in *MüKoHGB*, § 238 Rn. 31.

³⁷⁷ Ähnlich *Ballwieser* in *MüKoHGB*, § 238 Rn. 31.

tigen auch Dritte, wie beispielsweise Aktionäre, eine verlässliche Bestätigung über die Angaben, sodass sie auf eine vertrauenswürdige Instanz angewiesen sind. Die Blockchain ermöglicht es, für eine Vielzahl von Buchungen der doppelten Buchführung eine solche vertrauenswürdige Plattform zu schaffen. Die darin enthaltenen Transaktionen spiegeln sich in den Buchungen der Rechnungslegung wider und sind zugleich kryptografisch gesichert, sodass sie nicht manipuliert werden können.³⁷⁸ Aus der doppelten Buchführung wird für zahlreiche Geschäftsvorfälle eine dreifache Buchführung. Wird beispielsweise der Kauf von Waren mit Zahlungsziel über die Blockchain gespeichert, würde die Transaktion die jeweiligen Buchungen über Warenabgänge und -zugänge, zu buchende Forderungen und Verbindlichkeiten, sowie den mit Zeitstempel versehenen digitalen Beleg enthalten. Die Transaktion wird durch das dezentrale Netzwerk bestätigt und durch die dezentrale Speicherung des Registers vor unberechtigten Änderungen geschützt.³⁷⁹ Unternehmen sind dadurch in der Lage, in Echtzeit die getätigten Buchungen zu überprüfen und bei den Stakeholdern ein höheres Vertrauen in die korrekte Buchhaltung ermöglichen.

Angesichts der hohen regulatorischen Anforderungen bei der Aufbewahrung von Unterlagen könne insbesondere die Nutzung digitaler Dokumente erleichtert werden, da umfangreiche präventive Maßnahmen gegen Datenmanipulation redu-

³⁷⁸ Dazu *Kiviat*, „Smart“ Contract Markets: Trading Derivates Contracts on the Blockchain, 2015, 20.

³⁷⁹ Hierzu *Deloitte*, Blockchain Technology – A game-changer in Accounting?, 2016, 3.

ziert werden könnten.³⁸⁰ Die Blockchain könnte also dazu beitragen, steuer- und handelsrechtliche Dokumente in digitalisierter Form revisionsicher zu speichern,³⁸¹ da sie eine verlässliche und authentifizierbare Datensicherung ermöglicht.³⁸² Zudem ist es vorstellbar, dass die in diesem Fall als Accounting-Register angelegte Blockchain auf die Bestätigung von Buchungssätzen und zugehörigen Dokumenten außerhalb der Interaktion mit Dritten ausgeweitet wird, sodass Geschäftsprozesse vollständig digitalisiert vorliegen würden.³⁸³ Ein Beispiel hierfür wären Neubewertungen. Eine vollständige Abbildung der Geschäftsprozesse auf einer Blockchain erfordert jedoch deutlich höhere Speicherkapazitäten und Rechnerleistungen bei den Unternehmen, um die ohnehin schon wachsenden Datenmengen adäquat verarbeiten zu können.³⁸⁴ Hinzu kommen automatisierte Transaktionsabwicklungen durch die Integration von Smart Property und Smart Contracts, sodass mit einer Veränderung der Rechnungslegung durch die Blockchain unter Berücksichtigung der jeweils vorhandenen Kapazitäten zu rechnen sein wird. Obwohl die digital verifizierten Belege einen hohen Informationsgrad

³⁸⁰ Hierzu *Deloitte*, Blockchain Technology – A game-changer in Accounting?, 2016, 3.

³⁸¹ Näheres dazu *Deloitte*, Blockchain-Technologie – Revisions sichere Archivierung, 2016, 2.

³⁸² Zu den Eigenschaften revisions sicherer Speicherung *Lemieux*, Trusting Records: Is Blockchain Technology the Answer?, Records Management Journal 2016, 110, 112-113.

³⁸³ Ebenso *Deloitte*, Blockchain Technology – A game-changer in Accounting?, 2016, 4.

³⁸⁴ Hierzu *Loitz*, Löst sich die Abschlussprüfung durch die Blockchain im Netz auf?, DB Nr. 42, 2016, M5, M5.

aufweisen, wird für das Verständnis der Unternehmensprozesse weiterhin die doppelte Buchführung benötigt. Allerdings wird die Kombination der zwei bestehenden Buchungssätze mit Anknüpfung an die dritte Buchung in der Blockchain zu einer sichereren Rechnungslegung führen, welche die Einhaltung der rechtlichen Vorgaben vereinfacht und gegenüber Stakeholdern ein höheres Vertrauen in die Unternehmensangaben etabliert. Triple-Entry Accounting ist jedoch nicht gleichbedeutend mit einer Abwehr aller potenziellen Manipulationen, welche die Rechnungslegung betreffen. Auch weiterhin sind nicht rechtskonforme Aktivitäten möglich, beispielsweise bei einer fehlenden buchhalterischen Erfassung. Folglich könnte auch der regulatorische Fokus verstärkt auf diese Aktivitäten gelegt werden, da reguläre Buchungen besser gesichert würden.

2. Prüfungshandlungen des Wirtschaftsprüfers

Angesichts der Erfassung rechnungslegungsrelevanter Daten auf einer Blockchain könnte die Technologie auch den Bereich der Abschlussprüfung nachhaltig verändern. Insbesondere im vergleichsweise einfach auf der Blockchain abzubildenden Bankenwesen sei zudem sogar die Integration der Ergebnisse der Abschlussprüfung in das Netzwerk selbst vorstellbar, um sie mit den Adressaten zu teilen.³⁸⁵ Die Technologie könnte jedoch auch eine effizientere Gestaltung der Prüfungshandlungen bei der Abschlussprüfung herbeiführen, indem die dezentral gespeicherten Informationen gezielt für Prüfungs-

³⁸⁵ Id.

handlungen herangezogen werden. Um mögliche Anwendungsfelder zu identifizieren, soll beispielhaft die Prüfungshandlung der Einholung von Bestätigungen Dritter unter Nutzung der Blockchain betrachtet werden.³⁸⁶ In welchem Ausmaß der Abschlussprüfer Einzelfallprüfungen wie die Einholung von Bestätigungen Dritter ausführen muss, ist von den Ergebnissen der Prüfung des internen Kontrollsystems und der aussagebezogenen analytischen Prüfungshandlungen abhängig.³⁸⁷ Demnach trägt ein funktionierendes rechnungslegungsbezogenes IKS beim Unternehmen dazu bei, die Anzahl der benötigten Einzelfallprüfungen zu reduzieren. Zu den Einzelfallprüfungen gehören unter anderem sogenannte Saldenbestätigen. Dies sind schriftliche Bestätigungen externer Dritter, welche die Höhe des Saldos zum geprüften Unternehmen bestätigen sollen.³⁸⁸ Saldenbestätigungen können beispielsweise bei der Prüfung der Forderungen aus Lieferungen und Leistungen notwendig sein. Sie sind Bestandteil von Routinetransaktionen,³⁸⁹ sodass dem IKS in der Sicherstellung der korrekten Ausführung eine hohe Bedeutung zukommt. Es besteht jedoch das Risiko, dass die Anfragen an Dritte unbeantwortet bleiben, sodass weitere Prüfungshandlungen nötig

³⁸⁶ Die Einholung von Bestätigungen Dritter ist Bestandteil der Prüfungshandlungen nach ISA 505 bzw. IDW PS 302 n.F.

³⁸⁷ Vgl. *IDW*, WPH Edition, Wirtschaftsprüfung und Rechnungslegung, Kap. L Tz. 855.

³⁸⁸ Hierzu *IDW*, WPH Edition, Wirtschaftsprüfung und Rechnungslegung, Kap. L Tz. 856.

³⁸⁹ Vgl. *IDW*, WPH Edition, Wirtschaftsprüfung und Rechnungslegung, Kap. L Tz. 855.

werden.³⁹⁰ Zudem müssen zusätzlich für Bundesbankguthaben und Guthaben bei Kreditinstituten Bankbestätigungen zum Abschlussstichtag,³⁹¹ sowie Informationen über die weiteren Geschäftsbeziehungen zu Kredit- und Finanzdienstleistungsinstituten eingeholt werden.³⁹²

Wird das IKS durch die Nutzung der Blockchain unterstützt, resultieren daraus veränderte Anforderungen an die Einzelfallprüfungen. Bei der Prüfung des IKS wird unter anderem ermittelt, wie die Richtigkeit der Rechnungslegung und die Einhaltung von rechtlichen Bestimmungen durch interne Kontrollmechanismen sichergestellt werden.³⁹³ Durch die Validierung und Abbildung zahlreicher Transaktionen durch die Blockchain sind die in der Rechnungslegung festgehaltenen Buchungen zu den Transaktionen ebenfalls effizienter auf ihre Richtigkeit zu überprüfen. Mithilfe der Blockchain könnte somit das bestehende Kontrollsystem zur Vermeidung und Aufdeckung von Fehlern verbessert werden. Dies hat einerseits zur Folge, dass weniger Einzelfallprüfungen durch den Abschlussprüfer vorgenommen werden müssen.³⁹⁴ Andererseits könnte auch der Abschlussprüfer durch einen temporä-

³⁹⁰ In Anlehnung an *IDW, WPH Edition, Wirtschaftsprüfung und Rechnungslegung*, Kap. L Tz. 862.

³⁹¹ Vgl. *IDW, WPH Edition, Wirtschaftsprüfung und Rechnungslegung*, Kap. L Tz. 856.

³⁹² Vgl. *IDW, WPH Edition, Wirtschaftsprüfung und Rechnungslegung*, Kap. L Tz. 890-891.

³⁹³ Hierzu *IDW, WPH Edition, Wirtschaftsprüfung und Rechnungslegung*, Kap. L Tz. 329.

³⁹⁴ Bei Annahme eines konstanten Prüfungsrisikos kann ein höheres Entdeckungsrisiko durch ein geringeres Fehlerrisiko aufgrund eines wirksamen IKS kompensiert werden. Hierzu *IDW PS 261 n.F. Tz. 2.1.*

ren Zugang Einsicht in das transparente Transaktionsregister nehmen. Dies bietet sich bei der Einholung von Bestätigungen Dritter an, falls die zu bestätigenden Werte wie beispielsweise Forderungen aus Lieferungen aus Leistungen auf der Blockchain gespeichert oder sogar ausgeführt werden. Anstelle schriftlicher Anfragen an Dritte könnte der Abgleich der gebuchten Werte direkt mit den Transaktionen in der Blockchain verglichen werden. Der Abschlussprüfer wäre bezüglich dieser Angaben nicht mehr auf nicht verpflichtende Antworten von Dritten angewiesen. Gleichsam könnten die benötigten Informationen zu den Geschäftsbeziehungen mit Kredit- und Finanzdienstleistungsinstituten zu zahlreichen Finanztätigkeiten auf der Blockchain ablesbar sein. So müsste beispielsweise die Bestätigung der Banksalden nicht mehr explizit angefordert werden. Auskünfte Dritter wären folglich nur noch für komplexere Geschäftsvorfälle notwendig. Anstelle der Einholung zeitaufwendiger Bestätigungen Dritter würde für viele Geschäftsvorfälle ein effizienter Prozess des Datenabgleichs anhand dezentraler und fälschungssicherer Register treten.

Die Nutzung der Blockchain-Technologie zum Zweck der Rechnungslegung ermöglicht eine erhebliche Reduktion des Aufwands für bestimmte Prüfungshandlungen, aber auch des Prüfungsbedarfs bei den Unternehmen. Nichtsdestotrotz bleibt die Funktion des Abschlussprüfers erhalten, da viele Prozesse weiterhin von menschlichen Entscheidungen und Ermessensspielräumen geprägt sein werden.³⁹⁵ So sind bei-

³⁹⁵ Ebenso *Loitz*, Löst sich die Abschlussprüfung durch die Blockchain im Netz auf?, DB Nr. 42, 2016, M5, M5.

spielsweise weiterhin eine Überprüfung der Rückstellungen bezüglich der angemessenen Höhe oder die Bewertung der festgestellten Unternehmensrisiken nicht ersetzbar.³⁹⁶ Ebenso rechtfertigten bestehende technische Schwächen der Blockchain, die manuelle Eingriffe zur Folge hätten, eine Überprüfung durch vertrauenswürdige Dritte.³⁹⁷ Abschließend ist festzustellen, dass die Unterstützung der Prüfung durch die Blockchain gleichzeitig eine Ausweitung anderer, anspruchsvollerer Prüfungshandlungen ermöglicht, sodass eine Qualitätssteigerung der Abschlussprüfung zu erwarten ist.

³⁹⁶ Id.

³⁹⁷ Id.

E. Technische Voraussetzungen für eine erfolgreiche Umsetzung

Die Analyse ausgewählter Anwendungsfälle für verschiedene Geschäftsfelder hat das Potenzial der Blockchain-Technologie für bestehende als auch neue Prozesse aufgezeigt. Gleichzeitig wurden jedoch technische Herausforderungen ersichtlich, welche die erfolgreiche Umsetzung der Mehrheit der diskutierten Anwendungsfälle behindern. Häufig auftretende Probleme betreffen unter anderem die Skalierbarkeit und den verwendeten Consensus Mechanismus, die Einschränkung der Datensichtbarkeit im Hinblick auf den Datenschutz, sowie die Fehlerberichterstattung von Codes und Daten.

Aus der Dezentralisation der Blockchain resultiere durch den dezentralen Validierungsprozess ein Trade-Off zur Skalierbarkeit,³⁹⁸ die jedoch für eine effiziente Performance beispielsweise im Finanzsektor benötigt werden. Größere Datenblöcke gingen zwar mit höheren Transaktionsraten einher, verursachten allerdings einen höheren Aufwand beim Proof-of-Work bei den Netzwerkteilnehmern.³⁹⁹ Dadurch würden die Dauer der Validierung und die Kosten steigen. Die Kapazitäten, die eine Blockchain allein für den Finanzsektor erreichen müsste, veranschaulicht bereits der Teilbereich der Transaktionsanzahl im bargeldlosen Zahlungsverkehr in der Europäischen Union. Schon hier wurden 2015 über 300 Mio. Transak-

³⁹⁸ Dazu *Back, et al.*, Enabling Blockchain Innovations with Pegged Sidechains, 2014, 4.

³⁹⁹ Vgl. *Back, et al.*, Enabling Blockchain Innovations with Pegged Sidechains, 2014, 4.

tionen pro Tag verzeichnet,⁴⁰⁰ denen nach heutigem Stand lediglich knapp 300.000 Transaktionen in der Bitcoin Blockchain mit dem derzeitigen Algorithmus entgegenstehen.⁴⁰¹ Weitere Anwendungsfälle, wie beispielsweise der vorgestellte Datenaustausch im Gesundheitswesen, würden die dezentral zu bestätigende Datenmenge erheblich steigern. Für Anwendungen wie das Clearing und Settlement zwischen Finanzinstituten entfällt jedoch aufgrund der fehlenden Anonymität der Akteure und der höchstwahrscheinlich zugangsbeschränkten Blockchain die Motivation für das Proof-of-Work.⁴⁰² Folglich sind alternative Consensus Mechanismen notwendig, um die Latenzzeiten zu verringern und die Skalierbarkeit der Blockchain zu erhöhen.⁴⁰³ Eine Vielzahl alternativer Mechanismen mit neuen Eigenschaften, die eine effizientere Validierung ermöglichen sollen, wird bereits getestet.⁴⁰⁴ Diese könnten in Abhängigkeit von den Anforderungen der betrachteten Anwendungsfälle für die jeweilige Blockchain implementiert werden.

⁴⁰⁰ Berechnung nach *Statista*, Anzahl der Transaktionen im bargeldlosen Zahlungsverkehr in den Mitgliedsländern der EU in den Jahren von 2011 bis 2015 (in Milliarden), *statista.com*, Stand: 14.03.2017.

⁴⁰¹ Vgl. *Blockchain Info*, Confirmed Transactions per Day, *blockchain.info*, Stand: 14.03.2017.

⁴⁰² Ebenso *Morini*, From „Blockchain hype“ to a real business case for Financial Markets, 2016, 4.

⁴⁰³ Hierzu *Mills, et al.*, Distributed ledger technology in payments, clearing, and settlement, Finance and Economics Discussion Series 2016-095, 2016, 14.

⁴⁰⁴ Näheres dazu *Matilla*, The Blockchain Phenomenon, ETLA Working Papers No. 38, 2016, 25.

Ein weiterer kritischer Punkt ist die technische Gewährleistung des Schutzes Transaktionsdaten vor Einsichtnahme durch Dritte. Insbesondere dem Schutz des privaten Schlüssels kommt eine entscheidende Bedeutung zu, da Transaktionen mit dem zugehörigen öffentlichen Schlüssel signiert werden müssen.⁴⁰⁵ Die Codes von Smart Contracts und Transaktionen sind für alle Netzwerkteilnehmer sichtbar, sodass hier unerwünschte Zugriffe auf Informationen erfolgen könnten.⁴⁰⁶ Unternehmen wie Banken können jedoch nicht nur über ihren öffentlichen Schlüssel in Erscheinung treten, wenn Vertragspartner mit ihnen interagieren sollen. Sie müssen ihre Identität preisgeben. Dies widerspricht dem berechtigten Interesse von Unternehmen oder Verbrauchern, Vertragshandlungen nicht öffentlich zugänglich machen zu müssen. Analog zur Verbesserung der Skalierbarkeit müssten alternative Mechanismen genutzt werden, um die Transaktionen nur unter Einschluss der Beteiligten zu validieren und die Sichtbarkeit auf der Blockchain nach Zugriffsrechten zu staffeln. Es sei daher in der Industrie damit zu rechnen, dass zugangsbeschränkte Blockchains schneller implementiert würden, da sowohl der Datenschutz, als auch die Skalierbarkeit in einem Umfeld aus bekannten Akteuren einfacher realisiert werden könnten.⁴⁰⁷ Doch auch innerhalb einer öffentlich nicht zugänglichen Blockchain sind die Akteure daran interessiert, unbeteiligte Netzwerkteilnehmer von Transaktionsdaten auszuschließen,

⁴⁰⁵ Ebenso *Peters/Panayi*, *Understanding Modern Banking Ledgers through Blockchain Technologies*, 2015, 9.

⁴⁰⁶ Hierzu *Ream, et al.*, *Upgrading blockchains: Smart contract use cases in industry*, Deloitte University Press, 2016, 6.

⁴⁰⁷ *Id.*

um unternehmerisch und strategisch relevante Informationen zu schützen. Von Bedeutung werden daher bilaterale Consensus Mechanismen sein, die eine solche Privatsphäre unter bekannten Netzwerkteilnehmern einer geschlossenen Blockchain ermöglichen.⁴⁰⁸ Bekannte öffentliche Blockchains, wie Bitcoin oder Ethereum, können in ihrer derzeitigen Funktionsweise die Privatsphäre und den Datenschutz nicht gewährleisten.⁴⁰⁹ Obwohl dies eine sinnvolle Weiterentwicklung für Unternehmen darstellt, erfolgt damit eine erhebliche Entfernung von der Funktionsweise der Blockchain, wie sie ursprünglich gedacht war.

Eine weitere wesentliche technische Hürde ist die inhärente Eigenschaft der Blockchain, aufgrund der dezentralen Speicherung und Verifizierung fälschungssicher zu sein. Diese Eigenschaft, die Vertrauen insbesondere bei nicht bekannten Transaktionspartnern schafft, ist gleichzeitig ein Problem für viele Anwendungen und die Einhaltung von rechtlichen Vorgaben. Kommt es zu fehlerhaften Dateneingaben oder Codes, ist in der ursprünglichen Blockchain kein Korrekturmechanismus vorgesehen. Die Abhängigkeit der aufeinanderfolgenden Datenblöcke in der Blockkette und der darin integrierten Automatisierungen würden zu schwerwiegenden weiterlaufenden Fehlern führen, deren Rückabwicklung zu mehr Komplexität

⁴⁰⁸ Einen solchen Node to Node Mechanismus beinhaltet bspw. R3 Corda für Finanzdienstleistungen des R3 Consortiums. Näheres dazu r3cev.com, Stand: 10.03.2017.

⁴⁰⁹ Hierzu *Morini*, From „Blockchain hype“ to a real business case for Financial Markets, 2016, 4.

xität des Systems beitragen würde.⁴¹⁰ Bei der Dateneingabe und bei der Programmierung von Smart Contracts muss daher im derzeitigen System besonders sorgsam vorgegangen werden, da Fehler nicht auf dem selben Weg behoben werden können. Vielmehr müssten beispielsweise alle Eventualitäten eines Smart Contracts programmiert werden. Da jedoch dort, wo menschliche Eingriffe benötigt werden, Fehler nicht auszuschließen sind, muss auch hier ein effizienter und schneller Mechanismus zur Korrektur geschaffen werden. Es bleibt daher festzuhalten, dass die grundlegende Funktionsweise der Blockchain eine Reihe von technischen Weiterentwicklungen benötigt, um rechtlichen und unternehmerischen Ansprüchen zu genügen. Diese Entwicklungen werden bereits vorangetrieben, um anwendungsspezifische Blockchains zu ermöglichen und auch weitere Aspekte wie die Datenkapazität und Kompatibilität mit externen Datenquellen zu verbessern. Es muss jedoch in Kauf genommen werden, dass die ursprünglichen Charakteristika der Blockchain erheblich modifiziert werden.

⁴¹⁰ Ebenso an *Shrier, et al.*, Blockchain & Transactions, Markets and Marketplaces, MIT, 2016, 10.

F. Fazit und Ausblick

Die Analyse ausgewählter Anwendungsfälle für die Blockchain-Technologie und der damit zusammenhängenden Smart Property und Smart Contracts zeigt das enorme Potenzial der dezentralen Netzwerke auf. Die wesentlichen Vorteile bestehen dabei in der Fälschungssicherheit, in der Schaffung von Vertrauen durch Dezentralität, der automatisierten Prozessausführungen und dem Verzicht auf Intermediäre. Besonders geeignet ist der Finanzsektor, da hier ein hoher Digitalisierungsgrad der Prozesse möglich ist. Die Ausübung und Einhaltung von Rechtsvorschriften kann sowohl durch die Blockchain erleichtert werden, als auch erschwert werden. Deutlich wird dies besonders am Beispiel von Smart Contracts. Einerseits ermöglichen sie die Sicherstellung der korrekten Vertragsausführung. Andererseits sind Rechte wie die Anfechtung technisch nicht vorgesehen. Ebenfalls zeigen sich die zu nehmenden Hürden bei der Skalierbarkeit, der Kompatibilität, dem Datenschutz und der Fehlerberichtigung. Es ist damit zu rechnen, dass eine flächendeckende Implementierung der vorgestellten Anwendungskonzepte trotz erster erfolgreich durchgeführter Testanwendungen noch eine mehrjährige Umsetzungsdauer erfordern wird. Dies liegt zum einen an den erforderlichen technischen Nachbesserungen an der Blockchain, um unter anderem prozessbedingte und rechtliche Korrekturerfordernisse gewährleisten zu können. Darüber hinaus muss zunächst die notwendige IT-Infrastruktur geschaffen werden, welche die zu erwartenden Datenmengen effizient verarbeiten und mit bestehenden Prozessstrukturen interagieren kann. Zum anderen liegen die

Prioritäten der Unternehmen zum derzeitigen Zeitpunkt möglicherweise bei anderen unternehmerischen Herausforderungen, die Investitionen in die Blockchain-Technologie hemmen. So sind beispielsweise Finanzinstitute im Zuge der Finanzkrise mit der Erfüllung hoher regulatorischer Anforderungen und Eigenkapitalerfordernisse konfrontiert, während die Niedrigzinsphase die Verdienstmöglichkeiten schmälert. Umfangreiche Systeminnovationen stehen zunächst nicht im Fokus. Der Kostendruck durch die niedrigen Zinsen könnte allerdings auch einen Anreiz hierfür schaffen, da die Blockchain durch automatisierte Prozessabwicklungen erhebliche Einsparpotenziale birgt. Insbesondere können First Mover diejenigen Akteure sein, welche die Infrastruktur kontrollieren und somit zusätzliche Gewinne erwirtschaften.

Darüber hinaus muss zwischen zugangsbeschränkten und öffentlichen Blockchains unterschieden werden. Während die Skalierbarkeit und der Schutz von Daten für zugangsbeschränkte Anwendungen, welche die meisten Unternehmen für ihre Angebote und Entwicklungen anstreben, ein geringeres Problem darstellt, wird dies eine Hürde für öffentliche Blockchains sein. Basisdemokratisch geprägte Projekte, die Vertrauen einzig durch die Dezentralität erzielen wollen, verteilen mehr Transaktionsinformationen über das Netzwerk als die diskutierten bilateralen Consensus Mechanismen in geschlossenen Systemen, in denen die Teilnehmer bekannt sind. Die Skalierbarkeit der beispielsweise mit Ether oder Bitcoin betriebenen Blockchains erfordert auch hier einen Wechsel zu alternativen Mechanismen, die schneller und energiesparender als der Proof-of-Work funktionieren. Für beide Anwendungsformen kommen unterschiedliche Ausgestaltungen in

Frage, wobei sich globale Blockchains wie bei der Bitcoin oder Systeme für einen spezifischen Zweck wie dem Clearing und Settlement Prozess etablieren könnten.

Die Bedeutung der Kryptowährungen ist zwar im Vergleich zum internationalen Finanztransaktionsvolumen trotz steigender Nutzerzahlen verschwindend gering. Doch gerade radikal dezentralisierte Blockchains sind auf ein funktionierendes Vergütungssystem angewiesen, um die Validierung der Transaktionen durchführen zu können. Für Transaktionen zwischen Privatpersonen, die nicht auf eine geschlossene Blockchain zurückgreifen können, könnten sich offene Plattformen wie Ethereum mit der Kryptowährung Ether durchsetzen, da sie weiterhin auf Intermediäre verzichten. Aus diesem Grund spielen klare rechtliche Einordnungen und die Regulierung der Kryptowährungen für die Zukunft zahlreicher Blockchainanwendungen und -unternehmen eine entscheidende Rolle. Sie sind notwendig, um den bisher kaum existierenden Verbraucherschutz und die Regulierung für Anwendungen unter Nutzung von virtuellen Währungen zu gewährleisten. Die bisherigen Einstufungen des EuGH oder der BaFin werden zu Recht als mangelhaft kritisiert. Bereits vorhandene Regulierungen sind wie die New Yorker Vorschriften räumlich beschränkt wirksam. Neu aufkommende Finanzdienstleister für Kryptowährungen erfordern jedoch, dass auch diese die Finanzmarktregulierungen erfüllen. Als Grundsatz sollte gelten, dass bankgleiche Geschäftsmodelle zu bankgleichen Risiken führen und somit rechtlich auch so zu handhaben sind. Die Kontrolle der dezentralen Plattformen selbst ist jedoch eine Herausforderung für die Regulierung, die keine dezentralen, sondern intermediäre Strukturen annimmt. Folg-

lich sollte eine Regulierung branchenunabhängig und möglichst auf länderübergreifender Ebene für die auf der Blockchain agierenden Dienstleister fokussiert werden.

Smart Contracts stellen wiederum eine besondere Herausforderung für das Rechtsverständnis dar. Zwar sind sie im Allgemeinen eindeutig keine Verträge im Rechtssinne. Sie können im Rahmen der Vertragsfreiheit jedoch als solche gestaltet werden, wobei durch die festgelegte Programmierung von Vertragsbedingungen andere rechtliche Handlungen nicht vorgesehen wären. Für den Gesetzgeber sind zwei Optionen möglich. Zum einen könnte mit der bestehenden Gesetzgebung oder gar einem spezifischen Gesetz für programmierte Verträge der Verbraucherschutz gestärkt werden, um dem Rechtsrahmen regulärer Verträge zu folgen. Insbesondere bei Vertragsbeziehungen zwischen Privatpersonen könnte durchaus auch ein alternativer Weg beschritten werden. Hierzu könnte der Ansatz des proaktiven Rechts genutzt werden, bei dem eine frühzeitige Optimierung von Vertragsgestaltungen eventuell kostspielige und zeitaufwendige Dispute nach Vertragsschluss verhindern soll.⁴¹¹ Das Recht sollte bei der Gestaltung von Smart Contracts dazu dienen, potenzielle Fehler zu entdecken und somit zu „besseren“ Verträgen führen. Der Ansatz setzt zwar ein höheres Maß an Eigenverantwortung bei den Vertragspartnern voraus. Allerdings ermöglicht er auch eine freiere Vertragsgestaltung, die Smart Contracts fördern würde.

⁴¹¹ Hierzu *Haapio*, Introduction to Proactive Law: A Business Lawyer's View, Scandinavian Studies in Law Vol. 29: A Proactive Approach, 2010, 21, 25.

Neue Technologien, wie einst das Internet, sind von jeher eine Herausforderung für die Gesetzgebung und Aufsichtsbehörden gewesen. Auch im Falle der Blockchain ist die Entwicklung und Nutzung von Kryptowährungen, Smart Contracts und Smart Property fortgeschritten, sodass der Gesetzgeber den identifizierten Risiken für die Märkte und Verbraucher begegnen muss. Obwohl die Blockchain als solches nicht reguliert werden kann, so können doch involvierte Unternehmen einer Regulierung unterworfen werden oder unterliegen diesen bereits umfassend, wie im Falle des hochgradig regulierten Finanzsektors. Mit den Chancen der Blockchain ergeben sich neue rechtliche Herausforderungen. Digital verwaltete Identitäten, die an die Identität der Nutzer geknüpft sind, werden eine hohe Bedeutung für digitale Authentifizierungsprozesse und die Nutzung von Smart Contracts erlangen. Sie sind jedoch auch ein Ziel für kriminelle Handlungen, da im Falle eines Identitätsdiebstahls weitaus umfangreichere Verträge geschlossen werden könnten. Dies erfordert somit den Schutz der digitalen Identität sowie der mit ihr verknüpften persönlichen Daten und Transaktionsinformationen. Maßgeblich für kommende Regulierungsbestrebungen werden auch Rechtsstreitigkeiten sein, die sich aus der Wirkungsweise der Blockchain ergeben. So könnten nicht löschbare Daten auf der Blockchain dem Recht auf Vergessenwerden,⁴¹² das ohnehin schon schwer im Internet umgesetzt werden kann, entgegenstehen. Auch Eigentumsübertragungen über die Blockchain könnten dann ein Problem darstellen, wenn eine

⁴¹² EuGH, Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 2.

Weiterveräußerung nicht wieder registriert wird und damit ab diesem Zeitpunkt kein verlässliches Eigentumsregister durch die Blockchain gegeben ist. Dies gilt ebenso im Falle von Smart Property, bei dem die Grenzen für einen automatisierten Nutzungsausschluss klar definiert sein müssen, um rechtliche Konflikte zu vermeiden.

Eine mögliche Regulierung der Blockchain-Technologie stellt jedoch keinesfalls eine Hürde für die Implementierung der vielfältigen Anwendungsmöglichkeiten dar. Vielmehr kann ein regulatorischer Rahmen dort, wo es notwendig erscheint, einen sicheren Umgang mit der Technologie schaffen. Notwendig ist hierfür ein rechtliches Umfeld, das sowohl Innovationen zulässt, als auch Verbraucher zuverlässig schützt. Gelingt dies, wird die Blockchain Geschäftsprozesse automatisieren und beschleunigen, und somit einen signifikanten Beitrag zur Digitalisierung der Wirtschaft beitragen.

Literaturverzeichnis

Accenture, & Clearstream, Collateral Management – Unlocking the Potential in Colleteral, 2011, unter: <http://www.clearstream.com/blob/10620/e5bf3b589c8f3ff6afd19166f9d53d3b/accenture-collateral-report-pdf-data.pdf> (Stand:20.03.2017).

Allianz, Erfolgreiches Pilotprojekt: Allianz Risk Transfer und Nephila realisieren Katastrophen-Swap mit Blockchain-Technologie Pressemitteilung vom 15.06.2016, unter: https://www.allianz.com/v_1465997377000/media/press/document/Press_Release_ART_Blockchain_pilot_DE_final.pdf (Stand: 29.01.2017).

Auffenberg, Lutz, Bitcoins als Rechnungseinheiten – Eine kritische Auseinandersetzung mit der aktuellen Verwaltungspraxis der BaFin, Neue Zeitschrift für Verwaltungsrecht 2015, 1184-1187.

Back, Adam, & Corallo, Matt, & Dashjr, Luke, & Friedenbach, Gregory, et al., Enabling Blockchain Innovations with Pegged Sidechains, 2014, unter: http://newspaper23.com/ripped/2014/11/http-____-____-__www__-blockstream__-com__-__sidechains.pdf (Stand: 07.02.2017).

BaFin, BaFin Merkblatt Finanzinstrumente (Aktien, Vermögensanlagen, Schuldtitel, sonstige Rechte, Anteile an Investmentvermögen, Geldmarktinstrumente, Devisen und Rechnungseinheiten), unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html;jsessionid=7BE2FD8DC7BD9F7AA3D18219CA772126.1_cid363

?nn=8236192#doc7852552bodyText4 (Stand: 28.01.2017).

Ballwieser, Wolfgang, in: Münchener Kommentar zum Handelsgesetzbuch, 3. Auflage, 2013.

Barber, Simon, et al., Bitter to Better – How to Make Bitcoin a Better Currency, in Financial Cryptography and Data Security, editiert von Keromytis, Angelos D., Springer Berlin Heidelberg, 2012, 399-414.

Beike, Rolf, & Schlütz, Johanna, Finanznachrichten lesen – verstehen – nutzen, Handelsblatt Bücher, 5. Auflage, 2010.

Bergmann, Christoph, Bitcoin und Geldwäsche – keine gute Idee, BitcoinBlog.de, Artikel vom 11.06.2014, unter: <https://bitcoinblog.de/2014/06/11/bitcoin-und-geldwasche-keine-gute-idee/> (Stand: 24.01.2017).

Biella, Matteo, & Zinetti, Vittorio, Blockchain Technology and Applications from a Financial Perspective, Technical Report Version 1.0, Unicredit, 2016, unter: <http://www.the-blockchain.com/docs/UNICREDIT%20-%20Blockchain-Technology-and-Applications-from-a-Financial-Perspective.pdf> (Stand: 16.08.2016).

Bitcoin.org, Bitcoin FAQ, unter: <https://bitcoin.org/de/faq> (Stand: 22.08.2016).

Bitcoinwiki, FAQ, 2016, unter: https://de.bitcoin.it/wiki/FAQ#Wie_lange_wird_es_da_uern_bis_alle_M.C3.BCnzen_generiert_sind.3F (Stand: 23.08.2016).

- Bitcoinwiki*, Browser based wallet, 2016, unter: [bithttps://en.bitcoin.it/wiki/Browser-based_wallet](https://en.bitcoin.it/wiki/Browser-based_wallet) (Stand: 30.08.2016).
- Blockchain Info*, Confirmed Transactions per Day, 2017, unter: <https://blockchain.info/de/charts/n-transactions> (Stand: 14.03.2017).
- Blockchain Info*, Blockchain Wallet Benutzer, 2017, unter: <https://blockchain.info/de/charts/my-wallet-n-users> (Stand: 20.01.2017).
- Blockchain Info*, Gesamtzahl der Bitcoins im Umlauf, 2016, unter: <https://blockchain.info/de/charts/total-bitcoins?timespan=all> (Stand: 23.08.2016).
- Blockchain Info*, Marktkapitalisierung, 2016, unter: <https://blockchain.info/de/charts/market-cap> (Stand: 23.08.2016).
- Boianovsky, Mauro*, Wicksell on Deflation in the Early 1920s, *History of Political Economy* 30(2), 1998, 219-275.
- Boehm, Franziska, & Pesch, Paulina*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Wahrung – Eine erste juristische Einordnung, *MultiMedia und Recht* 2014, 75-79.
- Bourque, Samuel, & Fung Ling Tsui, Sara*, A lawyer’s introduction to Smart Contracts, *Scientia Nobilitat Reviewed Legal Studies*, 2014, 4- 23.
- Braeckvelt, Francis*, Clearing, settlement and depository issues, *BIS Papers No 30*, 2006, 284-332, unter:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.1538&rep=rep1&type=pdf#page=293> (Stand: 12.02.2017).

Braun, Ulrich, in: Boos/Fischer/Schulte-Mattler, Kommentar zu Kreditwesengesetz, VO (EU) Nr. 575/2013 (CRR) und Ausführungsschriften, Band 1, 5. Auflage, 2015.

BTC-Echo, Bitcoin Akzeptanzstellen, unter: <https://www.btc-echo.de/bitcoin-akzeptanzstellen/> (Stand: 28.01.2017).

BTC-Echo, Bitcoin Wallet: Bitcoins sicher aufbewahren, [btc-echo.de](https://www.btc-echo.de/bitcoin-wallet/), unter: <https://www.btc-echo.de/bitcoin-wallet/> (Stand: 15.01.2017).

Bundesministerium der Finanzen, Antwortschreiben des BMF vom 20.06.2013 auf eine Schriftliche Anfrage des MdB Frank Schäffler, unter: http://wp1183395.server-he.de/FDP-Webseiten/FDP-www.frank-schaeffler.de/wp-content/uploads/2013/08/2013_06_20-Antwort-Bitcoin-Koschyk.pdf (Stand: 28.01.2017).

Bundesministerium der Finanzen, Antwortschreiben des BMF vom 07.08.2013 auf eine Schriftliche Anfrage des MdB Frank Schäffler, unter: http://www.frank-schaeffler.de/wp-content/uploads/2013/08/2013_08_07-Antwort-Koschyk-Bitcoins-Umsatzsteuer.pdf (Stand: 28.01.2017).

Burdekin, Richard C. K., & Siklos, Pierre L., Deflation – Current and Historical Perspectives, Cambridge University Press, 2004.

BusinessDictionary.com, front end application, unter:
<http://www.businessdictionary.com/definition/front-end-application.html> (Stand: 26.08.2016).

Busche, Jan, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 7. Auflage, 2015.

Buterin, Vitalik, A Next Generation Smart Contract & Decentralized Application Plattform, Ethereum White Paper, 2015.

Buterin, Vitalik, On Public and Private Blockchains, Ethereum Blog, 2015, unter:
<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> (Stand: 17.08.2016).

Chamber of Digital Commerce, Smart Contracts: 12 Use Cases for Business & Beyond – A Technology, Legal & Regulatory Introduction – Forward by Nick Szabo, White Paper, 2016, unter: <https://digitalchamber.org/smart-contracts/> (Stand: 20.02.2017).

Clack, Christopher D., & Bakshi, Vikram E., & Braine, Lee, Smart Contract Templates: foundations, design landscapes and research directions, Barclays, 2016, unter: <http://arxiv.org/abs/1608.00771> (Stand: 01.11.2016).

CoinGecko.com, Counterparty/US-Dollar Marktkapitalisierung, 2016, unter:
<https://www.coingecko.com/de/marktkapitalisierung/counterparty/usd> (Stand: 23.08.2016).

CoinGecko.com, Ethereum/US-Dollar Marktkapitalisierung, 2017, unter:

https://www.coingecko.com/en/market_cap/ethereum/usd (Stand:25.01.2017).

CoinGecko.com, Litecoin/US-Dollar Marktkapitalisierung, 2016, unter: <https://www.coingecko.com/de/marktkapitalisierung/litecoin/usd> (Stand: 23.08.2016).

Conrad, Isabel, & Hupertz, Peter, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Auflage, 2016.

Crosby, Michael, & Nachiappan, & Pattanayak, Pradan, & Verma, Sanjeev, & Kalyanaraman, Blockchain technology: Beyond bitcoin, Applied Innovation Review Issue No.2 2016, 6-19.

Dapp, Thomas F., & Karollus, Alexander, Blockchain – attack is probably the best form of defence, Deutsche Bank Research, 2016, unter: https://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD000000000359046.pdf (Stand: 09.01.2017).

De la Merced, Michael J., Bitcoin Rules Completed by New York Regulator, nytimes.com, Artikel vom 03.06.2015, unter: <https://www.nytimes.com/2015/06/04/business/dealbook/new-york-regulator-announces-final-rules-on-bitcoin.html> (Stand: 01.02.2017).

Deloitte, Blockchain-Technologie – Revisions sichere Archivierung, 2016, unter: <https://www2.deloitte.com/content/dam/Deloitte/de/>

Documents/Innovation/Blockchain_Revisionsssichere%20Archivierung.pdf (Stand: 24.02.2017).

Deloitte, Smart ID, unter: <http://www.deloitte.co.uk/smartid/> (Stand: 24.02.2017).

Deutsche Bundesbank, Glossar, unter: https://www.bundesbank.de/Navigation/DE/Service/Glossar/_functions/glossar.html?lv2=32052 (Stand: 30.12.2016).

Eckert, Hans-Werner, in: *Bamberger/Roth, Beck'scher Online-Kommentar BGB*, 41. Edition, 2016.

Engelhardt, Christian, & Klein, Sascha, Bitcoins – Geschäfte mit Geld, das keines ist – Technische Grundlagen und zivilrechtliche Betrachtung, *MultiMedia und Recht* 2014, 355-360.

Ethereum.org, FAQ: Who needs Ether?, 2016, unter: <https://www.ethereum.org/ether> (Stand: 24.08.2016).

Europäische Zentralbank, Die geldpolitische Strategie der EZB, 3. Auflage, 2011, unter: <https://www.ecb.europa.eu/pub/pdf/other/monetarypolicy2011de.pdf?0651d17c4b69dd55f5d21d93aa600694> (Stand: 29.03.2017).

Europäische Zentralbank, Virtual Currency Schemes, 2012, unter: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrency201210en.pdf> (Stand: 02.02.2017).

European Central Bank, Distributed Ledger Technology, In Focus Issue 1, 2016, unter:

https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf (Stand: 12.01.2017).

European Securities and Markets Authority, The Distributed Ledger Technology Applied to Securities Markets, Discussion Paper ESMA/2016/773, 2016, unter: https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf (Stand: 09.08.2016).

Europol, The Relentless Growth of Cybercrime, Pressemitteilung vom 27.09.2016, unter: <https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime> (Stand: 02.01.2017).

Everledger, *Everledger* Media One-Pager, unter: http://media.everledger.io/wp-content/uploads/2016/09/Everledger_OnePager_2016-1.pdf (Stand: 01.03.2017).

EY, Blockchain in health – How distributed ledgers can improve provider data management and support interoperability, 2016, unter: <https://www.hyperledger.org/wp-content/uploads/2016/10/ey-blockchain-in-health.pdf> (Stand: 24.02.2017).

Financial Crimes Enforcement Network, Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance, Subcommittee on Economic Policy, 19.11.2013, unter: <https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf> (Stand: 30.01.2017).

Finextra, Banking on Blockchain: Charting the Progress of Distributed Ledger Technology in Financial Services, White Paper, Finextra Research, 2016, unter: <https://www.ingwb.com/media/1609652/banking-on-blockchain.pdf> (Stand: 12.08.2016).

GEMA, Berechtigungsvertrag Fassung April 2016, § 1, unter: https://www.gema.de/fileadmin/user_upload/Gema/Berechtigungsvertrag.pdf (Stand: 20.02.2017).

Goetz, Charles J., & Scott, Robert E., Principles of Relational Contracts, 67 Virginia Law Review 1089 (1981).

Government Office for Science, Distributed Ledger Technology: beyond block chain – A report by the UK Government Chief Scientific Adviser, 2016, unter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Stand: 15.08.2016).

Grützner, Thomas, & Jakob, Alexander, in: Grützner/Jakob, Compliance von A-Z, 2. Auflage, 2015.

Guadamuz, Andres, & Marsden, Chris, Blockchains and Bitcoin: Regulatory responses to cryptocurrencies, First Monday Volume 20 Number 12-7, 2015.

Haapio, Helena, Introduction to Proactive Law: A Business Lawyer's View, Scandinavian Studies in Law Vol. 29: A Proactive Approach, 2010, 21-34.

Harper, Robert, Practical Foundations For Programming Languages, Cambridge University Press, 2016.

- Hartenberger Heike*, in: Beck'sches IFRS Handbuch, 5. Auflage, 2016.
- Herrmann, Andreas, & Huber, Frank*, Produktmanagement: Grundlagen – Methoden – Beispiele, Springer Gabler, 3. Auflage, 2013.
- J. P.*, Virtual Currency: Bits and bob, THE ECONOMIST, Artikel vom 13.06.2011, unter: <http://www.economist.com/blogs/babbage/2011/06/virtual-currency> (Stand:26.08.2016).
- Juels, Ari, & Kosba, Ahmed, & Shi, Elaine*, The Ring of Gyges: Using Smart Contracts for Crime, arXiv 2015, 54-85.
- Kaskaloglu, Kerem*, Near Zero Bitcoin Transaction Fees Cannot Last Forever, The International Conference on Digital Security and Forensics, DigitalSec 2014, 91-99.
- Kaplanov, Nikolei M.*, Nerdy Money: The Private Digital Currency, and the Case Against its Regulation, 5 Loyola Consumer Law Review 111 (2012).
- Kaulartz, Markus*, Die Blockchain-Technologie – Hintergründe zur Distributed Ledger Technology und zu Blockchains, Computer und Recht 2016, 474-480.
- Kaulartz, Markus, & Heckmann, Jörn*, Smart Contracts – Anwendungen der Blockchain-Technologie, Computer und Recht 2016, 618-624.
- Kaye Scholer*, An Introduction to Bitcoin and Blockchain Technology, 2016, unter: <http://www.kayescholer.com/docs/IntrotoBitcoinandBlockchainTechnology.pdf> (Stand: 16.08.2016).

Kindl, Johann, in: Bamberger/Roth, Beck'scher Online-Kommentar BGB, 41. Edition, 2016.

Kiviat, Trevor I., „Smart“ Contract Markets: Trading Derivates Contracts on the Blockchain, 2015, unter: http://www.academia.edu/10766594/_Smart_Contract_Markets_Trading_Derivatives_on_the_Blockchain (Stand: 01.02.2017).

Kociok, Carsten, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Auflage, 2016.

Kölvart Merit, & Poola, Margus, & Rull, Addi, Smart Contracts, in: Kerikmäe, Tanel, & Rull, Addi, The Future of Law and eTechnologies, Springer International Publishing, 2016, 133-147.

Krawiec, RJ, & Housman, Dan, & White, Mark, & Filipova, Mariya, & Quarre, Florian, et al., Blockchain: Opportunities for Health Care, Deloitte, 2016, unter: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf> (Stand: 24.02.2017).

Künnapas, Kaido, From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda?, in: Kerikmäe, Tanel, & Rull, Addi, The Future of Law and eTechnologies, Springer International Publishing, 2016, 111-131.

Lee, Larissa, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, 12 Hastings Business Law Journal 81 (2016).

Lemieux, Victoria L., Trusting Records: Is Blockchain Technology the Answer?, *Records Management Journal* 2016, 110-139.

Lessig, Lawrence, Code – Version 2, Basic Books, 2006.

Loitz, Rüdiger, Löst sich die Abschlussprüfung durch die Blockchain im Netz auf?, *Der Betrieb* Nr. 42, 2016, M5.

Lopatta, Kerstin, & Kaspereit, Thomas, & Böttcher, Katarina, & Geils, Christina, Kritischer Vergleich der Wertminderungsmodelle nach IAS 39 und IFRS 9 – eine Fallstudie, *Zeitschrift für Internationale Rechnungslegung* 2016, 499-505.

Mainelli, Michael, & Milne, Alistair, The Impact and Potential of Blockchain on The Securities Transaction Lifecycle, *Swift Institute Working Paper No. 2015-007*, 2016, unter: <https://www.swiftinstitute.org/papers/the-impact-and-potential-of-blockchain-on-securities-transaction-lifecycle/> (Stand: 16.08.2016).

Matilla, Juri, The Blockchain Phenomenon – The Disrupted Potential of Distributed Consensus Architecture, *ETLA Working Papers No. 38*, 2016, unter: <https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdf> (Stand: 09.08.2016).

Menn, Andreas, Wie Industrie 4.0 die Welt verändert, *wiwo.de*, Artikel v. 07.09.2016., unter: <http://www.wiwo.de/technologie/digitale-welt/industrielle-revolution-wie-industrie-4-0-die-welt-veraendert/14513854.html> (Stand: 30.03.2017).

Mills, David, & Wang, Kathy, Malone, Brendan, & Ravi, Anjana, et al., Distributed ledger technology in payments, clearing, and settlement, Finance and Economics Discussion Series 2016-095, Washington: Board of Governors of the Federal Reserve System, 2016, unter: <https://doi.org/10.17016/FEDS.2016.095> (Stand: 20.03.2017).

Monitor Deloitte, Blockchain @ Telco – How Blockchain can impact the telecommunication industry and its relevance to the C-suite, Informationsheft, 2016.

Morgan Stanley, Global Insight: Blockchain in Banking: Disruptive Threat or Tool?, 2016, unter: <http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf> (Stand: 17.08.2016).

Morini, Massimo, From „Blockchain hype“ to a real business case for Financial Markets, 2016, unter: <https://poseidon01.ssrn.com/delivery.php?ID=714022009114094069113066090097094126021037057034004075122020005076104021076119124117023061006041103116116085007004123067109120019027055089080084121069087080097072035043045027097066013103014064069088076120084029015109029120093096098020092065105090092&EXT=pdf> (Stand: 04.02.2017).

Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, unter: <https://bitcoin.org/bitcoin.pdf> (Stand: 09.08.2016).

Nees, Franz, Zukunft der Blockchain III: Banken vs. FinTechs – wer hat die Nase vorn?, finance-it-blog.de, Artikel v.

20.02.2017, unter: <http://www.finance-it-blog.de/hypes-trends-challenges/zukunft-der-blockchain-iii-banken-vs-fintechs-wer-hat-die-nase-vorn/> (Stand: 27.02.2017).

Nguyen, Tho Manh, Complex Data Warehousing and Knowledge Discovery for Advanced Retrieval Development: Innovative Methods and Applications, IGI Global, 2010.

Oechsler, Jürgen, in: Münchener Kommentar zum BGB, 7. Auflage, 2017.

Ogundeji, Olusegun, World Markets in Selloff, Trump Presidency Spikes Bitcoin Price, cointelegraph.com, 09.11.2016, unter: <https://cointelegraph.com/news/world-markets-in-selloff-trump-presidency-spikes-bitcoin-price> (Stand: 15.12.2016).

Papapaschalis, Panagiotis, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Auflage, 2015.

Peters, Gareth W., & Panayi, Efstathios, Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, 2015, unter: <http://papers.ssrn.com/abstract=2692487> (Stand: 09.08.2016).

Pilkington, Marc, Blockchain Technology: Principles and Applications, 2015, unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660 (Stand: 12.08.2016).

PwC, Bilanzierung von Finanzinstrumenten bleibt komplex auch mit dem neuen IFRS 9, unter: <http://www.pwc.de/de/kapitalmarktorientierte-unternehmen/bilanzierung-von-finanzinstrumenten-bleibt-komplex-auch-mit-dem-neuen-ifrs-9.html> (Stand: 14.03.2017).

Rath, Martin, Smart Contracts und das Blockchain-Prinzip – Das Ende der Juristen?, Ito.de, Artikel v. 30.08.2015, unter: <http://www.ito.de/recht/feuilleton/f/smart-contract-privatrecht-auto-vertrag-juristen-ersetzbar/> (Stand: 20.03.2017).

Ream, John, & , Chu, Yang, & Schatsky, David, Upgrading blockchains: Smart contract use cases in industry, Deloitte University Press, 2016.

Reid, Fergal, & Ferrigan, Martin, An Analysis of Anonymity in the Bitcoin System, in Security and Privacy in Social Networks, editiert von Altshuler, Yaniv, et al., Springer New York, 2012, 197-223.

Riedl, Thorsten, Derivate auf Knopfdruck, sueddeutsche.de, Artikel v. 23.09.2015, unter: <http://www.sueddeutsche.de/wirtschaft/blockchain-derivate-auf-knopfdruck-1.2661444> (Stand: 27.02.2017).

Saunders, Anthony, & Cornett, Marcia, Millon, Financial Institutions Management: A Risk Management Approach, Mc Graw Hill Education, 8. Auflage, 2014.

- Schmies, Christian*, Blockchain und Wertpapierabwicklung – Neue Technik bringt disruptive Veränderungen, Börsenzeitung, Ausgabe 232, Seite B14, 01.12.2016.
- Schulz, Bettina*, Die Spuren des Geldes – Die Digitalwährung Bitcoin hat die Blockchain bekannt gemacht – und zeigt gleichzeitig ihre Grenzen auf, DIE ZEIT Nr. 3/2016, 14.01.2016.
- Scott, Brett*, How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?, United Nations Research Institute for Social Development, Working Paper 2016-1, 2016, unter: <http://www.unrisd.org/brett-scott> (Stand: 15.08.2016).
- Shcherbak, Sergii*, How should Bitcoin be regulated?, European Journal of Legal Studies, Volume 7, Issue 1, 2014, 41-83.
- Shrier, David, & Iarossi, Jaclyn, & Sherma, Deven, Pentland, Alex*, Blockchain & Transactions, Markets and Marketplaces, Part 2, MIT Connection Science, 2016, unter: https://cdn.www.getsmarter.com/career-advice/wp-content/uploads/2016/12/mit_blockchain_transactions_report.pdf (Stand: 27.03.2017).
- Sinz, Ralf*, in: Uhlenbruck, Insolvenzordnung, 14. Auflage, 2015.
- Sixt, Elfriede*, Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie, Springer Gabler, 2017.

Sprenger, Bernd, & Herzog, Bodo, Währungsreform und soziale Marktwirtschaft, Konrad-Adenauer-Stiftung e.V., 2008.

Stagl, Jakob Fortunat, Die Eigentumsübertragung beim Kauf beweglicher Sachen – Gedanken über die Methode der Rechtsvereinheitlichung am Beispiel der Study Group on a European Civil Code, Jahrbuch Junger Zivilrechtswissenschaftler – Europäisches Privatrecht: Über die Verknüpfung von nationalem und Gemeinschaftsrecht, 2005, 369-397.

Statista, Anzahl der aktiven Accounts bei Paypal weltweit vom 1. Quartal 2010 bis zum 3. Quartal 2017 (in Millionen), unter:

<https://de.statista.com/statistik/daten/studie/300180/umfrage/aktive-accounts-bei-paypal-weltweit-quartalszahlen/> (Stand: 20.01.2017).

Statista, Anzahl der Transaktionen im bargeldlosen Zahlungsverkehr in den Mitgliedsländern der EU in den Jahren von 2011 bis 2015 (in Milliarden), unter: <https://de.statista.com/statistik/daten/studie/202811/umfrage/transaktionen-im-bargeldlosen-zahlungsverkehr-in-der-eu-ab-2006/> (Stand: 14.03.2017).

Statista, Bargeldumlauf im Euro-Währungsgebiet von 1999 bis zum 1. Halbjahr 2016 (in Milliarden Euro), unter: <https://de.statista.com/statistik/daten/studie/488222/umfrage/bargeldumlauf-im-euro-waehrungsgebiet/> (Stand: 24.01.2017).

Stobart, Simon, & Parsons, David, Dynamic Web Application Development: Using PHP and MySQL, Cengage Learning EMEA, 2008.

Surden, Harry, Computable Contracts, 46 U.C. Davis Law Review 629 (2012).

Swan, Melanie, Blockchain – Blueprint for a New Economy, O'Reilly Media, 2015.

Swanson, Tim, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015, unter: <https://de.scribd.com/doc/261055188/Consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems> (Stand: 01.03.2017).

Szabo, Nick, Smart Contracts, 1995, unter: <http://szabo.best.vwh.net/smart.contracts.html> (Stand: 20.05.2016).

Szabo, Nick, Formalizing and Securing Relationships on Public Networks, First Monday, Volume 2 Nr. 2, 1997.

Thoma, Jörg, Die Macht der Mining Pools, 2014, unter: <http://www.golem.de/news/bitcoin-die-macht-der-mining-pools-1403-105367.html> (Stand: 22.08.2016).

Thomas, Stefan, & Schwartz, Evans, Smart Oracles: A Simple, Powerful Approach to Smart Contracts, Artikel vom 17.07.2014, unter: <https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts> (Stand: 01.03.2017).

Thurow, Christian, Bitcoin in der IFRS-Bilanzierung, Zeitschrift für Internationale Rechnungslegung 2014, 197-198.

Tuttle, Brad, Bitcoin Prices Are Surging Again Amid Global Uncertainty, time.com, 28.12.2016, unter: <http://time.com/money/4618968/bitcoin-value-donald-trump-brexit-1000-dollars/> (Stand: 15.01.2017).

Ujo Music, The Problem, unter: www.theproblem.wtf (Stand: 18.02.2017).

U.S. Department of Health & Human Services - Office for Civil Rights, Breaches Affecting 500 or More Individuals, 2015, unter: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Stand: 24.02.2017).

Van de Velde, Jo, & Scott, Angus, & Sartorius, Katrina, & Dalton, Ian, Blockchain in Capital Markets – The Prize and the Journey, Euroclear, u. Oliver Wyman, 2016, unter: <http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf> (Stand: 14.01.2017).

Von Haller Grønbaek, Martin, Blockchain 2.0, smart contracts and challenges, Bird&Bird, Artikel vom 16.06.2016, unter: <https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges> (Stand: 28.02.2017).

Wäger, Christoph, in: Sölch/Ringleb, Umsatzsteuergesetz, 78. Ergänzungslieferung, Stand 09/2016.

Wetzel, Katharina, Im Fieber, Sueddeutsche.de, Artikel vom 16.03.2016, unter: <http://www.sueddeutsche.de/wirtschaft/blockchain-im-fieber-1.2908084> (Stand: 12.12.2016).

Winnefeld, Robert, in: Winnefeld, Bilanz-Handbuch, 5. Auflage, 2015.

Wright, Aaron, & De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 2015, unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (Stand: 29.03.2017).

Wu, Roger, Why We Accept Bitcoin, Forbes, 2014, unter: <http://www.forbes.com/sites/groupthink/2014/02/13/why-we-accept-bitcoin/#351e1f5b130b> (Stand:24.08.2016).

Yermack, David, Corporate Governance and Blockchains, National Bureau of Economic Research, Working Paper 21802, 2015, unter: <http://www.nber.org/papers/w21802> (Stand: 17.08.2016).

Zyskind, Guy, & Nathan, Oz, & Pentland, Alex, Enigma: Decentralized Computation Platform with Guaranteed Privacy, Whitepaper, 2015. unter: <https://arxiv.org/pdf/1506.03471.pdf> (Stand: 12.02.2017).

