UNIVERSITÄT LEIPZIG

Juristenfakultät

JUSTiCE

Gutachten

BLOCKCHAIN-TECHNOLOGIE, SMART CONTRACTS UND SELBSTVOLLZIEHENDE VERTRÄGE

Eine Analyse der Chancen und Risiken einer Zukunftstechnologie sowie der Vereinbarkeit der Systemkreise Technik und Recht

Erstellt für das Bundesministerium der Justiz und für Verbraucherschutz vom Lehrstuhl für Bürgerliches Recht, Rechtsgeschichte und Europäische Rechtsharmonisierung, Universität Leipzig im Rahmen des Projekts *JUSTiCE*

Stand: Juni 2019

ptble
Projektträger Bundesanstalt für Landwirtschaft und Ernährung

Gefördert durch:
Bundesministerium der Justiz und für Verbraucherschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge

Eine Analyse der Chancen und Risiken einer Zukunftstechnologie sowie der Vereinbarkeit der Systemkreise Technik und Recht

Nico Bilski, Universität Leipzig

Juni 2019

Die Förderung des Vorhabens erfolgte aus Mitteln des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) aufgrund eines Beschlusses des deutschen Bundestages. Die Projektträgerschaft erfolgte über die Bundesanstalt für Landwirtschaft und Ernährung (BLE) im Rahmen des Programms zur Innovationsförderung.

Inhaltsverzeichnis

Vorwort

Nur wenige Informationstechnologien erfreuten und erfreuen sich in den letzten Jahren ähnlicher Aufmerksamkeit wie die Distributed- Ledger-Technologien: Ihre bekannteste Ausformung – die Blockchain – und deren Referenzimplementation „Bitcoin“ lösten in den Massenmedien einen regelrechten Hype aus, der Schlagworte wie „Smart Contracts“ oder „Krypto-Token“ in die politischen, wirtschaftlichen und gesellschaftlichen Diskussionen brachte. Getragen wurde diese Euphorie von dem Glauben, dass die Distributed-Ledger-Technologie zur „Disruption“ bestehender zentraler Machtstrukturen und deren Ersetzung durch dezentrale Systeme führen könnte.

Auch in der juristischen Fachliteratur erregte die Blockchain beachtliches Interesse. Die hierdurch hervorgerufene Flut rechtswissenschaftlicher Beiträge überzeugt jedoch nicht immer. Die Schwäche der juristischen Literatur liegt dabei vor allem im technischen Bereich: Schon die oft ungenaue Verwendung der Fachbegriffe zeigt in vielen Fällen, dass sich die Verfasser nur oberflächlich mit den technischen Aspekten auseinandergesetzt haben; in etlichen Beiträgen trifft man zudem eher auf auf Aneinanderreihungen von *buzzwords* als auf klare Zuordnungen von Technologien zu rechtlichen Konzepten. Die Grenzen zwischen informativ-wissenschaftlichen und werbenden Publikationen verschwimmen dabei und erschweren die Bewertung von Anwendungsszenarien und -potentialen; in mancherlei Hinsicht scheint der juristische Diskurs sogar völlig von den technischen Entwicklungen und ihrer kommerziellen und industriellen Anwendung entkoppelt zu sein. Dieser Zustand macht es für Unternehmen und Politik schwierig, klare und rechtlich abgesicherte Zielvorgaben mit der Technologie zu verbinden.

Das vorliegende Gutachten adressiert dieses Defizit, indem es die zugrundeliegenden technischen Aspekte und Konzepte darstellt, in die jeweiligen Kontexte einordnet und versucht, die technischen Neuerungen in rechtlichen Kategorien zu erfassen. Einen Schwerpunkt bildet das Konzept des *Smart Contract*, das schon wegen seiner unglücklichen Benennung regelmäßig zu Missverständnissen führt. Das Gutachten geht soweit auf dieses Konzept ein, wie es für das juristische Verständnis erforderlich ist und analysiert zudem die Einsatzpotenziale „intelligenter Verträge“. Dabei zeigt es, dass ein vollautomatisierter und verselbständigter Vertragsvollzug keineswegs so vorteilhaft ist, wie es von einigen Seiten behauptet wird.

Das Gutachten wurde für das Bundesministerium der Justiz und für Verbraucherschutz von Herrn Nico Bilski unter der Betreuung von Herrn Prof. Dr. Michael Zwanzger verfasst. Es handelt sich um ein Teilergebnis des Forschungsprojekts JUSTiCE (Branchenübergreifende juristische, technische sowie ökonomisch-soziale Analyse von Smart Contracts im Kontext der Sharing Economy und Evaluation von Chancen, Risiken und Gestaltungsaspekten des Verbraucherschutzes unter Einsatz der Blockchain-Technologie in Deutschland und im europäischen Rechtsraum). Das Projekt ist Teil des vom BMEL ausgeschriebenen Programms „Wandel der Verbraucherrollen – Prosuming, kollaborativer Konsum, Ko-Produktion et.“ im Rahmen des Programms zur Innovationsförderung im Verbraucherschutz in Recht und

Wirtschaft. Die Untersuchung gliedert sich dabei in folgende Kapitel: Zunächst erfolgt eine technologische Beschreibung der Blockchain-Technologie (I) unter Einbeziehung der Entwicklungsgeschichte und Risikobewertung. Anschließend erfolgt eine technische und rechtliche Einordnung sog. Smart Contracts (II) sowie eine Einführung in weitere technische Konzepte im Kontext der Blockchain (III). Nachdem die Erwartungen an selbstvollziehende Verträge betrachtet wurden (IV), werden deren Erfolgserwartungen anhand der technischen (V) und rechtlichen Risikoanalyse (VI) evaluiert und Handlungsstrategien erarbeitet, wie sich Smart Contracts und selbstvollziehende Verträge in das Rechtssystem einbetten lassen (VII). Die folgenden Kapitel widmen sich einigen Einzelfragen, u.a. der Einordnung sog. Token (VIII), aufsichts- und regulierungsrechtlichen Fragestellungen im Überblick (IX), gesellschaftsrechtlichen Implikationen bei dezentralen Netzwerken (X) sowie dem Datenschutz (XI). Nach einem Blick auf die Alleinstellungsmerkmale und Perspektiven konsortial ausgerichteter Netzwerke (XII) werden schließlich die aktuellen Entwicklungen unter dem Blickwinkel des Verbraucherschutzes betrachtet (XIII). In den abschließenden Kapiteln erfolgt vor der Zusammenfassung der Ergebnisse noch eine Evaluation gesetzgeberischen Handlungsbedarfs sowie ein Ausblick auf die Entwicklungsperspektiven der Technologie.

Leipzig, 30.06.2019

I. Die Blockchain-Technologie

1. Einführung

a) Terminologie

Die Blockchain lässt sich den sog. **Distributed-Ledger-Technologien** zuordnen. Im Prinzip geht es um die verteilte und geteilte Verwaltung von Datensätzen in einem dezentralen dezentralen Datenregister. Durch die unmittelbare Verknüpfung aller am Netzwerk beteiligten Personen entsteht zugleich ein Netzwerk. Damit können nicht nur Transaktionsergebnisse und andere Informationen sicher gespeichert und später verifiziert, sondern zugleich auch digitale Werte an andere Netzwerkteilnehmer übertragen bzw. mit diesen getauscht werden.[1] Das besondere Konsens- und Validierungssystem sowie verschiedene kryptografischen Verfahren sorgen für eine besonders hohe Sicherheit und Authentizität der gespeicherten Daten.

Man kann sich das System wie das **Transaktionsregister** eines klassischen Handelsbuchs vorstellen, das in einer Tabelle Urheber, Adressat, Zeit und Inhalt von Transaktionen oder sonstigen Einträgen auflistet, und dessen Einträge mit einer entsprechenden Berechtigung verändert werden können.

Nr.	Nutzer	Einheit	Menge	Zeit
1	System an A	Bitcoin	50	12/02/18, 12:12:12
2	System an B	Bitcoin	50	12/02/18, 12:12:13
3	A an B	Bitcoin	30	13/02/18, 14:19:24
4	B an C	Bitcoin	20	13/02/18, 14:34:46

Diese Daten werden jedoch nicht bei einer zentralen Stelle, sondern **redundant** in einer auf vielen Rechnern gleichzeitig gepflegten Datei abgespeichert – daher die Bezeichnung als **verteiltes Kassenbuch** (*engl.* = Distributed-Ledger).[2]

Bei einer **Blockchain** handelt es sich um einen besonderen Fall einer solchen Datenstruktur, bei der die eingehenden Transaktionen zunächst gesammelt und zu verschlüsselten **Blöcken** gebündelt werden. Anschließend wird der neue Block an die Reihe bereits bestehender Blöcke angefügt, wobei sie linear und untrennbar miteinander **verkettet** werden. Durch die feste Verknüpfung entsteht aus den zahlreichen Einzeltransaktionsdaten ein umfassendes, chronologisches Register. Jeder Teilnehmer ist im Besitz einer eigenen, lokalen Kopie dieser Kette an Blöcken – der Blockchain.

[1] Vgl. *Walport*, Distributed-Ledger Technology, S. 5.

[2] *Walport*, S. 17. Nachfolgend werden als Akronyme für die Begriffe Distributed-Ledger "DLßowie für Distributed-Ledger-Technologie "DLT"verwendet.

b) Wesentliche Vorzüge der Technologie

Der Kernvorteil dezentraler **Datenstrukturen**, im Folgenden auch **Ledger**, besteht in ihrer besonderen **Nachvollziehbarkeit** und **Fälschungssicherheit**. Die Informationen werden nicht bei einer einzigen Stelle, sondern dezentral verwaltet, alle Daten vor der Abspeicherung verifiziert und durch die Verteilung so gespeichert, dass sie später grundsätzlich nicht mehr verändert werden können. Eine Manipulation ist nach dem Systemgedanken nicht bzw. nur unter prohibitiven Kosten möglich. Die DL-Technologie soll damit insbesondere den Verzicht auf eine zentrale, alle Daten allein bei sich speichernde Instanz ermöglichen.[3]

Wo es normalerweise eines unabhängigen Vermittlers, einer „Trusted 3rd Party", bedarf, um die Richtigkeit von Transaktionsdaten zu gewährleisten, wird die **vertrauensstiftende Funktion** durch das Netzwerk selbst erfüllt. Jeder kann anhand seiner eigenen Kopie des Ledger jederzeit anonymisiert und zweifelsfrei nachvollziehen, wer gerade im Besitz eines (digitalen) Wertes ist (**Auditierbarkeit**). Klare Regeln geben dabei vor, welche Version der Blockchain als die richtige gilt – über welche sog. Konsens herrscht.

Das Potential der Blockchain zeigt sich etwa beim **Zahlungsverkehr**. Bislang verifiziert klassischerweise eine Bank als neutrale Vermittlerin eine entsprechende Kontodeckung, bevor eine Übertragung akzeptiert wird. In einem DL-System übernimmt diese Funktion das Netzwerk selbst.[4] Durch den offenen Zugang und den **Wegfall zentraler Instanzen** stößt die DLT auch im Bereich der Sharing Economy auf Interesse, da sie Verbrauchern neue Teilhabemöglichkeiten am Wertschöpfungsprozess bietet und ihr deshalb insbesondere das Potential zugeschrieben wird, zentrale Plattformanbieter durch selbstorgansierte oder jedenfalls kostengünstigere und transparentere Strukturen abzulösen.[5]

Als weiterer Vorteil der Technologie kommt hinzu, dass die Gefahr der Zensur durch oder des Angriffs auf eine zentrale Stelle entfällt. Es gibt damit **keinen „(single) point of failure"**, sodass eine Manipulation bzw. der Ausfall einzelner Netzknoten das Gesamtsystem nicht beeinträchtigen würde.

c) Bitcoin als erster Anwendungsfall

Die erste erfolgreiche Umsetzung eines DL gelang im Jahre 2008 in Form mit der Kryptowährung **Bitcoin**.[6] Das technische Konzept der zugrundeliegenden Blockchain wurde unter dem Pseudonym[7] Satoshi Nakomoto in „Bitcoin: A Peer-to-Peer Electronic Cash System" veröffentlicht. Im Jahr

[3] *Walport*, S. 14.

[4] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 2.

[5] Vgl. auch *Lauslathi/Mattila/Sepällä*, Smart Contracts, S. 7 f. Zum derzeit dennoch begrenzten Einsatz im Verbraucherkontext S. 112 ff.

[6] Eine Währung im eigentlichen Sinne liegt bei Bitcoin jedoch nicht vor. Es werden lediglich digitale Assets gehandelt, die teilweise als Zahlungsmittel akzeptiert werden. Sie sind hingegen im Gegensatz zu Fiatgeld weder von einer öffentlichen Stelle ausgegeben noch kontrolliert, vgl. auch *Langenbucher*, AcP 218 (2018), 385 (394 ff.).

[7] Es ist bis heute unklar, welche Person oder Personengruppe hinter dem Namen steht.

2009 erfolgte schließlich die Umsetzung durch die Online-Stellung des Bitcoins. Der Durchbruch gelang insbesondere deshalb, weil Bitcoin erstmals das sog. *Double-Spending*-Problem lösen konnte, es also trotz des Fehlens einer alle Transaktionen kontrollierenden Stelle verhindert, dass Werte mehrfach ausgegeben bzw. versendet werden.[8]

d) Die Blockchain als Teil des dezentralisierten Webs

Die Erfolgsgeschichte des World Wide Web (WWW) begann Anfang der 1990er Jahre. Das TCP/IP-Protokoll stellte die Infrastruktur für einen digitalen und damit globalen Informationsaustausch bereit. In dieser ersten Generation ("Web 1.0") war jedoch noch nicht viel mehr als das statische Bereitstellen von Daten (quasi das Hochladen einer PDF-Broschüre) oder senden elektronischer Nachrichten möglich.[9] Anfang der 2000er Jahre vollzog sich mit der Erweiterung des Informationsnetzwerks um programmierbare Anwendungen ein weiterer Entwicklungsschritt hin zum sog. "Web 2.0". Jedermann konnte nun Inhalte nach Belieben bearbeiten und verteieln. Interaktive Websites und Social-Media-Anwendungen, wie wir sie heute kennen, sind die Früchte dieser neuen Entwicklungsstufe. Die Betreiber solcher Websites kamen jedoch mit steigenden Nutzerzahlen und Datenmengen zu einer größeren Marktmacht. Große Plattformen erzeugen Abhängigkeiten, sei es in ihrer Funktion als Intermediäre, aber auch im Hinblick auf die Nutzer bestimmter Anwendungen. Wie die nächste Entwicklungsstufe des WWW aussehen könnte, ist offen. Für einige könnte diese darin bestehen, den Nutzern mehr Einfluss zu geben, indem neue Technologien die derzeitigen Machtstrukturen aufbrechen und diese durch dezentrale Systeme ersetzen.[10]

Ob die DLT tatsächlich zu einem "Web 3.0"führt, sei an dieser Stelle dahingestellt. Eine Blockchain wäre im Zusammenhang des **dezentralisierten Webs** jedenfalls nur als ein **Baustein** zu sehen. Sie übernimmt unter anderem die Aufgabe der Datenverarbeitung, vergleichsweise eines Prozessors eines dezentralen Computers.[11] Für ein funktionierendes dezentrales Ökosystem müssen jedoch u.a. noch Protokolle, Anwendungsebenen, Interaktionsschnittstellen für den Nutzerzugriff (sog. *user interface*, Kommunikationskanäle und Speichersysteme hinzukommen. Die Blockchain-Technologie ist für die soeben aufgezählten Funktionen alleine weder geeignet noch gedacht.

Die **Dezentralität** zielt dabei auf ein spezifisches Problem ab. Bislang mussten die Nutzer eines Systems einer zentralen Stelle vertrauen, die alle Informationen speichert und bereitstellt. Das konnte bislang etwa ein Website-Betreiber sein. Bedeutsam war und ist aber insbesondere der Fall, dass mit einer bislang unbekannten oder jedenfalls nicht vollständig vertrauenswürdigen Partei kontrahiert werden sollte. Um nicht selbst aufwands- und kos-

[8] Ausführlich dazu *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2093 f.).

[9] Vgl. zum Ganzen *Voshmgir*, Blockchains, Smart Contracts und das Dezentrale Web, S. 10.

[10] So etwa *Voshmgir*, S. 10. Für andere ist das "Web 3.0"hingegen das "Webäutonomer Maschinen oder das "Webïntelligenter Datenverarbeitung. Es handelt sich insofern nicht um gesetzte Begriffe.

[11] *Voshmgir*, S. 10.

tenintensiv die Integrität der Person und relevanter Daten überprüfen zu müssen, wurde häufig ein Intermediär zwischengeschaltet. Hierdurch entstanden aber ebenso Kosten, verbunden mit einer Machtkonzentration in der Person des Intermediärs. Die DLT will dieses Phänomen aufbrechen, indem das dezentrale Netzwerk aus sich selbst heraus vertrauensstiftendend wirken soll. Kann eine verteilte Verantwortung tatsächlich die versprochene Sicherheit und Integrität gewährleisten? Wann und unter welcher Gestaltung tatsächlich entsprechende Vorteile absehbar sind, soll im Folgenden näher dargelegt werden.

2. Ausgestaltungsmöglichkeiten und Typen dezentraler Systeme

Es gibt nicht *die eine* Blockchain, sondern eine große **Bandbreite** an Möglichkeiten, wie man ein DL-System ausgestalten kann. Eine wesentliche Kategorisierung lässt sich sowohl danach vornehmen, wer Teilnehmer einer Blockchain sein kann, wie auch, für wen die gespeicherten Informationen einsehbar sind.

a) Permissionless oder permissioned (Schreib- und Zugangsberechtigung)

Steht die Teilnahme und Schreibberechtigung grundsätzlich jedem offen, handelt es sich um eine **zulassungsfreie (*unpermissioned* bzw. *permissionless*)** Blockchain. Auch hier kann es freilich Nutzer mit Sonderrechten oder verschiedene Rollenmodelle geben. In *permissioned* Ledger hängt die Zulassung hingegen von bestimmten Kriterien, insbesondere der Zustimmung eines oder mehrerer Teilnehmer ab.

Ein Sonderfall sind dabei die nach einem sog. **Konsortialsystem** aufgebauten Netzwerke, bei denen nicht eine einzelne Stelle über die Teilnahme entscheidet, sondern ein Zusammenschluss mehrerer, häufig gleichberechtigter Akteure zu einem Netzwerk erfolgt.[12] Diese können sich dann etwa per Mehrheitsentscheidung abstimmen oder einen Regulator einsetzen, der bestimmte Prozesse überwacht und leitet.[13]

b) Public oder private (Leseberechtigung)

In einem **öffentlichen (*public*) Ledger** können die Inhalte von jedermann frei und in Echtzeit gelesen werden. In einer **privaten** Blockchain stehen die Einsichtsrechte wiederum nur den jeweiligen Teilnehmern zu. Die meisten privaten Blockchains sind gleichzeitig zulassungsbeschränkt, sodass in einigen Publikationen oder Technologiebeschreibung schlicht von privaten Blockchains gesprochen wird. Es kann jedoch auch in zulassungsbeschränkten Systemen ein besonderes Interesse an der Transparenz und Nachvollziehbarkeit der gespeicherten Daten bestehen, sodass ein zulassungsbeschränkter oder konsortialer Ledger *public* ausgestaltet ist.

[12] *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (141).
[13] Vgl. auch *Swanson*, Consensus-as-a-service, S. 21 f.

c) Zahlreiche Gestaltungsmöglichkeiten

Das von vielen als „Idealfall“ beschriebene dezentrale Netzwerk ist öffentlich und zulassungsfrei ausgestaltet, wobei alle Nutzer über dieselben Rechte verfügen. Insbesondere in den zulassungsbeschränkten Systemen sind jedoch **zahlreiche Gestaltungsmöglichkeiten** denkbar: So könnten etwa nur bestimmte Teilnehmer über Einsichts- oder Bearbeitungsrechte verfügen, Schlichtungsverfahren abgebildet oder Mehrheitsentscheidungen vorgesehen werden. Durch die Einrichtung von **Kanälen** (sog. Channel), wie sie bei privaten Blockchains basierend auf *Hyperledger Fabric* verwendet werden, ist auch eine selektive Informationsverbreitung möglich. Dabei werden die Daten nur mit den Teilnehmer des jeweiligen Channel geteilt, während auf dem allen Teilnehmern offenstehenden Hauptkanal (Main-Channel) nur ein verschlüsselter[14] Nachweis zur späteren Verifikation hinterlegt wird.[15] Private Channel können so als eine Art Subnetz zur Abwicklung vertraulicher Geschäfte oder dem Austausch vertraulicher Informationen verwendet werden.

Ähnlich wie im Beispiel der ***Channel*** können auch selbständige DL-Systeme miteinander **verknüpft** werden. Denkbar wäre etwa, dass eine sog. Relaychain (Verknüpfungskette) Daten zweier Ledger zusammenführt oder dass einzelne Blöcke oder Blockinhalte auf dritte Ledger (sog. Sidechains) ausgelagert werden.[16] Beispielsweise könnte man einen Ledger, der die einzelnen Stationen einer Wertschöpfungskette überwacht, mit den Daten eines Vertragsbeziehungen und Abrechnungen verwaltenden Ledgers koppeln.

d) Überblick zu den Entwicklerplattformen

Die Dezentralität ist, wie gezeigt, stark systemabhängig. Maßgeblich ist im Einzelfall das verwendete Protokoll.[17] Neben der viel beachteten Bitcoin-Blockchain sind vor allem drei Netzwerke beachtlich: **Ethereum**, das als erste eine populäre Grundlage zur Implementierung von ausführbarem Programmcode und damit Business-Logiken anbot, die **Hyperledger Fabric**, ein Teilprodukt des Hyperledger Projekts unter besonderem Einfluss von **IBM**, welches sich insb. auf die Ausarbeitung sog. privater oder zulassungsbeschränkter Blockchain-Anwendungen konzentriert, und **IOTA**, mit welchem die IOTA-Foundation auf Schnittstellen zum sog. Internet of Things (IoT)[18] abzielt.

[14] Zum Verfahren S. 8 ff.

[15] *Wagner/Groß*, Blockchain, S. 21.

[16] Vgl. *Kolain/Wirth*, DSRI 2017, 845 (849 f.), *Grigg*, The sum of all chains.

[17] Unter einem Protokoll versteht man den programmierten Regelsatz für die Interaktion in einem Netzwerk und dessen Funktionsweise, inklusive möglicher Inhalte, Handlungen, Bezeichnungen, etc. Ein Kommunikationsprotokoll definiert beispielsweise Format, Abfolge, Inhalt und Bedeutung der auszutauschenden Nachrichten. Das Protokoll eines DL regelt entsprechend die Funktionsweise des Systems

[18] Das sog. Internet der Dinge bezeichnet die Vision von miteinander vernetzten Maschinen und Geräten, die damit selbständig kommunzieren und ihre Aufgaben autonom erfüllen können.

3. Grundkonzepte

Die Grundkonzepte von DL-Systemen sollen im Folgenden am Beispiel der Blockchain-Technologie erläutert werden.[19]

a) P2P-Netzwerk

Erstes kennzeichnendes Element ist die Struktur als sog. **Peer-to-Peer-Netzwerk** (P2P-Netzwerk). Im Gegensatz zu herkömmlichen Netzwerken, bei denen alle Daten bei einer zentralen Stelle liegen und dieser entsprechend großer Einfluss zukommt, sind in einem P2P-Netzwerk alle teilnehmenden Rechner gleichberechtigt und ohne Zwischenschaltung einer zentralen Instanz über die Struktur des Internets miteinander verbunden.[20] Grundsätzlich kommen dabei auch jedem Netzwerkknoten die gleichen Rechte zu.

Im Zuge der unmittelbaren Kommunikation entsteht durch den direkten Austausch von Daten, die anschließend verteilt verarbeitet werden, das Netzwerk.[21] Der globale Datenaustausch wird, wie schon bei Teilnehmern des Internets, durch entsprechende Netzwerkprotokolle ermöglicht, die eine gemeinsame Sprache und Regeln festschreiben.

Im DLT-Kontext findet sich häufig die Bezeichnung der teilnehmenden Rechner (Netzwerkknoten) als **Nodes**. Wichtig, insbesondere aus juristischer Perspektive, ist dabei, dass mit Node nicht der menschliche Nutzer benannt ist, sondern nur der mit dem Netzwerk verbundenen Rechner. Ein Node ist der Zugangspunkt, um Transaktionen ausführen zu lassen oder sonst mit den anderen Teilnehmern zu interagieren. Mehrere Nutzer können auch über denselben Node auf das Netzwerk zugreifen; zugleich muss der Betreiber eines Nodes nicht zwangsläufig selbst Nutzer sein, sondern kann den Zugang ausschließlich fremden Personen zur Verfügung stellen. In letzterem Fall verwalten häufig Anbieter ein zentrales Wallet für alle Kunden oder nutzen hybride Ansätze.[22]

Wenn ein Node eine lokale Kopie der Blockchain hält und am Kommunikationsverkehr mit den anderen Clients teilnimmt, ist er Teil des operierenden Netzwerks.[23] Wird die vollständige Version der Kette gespeichert, handelt es sich um einen sog. Full-Node. Nur Full-Nodes können am Bestätigen von Transaktionen und dem Schaffen neuer Blöcke teilnehmen. Da jedoch die gesamte Blockchain auf dem System des Nodes repliziert wird, stellt der teils enorme Speicherbedarf für einige potentielle Nutzer ein Zugangshindernis dar.[24] Eine Alternative ist die Verwendung eines sog. Light-Nodes,

[19] Zugrunde gelegt wird eine vereinfachte Version der Bitcoin-Blockchain.
[20] *Nakamoto*. S. 3.
[21] Vgl. zum Ablauf am Beispiel des Bitcoin-Protokolls auch *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2098 f.). Die Netzwerk-Topologie erläutern *Bonneau* et. al., Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, S. 5.
[22] Vgl. zum Ganzen *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2092 f.).
[23] *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2293, 2297);
[24] Anfang 2019 erreichte Bitcoin beinahe 200 Gigabyte, vgl. https://www.statista.com/statistics/647523/worldwide-Bitcoin-blockchain-size/ (alle Online-Inhalte zuletzt aufgerufen am 25.06.2019).

der nur eine komprimierte und verschlüsselte[25] Kopie der Blockchain von einem Full-Node herunterlädt, um anhand derer fremde Transaktionen verifizieren zu können. Der Light-Node nimmt jedoch selbst nicht am Netzwerk teil und kann keine eigenen Transaktionen absenden. Man kann ihn sich wie einen Kontoauszug vorstellen, den sich der Nutzer von der aktuellen Blockchain erstellen lässt und der später zu Kontrollzwecken dienen kann.

b) Kryptografie

Das zweite wichtige Element der Blockchain-Technologie ist die **Kryptografie**.

aa) *Public* und *private key* Die Identifikation der Teilnehmer einer Blockchain erfolgt über den sog. **öffentlichen Schlüssel (*public key*)** – eine pseudonyme Adresse in Form einer Zeichenkette.[26] Sie stellt die öffentlich einsehbare Empfangsadresse dar und ist vergleichbar mit einer Kontonummer. Da die anderen Netzwerkteilnehmer (in der Regel) jedoch nur die Zeichenfolge, nicht aber den Namen der dahinterstehenden Person oder Organisation kennen, schafft das eine sog. relative Anonymität.[27] Mit zusätzlichen Informationen oder unter Heranziehung von Hilfsmitteln, wie etwa Big-Data Analysetools, lässt sich die Identität der dahinterstehenden Person jedoch in vielen Fällen ermitteln, wenn nicht für jede Transaktion ein neuer öffentlicher Schlüssel verwendet wird. [28]

Einer ID kann auch gleichzeitig eine bestimmte **Rolle** im System zugewiesen werden. Während im Bitcoin-Netzwerk alle Teilnehmer die gleichen Rechte haben, kann es besonders in zulassungsbeschränkten Netzwerken relevant sein, verschiedene Zugangsrechte zu definieren und damit etwa Entscheidungsprozesse abzubilden. Hierbei kann auch die Pseudonymisierung erhalten bleiben: Die Netzwerkteilnehmer erfahren zwar, dass die zuständige Stelle eine Anfrage signiert hat; nicht mitgeteilt wird jedoch die eigentliche Identität der handelnden Person oder sonstige Interna der handelnden Stelle.

Neben dem öffentlichen Schlüssel erhält jeder Teilnehmer einen **privaten Schlüssel (*private key*)**, der nur ihm bekannt sein sollte. Er erfüllt die Funktion einer Geheimnummer (PIN), indem er für den Nutzer, der mit einer Transaktion über das Guthaben oder sonstige seinem öffentlichen Schlüssel zugeordneten Werte verfügt, eine Signatur erzeugt. Jeder andere Nutzer kann anhand der Signatur zweifelsfrei nachvollziehen, ob die

[25] Kopiert werden die sog. Block-Header, weiterführend (auch zum *Hash*-Verfahren) nachfolgend S. 8 f.

[26] Pseudonym bedeutet, dass die vorgenommenen Transaktionen zwar anhand des öffentlichen Schlüssels einer bestimmten Identität zugeordnet werden könne, jedoch die hinter dieser Identität stehende Person nur unter Hinzuziehung zusätzlicher Informationen ermittelt werden kann, vgl. auch Art. 4 DSGVO.

[27] *Voshmgir*, S. 13.

[28] Mit diesem Vorschlag u.a. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2088). Freilich ist u.U. auch dann ein Tracking der IP-Adresse möglich. Vgl. zum Datenschutz S. 94 ff.

Transaktion auch tatsächlich von dem öffentlichen Schlüssel des Absenders stammt.[29]

Der Ort, an dem ein Nutzer sein Schlüsselpaar bzw. seine Schlüsselpaare speichert, wird als sog. ***Wallet*** (Geldbörse) bezeichnet. Praktisch am verbreitetsten ist die Verwendung eines sog. *Software-Wallet*. Das kann selbst ein vollwertiger *Node* sein, in dessen System das Schlüsselpaar gespeichert ist, oder aber der verschlüsselte Zugang zu einem der zahlreichen "Wallet-Anbieter"wie coinbase.com oder blockchain.info. Diese Anbieter verwalten die Konten vieler Nutzer in eigener Verantwortung und häufig mit einem einzigen Node, über welchen sie angewiesene Transaktionen ausführen. Wie auch immer der Nutzer den Zugriff auf die digitalen Werte jedoch gestaltet, ist im Hinblick auf die Aufbewahrung des *private keys* besondere Vorsicht geboten: Jeder, der im Besitz des privaten Schlüssels ist, kann auf das Konto zugreifen, aber auch nur, wer in dessen Besitz ist. Bei einem Verlust des keys sind alle der öffentlichen Adresse zugeschriebenen Werte unwiederbringlich verloren.

Besondere **Multisignature-Verfahren** (Multisig) können vorsehen, dass für die Vornahme einer bestimmten Transaktion mehrere private Schlüssel zusammenwirken müssen.[30] Auf diese Weise lassen sich u.a. auch Schiedsentscheidungen (2-of-3-Multisig)[31] oder Abstimmungsverfahren abbilden.

bb) Hashing Die Verschlüsselung der in einer Blockchain gespeicherten Daten erfolgt mittels einer sog. Hash-Funktion. Diese sorgt dafür, dass jede in einem Block enthaltene Botschaft, gleich wie lange, zu einer individuellen Zeichenfolge mit festgelegter Ziffernzahl, dem **Hash-Wert**, chiffriert wird. Er funktioniert gewissermaßen wie eine Einbahnstraße. Dieselbe Eingabe führt stets zum selben Hash-Wert; jedoch kann aus dem Hash-Wert gerade nicht der ursprüngliche Input errechnet werden. Jede geringste Änderung der Inputdaten führt zu einem völlig veränderten Output der Hash-Funktion.[32] Die geläufigste Hash-Funktion ist SHA-256.[33] Daneben existieren aber auch andere Funktionen wie Blake-256, Scrypt oder Myriad, letzteres eine Kombination mehrerer Algorithmen.[34]

In einem sog. **Block-Header** befindet sich stets ein Hash-Wert, der alle Informationen des jeweiligen Blocks zusammenfasst.[35] Man erstellt dabei einen sog. Merkle-Tree. Hierbei wird anhand eines mathematischen Hash-Verfahrens ein Baum, der die Hash-Werte einzelner Informationen zunächst als viele einzelne Äste darstellt, die sich nach und nach zu neuen Hash-Werten kombinieren, bis sie zu einem Baum zusammenwachsen, dessen Krone der zusammenfassende Hash für alle am Fuße aufgenommenen Informationen enthält.[36]

---

[29] Verfahren der asymmetrischen Verschlüsselung, vgl. *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2293).

[30] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2090).

[31] Vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2090).

[32] *Bonneau* et al., S. 4; *Clack/Bakshi/Braine*, *Smart Contract* Templates II, S. 9.

[33] Vgl. zu einer Bewertung die Studie des *BSI*, Technische Richtlinie – Kryptographische Verfahren, S. 39 f.

[34] *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2294) m.w.N.

[35] *Nakamoto*, S. 4.

[36] Vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2101).

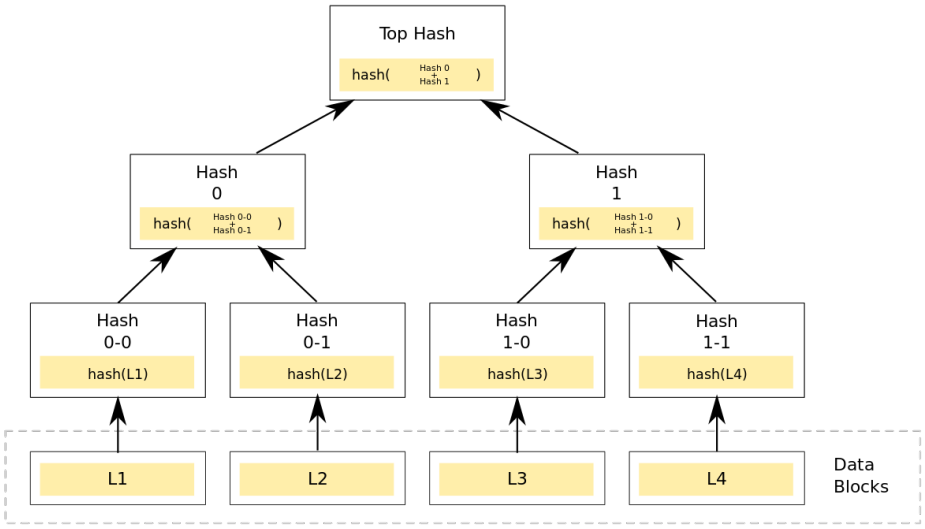

Abbildung 1: Merkle-Tree

Der auf diesem Wege erstellte Block-Header wird als sog. **Previous-Block-Hash** zusammen mit den anderen Informationen, also der der jeweiligen Liste an Transaktionsergebnissen, einem Zeitstempel und der Versionsnummer in den neuen Block aufgenommen.[37] Durch diesen Verweis auf den vorangehenden Block ergeben sich zwei bedeutende Vorteile: Erstens kann anhand eines Abgleichs der Hashwerte auf einfache Weise die Integrität der gesamten Kette verifiziert werden. Zweitens wird erst durch die Verkettung die Reihenfolge der Blöcke unveränderbar festgelegt und der Datensammlung der Charakter einer umfassenden, stetig fortgeschriebenen Historie verliehen, aus der sich verlässliche Aussagen ableiten lassen.[38]

Mit diesem Verfahren hatte der Entwurf des Bitcoin-Netzwerks erstmals eine Lösung für das sog. **Double-Spending-Problem** in der Hand: Es war sichergestellt, dass niemand dasselbe digitale Zahlungsmittel zweimal ausgeben kann. Die Idee ist simpel: Wenn nur das erstmalige Ausgeben eines Bitcoins akzeptiert wird und alle Teilnehmer über eine Kopie bisheriger Transaktionen verfügen, muss nur die neue Transaktion öffentlich angekündigt werden und jeder kann nachvollziehen, ob ein erstmaliges Versenden des Bitcoin vorliegt.[39] Durch die Systemarchitektur besteht nicht einmal Bedarf für digitale Münzen. Der Kontostand an Bitcoins wird bei Bitcoin alleine aus der Summe bzw. Differenz vorangegangener Einzeltransaktionen abgeleitet.[40] Den Saldo muss der Nutzer mit besonderen Programmen anbieten, wobei häufig Wallet-Lösungen eine solche Funktion integriert haben.

cc) Blockvalidierungssystem – Ablauf einer Transaktion

[37] *Bonneau* et al., S. 3.
[38] *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2293); *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2087).
[39] *Nakamoto*, S. 2 ff.
[40] *Nakamoto*, S. 2; *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2088).

(1) Konsensverfahren und Rolle der Miner Die Zusammenfassung der Transaktionsdaten, Verschlüsselung und Berechnung der neuen Blöcke erfolgt dezentral durch besondere Teilnehmer, die sog. **Miner**. Die Bezeichnung als „Schürfer" rührt aus dem Anreizsystem der DL-Netzwerke: Im klassischen Bitcoin-Netzwerk erhält der Miner für das Überprüfen, Berechnen und Anfügen neuer Blöcke[41] als Belohnung das Recht, sich in dem neuen Block auch gleich eine festgelegte Belohnung zuzuschreiben. Er schürft damit quasi neues Geld. Wie schafft es also ein Miner erfolgreich zu sein?

In einem DL findet ein Verfahren **kollektiver Buchführung** statt. Jeder Teilnehmer verfügt über eine eigene Kopie des Ledger und überprüft selbständig, ob er Transaktionen an seine Kette anhängt oder sie verwirft. Da die Miner im dezentralen System jedoch parallel arbeiten und errechnete Blöcke verteilen, können die Ketten voneinander abweichen. Um nicht im Chaos zu enden, muss es eine ordnende Regel geben, die festlegt, welche Version der Ketten die gültige ist. Dass diese **schlüssige Transaktionen** beinhalten, also logisch an den bisherigen Transaktionsverlauf anknüpfen, ist zwar notwendig, aber nicht ausreichend.

> Ein **Beispiel**: Nehmen wir an, Teilnehmer A schuldet B 2 und C 4 Bitcoin, hat selbst aber nur 5. Er könnte versuchen, dem einen Netzwerkteil eine Transaktion an B i.H.v. 2 Bitcoin, gleichzeitig dem anderen Teil eine Transaktion an C über 4 Bitcoin zu übermitteln. Beide Transaktionen können schlüssig an den bisherigen Transaktionsverlauf anknüpfen. Jedoch käme es zu zwei Versionen der Blockchain. Auf was soll sich jemand, der die Informationen ausliest einstellen? Welche der Transaktionen wäre gültig, wenn es beide gleichzeitig nicht sein können?

Ein verteilter Datensatz ist sinnlos, wenn keine Regel besteht, wie der maßgebliche Datensatz zu ermitteln ist. Oberstes Ziel ist also die Herstellung von Konsens. Wie dieser Konsens herstellen zu ist bzw. das sog. **Konsensverfahren**, regelt das Protokoll des jeweiligen DL. Doch das ist gar nicht so einfach.

Ein simples, aber nicht funktionables System wäre es, schlicht die Nodes im Netzwerk abstimmen zu lassen. In diesem Fall würde die von den meisten Nodes gehaltene Version der Blockchain als die richtige gelten. Ein Angreifer könnte dieses System jedoch leicht manipulieren, indem er sich eine Vielzahl von Nodes beschafft und diese in seinem Sinne abstimmen lässt (sog. Sybil Attack).[42]. Zahlenmäßige Mehrheit ist nur dann ein taugliches Mittel, wenn die Identitäten der Teilnehmer abgesichert und Mehrfachabstimmungen ausgeschlossen sind.

Bei öffentlichen Blockchains kann theoretisch jeder einen oder mehrere Nodes anmelden. Die Berechtigung, neue Blöcke an die Blockchain anhängen zu dürfen, muss daher anders verteilt werden. Zudem sollte leicht überprüft werden können, ob eine Version der Blockchain inhaltlich schlüssig und zudem die maßgebliche ist. Im Grundsatz gilt bei den meisten öffentlichen Blockchains das Prinzip, dass stets „die längste" gültige Kette die

[41] In anderen Distributed-Ledger-Systemen kann anstelle von Blöcken auch schlicht ein Registereintrag oder eine Transaktion selbst dem Konsensmechanismus unterstellt sein.
[42] Vgl. *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2294).

"richtige"Version des Ledger ist (**Longest-Chain-Rule**). Bestehen daran anküpfend besondere Hindernisse, die vermeiden, dass jeder gültige Blöcke anhängen oder bestehende manipulieren kann, kommt der längsten Kette auch tatsächlich eine Bedeutung bei. Ob As Transaktion an B oder an C maßgeblich ist, hängt also davon ab, welche in der längsten Kette landet. Der Schlüssel ist also die Definition der Gültigkeit eines Blocks. Welche Bedingungen hierfür erfüllt sein müssen, hängt vom Protokoll des jeweiligen Systems ab, wobei verschiedene Verfahren und Modelle debattiert werden.

(2) Proof-of-Work (PoW) Das prominenteste Verfahren ist das sog. **Proof-of-Work**, wie es bei der Bitcoin-Blockchain angewendet ist. Um einen gültigen Block an die Kette anhängen zu dürfen, wird die Erbringung einer besonders intensiven Rechenleistung (des Proof-of-Work) durch Lösung einer Rechenaufgabe verlangt. Man nimmt folglich an, dass für Errechnung der längsten und damit gültigen Kette die meiste Rechenleistung aufgewendet wurde.[43] Anschließend wird davon ausgegangen, dass der am schnellsten gefundene, gültigen Block von jedem übernommen und an der Fortschreibung des daran anküpfenden Blocks gearbeitet wird.[44]

(a) Funktionsweise Die Aufgabe knüpft an die Struktur der Blöcke als Merkle-Trees an und liegt in der Regel darin, den zusammenfassenden Hash-Wert eines jeden Blocks (Block-Header)[45] eine vorher festgelegte Bedingung erfüllen zu lassen. Die Bedingung für die Gültigkeit eines Blocks lautet dann meist (wie im Bitcoin-Netzwerk): „der Hash-Wert des Block-Header beginnt mit X Nullen“, wobei X für eine beliebige Anzahl Nullen steht.[46] Zur Erinnerung: Jede Eingabe in eine Hash-Funktion erzeugt einen individuellen Hash-Wert.[47] Der restliche Inhalt eines Blocks ist bereits durch die Zusammenfassung der Transaktionen, etc. vorgegeben, sodass der Miner, um die Aufgabe zu erfüllen, eine zusätzliche Zahl erraten bzw. im Zufallsverfahren berechnen muss, unter deren Hinzufügung der Blockinhalt einen Hash-Wert ergibt, der mit den geforderten X Nullen beginnt. Diese Zahl wird auch als ***Nonce*** bezeichnet.[48] Die statistische Rate (sog. Hash-Rate), mit der ein Miner gültige Blöcke errechnet, hängt von seiner relativen Rechenleistung im Netzwerk ab. Dem Rechner mit der höchsten Rechenkraft wird es daher am wahrscheinlichsten gelingen, den neuen Block zu errechnen. Natürlich kann im Einzelfall auch einmal ein schwächerer Rechner Rateglück haben kann.

Um die durchschnittliche Zahl an Blöcken pro Stunde konstant zu halten, wird der Schwierigkeitsgrad – die Zahl der geforderten Nullen –regelmäßig an die im Netzwerk vertretene **Rechenstärke** angepasst.[49] Eine größere Re-

[43] *Bonneau* et al., S. 4.
[44] *Bonneau* et al., S. 4.
[45] Siehe zuvor S. 8.
[46] *Nakamoto*, S. 3.
[47] Jede kleinste Veränderung der Input-Daten generiert einen völlig anderen Output.
[48] *Bonneau* et. al., S. 4 f.
[49] Bei Bitcoin gilt als Zielgröße, dass in etwa alle 10 Minuten ein Block berechnet wird, *Nakamoto*, S. 3; vgl. auch vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2112). Wird diese Zielgröße stark über- bzw. unterschritten, sieht das Protokoll eine Anpassung vor.

chenkraft durch mehr und stärkere Nodes führt daher zu einer Steigerung des Schwierigkeitsgrades, nicht aber zu mehr errechneten Blöcken.

(b) Ablauf einer Transaktion Ein Node sendet eine ausgehende Transaktion zunächst an alle Teilnehmer des Netzwerks (*Broadcast*).[50] Gleichzeitig erhält die Transaktion dabei einen Zeitstempel, um die spätere Reihenfolge für alle Teilnehmer verbindlich festzulegen. Die Nodes, welche die neuen Blöcke berechnen (Miner), bündeln bei ihnen eintreffende Transaktionen zu Blöcken. Da eine parallele Datenverarbeitung erfolgt und einzelne Miner u.U. unterschiedliche Versionen der Blockchain gespeichert haben, können hierbei auch unterschiedliche Zusammensetzungen der Blöcke entstehen.

> Im Beispiel ist es etwa möglich, dass ein Miner an einem Block mit A´s Transaktion an B arbeitet, während ein anderer Miner die Übertragung an C einbindet.

Zu den Transaktionen fügen die Miner noch den den Previous-Block-Hash ebenso wie den an sie adressierten Block-Reward hinzu. Anschließend versuchen sie, eine geeignete *Nonce* zu finden. Sobald ein Node eine gültige *Nonce* errechnet und damit den Proof-of-Work erbracht hat, versieht er den Block mit dem passenden Block-Header und *broadcasted* ihn an die übrigen Netzwerkteilnehmer.

Da jeder Node über eine lokale Kopie der Kette vorangegangener Transaktionen verfügt, kann er den nun erforderlichen Abgleich selbst vornehmen. Überprüft wird zum einen die Erfüllung der Proof-of-Work-Aufgabe und der korrekte Anschluss an den referenzierten *previous block*, zum anderen, ob alle Transaktionen valide sind. Auf Basis der Transaktionshistorie muss dem jeweiligen Absender dabei tatsächlich die behauptete Berechtigung, etwa ein ausreichendes Guthaben an Coins, ein Stimmrecht, etc., zustehen und die Transaktion mittels des mit dem öffentlichen Schlüssel korrespondierenden *private key* signiert worden sein. Liegen alle Voraussetzungen vor, fügt der Node den Block an seine Blockchain an. Anschließend beginnt das Spiel von vorne.

„Ehrliche“ [sic!] Nodes bzw. Miner sollen immer die längste Version der Kette als die gültige anerkennen und versuchen, diese zu verlängern.[51] Die nötigen Anreize schafft eine Belohnungsstruktur, bei welcher für das erfolgreiche Errechnen eines Blocks neue Bitcoins vergeben werden, hinter welcher einige spieltheoretische Überlegungen stehen:

c) Spieltheorie

Die Spieltheorie ist das dritte Grundkonzept von Distributed-Ledger-Systemen. Auf ihren theoretischen Grundlagen basierende ökonomische Incentivierungssysteme sorgen für eine ausreichende Zahl an teilnehmenden Rechnern bzw. Miner*n* und sichern so den Fortbestand des Netzwerks, ohne

[50] Vgl. hierzu *Nakamoto*, S. 3 ff.; ferner *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2293 f.) sowie *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2100).
[51] *Bonneau* et al., S. 4.

dass es einer zentralen, die Investitionen steuernden Stelle bedarf.[52] Dies wird erreicht, indem ein sog. Nash-Gleichgewicht angestrebt wird. Hiernach muss es für die Teilnehmer ökonomisch am sinnvollsten sein, mit den Regeln des Systems und somit zum Vorteil des Netzwerks zu kooperieren.[53]

Ein Aspekt ist die für das Errechnen neuer Blöcke (Proof-of-Work) bzw. deren Verifizierung (*Proof-of-Stake*) vergebene Belohnung (*Block Reward*). Allerdings sorgt ein Algorithmus dafür, dass sich die zu erhaltene Belohnung mit steigender Größe der Blockchain jeweils halbiert, alle 210 000 Blöcke, bis er nach 64 Halbierung unter die minimale Einheit *satoshi* (10^{-8} BTC) erreicht.[54] Zum Ausgleich dafür und um die Aufnahme einer eigenen Transaktion in den Block für den Miner interessanter zu machen, kann von den Nutzern eine zusätzliche Transaktionsgebühr gezahlt werden. Da nur der Miner eine Belohnung erhält, der eine Transaktion als erstes in einen gültigen Block verschlüsselt, entsteht ein Wettbewerb. Ökonomisch sinnvoll ist entsprechend nur ein Bemühen um einen Block, der später auch von der Mehrheit des Netzwerks als gültig erachtetet wird.[55]

Je mehr sich das Netzwerk schließlich vergrößert, desto unwahrscheinlicher wird eine Fälschung bzw. Zensur, da mehr Rechenkraft erforderlich wird.

d) Weitere Aspekte des Konsensverfahrens

aa) Fälschungsszenario bei Proof-of-Work (51 %-Attacke) Als Vorteil des Proof-of-Work-Ansatzes wird immer wieder die besonders hohe Fälschungssicherheit genannt. Wie kommt diese zustande?

In jedem Block ist ein Previous-Block-Hash enthalten, der dem Block-Header des vorangehenden entspricht und somit auf diesen verweist. Wird der Inhalt eines Blocks manipuliert, ändert sich dessen Block-Header und damit auch der Verweis, der in den folgenden Block aufgenommen werden müsste. Die bislang für den Folgeblock errechnete *Nonce* passt hierauf nicht und müsste daher neu berechnet werden, um die Bedingung des Konsensverfahrens zu erfüllen. Für eine erfolgreiche Manipulation muss daher nicht nur der zu manipulierende, sondern auch sämtliche folgenden Blöcke neu berechnet und jeweils der Proof-of-Work erbracht werden.[56]

Das Fälschen der gesamten Kette wird damit derart **ressourcenintensiv**, dass angenommen wird, dass es (in der Regel) wirtschaftlich nicht rentabel sein dürfte. Im Umkehrschluss kann eine Transaktion als umso gesicherter gelten, je länger die darauffolgende Kette ist.[57] Wie bei allen kryptografischen Verfahren kann hierdurch eine Manipulation zwar nicht vollständig ausgeschlossen werden; solange die verbleibende Schwachstelle jedoch als

[52] Vgl. zu den Mechanismen *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2114).
[53] Vgl. *Glatz*, in: Breidenbach/Glatz, Blockchain, Rn. 27. Potentielle Risiken werden untersucht von *Bonneau* et. al., S. 6 ff.
[54] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2087).
[55] *Nakamoto*, S. 4.
[56] *Nakamoto*, S. 3.
[57] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2090).

kaum oder nur mit prohibitiven Kosten zu überwinden gilt und dies im Fall des Gelingens jedenfalls nicht rentabel sein dürfte, soll das System als vertrauenswürdig gelten.[58]

Konsequenterweise ist damit aber auch die Sicherheit eines Blockchain-Netzwerks von der Anzahl der Teilnehmer bzw. der Konzentration der Mining-Power abhängig. Dies erschließt sich am einfachsten, wenn man das wahrscheinlichste **Fälschungsszenario** betrachtet. Gelingt es einem Angreifer schneller als alle anderen neue Blöcke zu errechnen, könnte er die Transaktionshistorie ungehindert fort-, ggf. die bisherige Historie sogar umschreiben.[59] Seine Blöcke müssen weiter schlüssig sein; er kann jedoch einzelne Transaktionen blockieren, bestimmte Nutzer zensieren und zeitgleich alle Block-Rewards selbst einfordern.[60] Ferner könnten Coins doppelt ausgegeben werden (Double-Spending):

> Erneut am obigen Beispiel anknüpfend: Nachdem A bereits 2 Bitcoin an B gesendet hat und die Transaktion in die Blockchain übernommen wurde, könnte er am Block vor seiner Transaktion aknüpfend eine neue Kette schaffen, in der stattdessen 4 Bitcoin an C transferiert werden. Sobald A eine hinreichende Anzahl neuer Blöcke hinzugefügt hat und die neue Kette die alte überholt, wird das Netzwerk diese als die gültige erachten, vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2088, 2093 f.). B´s Zugewinn ist aus der aktuellen Version der Blockchain verschwunden, während A faktisch einen Bicoin doppelt ausgeben konnte.

Erforderlich hierfür ist, dass ein einzelner Teilnehmer 51 Prozent der gesamten Rechenstärke im Netzwerk auf sich vereint, da es dann aller Wahrscheinlichkeit nach immer gelingt, den nächsten gültigen Block zu errechnen (sog. **51-Prozent-Attacke**).[61]

Für das Erlangen der Deutungshoheit müsste ein Angreifer eine Rechenkraft von 51 entsprechend alleine auf der Annahme, dass die **Kosten prohibitiv** wirken. Die erforderlichen Kosten dürften bei wirtschaftlichen Transaktionen den Vorteil einerManipulation bei weitem übersteigen, zumal beteiligte Coins bei einem (aufgrund der Sicherungsmechanismen früher oder später bemerkten) Angriff vermutlich an Marktwert verlieren würden. Augeschlossen ist eine Manipulation indes nicht. Aussagen, die der Blockchain-Technologie eine Immunität gegen Manipulationen versprechen, sind insofern falsch bzw. irreführend.

---

[58] Vgl. *Szabo*, First Monday, Volume 2, Number 9 (1997), abrufbar unter http://firstmonday.org/ojs/index.php/fm/article/view/548/469. Das gilt freilich nicht zwangsläufig auch bei nicht-wirtschaftlichen Interessen.

[59] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2088, 2094).

[60] Da das Ausbleiben von Block-Rewards andere Miner aus dem Netzwerk vertreiben wird, erhält der Angreifer mit der Zeit noch mehr Einfluss. Aus diesem Grund wird eine solche Attacke als das Worst-Case-Szenario beschrieben, vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2094).

[61] Praktisch könnte die erforderliche Schwelle jedoch erheblich geringer sein, vgl. *Swanson*, S. 9. Mittels einer Brute-Force-Attacke, also schlichtem Raten der erforderlichen *Nonce* und entsprechenden Glück kann auch sonst ein falscher Block angehängt werden, *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2095).

Dies erweist sich insbesondere deshalb als problematisch, weil in der Praxis sog. **Mining-*Pools*** bzw. **Mining-Farmen** teilweise einen Großteil der Rechenkapazität auf sich vereinigen und ein Zusammenschluss damit eine reale Gefahr darstellt.[62] Die Sicherheit vor 51-Prozent-Attacken verhält sich proportional zur jeweiligen Rechenkraft im Netzwerk (Hash-Rate bei Bitcoin).

Nur ein hinreichend großes Netzwerk erweist sich daher unter Verwendung von Proof-of-Work als stabil, weshalb es in Zukunft unter den zulassungsfreien Systemen eher mehrere große, als unzählige kleine, nach diesem Konzept vorgehende Systeme geben wird.[63] Mit der Entwicklung von **Quantencomputern** könnte jedoch nicht nur das Konzept Proof-of-Work, sondern sogar die Verlässlichkeit der Hash-Verschlüsselung selbst auf dem Prüfstand stehen, deren Entwicklung jedoch zeitlich noch nicht absehbar ist.

bb) Vor- und Nachteile von Proof-of-Work Abgesehen von dem als unwahrscheinlich erachteten Fälschungsszenario sorgt der Mechanismus jedoch grundsätzlich dafür, dass einmal gespeicherte Informationen unabänderlich in den Kopien der Blockchain fortbestehen und nicht wieder verändert werden können (**Authentizität**). Hierdurch eignet sich die Technologie in besonderer Weise für die Erschaffung von Zahlungsmitteln.[64]

Mit dem Proof-of-Work-Verfahren wird jedoch auch die Anzahl der durchführbaren Transaktionen pro Sekunde begrenzt, was als Problem der **beschränkten Skalierbarkeit** bezeichnet wird. Im Hinblick auf Bitcoin wird derzeit über eine Vergrößerung der Blockgröße debattiert, die mehr Transaktionen pro Minute, aber damit zugleich eine geringere Sicherheit mit sich bringen würde.

Hinzu kommt ein generelles Problem dezentraler Ansätze, die darauf aufbauen, dass jeder vollwertige Nutzer ein vollständiges Abbild der Blockkette auf seinem Rechner hält: der stetig **wachsende Speicherbedarf**, den die immer größer werdende Kette in Anspruch nimmt.[65] Ziel muss es sein, den tatsächlich in dem Ledger (on-chain) zu speichernden Inhalt möglichst klein zu halten. Anstelle des gesamten Blockinhalts könnte man auch nur ein zusammenfassende Hash, die Krone eines Merkle-Tree, hinterlegen.[66] Nichtsdestotrotz wächst die Kette stetig und mit ihr auch der Speicherbedarf. Weitere Verfahren, die Abhilfe schaffen sollen, versuchen etwa nachträglich nicht mehr benötigte Blöcke oder Inhalte zu bereinigen (sog. Pruning) oder große Mengen an Zwischentransaktionen off-chain[67] zu speichern; so zum Beispiel das Lightning-Netzwerk.[68] Sie führen jedoch nicht

[62] *Swanson*, S. 8 f.; *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2096 f.).

[63] Kleinere Netzwerke setzen in ihrer Wachstumsphase deshalb teilweise noch auf Absicherung durch eine Zentralstelle, zum Beispiel IOTA mit dem „Coordinator", vgl. https://blog.iota.org/coordinator-part-1-the-path-to-coordicide-ee4148a8db08.

[64] *Heckelmann*, NJW 2018, 504 (505).

[65] Vgl. *Nakamoto*, S. 4.

[66] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2101).

[67] Zur Terminologie *Swanson*, S. 5.

[68] Vgl. https://lightning.network/lightning-network-summary.pdf.

in allen Anwendungsfragen weiter und zwingen jedenfalls zu Konzessionen im Hinblick auf die Vollständigkeit und Transparenz des Transaktionsregisters.

Als größtes Problem fällt der immense **Energieverbrauch** auf, der mit dem Mining verbunden ist. Begleitet von einem Wettrüsten an Grafikkarten wird aktuell ein jährlicher Strombedarf geschätzt, der sich allein für Bitcoin-Netzwerk im Bereich eines Landes mittlerer Größe bewegt und heruntergebrochen auf eine Einzeltransaktion ein 200.000-faches einer Visatransaktion erfordert.[69]

cc) Andere Konsensverfahren Neben Proof-of-Work sind deshalb auch zahlreiche **weitere Verfahren** in Verwendung bzw. Entwicklung, die für eine ähhliche Authentizität der Daten sorgen sollen. Der größte Konkurrent im Rahmen von öffentlichen DL ist das sog. Proof-of-Stake-Verfahren (PoS).[70] Hierbei müssen die validierenden Netzwerkteilnehmer nicht eine besondere Rechenaufgabe lösen, sondern eine Art **Einsatz** leisten. Dabei zählt nicht mehr die vermutete aufgewendete Rechenkraft, sondern die Höhe eines Einsatzes.

Beispielhaft erläutert sei hier das sog. Coin-Age-PoS:[71] Es wird der Block des Miners als nächster hinzugefügt, der das meiste "Coin Ageäuf diesen eingesetzt bzw. quasi gewettet hat. Unter dem Coin Age versteht man die Summe an Tagen, die ein Coin bereits im Besitz einer öffentlichen Adresse ist. Der Miner kann anschließend beliebig viele Coins mit ihrem jeweiligen Coin Age zu dem neuen Block hinzugefügt, adressiert an sich selbst und zuzüglich eines prozentualen Gewinns (sog. Coinstake Transaction). Der Block, auf den das meiste Coin Age gesetzt wurde, ist der nächste Block der Kette. Das Alter des Coins wird bei diesem Vorgang zurückgesetzt, sodass jeder bezogen auf einen einzelnen Coin die gleichen Startchancen hat. Im Ergebnis wird die Kette als die gültige anerkannt, bei welcher die größte Summe an Coin Age eingesetzt und damit verbraucht wurde.

Eine **51-Prozent-Attacke** ist auch bei diesem System möglich. Hierfür müsste jemand so viele Coins auf sich vereinigen, dass er auch nach den Aufwendungen für den ersten Block ausreichend Einsatz für die folgenden Manipulationen übrig hat. Das ist umso unwahrscheinlicher, je größer das Netzwerk ist. Das Alter wird jedoch ab dem Zeitpunkt des Erwerbs gemessen, so dass kein Anreiz besteht, den Node dauerhaft am System teilnehmen zu lassen. Indem dazu noch jede andere Transaktion das Coin Age reduziert, wird hierdurch sogar das Horten von Münzen incentiviert,was wiederum Angriffe erleichtert.[72]

Andere Vorschläge gehen deshalb dahin, auch die **aktive Teilnahme** am Netzwerk mit einzubeziehen (Proof-of-Activity).[73] Einige Netzwerke, zum

[69] Berechnungen von Digiconomist zufolge lag der am Beispiel des 12.11.2018 geschätzte Jahresverbrauch bei 73,12 TWh, was leicht über dem jährlichen Energiebedarfs Österreichs (72 TWh) liegt. Juni 2019 kam er mit ca. 67 TWh in die Nähe der Tschechischen Republik. Vgl. auch zu aktuellen Zahlen https://digiconomist.net/bitcoin-energy-consumption.

[70] Einen Überblick liefern *Bonneau* et. al., S. 13.

[71] Vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2114 f.).

[72] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2116).

[73] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2116).

Beispiel Ethereum, testen **kombinierte Verfahren** von Proof-of-Work und Proof-of-Stake.[74]

dd) Situation in zulassungsbeschränkten Netzwerken In **zulassungsbeschränkten** (permissioned) Ledger stellt sich die Frage, ob es überhaupt eines derart umfassenden Proof-of-Algorithmus bedarf. Kennen sich die Parteien bzw. ist zumindest ein hinreichender Spam-Schutz gewährleistet, können **weniger ressourcenintensive Verfahren** zum Einsatz kommen. Entscheidend ist dann nur eine gerechte Verteilung der Blockgenerierung, um den dezentralen Ansatz zu wahren.[75] Die Schlüssigkeit der Kette und Validität der Signaturen wird weiter überprüft, jedoch muss das System nicht gegen Angreifer von außen abgesichert werden. Bspw. kann jedem Teilnehmer eine zufällige Wartezeit zugewiesen wird, nach welcher er einen neuen Block berechnen und hinzufügen darf (sog. Proof-of-Elapsed-Time).[76] Alternativ kann man auch zu zentralistischen Ansätzen zurückkehren und eine vertrauensvolle Stelle bzw. einen Kreis vertrauenswürdiger Teilnehmer zum Validieren der Transaktionen autorisieren (Proof-of-Authority).

ee) Forks Es wurde bereits angesprochen, dass es dazu kommen kann, dass mehrere Miner gleichzeitig einen validen Block errechnen und an das Netzwerk senden. Da jeder Node den zuerst empfangenen Block an seine Kette anhängen wird, kommt es innerhalb des Netzwerks zu einer Aufgabelung, einem sog. **Fork**. Jeder Rechner wird zunächst an den zuerst empfangenen Block anknüpfen, jedoch den später empfangenen zwischenspeichern, falls die andere Version der Kette die längere wird. Für eine kurze Zeit bestehen also mehrere, dem Anschein nach gültige Versionen der Blockchain, je nachdem, bei welchem Client man anfragt.[77]

Der Mechanismus der Blockchain ist mit der Longest-Chain-Rule so angelegt, dass sich irgendwann die Mehrheit der Teilnehmer für eine Abzweigung entscheiden muss. Die kürzeren Enden werden dabei verworfen (sog. Waisen).[78]. Im Transaktionsbeispiel wird deshalb früher oder später eine der Transaktionen des A verworfen werden.

Es kann vorkommen, dass Einzeltransaktionen deshalb (zunächst) nicht in die endgültige Blockchain übernommen bzw. aufgrund einer überholenden Kette wieder verworfen werden.[79] Dabei kommt es jedoch grundsätzlich nicht zu einem Verlust, da die in den kürzeren Ästen enthaltenen Transaktionen in den Pool unbestätigter Transaktionen zurückgelegt werden.[80] Solange die Mehrheit des Netzwerks den Auftrag als legitim bewertet, wird er später auch in einen anderen Block aufgenommen werden. Die

[74] Vgl. zu dem Plan von Ethereum zum schrittweisen Übergang zu Proof-of-Stake https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.
[75] *Swanson*, S. 8.
[76] So etwa bei dem privaten Blockchain-Netzwerk basierend auf Hyperledger Sawtooth, vgl. https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp.
[77] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2087 f.). Dasselbe geschieht, wenn Blöcke zeitverzögert versendet werden.
[78] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2088).
[79] *Bonneau* et al., S. 3.
[80] *Schulz*, c´t 2017, 102 (104 f.).

meisten Teilnehmer gehen aufgrund der mit der möglichen Kürzung der Äste verbundenen Verzögerung erst ab **sechs Blöcken** von einer gesicherten Transaktion aus.[81] Diese (zufällig gewählte) Zahl könnte auch höher liegen, wodurch mit der größeren Anzahl bestätigender Blöcke auch die Wahrscheinlichkeit, dass die jeweilige Transaktion auch tatsächlich Teil der endgültigen Kette wird und kein Double-Spending erfolgte, steigt.

Gravierende rechtliche Problemstellungen sind hiermit nicht verbunden.[82] Im Ergebnis muss, wie bei jeder anderen technischen Dokumentationsform, eine korrekte Übertragung der Information in das System überprüft werden. Zugangsfragen sollen nachfolgend im Kontext rechtlicher Problemstellungen erörtert werden.[83] Forks können aber auch einem **Update** der Blockchain bzw. ihres Protokolls dienen, worauf sogleich einzugehen ist.

4. Weitere technische Gestaltungsaspekte

a) Updates der Blockchain

Wie die meiste Software müssen auch DL-Systeme regelmäßig geupdated werden, um Fehler zu korrigieren, Sicherheitslücken zu schließen oder sonstige Anpassungen vorzunehmen. Aus diesem Grund sind selbst dezentrale, öffentliche und zulassungsfreie DL nicht völlig unabhängig von jeder menschlichen Einflussnahme.[84]

Einfachere **Softwareupdates** (sog. **Soft Forks**) beinhalten lediglich einige leichte Protokollaktualisierungen. Nicht mehr abwärtskompatibel ist hingegen ein sog. **Hard Fork**, bei dem es zu einer Spaltung des Netzwerks kommt. Theoretisch könnte bei einem Update jeder Aspekt, selbst Accountinhaberschaften, etc., geändert werden. Die Nodes, insb. die Miner müssen sich dabei bewusst für die Aktualisierung entscheiden, indem sie das Update installieren und die künftigen Blöcke entsprechend des neuen Protokolls berechnen. Erforderlich ist demnach eine hinreichend große Nutzerzahl, die von nun an dem neuprogrammierten Zweig folgt.[85] Sollte keine Übereinkunft zu den Neuerungen entstehen, können durchaus beide Enden weitergeführt werden, sodass sich die Community entsprechend aufspaltet – so geschehen z.B. bei Bitcoin und Bitcoin *Cash*, als ein Teil der Community eine andere Block-Größe favorisierte und keine Einigung erzielt werden konnte,[86] oder nach dem sog. DAO-Hack mit ETH (*Ethereum*) und ETC (*Ethereum Classic*)[87].

---

[81] *Bonneau* et. al., S. 4. Vgl. zu Strategien, um nicht die in etwa erforderliche Stunde im Falle Bitcoin warten zu müssen, vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2100).

[82] Zweifelnd dagegen *Heckelmann*, NJW 2018, 504 (505 f.).

[83] Siehe S. 57

[84] Vgl. auch zum Folgenden *Walport*, S. 43.

[85] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2117).

[86] Mit der Folge, dass faktisch jeder Nutzer über dieselbe Menge BTC (Bitcoin) und BCH (Bitcoin Cash) verfügte; vgl. zur Spaltung https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/neue-waehrung-Bitcoin-cash-heute-kommt-die-Bitcoin-spaltung/20132148.html?ticket=ST-4795483-cbaWURobc5XMSqCB7lqB-ap3.

[87] https://Bitcoinblog.de/2016/08/06/100-eth-entwickler-community-stellt-sich-hinter-ethereum-ohne-classic/

Im Fall von Bitcoin wurde die Verantwortung für allgemeine Updates von Nakamoto an Gavin Andresen, einem australischen Programmierer übergeben. Dieser benannte einen Rat aus fünf Entwicklern, die alleine einem selbst erdachten (rechtlich nicht bindenden) Kodex unterliegen, wonach wichtige Änderungen allein in Übereinstimmung mit einem breiten Konsens der Community erfolgen sollen. Auf einen Vorschlag („Bitcoin Improvement Proposal") hin wird über dessen Annahme in entsprechenden Community-Foren diskutiert.[88]

Mangels festgelegter Verfahren, um sich auf Änderungen zu verständigen, führen Vorschläge jedoch teils zu heftigen Debatten. Auch wenn theoretisch jeder Nutzer Updates vorschlagen könnte, zeigt sich schon bei Bitcoin, dass das Erfordernis einer zentralistischen Organisation von Änderungen ohne feste Bindung an Community-Interessen dem Gründungsmythos eines egalitären, institutionslosen Netzwerks widerspricht.[89] Der Anschein einer organisationslosen Struktur wird insofern an seine Grenzen gebracht. Bei geschlossenen Netzwerken erweist sich die Verantwortungsverteilung und Abstimmung freilich einfacher: Hier kann entweder der Betreiber oder das Konsortium im Rahmen eventueller Vereinbarungen ein Update schlicht durchsetzen.

b) Speicherung von Daten auf einer Blockchain

Ob sich trotzdem über Transaktionsergebnisse, Identitäten und ausführbaren Code (Smart Contracts) hinaus noch andere **Inhalte auf der Blockchain** speichern lassen, hängt von der jeweiligen Chain-Struktur ab. Wie eine Studie zur Bitcoin-Blockchain[90] zeigt, lassen sich trotz der Ausrichtung des Netzwerks auf Transaktionen und Transaktionsergebnisse kleinere Texte als zusätzliche Inhalte in der Coinbase (bis zu 100 Byte für besondere Markierungen) oder mit der Funktion *OP_Return* (80 Byte zur Beschriftung von Transaktionen) abbilden. Durch die Verwendung von Fake-Adressen können sogar größere Texte eingeschleust werden, indem man Transaktionen schlicht ins Leere sendet, die Inhalte aber dennoch unabänderlich in die Chain geschrieben werden. Schwierigkeiten ergeben sich immer dann, wenn eine rechtliche Löschungspflicht besteht, da dann die Rechtspflicht mit der Unabänderlichkeit der Blockchain kollidiert.[91] Neben angeblichen Urheberrechtsverletzungen wurde etwa bereits eine Liste mit Links zu strafrechtlich relevanten Inhalten bzw. Fotografien entdeckt.[92]

[88] *Walport*, S. 43.
[89] *Walport*, S. 44.
[90] *Matzutt* et. al, A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin.
[91] Vgl. auch zum Folgenden *Beaucamp/Henningsen/Florian*, MMR 2018, 501 ff.
[92] Vgl. *Matzutt* et. al, A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. Die Bilder werden jedoch als deart verkleinert abgespeichert, dass man sie erst in einem aufwendigen Verfahren zusammensetzen müsste und nicht ohne weiteres betrachten kann.

5. Bewertung der Technologie

a) Vorteile

Die DLT erlaubt die Schaffung sicherer **Datenregister**, deren Führung einer verteilten, dezentralen Verantwortlichkeit bzw. Machstruktur unterliegt.

Die Nutzer sind in den **Netzwerken** unmittelbar miteinander verbunden und können innerhalb eines Netzwerks interagieren, dessen Funktionieren grundsätzlich nicht von einer zentralen Stelle abhängig ist. Die gespeicherten Daten liegen nicht auf einem einzigen Server, sondern sind, jeweils durch lokale Kopien, auf die Gesamtheit der Netzwerkteilnehmer verteilt.

Gegenüber anderen verteilt funktionierenden Datenbanken hebt sich die Technologie sowohl durch die besondere **Fälschungssicherheit** als auch durch die **Transparenz** ab, da sämtliche Änderungen an die vorgegebenen Regeln gebunden und von allen kontrolliert werden. **Manipulationen** werden durch die kryptographische Struktur nicht nur erschwert, sondern könnten überdies sofort bemerkt werden.

Ein weiterer Vorteil gegenüber herkömmlichen Systemen ist die nachfolgend näher zu beschreibende Möglichkeit, **ausführbaren Programmcode** einzubinden. Da sich die Manipulationsresistenz und Transparenz des DL auch auf den automatisiert vollzogenen Programmcode erstreckt, können hierdurch **Businessprozesse** und **-logiken** abgebildet werden, die später garantiert vom System ausgeführt werden.

b) Herausforderungen

Auf der anderen Seite sind insbesondere die folgenden Herausforderungen zu benennen:

Die größten Schwierigkeiten bereitet die Suche nach tauglichen **Konsensverfahren**, um zulassungsfreien Netzwerken die nötige Ordnung und Struktur zu geben. Insbesondere Proof-of-Work gerät mit dem hohen Ressourcenverbrauch, den immer höher werdenden Hardwareanforderungen beim Mining und der schlechten **Skalierbarkeit** in berechtigte Kritik. Selbst in größeren Netzwerken gefährden Mining-Pools mit ihrer konzentrierten Rechenkraft die Verlässlichkeit des Systems.

Kleinere öffentliche Netzwerke sind mit den gängigen Konsensmechanismen anfällig für 51-Prozent-Attacken Um dezentral funktionieren zu können, setzen die meisten vertrauensunabhängigen Sicherungsmechanismen in der Regel eine bestimmte Netzwerkgröße voraus, wobei die Schwelle nicht klar zu bennenen ist.[93]

Weiterhin ist das **Integritäts- und Sicherheitsversprechen** eines Systems nur dann valide, wenn auch der zugrundeliegende Programmiercode bzw. das Protokoll **frei von Fehlern** sind. Das Ausnutzen einer solchen Lücke

[93] Vgl. jüngst den Fall des Ethereum-Forks Ethereum Classic, *Kannenberg*, https://www.heise.de/newsticker/meldung/Kryptogeld-Mutmasslich-51-Prozent-Attacke-gegen-Ethereum-classic-4268053.html.

ist noch wahrscheinlicher, als eine 51 Beispiel des sog. DAO-Hacks belegt, bei dem durch das Ausnutzen eines Programmierfehlers im Ethereum-Netzwerk ohne tiefergehende Systemeingriffe Kryptowährung im Wert von mehreren Millionen Euro entwendet werden konnten.[94]

Problematisch sind zudem die schwankenden Bestätigungsraten (**Latenz**) sowie der Umstand, dass ein überholender Fork nur unwahrscheinlicher, nicht aber ausgeschlossen wird und auf den Bestand eines Blocks daher nur eingeschränkt vertraut werden kann. Bei wirtschaftlich bedeutsamen Transaktionen muss entweder eine schnellere Bestätigungsrate oder ein alternatives Validierungsverfahren für die notwendige Sicherheit sorgen.

Schließlich ist die **Interoperabilität** zwischen verschiedenen Technologien erst noch herzustellen. Um Kollaboration zu ermöglichen und eine Anbindung an bestehende Systemen zu erlauben, müssen gemeinsame Standards etabliert werden.

6. Fortentwicklung dezentraler Ansätze

a) Alternative Systemarchitekturen

Anstatt mit der Blockchain auf eine strikte Reihe von Transaktionsblöcken zurückzugreifen, finden sich neue Lösungsansätze, etwa *IOTA*. Durch die Strukturierung der Daten als ein gerichteter azyklischer Graph („DAG“[95]), in dem jeder Transaktionsblock beim Absenden zwei weitere validiert und damit auf diese verweist, wird auf Mining im klassischen Sinne komplett verzichtet.[96] Hierdurch fallen Transaktionsgebühren weg, was die Einführung von Mikrotransaktionen oder das Versenden von Dateninhalten ohne Werttransfer (etwa um die Wartungsdaten einer Maschine zu protokollieren) ermöglicht. Außerdem skaliert die Transaktionsbestätigungsrate mit der Zahl der Teilnehmer, während eine gelegentliche Validierung durch Proof-of-Work als reiner Spamschutz dient. In regelmäßigen Abständen sichert ein Snapshot den aktuellen Stand des Graphen, der in validierter Form als Grundlage für den weiteren Transaktionsverlauf dienen kann und so vermeidet, dass stets die vollständige Transaktionshistorie gesichert werden muss. *IOTA* zielt dabei insbesondere auf die dezentrale Organisation des Internet of Things ab.

b) Forschung und Entwicklung

Die Bandbreite an Variationen ist nur schwer zu überblicken. Gegenwärtig kann nicht mit Sicherheit prognostiziert werden, ob und in welcher Form die Technologie langanhaltenden Erfolg haben wird. Das Konzept DLT steckt gewissermaßen noch in den Kinderschuhen; von einheitlichen oder etablierten Standards kann keine Rede sein. Großer **Forschungs- und Entwicklungsbedarf** trifft dabei mit der Komplexität der Umsetzung bereits existierender Konzepte zusammen.

---

[94] Vgl. *Hoppen*, „The DAO-Hack“ und der letzte Flug Otto Lilienthals am 09.08.1896 sowie S. 37 f.

[95] Bei IOTA der „Tangle“ genannt.

[96] https://blog.codecentric.de/2017/11/blockcentric-2-tangle-eine-einfuehrung/.

All dem zum Trotz könnte die Blockchain auch Wegbereiter für völlig neue, noch nicht absehbare technische Konzepte sein. Großes Automatisierungspotenial wird insbesondere in Verbindung mit der **Standardisierung** von Business-Abläufen gesehen, wobei die Flexibiltät der Ledger mit ihren vielseitigen Gestaltungsmöglichkeiten hervorgehoben wird.[97] Inwiefern sich der Verzicht auf Intermediäre durchsetzen lässt, bleibt abzuwarten; ebenso, ob die sich entwickelnden Netzwerke tatsächlich die derzeit stark monopolistisch geprägte Plattformökonomie aufbrechen und durch neue, dezentrale Ansätze ersetzen können.

Dabei können sich auch Mittelwege ergeben, bei denen nur einige Ansätze der Blockchain-Technologie aufgegriffen werden. **Ripple** etwa stellt mit seinem auf den internationalen Austausch von Geldwerten zwischen Finanzinstituten ausgerichteten Netzwerk eine verteilte Datenstruktur bereit, verzichtet aber vollständig auf Mining. Stattdessen sorgen in dem geschlossenen System 200 ausgewählte Mitglieder (*Trusted Validators*) mit Bestätigungen für die Integrität der Kette. Sog. *HashTrees* – gleichzusetzen mit den *Merkle Trees* – fassen die Daten zusammen, die anschließend verteilt auf zahlreiche Betriebsserver teilnehmender Finanzinstitute validiert werden.

[97] *Glatz*, in: Breidenbach/Glatz, Blockchain, Rn. 4.

II. Smart Contracts

In Verbindung mit DL-Systemen und Blockchains taucht immer wieder der Begriff des **Smart Contracts** auf. Die Meinungen, was hierunter zu verstehen ist, gehen teils stark auseinander. Um das zu verstehen, hilft ein Blick auf die Entwicklungsgeschichte.

1. Begriffsbestimmung

a) Begriffsschöpfung durch *Nick Szabo*

Die Begrifflichkeit des Smart Contract ist deutlich älter als die Blockchain-Technologie und wurde insbesondere durch den Computerwissenschaftler und Kryptografen ***Nick Szabo*** geprägt. Er beschrieb in seinen Publikationen ein Konzept automatisierter Vertragsabwicklung: Ein Smart Contract sei ein **computerbasiertes Transaktionsprotokoll**, das die Bedingungen eines Vertrags implementiert.[98] Das auf einem öffentlichen Netzwerk ausgeführte Programm soll (in Verbindung mit einem entsprechenden *user interface*[99]) eine formalisierte, fälschungs- und eingriffssichere sowie kostengünstigere Transaktionsabwicklung ermöglichen.[100]

Schon damals barg der Begriff jedoch großes **Missverständnispotential**. *Szabo*s Konzept umfasste nicht das *rechtliche Konstrukt* eines Vertrags, also eines rechtlichen Konstrukts, bei welchen sich die jeweiligen Vertragsparteien Rechte gewähren und Pflichten auferlegen können. Die Idee beschrieb vielmehr die Entwicklung eines Algorithmus, welcher die rechtlich definierten Vertragsbestimmungen automatisiert ausführt und sich mit seinen Folgewirkungen schrittweise den Bestimmungen des Vertrags annähert.[101] Es geht damit alleine um das Abwicklungsinstrument.

Bei einer juristischen Betrachtung sind jedoch solche **tatsächlichen Umstände** und ihre Auswirkungen strikt von der **rechtlichen Ebene** zu trennen. Rechtssätze bzw. Normen sind selbst keine Tatsachen, sondern machen Vorgaben für ihre Bewertung oder Einordnung und knüfpfen u.U. Folgen (Sollensanordnungen) daran. In anderen Worten: Die rechtliche Bewertung der Tatsachen bestimmt die rechtlichen Folgen. Beispielhaft kann hier auf die bedeutsame Unterscheidung in der allgemeinen Rechtsgeschäftslehre verwiesen werden, die zwischen dem Erklärungszeichen, etwa einem Brief oder Computersignal, und der Willenserklärung als Gebilde des Rechts vorzunehmen ist. Der Smart Contract ist schon nach *Szabo*s Definition entsprechend dem Erklärungszeichen eine rechtserhebliche Tatsache mit Bezug zum Verhalten der Parteien.[102] Die *Bewertung* des jeweiligen Sachverhalts durch das Recht, die möglicherweise ergeben kann, dass ein Vertrag vorliegt, steht auf einem anderen Blatt.

---

[98] Vgl. etwa *Szabo*, First Monday, Volume 2, Number 9 (1997).

[99] Als user interface bezeichnet man die Benutzeroberfläche einer Benutzerschnittstelle, also den Zugang, über den ein Mensch mit dem Computerprogramm interagieren und dessen Kommunikation wahrnehmen kann.

[100] Zu den Vorteilen und Eigenschaften näher *Szabo*, First Monday, Volume 2, Number 9 (1997).

[101] *Szabo*, First Monday, Volume 2, Number 9 (1997).

[102] Ebenso *Kaulartz/Heckmann*, CR 2016, 618 (621).

b) Aufgreifen der Terminologie durch die Blockchain-Community

Diese Verständnisproblematik vertiefte sich weiter, als der Begriff des Smart Contract im **Kontext der Blockchain-Technologie** übernommen wurde. Der Bezug zu einem Vertrag im Rechtssinne, wie er noch im Konzept Szabos vorhanden war, bleibt hier völlig außen vor. Vielmehr bezeichnet man als Smart Contract ein digitales regelbasiertes Protokoll, das in einem Distributed-Ledger Transaktionsergebnisse überprüfen, dokumentieren sowie selbständig Transaktionen durchführen, wenn vorher definierte Bedingungen erfüllt sind.[103] Vereinfacht gesprochen handelt es sich um Computerprogramme, die in der Umgebung eines dezentralen Netzwerks ausgeführt werden. Beispielsweise bezeichnet bei der Plattform Ethereum „Smart Contract"eine Programmiermöglichkeit, die es erlaubt, einen in Programmiersprache verfassten Algorithmus zu implementieren.[104] Auch andere Blockchain- bzw. DL-Systeme greifen diesen Begriff auf, ohne etwas an der generellen Funktionsbeschreibung zu ändern.

Damit liegt eine präzise, informationstechnische Beschreibung vor, was einen Smart Contract darstellt und was nicht. Im Ergebnis ist notwendige, aber auch hinreichende Voraussetzung für die Qualifikation als Smart Contract, dass es sich um **ausführbaren Code** bzw. eine **programmierbare Logik** in einer Blockchain handelt.[105] Sieht man die Blockchain als ein Datenregister, nimmt der Smart Contract die Rolle des Registerverwalters ein, der als neutrale Instanz entsprechend seines Kodex bestimmte Einträge vornehmen oder aufhalten kann.[106]

Der Smart Contract muss weder besonders komplex sein, noch darf die irreführenden[107] Bezeichnung als *smart* als Hinweis auf künstliche Intelligenz verstanden werden.[108] Bereits eine Wetter-App[109] oder eine App zur Regulierung der Heiztemperatur in der Wohnung, deren Code über eine Blockchain ausgeführt wird, fallen unter die Blockchain-bezogene Begriffsverwendung. Ein Smart Contract in diesem Sinne ist daher weder notwendig „smart" noch ein „contract".

---

[103] *Wright/De Filippi*, S. 11; *Lauslathi/Mattila/Sepällä*, S. 11; *Linardatos*, KR 2018, 85 (88, 91); *Jaccard*, JuS-Letter IT 23, November 2017, S. 2. Ähnlich auch die (soweit ersichtlich einzige) Legaldefinition aus Arizona, U.S, HB 2417: „[A *Smart Contract* is an] event driven program, with state, that runs on a distributed, decentralized,shared and replicated ledger that can take custody over and instruct transfer of assets on that ledger."

[104] Genauer gesagt ist der Smart Contract in der Sprache der objektorientierten Programmierung als Objekt die Instanz, einer Klasse. Seine Attribute (Eigenschaften, die ggf. veränderlich sind) und Methoden (mögliche Funktionen bzw. Ausführungsschritte, deren Parameter, etc.) werden in der Klasse definiert. Eine Transaktion, die eine Handlung des *Smart Contracts* auslöst, ist der Aufruf einer Methode. Vgl. zu den technischen Einzelheiten *Fazekas*, Wie funktioniert eigentlich die Blockchain: Teil 2, abrufbar unter https://www.iteratec.de/tech-blog/artikel/news/wie-funktioniert-eigentlich-die-blockchain-teil-2-smart-contracts-die-businesslogik-von-blockchai/.

[105] Vgl. *Stark,* Making Sense of Blockchain *Smart Contracts*, abrufbar unter: http://www.coindesk.com/making-sense-smart-contracts.

[106] *Paulus/Matzke*, ZfPW 2018, 431 (436).

[107] *Lauslathi/Mattila/Sepällä*, S. 17 Fn. 96; *Jacobs/Lange-Hausstein*, 10 (13); *Wagner*, BB 2017, 898; *Kaulartz/Heckmann*, CR 2016, 618 (619).

[108] *Kaulartz/Heckmann*, CR 2016, 618 (619).

[109] Vgl. *Mik*, Law, Innovation and Technology 2017 (9.2), p. 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 14.

c) Rechtlich geprägte Definitionsansätze und ihre Schwierigkeiten

In der juristischen Literatur finden sich gleichwohl Ansätze, die, offenbar teils von Missverständnissen der technischen Begriffsführung beeinflusst, versuchen, dem Begriff des Smart Contract einen **rechtlichen Bezug** zu verleihen. Manche definieren einen Smart Contract als Vertrag im Rechtssinne, der in Codeform verfasst und selbstvollziehend ist.[110] Teilweise wird dabei explizit auf die Umsetzung in einer Blockchain abgestellt.[111] Andere ordnen jeden Programmcode dem Begriff des Smart Contract unter, der Recht automatisiert durchsetzen soll[112] oder die Einschaltung einer bislang zur Durchsetzung erforderlichen Rechtsinstitution, insb. eines Gerichts, einer Behörde oder von Anwälten, obsolet macht.[113]

Diese Herangehensweise erweist sich jedoch als problematisch. In der Informatik wie auch der Entwicklerpraxis sind technische Konstrukte und Verfahren stets eindeutig definiert, ihre Bezeichnungen also stets mit einer festen Bedeutung versehen. Ein Smart Contract ist hiernach ein technisches Hilfsmittel, das im Wege der automatisierten Ausführung eines eingriffsresistenten Protokolls in einer DL-Umgebung sicherstellt, dass vorgegebene Bedingungen auch tatsächlich ausgeführt werden. Die juristische Aufarbeitung solcher Sachverhalte wird in keiner Weise gefördert, wenn **uneinheitliche Begriffsmaßstäbe** letztlich verdunkeln, worüber gesprochen wird.[114] Vorzugswürdig ist ein mehr an interdisziplinärer Kommunikation, wobei die in der Regel eindeutig definierten informationstechnologischen Begriffe für die juristische Subsumtion eher Tatsachen, als Rechtskategorien sein sollten, um zu verhindern, dass Fehlannahmen zu bestimmten Verfahren entstehen. Im Übrigen verwischt eine rechtlich geprägte Bezeichnung nur die Trennung zwischen Tatsachen- und Rechtsebene, da nicht klar wäre, ob mit dem Begriff nun der Programmcode oder die rechtlichen Wirkungen gemeint sind.[115]

Umso mehr ist zu berücksichtigen, dass willkürliche Begrifflichkeiten bei der rechtlichen Einordnung keine Rolle spielen. Zu beurteilen ist die Faktenlage, unabhängig von ihrer Benennung durch die involvierten Parteien. Möchte man im juristischen Bereich eigene Kategorien finden, um bestimmte Lebenssachverhalte etwa in die vertragsrechtliche Terminologie einzuordnen, sollten Brüche gegenüber technischen Funktionsbeschreibungen vermieden und ggf. ein neuer, juristischer Begriff gefunden werden.

---

[110] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Fries*, Compliance Alliance 2018, Vol 4, 11 (14); *Söbbing*, ITRB 2018, 43 (44).

[111] *Bertram*, MDR 2018, 1416.

[112] Spezifischer Bezug zur Vertragsausführung verlangen *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (12); *Buchleitner/Rabl*, ecolex 2017, 4 (6).

[113] So etwa *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (310), der vom klassischen („weak") den sog. „strong *Smart Contracts*" abgrenzt, in dessen Ausführung nicht einmal ein Gericht eingreifen könnte; weiter dagegen *Levy*, Engaging Science, Technology and Society 3 (2017), 1 (2), der auch Bußgeldbescheide erlassende Blitzer als *Smart Contracts* bezeichnen möchte.

[114] In diesem Sinne insb. *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 5 u. 7 f.

[115] Nicht zielführend ist dabei insbesondere die Gegenkritik von *Glatz*, in: Breidenbach/Glatz, *Smart Contracts*, Rn. 44 f., der darauf hinweist, dass sich *Smart Contracts* gerade nicht um das Recht kümmern sollen. Dass das Recht zu den tatsächlichen Abläufen Stellung beziehen kann und es in seinen eigenen Kategorien erfassen muss, steht nämlich ohne Frage.

In Anlehnung an die IT sollten damit weder das Auslösen von Rechtsfolgen noch eine sonstige Nähe zur Vertragsabwicklung eine Rolle für die Bezeichnung als Smart Contract spielen.[116]

d) Fazit

Insgesamt bestehen große begriffliche Unklarheiten. Zurecht wird darauf hingewiesen, dass sich die Terminologie des Smart Contract im Sinne der Blockchain-Terminologie kaum von normaler Anwendungssoftware unterscheiden lässt.[117] Wünschenswert wäre freilich, wenn in Zukunft weniger missverständliche Bezeichnung für informationstechnologische Konstrukte gefunden werden. Soweit sie allerdings in Verwendung sind, hilft es wenig, wenn sie in der juristischen Argumentation durch eigene Verständnisse ersetzt werden.

Dabei erscheint es möglich, einige **abgrenzende Merkmale** herauszustellen, ohne die diffuse Sachlage weiter zu verkomplizieren. Kennzeichnend ist erstens die Automatisierungsfunktion: Ein wird festgelegtes Regelwerk selbständig sowie in digitaler Form kontrolliert und durchgesetzt. Zweitens kann das System eine besondere **Eingriffssicherheit** bzw. grundsätzliche **Ausführungsgarantie** vorweisen. Der Programmablauf kann nicht einseitig von einer Partei beeinflusst werden, wenn das Protokoll einmal im Gang gesetzt wurde. Wird als Umgebung ein Distributed-Ledger gewählt, ist diese Eingriffssicherheit bereits durch deren besondere Eigenschaften gewährleistet. Die Definition kann gleichwohl **technologieoffen** gefasst werden, da die Voraussetzungen in gleicher Form auch von anderen Systemen gewährleistet werden können. Allerdings muss wie gezeigt Abstand von einem rechtlichen Element der Begriffsbestimmung genommen werden. Eine offene, technische Begriffsbestimmung vermeidet Missverständnisse und stellt so die Verselbständigung eines Handlungsablaufs durch technische Mittel in den Fokus.[118]

Demnach ist **folgende Definition** festzuhalten:

Smart Contracts sind digitale, regelbasierte Transaktionsprotokolle, die festgelegte Wenn-Dann-Bedingungen selbständig und eingriffssicher überprüfen und dokumentieren sowie Transaktionen ausführen bzw. hemmen können und damit als technische Hilfsmittel zur Automatisierung menschlicher Interaktionen dienen.

---

[116] Ebenso u.a. *Blocher*, AnwBl 2016, 612 (618); *Mann,* NZG 2017, 1014 (1016); *Schrey/Thalhofer*, NJW 2017, 1431; *Paulus/Matzke*, NJW 2018, 1905; *Paulus/Matzke*, ZfPW 2018, 431 (434 f.); *Linardatos*, KR 2018, 85 (91); *Blocher*, AnwBl 2016, 612 (618); *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 5 u. 8.

[117] *Paulus/Matzke*, NJW 2018, 1905.

[118] Für eine rein technische Definition auch *Schrey/Thalhofer*, NJW 2017, 1431; *Paulus/Matzke*, NJW 2018, 1905; *Paulus/Matzke*, ZfPW 2018, 431 (434 f.); *Linardatos*, KR 2018, 85 (91); *Blocher*, AnwBl 2016, 612 (618); *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 5 u. 8; *Szabos* Ansatz folgend *Heckelmann*, NJW 2018, 504 f.

2. Technische Eigenschaften von Smart Contracts in einem DL-System

Im Folgenden soll die Anwendung von Smart Contracts näher erläutert werden. Noch befindet sich die DLT in einem sehr frühen **Entwicklungsstadium**. Es kann daher nur versucht werden, die gegenwärtigen Ansätze einzubeziehen und mögliche Entwicklungstendenzen aufzugreifen; ob und in welcher Form die Technologie Bestand haben wird, ist noch nicht abzusehen.

a) Einführung

Wesentliche **Eigenschaften** eines Smart Contracts sind in der Regel, dass ein in einer Blockchain implementierter Programmcode ein digital nachprüfbares Ereignis („Trigger-Event“) verarbeitet und in Abhängigkeit vom Ergebnis der Prüfung eine (Trans-)Aktion ausführen kann (deterministische „Wenn-Dann-Struktur“).[119]

Smart Contracts kann auch eine **Dokumentationsfunktion** zukommen, indem sie bestimmte Ereignisse in einem Ledger zusammenfassen, referenzieren und ggf. sogar gesondert signieren. Hierdurch können bestimmte Ereignisse oder sogar ein Vertragstext relativ fälschungssicher festgehalten werden. Dass im Kontext eines Smart Contracts tatsächlich rechtserhebliche Erklärungen oder Bestimmungen abgegeben werden, ja sogar überhaupt eine vertragserhebliche Handlung durch das Programm auszuführen ist, wird jedoch, wie bereits erwähnt, nicht verlangt.

Je nach Anwendungsfall können **Zugangs-, Verfügungs-, Lese- oder Änderungsrechte** definiert werden, die Nutzern erlauben, entsprechend der im Code festgeschriebenen Bedingungen mit der Datenbank zu interagieren. Ferner können Smart Contracts sich gegenseitig aufrufen und so auch als Datenlieferanten füreinander dienen.[120] So ließen sich bspw. **Abwicklungssysteme** aus mehreren Smart Contracts zusammensetzen.[121] Mithilfe von Smart Contracts lässt sich weiter theoretisch jedes beliebige Gut oder Recht als Ledger-Eintrag digital abbilden, indem die Eigenschaften und damit verbundenen Handlungsmöglichkeiten im Code festgeschrieben werden.[122] Damit ermöglichen Smart Contracts den Aufbau eines Managements- bzw. Handelssystems.[123] Die Bedingungen des Codes können ferner Abbild eines Business-Prozesses sein, um dessen Logiken automatisiert und/oder transparent umzusetzen.

b) Implementierung und Ausführung

Smart Contracts erhalten eine eigene Adresse (*public key*) und werden als **Programmskript** unabänderlich in einer Blockchain gespeichert.[124]

[119] Vgl. *Kaulartz/Heckmann*, CR 2016, 618; *Paulus/Matzke*, CR 2017, 769 (772); ähnlich *Schrey/Thalhofer*, NJW 2017, 1431.
[120] *Heckelmann*, NJW 2018, 504 (505).
[121] *Lauslathi/Mattila/Sepällä*, S. 14.
[122] Vgl. zu sog. Token nachfolgend S. 83 ff.
[123] *Lauslathi/Mattila/Sepällä*, S. 12.
[124] *Lauslathi/Mattila/Sepällä*, S. 12.

Für die beschriebene Konzeption ist eine Blockchain mit einem *account-based-model* im Gegensatz zu einem *UTXO-model* wie bei der Bitcoin-Blockchain.[125] Dies ist erforderlich, da der Smart Contract als eigenständiger Akteur auftritt und dafür einen eigenen **Account** zugewiesen bekommt. Im sog. UTXO-Modell haben Nutzer keinen klassischen Account, auf den sie zugreifen können. Das Netzwerk listet wie in einem Kontobuch auf, welche Transaktionen aneinander anknüpfend getätigt wurden, unterscheidet aber weitergehend keine Accounts, Guthabenstände oder sonstige Zuordnungen zu den Nodes. Das *account-based-model* ermöglicht es, von den Nodes unabhängige Akteure im Netzwerk zu definieren. Hierdurch kann einem Smart Contract etwa "Guthaben auf ein eigenes Konto überwiesen werden.

Die populärste Smart Contract-fähige Plattform ist derzeit Ethereum, die mit ihrer integrierter Turing-vollständigen, d.h. universell ausgestaltete und uneingeschränkte Programmierung erlaubende, Programmiersprache eine universelle Arbeitsfläche (sog. Ethereum Virtual Machine als Laufzeitumgebung) für die Implementierung von Programmcode bieten soll.[126] Die vor allem auf Unternehmensanwendungen mit privaten Ledger ausgerichtete Plattform ***(R3) Corda*** sieht darüber hinaus in der Theorie auch die tatsächliche Bezugnahme auf rechtliche Verträge vor. Die Plattform wurde dabei mit Blick auf hochregulierte Finanzinstitutionen und Banken entwickelt.[127] Die Transaktionsprotokolle, hier sog. State Objects (teilweise „Smart Legal Contracts“) verlinken die Vertragsdokumente mit dem Code, stellen ihre Inhalte und gegenwärtigen Stand in Kategorien dar und sollen einzelne Klauseln direkt umzusetzen – so das White Paper.[128]

Wie alle Daten wird auch der Smart Contract-Code auf jedem (Full-)Node des P2P-Netzwerks hinterlegt. Änderungen am Code würden entsprechend nicht mehr der aktuellen Version der Kette entsprechen und durch die veränderten Hash-Werte sofort erkannt werden.[129] In dem Smart Contract sind die Bedingungen definiert, wann und durch wen er ausgelöst werden kann. Die Initiierung erfolgt insofern durch eine Transaktion im Netzwerk, die den Smart Contract referenziert. Jeder Miner prüft, ob bei einer empfangenen Transaktion eine solche Referenz enthalten ist und führt anschließend den jeweiligen Programmcode aus.[130] Dies kann, wie auch sonst, bei mehreren Minern simultan geschehen. Ein Miner kann eine Transaktion nicht falsch ausführen bzw. die Transaktionsgeschichte umschreiben; wie bereits bei der 51-Prozent-Attacke erörtert kann lediglich die Aufnahme bestimmter Transaktionen blockiert werden, was in der Regel aber nur zu einer Verzögerung führt.[131]

In Ethereum muss für das Ausführen des Codes, also jede kleinste Rech-

---

[125] *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2297 f.)

[126] Beispielhaft sei hier auf Ethereum verwiesen, wo die sog. Ethereum Virtual Machine (EVM) als Laufzeitumgebung die Ausführung von Programmcode ermöglicht, vgl. http://ethdocs.org/en/latest/introduction/what-is-ethereum.html.

[127] Vgl. *Brown/Carlyle/Grigg/Hearn*, Corda: An Introduction, S. 7.

[128] *Brown/Carlyle/Grigg/Hearn*, Corda: An Introduction, S. 8.

[129] *Spancken/Hellenkamp/Brown/Thiel*, S. 17; *Börding/Jülicher/Röttgen/v. Schönfeld*, CR 2017, 134 (139).

[130] *Lauslathi/Mattila/Sepällä*, S. 13.

[131] Mit Hinweis auf potentielle Zensurgefahr *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2300).

nung bzw. Abspeicherung von Daten, sog. **Gas** bereitgestellt werden.[132] Bei Gas handelt es sich um eine besondere Währungseinheit, die dem Miner als Entgelt für sein Tätigwerden zur Verfügung zu stellen sind. Reicht die zur Disposition gestellte Menge an Gas nicht aus, wird der Miner die Rechnung abbrechen, ohne dass eine Rückerstattung erfolgt.

Für die Nutzung bzw. **Ausführung** eines Smart Contracts bedarf es – ohne entsprechende Schnittstelle – nicht der Zustimmung einer zweiten Person, sondern nur des Aufrufs des Programms als Transaktion durch eine einzelne Person mithilfe ihres *private key*. Einmal im Gang gesetzt, lässt sich der Ablauf des Protokolls nicht mehr aufhalten. Eine entsprechende (Korrektur-)Schnittstelle könne zwar Abhilfe schaffen, muss sich jedoch vor dem Konzept des unaufhaltsamen und unabänderlichen deterministischen Vollzugssystems rechtfertigen.

c) Funktionsweise eines Smart Contracts

Ein Smart Contract „verfolgt" alleine seine eigene (programmierte) Logik, indem er den ihm vorgegebenen Code ausführt.[133] Alle Bedingungen sind **eindeutig definiert**. Durch die **deterministische Struktur** wird garantiert, dass derselbe Input immer denselben Output generiert.[134] Das Risiko menschlichen Eingreifens bzw. Andersentscheidens wird insoweit eliminiert. Es handelt sich bei dem Smart Contract quasi um einen **autonomen Akteur**, dessen Verhalten vollständig **vorhersehbar** ist.[135] Abweichungen aus Wertungsgründen sind dem System nicht zugänglich. Ohne entsprechende Schnittstelle sind jedoch auch keine Fehlerkorrekturen möglich.[136] Durch die Verteilung und identische Ausführung auf allen teilnehmenden Rechner des Netzwerks (Nodes) ist die Ausführung bzw. der Programmablauf nicht aufzuhalten.

d) Abgrenzung zum sog. Ricardian Contract

Im Kontext der automatisierten Vertragsabwicklung wird teilweise auch auf den sog. ***Ricardian Contract*** (Ricardianischer Vertrag) verwiesen. Dieser wurde in den 1990er Jahren von Ian Grigg, einem Experten im Feld der Finanzkryptografie, erdacht. Dabei ging es um die Entwicklung eines Systems zum Transfer digitaler Werte im Rahmen des Ricardo-Projekts.

Ursprünglich war es das Ziel, den Inhalt und die Konditionen eines emittierten Wertpapiers in der Form festzuschreiben, dass sich hieraus nicht nur der rechtliche Vertragstext, sondern auch der Wert des Emissionsguts, etwa zum Zwecke der Buchhaltung, ermitteln lässt. Die formale Ebene der (automatisierten) Finanzverwaltung sollte eine Verknüpfung mit der rechtlichen Ebene erfahren, indem der Vertragstext mit dem Code durch Parameter als vermittelndes Element verknüpft werden.[137] Es folgt der Annahme, dass

[132] Vgl. zur Funktionsweise von Gas in Ethereum https://blockgeeks.com/guides/ethereum-gas-step-by-step-guide/.
[133] *Wrigth/De Filippi*, 26; *Kaulartz/Heckmann*, CR 2016, 618 (619 u. 623).
[134] *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2297).
[135] *Christidis/Devetsiokiotis*, IEEE Access, 2016, 2292 (2298).
[136] *Kaulartz/Heckmann*, CR 2016, 618 (623)
[137] Vgl. auch *Clack/Bakshi/Braine*, *Smart Contract* Templates I, S. 3.

die Eigenschaften eines Wertpapiers nichts anderes als der Inhalt einer vertraglichen Vereinbarung sind. Daher soll in einer a) vertragsgleichen Vereinbarung b) in einem einzigen Dokument, das der Emittent an den Empfänger sendet und letzterer akzeptieren muss c) eine abschließende Vereinbarung über den Inhalt eines vom Empfänger zu haltenden, wertvollen Guts und die Konditionen dieser Ausgabe getroffen werden, wobei d) dieses Dokument besonderen Schutz erfährt, indem es kryptografisch gezeichnet und verifizierbar ist, eine eindeutige Identifizierungsnummer erhält sowie e) sowohl von Maschinen als auch Menschen gelesen werden kann.[138] Die Maschinenlesbarkeit soll durch die Verwendung einer entsprechenden Markup-Sprache sichergestellt werden, welche die natürliche Sprache des Rechts erfasst und die Parameter in Codeform niederschreibt.

Im Gegensatz zur Begriffsverwendung *Szabo*s ist der Inhalt des Ricaridan Contract daher stets Vertragstext in natürlicher Sprache und Transaktionsprotokoll in Codeform in einem. Diese doppelte Fassung des Inhalts hebt ihn von den Smart Contracts nach dem Verständnis der Blockchain-Community ab. Gemein hat er mit diesen hingegen die kryptografische Signatur durch privaten und öffentlichen Schlüssel, die eigene Kennung zur Identifizierung wie auch das Transparenzversprechen. Aufgrund der prinzipiellen Systemunabhängigkeit wäre es denkbar, den codierten Teil eines Ricardian Contracts als Smart Contract zu konstruieren und so eine Synergie zwischen DL-Systemen und dem Ricardianischen Modell herzustellen.[139]

Zugleich ist der Begriff jedoch höchst missverständlich und limitiert. So umfasst er nur einen genau festzulegenden Güteraustausch, dessen Elemente und Konditionen in jeder Hinsicht digital beschrieben werden können müssen. Auf der anderen Seite stellt er als „single source of truth“ einen Absolutheitsanspruch und eröffnet nicht die Möglichkeit, nur Teile eines Vertrags mithilfe eines technischen Systems abzubilden bzw. abzuwickeln. Ob es sich bei einem Ricardian Contract um einen Vertrag im Rechtssinne handelt, wollte *Grigg* ausdrücklich offenlassen,[140] auch wenn der Anspruch bestand, die rechtliche Ebene vollständig abzubilden und so ein gerichtlich vollziehbares Vertragsdokument zu schaffen. Auch hier kann jedoch nichts anderes gelten als bei einem Smart Contract: Ob die vorliegenden Tatsachen, abgebildet in der besonderen Vertragsurkunde, einen Vertrag im Rechtssinne darstellen, ist eine Frage des Rechts, nicht der Bezeichnung als „contract“.

e) Mögliche Defizite

Wie zu zeigen sein wird, führt das Konzept der „unaufhaltsamen“ Vertragsausführung bzw. Unabänderlichkeit des Codes von vorneherein zu stark **limitierten praktischen Anwendungsmöglichkeiten**. Hierauf ist insbesondere im Zuge der Erörterung von Divergenzrisiken einzugehen. Einige Aspekte sind allerdings schon an dieser Stelle aufzugreifen:

---

[138] *Grigg*, Ricardian Contracts.
[139] Dafür *Grigg*, On the intersection of ricardian and Smart Contracts.
[140] *Grigg*, Ricardian Contracts.

Erstens ist die mit öffentlichen Blockchains verbundene **Transparenz** nicht zwangsläufig von Vorteil. Für einige Parteien dürfte es nicht in Frage kommen, die Bedingungen ihres Business-Prozesses oder ggf. sogar ihrer vertraglichen Beziehung der Öffentlichkeit zur Schau zu stellen. Die mit der Blockchain verbundene Pseudonymität leistet keine vollständige Gewähr, dass die in dem Vertrag verwendeten öffentlichen Schlüssel nicht doch den tatsächlichen Vertragsparteien zugeordnet werden.[141]

Zweitens geht mit der Verwendung von Smart Contracts bei einem Leistungsaustausch das Problem einher, dass jede Leistung, die beim Erfüllen bestimmter Bedingungen an eine der Parteien freigegeben werden soll, zunächst von der anderen Partei an den Smart Contract transferiert werden muss und anschließend **eingefroren** wird. Nur dann kann der Smart Contract auch garantieren, dass das Zahlungsmittel zur Verfügung steht. Der Schuldner muss also stets, auch wenn die Leistungserfüllung noch unsicher ist, Sicherheit leisten.[142] Das entzieht nicht nur dem Markt,[143] sondern auch dem Schuldner **Liquidität**, da er die betroffenen Kryptowährungseinheiten nicht anderweitig einsetzen kann.[144] Schließlich wären die Coins bei einem endgültigen Ausbleiben der Trigger-Bedingung für immer auf dem Konto eingesperrt, sieht man keinen Abbruchmechanismus bzw. Auflösung des Smart Contracts durch Zeitablauf vor.

[141] Vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2107) sowie nachfolgend S. 94 ff.
[142] *Clack/Bakshi/Braine*, Smart Contract Templates I, S. 4.
[143] *Mainelli/Milne*, SWIFT Institute Working Paper No. 2015-007, S. 31.
[144] *Clack/Bakshi/Braine*, Smart Contract Templates I, S. 5.

III. Weitere technische Konzepte und Begrifflichkeiten

Bei der Betrachtung von Distributed-Ledger-Technologien sind einige weitere Begriffe von besonderer Bedeutung, die im Folgenden erläutert werden sollen.

1. Oracles – Schnittstellen zur „realen Welt"

a) Funktionsweise

Die Blockchain selbst ist ein **geschlossenes System**. Damit Daten von außerhalb in sie gelangen und ggf. von einem Smart Contract gelesen werden können, braucht es besondere **Schnittstellen**.[145] Im Kontext der Blockchain-Technologie werden diese als Oracles bezeichnet.[146] Das können ausgewählte, vertrauenswürdige (sog. *trusted sources*) oder auch ein Verbund an Quellen, die gegebenenfalls nach dem Konsensprinzip agieren, sein.[147] Es handelt sich bei Oracles häufig um eigenständige Anwendungen, die auf Webservern laufen und bestimmte Informationen bereitstellen.[148] Dabei schreiben Oracles entweder die erfassten Daten selbst auf die Blockchain, sodass sie anschließend von einem Smart Contract erfasst und die entsprechenden Folgen ausgelöst werden (etwa bei Ethereum), oder sie nehmen die Funktion eines privaten Schlüssels ein, indem sie eine im Smart Contract definierte Bedingung als *true* markieren und so eine vorgesehene Transaktion signieren.

b) Das Vertrauensproblem

Das Versprechen, man könne auf einen vertrauensvollen Intermediär verzichten, da alle Daten in der Blockchain fälschungssicher hinterlegt und nachvollziehbar seien, hat nur eine **begrenzte Reichweite**. Die Vorzüge der Blockchain-Technologie erstrecken sich nämlich nur auf jene Daten, die Ledger-interne Zustände bzw. Ereignisse betreffen, etwa die Transaktionshistorie eines Coin.[149] Die Verwaltung von **On-Chain-Assets,** etwa der Zahlungsverkehr mit Kryptowährungen, die Inhaberschaft bzw. Transaktionshistorie eines Token oder schlüsselbasierte Identitätsnachweise können insoweit **unproblematisch vertrauensunabhängig** verwaltet werden.[150] Hierzu zählen etwa auch Bewertungssysteme, bei denen das öffentliche

[145] Eine Schnittstelle stellt den Zugang von Informationen oder Interaktionen eines Systems mit einem anderen dar. Möchte eine Person mit einem System interagieren, zum Beispiel Befehle eingeben, bedarf es hierfür einer der Eingabemethode entsprechenden Schnittstelle (*user interface*).

[146] *Kaulartz/Heckmann*, CR 2016, 618. Beispiele für Verwendung in der Baubranche mit Beschleunigungspotential bei der Abwicklung bei *Eschenbruch/Gerstberger*, NZBau 2018, 3 (5 ff.).

[147] *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (92).

[148] Dabei liegt ein Router vor, der den Smart Contract mit einem oder mehreren Application Programming Interfaces (API) verbindet, *Lauslathi/Mattila/Sepällä*, S. 17.

[149] Dies wird häufig außer Acht gelassen, vgl. etwa *Wrigth/De Filippi*, S. 10.

[150] *Swanson*, S. 21.

Netzwerk die Bewertungen listet und sich die Teilnehmer über ihren öffentlichen Schlüssel zu erkennen geben. Der Ledger nimmt in letzterem Fall nur die Funktion einer unveränderbaren Liste ein.

Sämtliche Eingaben, die hingegen über Oracles in das System gelangen, können falsch sein und werden, ggf. ohne eine spätere Korrekturmöglichkeit, für immer in der dezentralen Datenbank festgeschrieben. Der Konsensmechanismus in DL-Systemen sorgt alleine dafür, dass Einigkeit über die richtige Version der Daten hergestellt und diese nicht manipuliert werden. Mit den Schnittstellen führt man daher einen **neuralgischen Punkt** ein: Man muss nun wieder Entitäten vertrauen, die selbst weder dezentral organisiert noch sonst vertrauensunabhängig strukturiert sind.[151]

c) Herausforderung für zulassungsfreie DL-Systeme

Dies stellt insbesondere für **zulassungsfreie** DL-Systeme, deren Teilnehmerkreis also potentiell unbegrenzt ist, eine **Herausforderung** dar. Sollen Off-Chain-Assets verwaltet oder Daten in den Ledger geschrieben werden sollen, die nicht ausschließlich ein Internum des Netzwerks darstellen, muss irgendjemand für die Integrität der Daten einstehen oder man sich zumindest auf ein vertrauenswürdiges Oracle einigen.[152]

Sind die relevanten Daten **öffentlich** und hinreichend verlässlich **verfügbar**, etwa Verspätungszeiten von Flügen oder Wetterlagen, ergibt sich schon **kein Vertrauensproblem**.[153] Eine solche vertrauenswürdige Quelle müsste die definierte Handlung nach objektiven Kriterien bewerten und dem Smart Contract in lesbaren Daten bereitstellen können sowie die Daten auch im Einzelfall zur Verfügung stehen.[154]

Im Übrigen muss bei **allen Zuständen der analogen Welt**, die in einem Ledger beschrieben oder zugeordnet werden sollen, eine vertrauenswürde Stelle, sei es Mensch oder Maschine, für die Integrität der Daten einstehen.[155] Andernfalls könnte beispielsweise beim Handel von PKWs niemand darauf vertrauen, ob ein in einer Blockchain als in einem ordnungsgemäßen Zustand befindlich dokumentiertes Fahrzeug auch tatsächlich diese Eigenschaft hat. Ein Nutzer am anderen Ende der Welt könnte sich nicht auf die eingetragenen Informationen verlassen. Dezentralität und andere Eigenschaften der DL-Systeme können das **Geschlossenheitsdefizit** nicht überspielen.[156]

---

[151] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 23, *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (142).

[152] *Lauslathi/Mattila/Sepällä*, S. 14.

[153] Mit einem solchen Beispiel *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (97).

[154] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 22.

[155] *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (142). Ggf. mag den Parteien dies hingegen vollkommen egal sein, sodass sie die Vorzüge des Sofortvollzugs einer Unrichtigkeit vorziehen.

[156] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 8.

d) Herstellung von Vertrauen

Immer dann, wenn eine „Schnittstelle zur realen Welt“ erforderlich ist, steht dies im Widerspruch zur Vision eines vollständig dezentralen und vertrauensunabhängigen Systems. **Vertrauen** muss erneut auf andere Weise hergestellt werden. Die Teilnehmer müssen sich auf eine Schnittstelle verständigen, ggf. auch darauf, was gelten soll, wenn die Schnittstelle ausfällt.

In **privaten** oder als **Konsortialsystem** strukturierten Blockchains mit einer überschaubaren Teilnehmerzahl erweist sich das als **weniger problematisch**. Entweder garantiert hier die Plattform als vertrauensstiftende Institution die Korrektheit der Daten und kann notfalls bei Fehlinformationen in Anspruch genommen werden oder man findet in einem Kooperationsprozess vertrauenswürdige Schnittstellen und bindet diese idealiter vertraglich ein.

Doch auch in einer **öffentlichen Blockchain** kann eine solche Verständigung erfolgen, vorausgesetzt, die Parteien kennen sich. Man könnte dann einen Smart Contract entwerfen, dessen Trigger durch die Signatur eines bestimmten Oracles freigegeben wird. Der öffentliche Ledger dient in diesem Fall als Infrastruktur, um einen unveränderbaren Nachweis der jeweiligen Daten zu erhalten.

Eine vollständig dezentrale Vernetzung zum gegenseitigen Güteraustausch, ohne Kenntnis der jeweiligen Identitäten, die potentiell globalen Charakter hat, zeigt sich damit jedoch als nur schwer realisierbares Konstrukt, solange Schnittstellen zur realen Welt erforderlich sind.

2. Token und ICO

Auf einer Blockchain kann theoretisch jedes beliebige Gut oder Recht, in der realen Welt existent oder nicht, digital beschrieben werden. Ein **Token** ist der hierzu verwendete digitale Wertbehälter: Wie in einem virtuellen Schließfach wird für den jeweiligen Inhaber ein Wert hinterlegt, indem ein kryptografisch gesicherter Datenbankeintrag erstellt wird, der dem als Inhaber eingetragenen eine entsprechende Berechtigung verleiht bzw. Stellung bescheinigt, z.B. im Eintausch gegen den Token eine Zahlung zu erhalten, an einer Abstimmungen teilnehmen zu dürfen oder auch nur der Nachweis der Beteiligung an einer Spendenaktion.[157] Es existieren damit spezifische Einträge im Netzwerk bzw. auf diese Weise eindeutig identifizierbare Token, die mit ihren jeweiligen Eigenschaften gesucht und referenziert werden können. Neben digitalen Währungseinheiten oder sonstigen unkörperlichen Positionen können Gegenstände der analogen Welt in einer Blockchain **virtualisiert** werden, indem der Eintrag als digitaler Repräsentationskörper angesehen wird.[158] Dies erlaubt etwa die Schaffung von Sachregistern.

[157] *Buterin*, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/. Freilich muss ein Token nicht zwangsläufig etwas Inhaltliches abbilden. Seinen Wert erfährt er allerdings erst durch die Verknüpfung mit einem spezifischen Inhalt, der ausschließlichen Verfügungsbefugnis des Inhabers sowie der mengenmäßigen Limitierung der Token im Netzwerk, vgl. *Kaulartz/Matzke*, NJW 2018, 3278.

[158] *Müller*, ZfiR 2017, 600 (608).

Die Token erhalten ihren Wert dadurch, dass der entsprechende Eintrag mittels Verschlüsselung eindeutig und manipulationssicher einem konkreten Inhaber zugeschrieben und eine Vervielfältigung damit ausgeschlossen ist. Ihre Übertragung erfolgt dann mittels Transaktion, indem jeweils Berechtigte einer Änderung des Inhaberschaftseintrags in der Datenbank mittels Private-Key-Signatur zustimmt. Erstmalig ausgegeben werden sie entweder automatisiert durch das Netzwerk, etwa als Belohnung für Mining, oder durch freies „Prägen", sog. Minting. Beim Minting werden die Token nach Bedarf kreiert und anschließend, etwa im Rahmen eines sog. **Initial Coin Offering** (**ICO**)[159], verteilt oder verkauft.[160] Ihre Funktionalität bzw. Verwaltung wird mittels eines Software-Programms (Smart Contract) gesteuert.[161]

Bei ICOs handelt es sich um eine Methode der **dezentralen Unternehmensfinanzierung**, die von Unternehmen unter Zuhilfenahme von DL-Systemen betrieben wird.[162] Wie beim Crowdfunding oder Crowdinvesting[163] werden im Rahmen eines ein- oder mehrstufigen Verfahrens Token zum Verkauf angeboten (Tokensale), um so, insbesondere in der Gründungsphase, Kapital einzusammeln.[164] Während im Jahr 2017 noch weltweit 5,4 Milliarden US-Dollar eingeworben wurden, waren es 2018 bereits 17 Milliarden.[165] Nicht nur hinsichtlich der rechtlichen Einordnung der Token selbst,[166] sondern auch in Bezug auf ICOs stellen sich zahlreiche rechtliche, insb. aufsichtsrechtliche Fragen (wie etwa die Einordnung als Wertpapier und damit insbesondere das Bestehen einer Prospektpflicht).[167] Letztere liegen jedoch außerhalb des Untersuchungsgegenstands, sodass an dieser Stelle nur auf weiterführende Literatur verwiesen werden soll.[168]

Bei der **Emission** können die Token beinahe beliebig **ausgestaltet** werden.[169] Allen gemein ist, dass der Erwerber, eine Handelbarkeit des Token an Sekundärmärkten vorausgesetzt, schon allein aufgrund potentieller Wertsteigerung ein Investmentinteresse haben kann. Mangels einer einheitlichen Terminologie ist eine rechtliche Einordnung stark einzelfallabhängig. Ein Versuch der Systematisierung kann etwa erfolgen in:[170]

---

[159] Teilweise auch Initial Token Offering (ITO) genannt, um die Unterscheidung Token / Coin herauszustellen.

[160] *Kaulartz/Matzke*, NJW 2018, 3278. Der geläufigste Standard ist ERC-20, auf den sich die Ethereum-Community verständigt hat.

[161] Selbst die Beschreibung, was ein Token ist, wie und wann er übertragen wird, etc., wäre ein ausführbarer Code und im Blockchain-Kontext mithin ein Smart Contract.

[162] *Borkert*, ITRB 2018, 39 (40).

[163] Crowdfunding im engeren Sinne ist spenden- oder belohnungsbasiert, während beim Crowdinvesting von einer Vielzahl (eher kleinerer) Anleger Geld investiert wird, um im Gegenzug Anteile oder eine Gewinnbeteiligung zu erhalten, vgl. *Borkert*, ITRB 2018, 39 (40).

[164] Vgl. auch zum Ablauf eines ICO und einem Vergleich zum klassischen Crowdfunding bzw. –investing *Borkert*, ITRB 2018, 39 (42 ff.).

[165] Vgl. die Statistik von Coindesk, abrufbar unter: https://www.coindesk.com/ico-tracker/

[166] Dazu unten S. 83 ff.

[167] Zu einigen Fragestellungen weiteführend *van Aubel*, in: Habersack/Mülbert/Schlitt, Unternehmensfinanzierung am Kapitalmarkt, § 20 Rn. 71 ff.

[168] Vgl. *Borkert,* ITRB 2018, 91 (93 ff.); *Weitnauer*, BKR 2018, 231 ff.; *Zickgraf*, AG 2018, 293 ff.; in sonstiger zivil- und steuerrechtlicher Hinsicht *Krüger/Lampert*, BB 2018, 1154 ff.

[169] *Borkert,* ITRB 2018, 91 (93).

[170] Bisher keine einheitliche Kategorisierung, vgl. etwa das Positionspapier des Bundesblocks zur Token-Regulierung, S. 10, abrufbar unter: https://www.bundesblock.de/wp-content/uploads/2018/04/180406-Token-Regulation-Paper-Version-2.0-deutsch_

a. **Currency Token** (Digitale Währung) = Token, dessen Anwendungszweck die Bezahlung von Gütern oder Dienstleistungen ist. Der Eintrag im Ledger wird in diesem Fall auch als Coin bezeichnet. Hierzu gehört etwa der Ether oder der IOTA-Coin, nicht aber der Bitcoin: Die Bitcoin-Blockchain enthält weder Nutzerkonten noch eigenständige Felder für Tokeneinträge, sondern nur eine Liste sämtlicher Einzeltransaktionen, aus deren Summe sich die Kontostände der einzelnen öffentlichen Schlüssel errechnen lassen.[171]. In der Praxis dienen diese sog. Kryptowährungen jedoch häufig als digitales Anlageobjekt.

b. **Utility Token** = Verleiht dem Nutzer eine Berechtigung, deren Funktionalität nur innerhalb des Netzwerks gegeben ist und dabei keinerlei Rechte am Projekt selbst abbildet, z.B. Zugriff auf bestimmte Funktionalitäten im Netzwerk. Hierzu zählen interne Währungen (z.B. Gas in Ethereum), Bezugsrechte oder die Möglichkeit es gegen andere Token oder Services einzutauschen, eine interne Währung (z.B. Gas in Ethereum). Der Token trägt damit einen inhärenten Wert.

c. **Security Token/Investment Token** = Token mit Charakter eines klassischen Finanzierungsinstruments (Wertpapiercharakter), das im Erfolgsfall einen Rückzahlungsanspruch gewährt. Vorgeschlagen wird eine Unterscheidung zwischen dem reinen Debt Token und dem Equity bzw. Trust Token.[172] Ersterer verspricht nur die Rückgewähr in Form eines Darlehens oder die Verleihung von Genussrechten (Gewinnbeteiligung, etc.); der Equity Token hingegen entspricht dem klassischen Investitionsmittel durch Anteilskauf, sodass eine Beteiligung am Projekt (je nach Ausgestaltung mit Stimmrechten) erfolgt.

d. **Donation Token** = Seltenere Bezeichnung eines Token, der der infolge einer Beteiligung oder Spende ausgegeben wird, ohne dass dem Erwerber Rechte verliehen oder der Token gehandelt werden kann – im Grunde eine Quittung.

e. **Asset Backed Token** = Token als virtuelle Repräsentation eines tatsächlich existierenden Anlageguts (z.B. Gold, Real Estate) oder Recht außerhalb des Netzwerks.[173] Dies kann auch ein Zugangsrecht, etwa zur Nutzung eines Mietwagens,[174] oder ein Lizenzrecht, sein. Solche Token sind eher nicht bei klassischen ICOs zu finden.

Derzeit sind Bestrebungen zur Entwicklung eines einheitlichen **Standards** zur Token-Klassifikation zu beobachten, was sich etwa die International Token Standardization Organization (ITSA) zum Ziel gesetzt hat.[175]

---

clean_14.00.pdf; *Zickgraf*, AG 2018, 293 (295 ff.); *Krüger/Lampert*, BB 2018, 1154 (1155 f.) oder *Borkert*, ITRB 2018, 39 (42).

[171] Vgl. *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2088).

[172] *Krüger/Lampert*, BB 2018, 1154 (1155 f.; *Zickgraf*, AG 2018, 293 (296).

[173] Sollte ein Recht/Anspruch „verbrieft" werden, könnte das Abspeichern des zugrundeliegenden Vertrags in den Metadaten des Token Rechtssicherheit schaffen, vgl. *Christidis/Devetsiokiotis*, IEEE Access 2016, 2292 (2301).

[174] Dies gelingt in Kombination mit einem (im Beispiel im Fahrzeug integrierten) Cyber-Physikalischen-System (CPS), also einer Schnittstelle, die mittels Sensoren bzw. Aktuatoren mit der Außenwelt in Kontakt treten und Informationen an ein Netzwerk übermitteln kann.

[175] Vgl. https://itsa.global/what-we-do/.

3. Decentralized autonomous organization (DAO)

Beim Konzept der sog. **DAO** (**Decentralized Autonomous Organization**)[176] handelt es sich eigentlich um einen Anachronismus. In der Theorie wird damit eine auf Dauer angelegte, dezentrale Gesellschaft bzw. Organisation beschrieben, bestehend aus einer Gruppe von Teilnehmern eines DLT-Netzwerks, seien es Menschen oder Softwareagenten.[177] Eine praktische Umsetzung des Konzepts gab es bislang jedoch noch nicht (zum Misserfolg der sog. "The DAO“ sogleich). Dennoch handelt es sich um eine vieldiskuierte Vision im Kontext der DLT, die daher im folgenden kurz vorgestellt werden soll.[178]

Dem Konzept nach soll ein Programmcode dezentral hinterlegt bzw. ausgeführt und der Organisation eigenes Kapital in Form einer Kryptowährung zur Verfügung gestellt werden.[179] Das Kapital wird insbesondere bei einem ICO eingeworben, wobei Netzwerkteilnehmer Beteiligungen an der Organisation erwerben. Die Beteiligungsverhältnisse werden anhand von Token virtualisiert. Die DAO operiert auf Basis eines Regelwerks, fixiert in einem Smart Contract, der gleichzeitig die Einhaltung überwacht und durchsetzt. Ähnlich einer Personengesellschaft sollen Kollektiventscheidungen getroffen werden, die anschließend durch den Programmcode umgesetzt werden, z.B. Investitionsentscheidungen.[180] Der regulierende Code ist für alle Beteiligten einsehbar (Open Source) und alle Abläufe können anhand des Protokolls nachvollzogen werden. Die extreme Transparenz ssoll Vertrauen schaffen.[181]

Damit beschreibt die Bezeichnung DAO jedoch entgegen ihres Namens keine autonome Organisation; vielmehr werden menschliche Entscheidungen automatisiert umgesetzt. Sind Menschen steuernd an den Entscheidungen beteiligt, liegt allenfalls eine **dezentrale Organisation** (DO) vor.[182] Erst mit einer vollkommenen Verselbständigung wäre eine tatsächlich autonome Organisation gegeben. Gegenwärtig handelt es sich hierbei aber nur um eine Zukunftsvision.[183]

Doch schon die praktische Umsetzung solcher dezentraleren Organisationen erscheint in vielerlei Hinsicht fraglich. So drängt sich neben einigen rechtlichen Risiken das Problem auf, dass der Programmcode in gewissen Fällen nicht schnell und fundiert genug auf komplexe Fragestellungen reagieren kann.[184] Wie ein einziger Fehler im Programmcode zu schwerwiegenden Folgen führen kann, zeigt das Scheitern des bislang einzigen Anlaufs (einer zumindest dezentralen Organisation), welchen die Gründer

[176] Teilweise auch „distributed autonomous organization“.
[177] *Vitalik Buterin*, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.
[178] Da kein einheitliches Konzept einer DAO besteht, versucht die folgende Darstellung sich den Grundtendenzen anzunähern. Vgl. zu einer weitergehenden rechtlichen Einordnung *Mann*, NZG 2017, 1014 ff.
[179] *Mann*, NZG 2017, 1014 (1015).
[180] Vgl. *Wright/De Filippi*, S. 15 f.
[181] *Wright/De Filippi*, S. 16.
[182] Vgl. zur Unterscheidung *Wright/De Filippi*, S. 17.
[183] Darauf hinweisend, dass auf längere Sicht die Einschaltung zumindest eines Treuhänders unverzichtbar erscheine, *Sattler*, BB 2018, 2043 (2251).
[184] *Sattler*, BB 2018, 2243 (2250).

von Slock.it im Jahr 2017 unternahmen:[185] „The DAO“ sollte ein auf Ethereum basierender, dezentraler Investmentfonds werden, dessen Entscheidungen durch Abstimmung der Tokeninhaber getroffen werden. Nachdem jedoch ca. 150 Mio. US-Dollar eingeworben wurde, gelang es einem unbekannten Hacker unter Ausnutzung einer Schwachstelle im Code eine anderweitig gedachte Funktion zur Absonderung von Token im Wert von 53 Mio. US-Dollar zu nutzen. Um zu verhindern, dass das Geld tatsächlich entwendet werden konnte, entschied sich die Ethereum-Community zum ersten Hard Fork ihrer Geschichte.[186]

[185] *Biederbeck*, Die DAO – Ein Wirtschaftskrimi aus Sachsen, abrufbar unter https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde.

[186] Vgl. dazu S. 37 f.

IV. Selbstvollziehende Verträge als Zukunftsperspektive?

1. Potential selbstvollziehender Verträge auf Basis der Blockchain Technologie

a) Vision

Gegenwärtig sind unter Smart Contracts, wie zuvor dargestellt, lediglich Computerprogramme zu verstehen. Ihr eingriffssicheres Protokoll erlaubt die garantierte Ausführung der vorgesehenen Aktionen beim Eintritt bestimmter Bedingungen. Dabei drängt sich die Frage auf, ob diese Bedingungen nicht auch die Bedingungen eines Vertrags sein könnten.[187] Viele Stimmen sprechen von dem Potential einer neuen Form der **automatisierten Vertragsabwicklung** bzw. **computerbasierten Vertragsumsetzung**. Aufgrund der deterministischen Struktur soll es möglich sein, Verträge bzw. Rechtsgeschäfte verschiedenster Art vollautomatisiert abzuschließen und „selbstvollziehend"[188] bzw. „selbstdurchsetzend"[189] ablaufen zu lassen. Hierfür ist die Blockchain zwar keine unabdingbare Voraussetzung, da sich solche Algorithmen praktisch in jeder Software oder Hardware implementieren lassen.[190] Sie bietet aber jedenfalls durch die Unabänderlichkeit der (Vertrags-)Bedingungen einen besonderen Vertrauenstatbestand und verschafft dem Vertrag eine gewisse Autonomie.[191] Werte könnten etwa eingefroren oder zuverlässig mit Nachweis einer Leistungshandlung freigegeben werden, wobei das System der Vertrauensträger ist. Verbunden mit der durch die dezentralisierte Struktur herbeigeführten Netzausfallsicherheit käme es, so die Theorie, zu einer **garantierten Ausführung** des programmierten Vertragsinhalts.[192]

b) Einführung einer neuen Rechtskategorie?

In der Debatte über die korrekte Definition eines Smart Contracts schlagen manche Autoren, die auf die informationstechnologische Definition Rücksicht nehmen, vor, eine Begriffsabwandlung wie etwa „smart legal contract" zu schaffen, um einen Smart Contract zu kennzeichnen, der gleichzeitig ein sich selbstvollziehender Vertrag im Rechtssinne ist.[193]

Abgesehen davon, dass erneut das *Buzzword* „smart" aufgegriffen wird, ohne dass damit ein Erkenntnisgewinn einhergeht, ist davon abzuraten, eine neue juristische Kategorie zu bilden. Die Aspekte des Selbstvollzugs sind in den jeweiligen Problemstellungen für den jeweiligen Anwendungsfall gesondert herauszustellen. Mögliche Begriffsneuschöpfungen, etwa die eines

[187] Ausführlich zu den rechtlichen Gestaltungsszenarien S. 64 ff.
[188] *Djazayeri*, jurisPR-BKR 12/2016, Anm. 1, S. 1.
[189] *Lauslathi/Mattila/Sepällä*, S. 3.
[190] Vgl. schon die allgemeine Idee *Szabos* in First Monday, Volume 2, Number 9 (1997).
[191] *Linardatos*, KR 2018, 85 (86); *Lauslathi/Mattila/Sepällä*, 12 f.
[192] *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (94).
[193] *Müller*, ZfIR 2017, 600 (610); ähnlich *Stark* „Making Sense of Blockchain Smart Contracts", der zwischen„Smart Contract code" (*Smart Contract* im herkömmlichen Sinne) und der tatsächlichen Abbildung eines Vertrags „smart legal code" unterscheidet.

„autonomen Vertrags“, lassen zu viele Unklarheiten: Ob tatsächlich ein gesamter Vertrag oder nur einzelne Bestimmungen umgesetzt werden sollen, wie eingriffsresistent das System ausgestaltet ist oder welche technische Konstruktion sonst zugrunde liegt, sind nur einige Gesichtspunkte. Letztlich geht es um Automatisierung, sodass von einer neuen Kategorie eher abgesehen werden.

c) Potentiale

Von besonderem Interesse ist die mit der **Automatisierung** verbundene **Zeitersparnis** gegenüber klassischen Abwicklungsmethoden.[194] Dieser Aspekt könnte gerade in Bereichen zum Tragen kommen, in denen sich Vertragsmuster leicht **standardisieren** lassen und eine hohe Nachfrage nach einheitlichen Abwicklungsinstrumenten besteht.[195]

Schon heute werden einzelne Abwicklungsschritte, etwa Bezahlvorgänge bei Wareneingang, automatisiert. Die für die jeweilige Handlung verantwortliche Partei kann jedoch nach ihrem Ermessen jederzeit die Ausführung stoppen. Interessant ist es daher, *Nick Szabos* Idee folgend, die menschliche Unwägbarkeit durch die technische Konstruktion zu überwinden. Heute wäre man bspw. noch auf einen Notar angewiesen, der das Geld bis zum Vollzug der vereinbarten Handlung verwahrt. Anstelle dieser *trusted third party* träte im Szenario der selbstvollziehende Vertrag.

Dies würde zudem für ein hohes Maß an **Transparenz** sorgen, da der Code wie auch sonst alle in einer Blockchain gespeicherten Informationen (grundsätzlich) von allen Teilnehmern einsehbar sind.[196] Für geheimhaltungsbedürftige Vereinbarungen erweist sich dies zwar als Nachteil. Auf der anderen Seite gibt es, ein hinreichendes Verständnis des Codes vorausgesetzt, keine versteckten Hintertüren und keine geheimen Vorbehalte einer Partei. Damit können die Beteiligten selbst alle künftig vorzunehmenden wie auch alle bereits vorgenommenen Handlungsschritte nachvollziehen und so auch beweisen (Auditierbarkeit).[197]

2. Verhältnis von Technik und Recht

Ob sich solche selbstvollziehenden Verträge etablieren lassen und welche **Chancen und Risiken** bestehen, soll im Folgenden näher untersucht werden. Dafür soll angenommen werden, dass einzelne Bestimmungen oder der gesamte Inhalt eines rechtlichen Vertrags mithilfe von Programmcode abgewickelt werden soll und die Abwicklungshandlung von dem Programm eigenständig und nach seinen Regeln (autonom) durchgesetzt, d.h. ohne einen einseitigen menschlichen Eingriff, initiiert bzw. gehemmt, werden kann.

Als Vorüberlegung muss jedoch ein Blick auf das Verhältnis der Systemkreise Technik und Recht geworfen werden.

---

[194] *Wright/De Filippi*, S. 15.

[195] Großes Potential spricht auch die Studie *PwC*, Blockchain, S. 23 ff. zu.

[196] *Kaulartz/Heckmann*, CR 2016, 618 (619).

[197] Vgl. zu den Vorteilen der Beobachtbarkeit *Szabo*, First Monday, Volume 2, Number 9 (1997).

a) Code is law?

In IT-Kreisen wird immer wieder das Dogma „**Code is Law**“[198] hochgehalten, wonach der Code die einzige Regelungsgrundlage eines digitalen Sachverhalts sein sollte und auf geltendes Recht keine Rücksicht zu nehmen braucht. Für den Juristen ist klar, dass sich solche Aussagen mit keiner Rechtsordnung vereinbaren lassen.[199] Ein Vertrag bleibt ein Vertrag, auch wenn man ihn auf die Blockchain verlagert; er steht nicht deshalb über dem Recht, sondern leitet allenfalls seine Verbindlichkeit aus diesem her.[200] Die normative Bewertung von Smart Contracts oder andere programmierte Regeln beruht alleine auf dem geschriebenen (bzw. respektive in dessen Rahmen zulässigerweise privatautonom gesetzten) Recht.[201] Der Gesetzgeber könnte sich zwar dazu entscheiden, Einträgen in einer Blockchain besondere rechtliche Wirkungen beizumessen oder sie als Legitimation eines Rechtsübergangs einzuordnen, hat hierfür aber bislang abgesehen.[202]

b) Warum „Code is Law“ nicht gewollt sein sollte

Wirtschaftlich denkende Vertragsparteien werden zudem mit einem Smart Contract kaum eine letztverbindliche Entscheidungsinstanz schaffen wollen, deren Code, komme was wolle, ausgeführt wird.[203] Wie im Folgenden zu zeigen sein wird, bringt alleine das technische Grunddesign eines Smart Contract zahlreiche Problemfelder mit sich. Jedenfalls in einem im Mindestmaß komplexen Sachverhalt darf darum nicht ohne weiteres unter dem „Code is law“-Dogma oder aufgrund des Gedankens der Dezentralität unterstellt werden, die Parteien würden sich bei Transaktionen in einem rechtsfreien Raum bewegen und auf richterlichen Schutz verzichten wollen.[204] Vielmehr besteht ein vitales Interesse, notfalls Gerichte anrufen zu können, die in Streitfällen oder bei einem technischen Versagen als staatlich legitimierte Stelle Abhilfe schaffen können.[205]

Beispielhaft genannt sei an dieser Stelle nur der Fall, dass ein Mietwagen mit einer Abschaltvorrichtung versehen ist, die den Motorstart technisch unterbinden kann. Vereinbart wurde, dass dem Mieter bei fehlendem Zahlungseingang der Zugang zum Wagen gesperrt werden kann. Ohne dies näher rechtlich einzuordnen: Angenommen sei, der Mieter zahlt, jedoch

[198] Beispielhaft *Kilic*, Sind Smart Contracts noch zu retten?, https://www.wired.de/article/sind-smart-contracts-noch-zu-retten; vgl. auch die Auseinandersetzung von *Abegg*, Code is Law? Not quite yet, abrufbar unter: https://www.coindesk.com/a-fight-is-breaking-out-over-Bitcoin-cash-and-it-just-might-split-the-code/.

[199] *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (96); *Kaulartz/Heckmann*, CR 2016, 618 (621).

[200] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1.

[201] *Djazayeri*, jurisPR-BKR 12/2016, Anm. 1, S. 3; *Kaulartz/Heckmann*, CR 2016, 618 (621); *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (96).

[202] Vgl. zum Regulierungsansatz des BMF mit dem BMJV betreffend die Regulierung elektronischer Wertpapiere und insb. sog. Krypto-Token deren Eckpunktepapier vom 07. März 2019, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Eckpunkte_Krypto_Blockchain.pdf?__blob=publicationFile&v=2

[203] *Wright/De Filippi*, S. 11 heben dies jedoch als neue Möglichkeit, Austauschbeziehungen abseits des (Vertrags-) Rechts zu organisieren, hervor.

[204] *Mann*, NZG 2017, 1014 (1017).

[205] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 13; *Jaccard*, JuS-Letter IT 23, November 2017, S. 10.

ist die Weiterleitung der Zahlungsbestätigung an den Smart Contract fehlerhaft oder der Mieter hat sich zulässigerweise durch Aufrechnung von der Forderung befreit. Würde ihn die Abschaltausrichtung nun aussperren, läge das im Widerspruch zur geltenden Rechtslage und es stünde die Frage im Raum, ob und wie der Smart Contract zur Freigabe des Wagens gebracht werden kann.

Die **Unwägbarkeiten**, die der Einsatz von Smart Contracts mit sich bringt, und das umfassend geltende staatliche Gewaltmonopol, auf das die Parteien außerhalb von rein digital abzuwickelnden Sachverhalten[206] angewiesen sind, ziehen es nach sich, dass selbstvollziehende Verträge zwar die Vermeidung von Rechtsstreitigkeiten und Einsparung von Transaktionskosten mit sich bringen können, aber Erörterungen über deren Potential als Ersatz für Gerichte und staatlichen Vollstreckungsmittel zu dienen wohl nur Spekulationen bleiben werden.[207] Selbst *Lawrence Lessig*, auf den die Formulierung „Code is Law“ überhaupt zurückgeht, beschrieb in seinem Werk „Code and other Laws of Cyberspace” bereits Notwendigkeit eines Staats, um persönliche Freiheit zu gewährleisten.[208]

c) Notwendige Betrachtung von Divergenzrisiken

Recht und Technik sind **zwei** voneinander zu trennende **Systeme**, die nach ihren **eigenen Regeln** und **Logiken** funktionieren. Bei der Einordnung eines selbstvollziehenden Vertrags muss daher stets zwischen den gesetzten Tatsachen, d.h. dem Code und auch den sonstigen Umständen, und der rechtlichen Ebene, die auf Basis dieser Tatsachen rechtliche Bewertungen vornimmt, differenziert werden.[209] Eine **Übereinstimmung** der programmierten Logik mit der Rechtslage ist möglich, aber nicht zwingend.[210]

Ziel muss es daher sein, dass die Rechtslage der technischen Abbildung entspricht und der Ledger die korrekte Rechtslage abbildet bzw. mittels Smart Contracts umsetzt. In anderen Worten muss die **korrekte Übertragung der Sachverhalte von der analogen Welt in die digitale**, sowie die **korrekte Übersetzung der rechtlichen Abläufe in den Code** gewährleistet werden.[211] Damit Verträge rechtskonform von einem System durchgesetzt werden können, muss dieses die Tatsachen zutreffend erfassen, der rechtlich angezeigten Folge zuordnen und schließlich die Rechtsfolge auch rechtskonform umsetzen können.[212] Ein Auweg wäre lediglich zu erreichen, dass das Recht umfassend an die Abläufe im DL angepasst sind, das Recht also stets dem Ledger folgt.

Um die verschiedenen Systemkreise in Einklang zu bringen und so ein Auseinanderfallen von Rechtslage und technischer Realität zu verhindern, müs-

[206] Einem *Smart Contract* kommt in gewisser Weise die Rolle eines digitalen Vollstreckers zu.
[207] *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (4).
[208] *Lessig*, Code and other Laws of Cyberspace, S. 19 ff
[209] *Jaccard*, JuS-Letter IT 23, November 2017, S. 8.
[210] *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (96); *Heckmann/Kaulartz*, c't 2016, 138 ff.; *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (12); *Lange-Hausstein*, ITRB 2017, 93; *Mik*, Law, Innovation and Technology 2017 (9.2), p. 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 5.
[211] *Kaulartz/Heckmann*, CR 2016, 618 (620 ff.); *Jacobs/Lange-Hausstein*, 10 (12 f.).
[212] *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (314).

sen die jeweiligen **Divergenzrisiken** betrachtet und Gestaltungsoptionen untersucht werden Soweit möglich, sollte durch Vertragsgestaltung versucht werden, dass das Recht der gewünschten Funktionsweise des Ledger folgt, wenn dieser die Rechtslage abbilden soll.[213] Dabei sollen zunächst aus dem Bereich der Technik stammende Risikopotentiale untersucht und anschließend die rechtliche Seite in den Blick genommen werden.

[213] Dazu mehr S. 64 ff.

V. Technische Divergenzrisiken und Vermeidungsstrategien

1. Voraussetzung der digitalen Überprüfbarkeit und Abbildbarkeit

Ein Smart Contract kann Informationen nur verarbeiten, wenn sie mit true oder false zu bewerten sind (**digitale Überprüfbarkeit** bzw. **Abbildbarkeit**).[214] Hierfür muss sie sich in Datenform darstellen und logisch-mathematisch entsprechend der vordefinierten Parameter überprüfen lassen. Die digitale Abbildbarkeit sowohl der auslösenden Ereignisse (Trigger) als auch der gewünschten Rechtsfolgen müssen gewährleistet sein.[215] Die potentiellen Einsatzgebiete von Smart Contract werden daher insbesondere dort zu finden sein, wo die Trigger **objektiv** bestimmbar und dadurch zumindest mit Sensoren oder anderen technischen Hilfsmitteln verifizierbar sind.[216] Alternativ kann die Bestimmung auch einer dritten Stelle überlassen werden.

Im Hinblick auf die korrekte und vollständige Berücksichtigung rechtserheblicher Tatsachen handelt es sich zum einen um eine **Design-** zum anderen um eine **Schnittstellenproblematik**. Das Design des Programms- wie auch des Vertrags muss sicherstellen, dass alle zu berücksichtigenden Tatsachen die Voraussetzungen der digitalen Überprüfbarkeit und Abbildbarkeit erfüllen. Andererseits muss für alle zu erfassenden Tatsachen eine entsprechende Schnittstelle eingerichtet sein. Die Erfüllung einer Leistungshandlung, etwa die Lieferung einer Ware, könnte durch das Oracle registriert und damit die gesetzte Bedingung für eine Auszahlung als *true* bewertet werden.[217] Fehlt sie, kann ein solcher Informationszugang nachträglich nicht mehr geschaffen werden. Dabei muss jedoch darauf geachtet werden, dass die Oracles hinreichend nachvollziehbar und mit einer entsprechenden Richtigkeitsgewähr den vollständigen Sachverhalt abbilden, ohne das Integritätsversprechen des DL-Systems in Frage zu stellen.[218]

2. Problemfelder aufgrund der technischen Struktur

Smart Contracts können, sobald sie in eine Blockchain implementiert wurden, grundsätzlich **nicht mehr (einseitig) verändert** werden.[219] Hierdurch können grundsätzlich nur die Vorgaben und Wertungen des Programmierers bei der Erstellung und das zu diesem Zeitpunkt geltende Recht berücksichtigt werden.[220] Ein einmal unterlaufener Fehler haftet

[214] *Wright/De Filippi*, S. 26, *Kaulartz/Heckmann*, CR 2016, 618 (620).
[215] Nach *Lange-Hausstein*, ITRB 2017, 93 (94) sog. „doppelt digitale" Fälle.
[216] Vgl. *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (95).
[217] Beispiel nach *Kaulartz/Heckmann*, CR 2016, 618 (620).
[218] Dazu, wie durch Schnittstellen das Integritätsversprechen der Blockchain hinfällig werden kann, bereits zuvor, S. 32 ff.
[219] *Kaulartz/Heckmann*, CR 2016, 618 (623 f.); *Djazayeri*, jurisPR-BKR 12/2016, Anm. 1, S. 4.
[220] *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (95 f.).

dem Algorithmus des Smart Contract auf Dauer an; einen Abbruchmechanismus gibt es grundsätzlich nicht.[221] Im Zusammenhang mit dieser Unabänderlichkeit ergeben sich verschiedene Problemfelder.

a) Programmierfehler

Zum einen müsste ein **unveränderbarer Code** in seiner Gänze perfekt sein. Jeder kleinste **Fehler** („Bug“) würde unaufhaltsam fortgeführt werden und könnte desaströse Auswirkungen haben. Während man den „unsicheren Faktor Mensch“ ausklammert, schafft man ein unübersehbares Exzesspotential des „*Smart*“ *Contracts*, dem nicht mehr beizukommen wäre.[222] Besonders kritisch ist: fehlerfreien Code zu programmieren kann jedenfalls bei komplexen Sachverhalten nicht garantiert werden.[223] Ein nicht durchdachter Umstand oder eine einzige falsche Programmzeile könnten das gesamte System in Frage stellen. Durch die automatisierte Ausführung des Codes kann es so zu unerwünschten Transaktionen kommen. Die häufigangepriesene Immunität der Blockchain gegen Hacker erweist sich insoweit als Scheinargument. Im Hinblick auf klassische Angriffe, die sich gegen die Schwachstellen einer zentralen Stelle richten und bereits festgeschriebene Daten manipulieren wollen, trifft die Feststellung im Wesentlichen noch zu; allerdings eröffnen Programmierfehler die Möglichkeit, durch geschicktes Ausnutzen von **Lücken** Eingriffe in das System vorzunehmen und digitale Güter zu entwenden.[224]

Hieraus leitet sich schon die erste Gestaltungsanforderung ab: den Umfang des Codes möglichst gering und übersichtlich zu halten. Eine nachträgliche Korrektur von Fehlern wäre alleine durch die betroffenen Parteien nicht mehr möglich.[225] Dass der Code öffentlich einsehbar ist und jeder mit einer öffentlichen Blockchain interagieren kann, erhöht das Risikopotential.

b) Geschlossenheit der Blockchain

Weiterhin stellt die **Geschlossenheit** des Systems Blockchain ein besonderes Problem dar.

aa) Limitierter Blickwinkel und Einflussbereich Trotz der Möglichkeit, über Schnittstellen (Oracles) außerhalb stattfindende Ereignisse einzubeziehen, kann der Smart Contract selbst keinen Blick auf die **Begleitumstände** in der realen Welt werfen, geschweige denn Rücksicht auf die

[221] Vgl. *Sachikoy*, There is no mechanism to abort chaincode even if it has an infinite loop, https://github.com/hyperledger-archives/fabric/issues/2232; *Hoppen*, „The DAO-Hack“ und der letzte Flug Otto Lilienthals am 09.08.1896.

[222] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 11.

[223] In Programmierer-Kreisen kursiert der Spruch „There is no such thing as bug free software“, vgl. etwa https://www.thinslices.com/blog/there-is-no-such-thing-as-bug-free-software.

[224] So geschehen im Fall der DAO, vgl. https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde.

[225] Es müsste, sollte es an einer entsprechenden Schnittstelle fehlen, die gesamte Blockchain verändert werden, wozu ein Hard Fork[226] erforderlich wäre; vgl. auch hier den Fall der DAO Fn. 228.

Hintergründe der Parteien und deren Absichten nehmen.[227] Eben auf diese kommt es jedoch nach rechtlichen Maßstäben an. Der Empfängerhorizont etwa spielt nicht nur bei der Auslegung von Willenserklärungen (§ 157 BGB), sondern auch bei der Frage der Teilbarkeit von Rechtsgeschäften (§ 139 BGB) oder Umdeutungen (§ 140 BGB) eine wichtige Rolle. Andere tatsächliche Umstände, wie etwa die Geschäftsunfähigkeit oder Minderjährigkeit einer Vertragspartei bleiben der Blockchain ebenso verborgen wie rechtliche Wertungen, angefangen bei der Sittenwidrigkeit bis hin zum Tatbestandsmerkmal „unverzüglich“ (§ 121 Abs. 1 S. 1 BGB). Auf einzelne Aspekte soll im Zuge der Erörterung rechtlicher Divergenzrisiken näher eingegangen werden.[228]

Soll der Smart Contract eine Handlung in der Außenwelt vollziehen und diese auch unter Garantie durchgeführt werden, stößt man schnell an technische Grenzen: Der **Einfluss** des Smart Contract reicht schlicht nicht weiter als an die Grenzen des Netzwerks.[229] Innerhalb des Netzwerks kann er theoretisch auf alle digitalen Assets zugreifen. Sollen jedoch im Ledger Gegenstände oder Rechte der analogen Welt gehandelt werden (Off-Chain-Assets), erweist sich die elektronische Durchsetzung der Systemlogik häufig als problematisch.[230] Mithilfe von Schnittstellen kann ggf. der Zugang reguliert werden, etwa zu einer Wohnung mittels eines vernetzten Schlosses („Smart Lock“).[231] Eine in der analogen Welt zu erbringende Dienstleistung kann der Smart Contract nie unmittelbar erzwingen; allenfalls können Kautionen oder sonstige Strafzahlungen vorgesehen werden.[232] In vielen Fällen bleibt daher nur der Rückgriff auf traditionelle Vollstreckungsmittel, die wiederum voraussetzen, dass man die andere Partei kennt.[233]

bb) Schnittstellen Mit den ggf. erforderlichen Schnittstellen gehen jedoch eigene Probleme einher.

So hängt zum einen die Vertrauenswürdigkeit des Systems von der **Vertrauenswürdigkeit der Oracles** ab.[234] Ist eine der im Smart Contract definierten Bedingungen eine solche der analogen Welt, muss sie zuverlässig dokumentiert werden können. Diese Schnittstellenproblematik dürfte die meisten Vertragsverhältnisse betreffen. Sollten fehlerhafte bzw. gar manipulierte Daten aufgenommen werden, bleibt die falsche Information ohne entsprechende Korrekturmöglichkeiten für immer im Ledger festgeschrieben und führt ggf. zur Auslösung bestimmter Aktionen des Smart Contracts.

Zum anderen bedeuten Schnittstellen häufig, dass es sich nicht mehr um ein in jeder Hinsicht objektiviertes, vertrauensunabhängig selbstvollziehen-

[227] *Mik*, Law, Innovation and Technology 2017 (9.2), p. 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 7.
[228] Siehe S. 52 ff.
[229] *Clack/Bakshi/Braine*, *Smart Contract* Templates I, S. 4 f.
[230] *Swanson*, S. 21.
[231] *Paulus/Matzke*, ZfPW 2018, 431 (435). Die Blockchain gewährleistet hier Transparenz und eine nötige Infrastruktur, jedenfalls solange auch tatsächlich ein solches Schloss existiert und niemand anderes in der Wohnung ist.
[232] Hier soll nur auf die technische Möglichkeit hingewiesen, nicht die rechtliche Zulässigkeit unterstellt werden.
[233] *Clack/Bakshi/Braine*, *Smart Contract* Templates I, S. 4.
[234] Dazu ausführlich oben S. 32 ff.

des System handelt. Möchte man nämlich jede menschliche Unwägbarkeit beseitigen, müssten zur Sicherstellung des korrekten Leistungsaustauschs die festgesetzten Bedingungen auch ohne Zutun eines Menschen verifiziert werden können.[235] Ein Zahlungseingang kann ohne Weiteres verifiziert werden, ebenso eine Lieferung. Schwieriger gestaltet sich die Bestimmung, ob sich die gelieferte Sache auch in einem vertragsgemäßen Zustand befindet. Entscheidend ist, dass die im Smart Contract definierte Bedingung von einem digitalen System nach objektiven Kriterien registriert werden kann. Dafür muss sie in digitalen Daten darstellbar sein, es muss eine Quelle existieren, welche Daten dieser Art an einen Smart Contract weiterleiten kann und die Daten müssen auch im Einzelfall zur Verfügung stehen.[236] Kann ein Aspekt, etwa die Mangelfreiheit, im Anwendungsfall nicht nach diesen Maßstäben festgestellt werden, kann auch eine vertrauenswürdige Person benannt werden, deren Signatur die Transaktion auslöst.

c) Unvorhergesehene Umstände

aa) Problemstellung Von den Parteien **unvorhergesehene** oder **unvorhersehbare Umstände** stellen eine besondere Herausforderung dar. Ein unabänderlicher, die Ausführung unbedingt garantierender Mechanismus, der vollkommen resistent gegen menschliches Eingreifen sein soll, ist aufgrund dieser technischen Struktur grundsätzlich auch unaufhaltbar. Einmal in Gang gesetzt, lässt sich der Vollzug bis zum Erreichen eines ggf. gesetzten Ablaufdatums nicht mehr aufhalten. Deshalb müsste es gelingen, jedes auch nur entfernt vorstellbare Ereignis bei der Erstellung des Codes zu berücksichtigen. Unbesehen des Bedürfnisses, langfristige Vertragsverhältnisse dynamisch und flexibel zu gestalten, ist jedenfalls das Vorhersehen jeder Eventualität nicht zu bewältigen. Menschliches Versagen wird (selbstverständlich) auch bei der Verwendung einer Blockchain weiter vorkommen, etwa wenn eine Partei ihren privaten Schlüssel vergisst und deshalb eine vorgesehene Transaktion nicht autorisieren kann.[237] Können Korrekturen oder Rückabwicklungsgründe wie etwa Anfechtungstatbestände nicht automatisiert und objektiviert berücksichtigt werden, sind die Parteien auf die herkömmlichen Wege der Vertragsabwicklung, notfalls den Gerichtsweg angewiesen.[238] Dafür muss es sich nicht einmal um unvorhersehbare Umstände bzw. höhere Gewalt handeln.

bb) Alternativen und deren Implikationen Freilich bleibt es den Parteien überlassen, zugunsten eines unaufhaltbaren Austauschs von Primärleistungen die Auflösung von eintretenden Diskrepanzen auf die Sekundärebene, also etwaige Gewährleistungsrechte oder sonstige Rechtsbehelfe bei Nicht- oder Schlechtleistung zu verlagern. Man könnte sich zunächst darauf einlassen, dem Vertrag seinen Lauf zu lassen, wie er sich im Code widerspiegelt, und notfalls die Gerichte anzurufen, um später eine Klärung herbeizuführen. Das setzt jedoch voraus, dass die Parteien einander ihre

[235] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 21.
[236] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 22.
[237] *Levy*, Engaging Science, Technology and Society 3 (2017), 1 (3 f.).
[238] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (14).

Identität offenbart haben. Doch selbst dann lässt sich die Gefahr irreversibler Schäden aufgrund unvorhergesehener Ereignisse nicht von der Hand weisen.

Jedenfalls müssen die Parteien sich bewusst machen, dass sie sich jeglicher **Spielräume** entledigen, vom Code abweichende Entscheidungen zu treffen. Im Geschäftsverkehr ist es etwa üblich, zur Pflege einer besseren Geschäfts- oder Kundenbeziehung etwaige Fehler aus **Kulanzgründen** oder um deren Geringfügigkeit Willen zu ignorieren.[239] *Levy* weist überzeugend darauf hin, dass in vielen Fällen die sozialen Auswirkungen eines unbestechlich vollstreckenden Technologieinstruments zu ungeahnten Folgen führen könnte, während sich andere Anreizsysteme (Bewertungen, Boni, etc.) potentiell besser eignen, um die Einhaltung eines Vertrags zu gewährleisten.[240] Möchte man derlei Risiken umgehen oder auf eine Identifikation gegenüber dem Vertragspartner verzichten, kommen von vorneherein nur Austauschverhältnisse in Betracht, bei denen ein geringes Risiko für Schlechtleistungen besteht oder der Smart Contract selbst auf der Ebene der Blockchain die Gewährleistungsinstrumente abwickeln kann.[241] Auch sonst ist alleine der mit einem automatisierten System verbundene Verlust bestimmter Gestaltungsrechte, etwa von Zurückbehaltungsrechten, nicht unbeachtlich und will im Einzelfall gut überlegt sein.

3. Lösungsstrategien

Im Folgenden sollen einige Handlungsoptionen aufgezeigt werden, um den technischen Divergenzrisiken entgegenzuwirken.

a) Limitierung des Übersetzungsgegenstands

Erstens sollten die Aspekte eines Vertrags, die in einem Smart Contract integriert werden, limitiert werden. Nicht alle Bestandteile eines rechtlichen Vertrags sollten auch einem selbstvollziehenden System überantwortet werden. Die Bedingungen der digitalen Abbildbarkeit bzw. Überprüfbarkeit und das Erfordernis einer hinreichenden Objektivität geben erste Anhaltspunkte dafür, welche vertraglichen Regelungen überhaupt einer automatisierten Umsetzung zugänglich sind. Kaum zu integrieren sein dürften beispielsweise sämtliche Neben- und Schutzpflichten. Auch wenn diese zur vollständigen Gewährleistung der beiderseitigen Rechte und Pflichten dazugehören, sind sie derart umfangreich und einzelfallabhängigen, dass eine vollständige Beschreibung die Grenze des Machbaren überschreitet.[242]

Es sollte daher im Einzelfall geprüft werden, welche **Konkretisierung der Vertragsbeziehung** bzw. welcher Aspekt des Business-Prozesses herausgegriffen und in einem Smart Contracts mit vertretbaren Risiken abgebildet werden kann.

---

[239] *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (11).
[240] *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (11 f.).
[241] *Kaulartz/Heckmann*, CR 2016, 618 (620).
[242] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 10.

b) Limitierung des *Chain Codes*

Zweitens sollte der Umfang des tatsächlich in einer Blockchain implementierten **Programmcodes** (*Chain Code*) **möglichst klein** gehalten werden. Je weniger Regeln, desto weniger Fehlerpotential und desto unwahrscheinlicher ist ein Änderungsbedarf. Dabei müssen nur solche Logiken in ein Ledger eingebunden werden, deren Vollzug vertrauensunabhängig erfolgen soll bzw. für die ein unabänderlicher Nachweis zu erbringen ist. Können Teilaspekte unproblematisch ausgelagert oder einem Oracle überantwortet werden, dessen Programmcode im Ernstfall angepasst werden kann, sollte dies geschehen.

c) Geringes Schlechtleistungsrisiko als Vorzugskriterium

Während häufig schon die jeweilige Erfüllungshandlung nicht ohne Weiteres digital darstellbar und überprüfbar ist, erweist sich die Beschreibung möglicher Gewährleistungsrechte als besonders problematisch. Je nach Vertragsinhalt müssten alle herzustellenden Eigenschaften erfasst werden können, was sich schon bei der Übersetzung in Code als schwierig erweisen dürfte. So sind etwa beim Autokauf derart viele Fehler denkbar, dass sie der Smart Contract selbst nicht erkennen kann.[243] Infolge dessen ist auch der Inhalt der Gewährleistungsrechte, die je nach Natur des Schuldverhältnisses und der sonstigen Umstände unterschiedlich ausfallen können, häufig nicht en détail festschreibbar bzw. auf ein schematisches Regelwerk zu reduzieren.[244] Zwar kommt im Einzelfall in Betracht, einzelne Rechte abzubedingen; insbesondere im Verbraucherkontext setzt das Recht jedoch auch hier Grenzen (vgl. § 476 BGB). Ein **geringes Schlechtleistungsrisiko** erweist sich daher als Vorzugskriterium.

Ist die **Identität** der anderen Partei unbekannt oder ist sie als Schuldner nicht greifbar, dürfte das für öffentliche DL-Systeme ein Hindernis bedeuten. Damit empfiehlt sich die Technologie insbesondere für Fälle mit geringem Schlechtleistungsrisiko.[245] Beispielhaft genannt sei der Domainkauf:[246] Ein Smart Contract könnte darauf programmiert werden, eine verfügbare Internet-Domain bei Zahlung einer entsprechenden Summe freizugeben. Der Bedingungseintritt (Zahlungseingang) lässt sich einfach feststellen und auch die Gegenleistung (Freischaltung der Domän) ohne weiteres digital auslösen.

d) Aufheben der Anonymität

Nach den vorgenannten Gründen erscheint es in den meisten Fällen ratsam, auf eine gegenseitige Identifizierung zu bestehen. In einigen Ge-

[243] Man könnte freilich einen neutralen Gutachter benennen, der die notwendige Signatur zur Freigabe des Kaufpreises nach einer Überprüfung des Fahrzeugs erteilt – freilich konträr zur Idee, Mittelsmänner loszuwerden.

[244] *Kaulartz/Heckmann*, CR 2016, 618 (620 f.) weisen entsprechend auf das Risiko hin, das ohne Identifizierung im Fall der Schlechtleistung besteht. Es ließe sich zumindest unter Kaufleuten daran denken, für die Fälle der Schlechtleistung eine spezifisches Gewährleistungsrecht, etwa nur Nachlieferung im Kaufrecht, festzuschreiben.

[245] *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (14).

[246] Beispiel von *Lauslathi/Mattila/Sepällä*, S. 19 f.

schäftsbeziehungen prägen **Know-Your-Costumer-Pflichten** (**KYC**) ohnehin die Geschäftsprozesse.[247] Kann das System einen reibungslosen Ablauf nicht in jeder Hinsicht garantieren, insbesondere wenn Off-Chain-Assets eingebunden sind, dürfte bei komplexeren oder wirtschaftlich bedeutsameren Geschäften kein Weg an einer Identifizierung vorbeiführen. So könnte etwa notfalls vor einem Gericht auf Freigabe einer Leistung (Signatur einer Transaktion) geklagt werden.

Helfen könnten hierbei insbesondere digitale Identitätsnachweise, die gegenwärtig in verschiedener Form entwickelt werden.[248] Man könnte etwa in einem Distributed-Ledger dem Nutzer eine unabänderliche ID zuweisen, mit der er sich in Verbindung mit seinem privaten Schlüssel identifizieren kann.[249] Hier könnte gerade eine staatliche Infrastruktur von großem Nutzen sein.

e) Korrekturschnittstellen

aa) Einbindung Um entsprechenden Fehlabläufen vorzubeugen, müssten von vorneherein entsprechende **Schnittstellen zur späteren Korrektur** oder notfalls zum Abbruch der Ausführung implementiert werden.[250] Die Verantwortung könnte dann entweder bei den Parteien gemeinsam liegen oder einer neutralen Stelle überantwortet sein. Der Vertrag wäre in diesem Fall zwar automatisiert, aber gleichzeitig – Kenntnis der Parteiidentitäten vorausgesetzt – gerichtlich durchsetzbar, indem die eine oder die andere Seite zur Ausführung der Signatur angehalten werden könnte (§ 888 ZPO).[251] Dabei müssen Korrekturen überhaupt nicht in die Transaktionshistorie eingreifen: Ist eine Schnittstelle implementiert, dürfte es in der Regel völlig ausreichen, den Ledger hin zur wahren Rechts- oder Tatsachenlage fortzuschreiben. Einer einzelnen Stelle als Regulator oder Korrektor die Möglichkeit zu Eingriffen zu geben, würde so nicht notwendigerweise auch die Beweiskraft des Ledger in Mitleidenschaft ziehen, wenn alle Rechte und deren Gebrauch zu Korrekturen transparent sind und nachvollzogen werden können.[252]

Für Fehleintragungen oder bewusst falsche Eintragungen genügt es entsprechend, dass eine neue Transaktion – mit Verweis auf die alte – die wahre Rechts- oder Tatsachenlage darstellt und das System fortan die Korrektur referenziert. Inwiefern Dritte auf die Eintragung vertrauen und deshalb ein möglicher Schaden zu ersetzen ist, ist eine andere Frage. Ungleich schwerer erweist sich die Durchsetzung einer vollständigen Löschung des alten Eintrags, etwa aufgrund von Persönlichkeitsrechtsverletzungen oder aus Datenschutzgesichtspunkten.

bb) Besondere Korrekturschnittstellen Teilweise wird ein solcher Regulator auch im Hinblick auf die Berücksichtigung von Gerichtsurteilen

[247] Siehe S. 90 ff.
[248] *Reed/Sathyanarayan/Ruan/Collins*, S. 14 f.
[249] *Reed/Sathyanarayan/Ruan/Collins*, S. 15.
[250] *Jaccard*, JuS-Letter IT 23, November 2017, S. 24.
[251] *Clack/Bakshi/Braine*, *Smart Contract* Templates II, S. 2.
[252] *Reed/Sathyanarayan/Ruan/Collins*, S. 23.

vorgeschlagen, der dann über eine „**Justizschnittstelle**“ Urteile oder andere Titel auch On-Chain vollstrecken könnte.[253] So sollen ggf. auch Anpassungen eines Protokolls oder Programmcodes autorisiert werden können. Weniger offiziell, jedoch mit gleicher Zielsetzung, käme die Einsetzung eines Schiedsgerichts in Betracht, das über eine spezielle Schnittstelle im Falle der Schlechtleistung oder sonstiger Streitigkeiten abhelfen könnte.[254] Neben dem Zugang müssen dabei alle Rechte und Handlungsoptionen von vorneherein hinzuprogrammiert werden.[255]

cc) Implikationen in zulassungsfreien Netzwerken In einem öffentlichen, völlig pseudonymisierten Netzwerk ergäben sich schnell Schwierigkeiten.[256] Korrekturen der Transaktionshistorie sind in diesen Fällen in der Regel nur durch einen *Hard Fork* möglich. Gerade Schnittstellen zur realen Welt bringen ein nicht außerhalb jeder Wahrscheinlichkeit liegendes Fehlerpotential mit sich. Sollte eine solche erforderlich sein, könnten sich öffentliche Netzwerke deshalb als ungeeignet erweisen. Ein zumindest in Teilen von einem Schlichter, Regulator oder sonstigen „Super-User“[257] kontrolliertes Netzwerk könnte in diesen Fällen besser geeignet sein. Das betrifft insbesondere Ledger, welche dingliche Rechtszustände dokumentieren sollen.

[253] *Kaulartz/Heckmann*, CR 2016, 618 (624).
[254] *Kaulartz/Heckmann*, CR 2016, 618 (620, 624); *Jaccard*, JuS-Letter IT 23, November 2017, S. 24.
[255] *Kaulartz/Heckmann*, CR 2016, 618 (624). Ein mögliches Verfahren wäre die Implementierung einer „2 of 3-MultiSig“-Transaktion: Eine Transaktion, sei es Leistung oder Rückabwicklung, wird ausgeführt, wenn beide Vertragsparteien zustimmen oder der Schlichter, als dritter Beteiligter, der einen oder der anderen Seite Recht gibt; vgl. *Blocher*, AnwBl. 2016, 612 (617).
[256] *Swanson*, S. 21.
[257] *Reed/Sathyanarayan/Ruan/Collins*, S. 18.

VI. Rechtliche Divergenzrisiken bei selbstvollziehenden Verträgen

Im Folgenden sind die rechtlichen Ursachen, die für ein Auseinanderfallen von Rechtslage und technischem Vertragsabwicklungsinstrument sorgen können, zu untersuchen und Handlungsstrategien aufzuzeigen.

1. Vorliegen eines Vertrags im Rechtssinne

Einer Blockchain lassen sich zunächst nur Tatsachen entnehmen, indem sie den Nachweis dafür liefert, dass eine Transaktion stattgefunden hat. Sie schafft hingegen als solche kein Recht oder rechtliche Gültigkeit. Selbst wenn eine Transaktion aussagt, es sei eine **vertragliche Einigung** zustande gekommen, muss diese Aussage noch einer rechtlichen Prüfung unterzogen werden.[258] Ausgangspunkt jeder rechtlichen Untersuchung muss daher sein, ob überhaupt ein Vertrag im Rechtssinne und somit eine privatautonome Gestaltung der Rechtslage vorliegt. Erforderlich ist eine mit Rechtsbindungswille getroffene Einigung, die alle wesentlichen Bestandteile einer Vertragsbeziehung abdeckt.

Nach allgemeinen Grundsätzen kommt es auf das Vorliegen mindestens zweier aufeinander Bezug nehmender **Willenserklärungen** an, aus denen sich ein Wille zur Vereinbarung einseitiger oder wechselseitiger Rechte und Pflichten ableitet. Eine Willenserklärung kann sowohl ausdrücklich, als auch durch schlüssiges Handeln (konkludent) abgegeben werden.[259] Signieren beide Parteien einen Smart Contract und setzen damit dessen Wirkungen in Gang, könnte dies als konkludente Einigung zu verstehen sein, entsprechend der Bedingungen des Codes kontrahieren zu wollen. Die Willenserklärung ergibt sich dann aus den **äußeren Umständen**.[260]

Dabei ist jedoch Vorsicht geboten: Grundsätzlich sollte bei der Ermittlung des Vertragsinhalts nicht alleine auf den Code abgestellt werden, da dieser für die meisten Nutzer unverständlich ist.[261] Der **gemeinsame Vorstellungshorizont**, insbesondere bezüglich der vermeintlichen Auswirkungen des Codes, ist stets anhand der Gesamtumstände zu ermitteln. Die Wahl eines Smart Contracts als Abwicklungsinstrument tritt demnach nur als ein Aspekt im Rahmen der Auslegung der schuldrechtlichen Einigung gem. §§ 133, 157 BGB auf.[262]

Bei der Identifizierung der **Erklärungszeichen** darf jedoch nicht vorschnell auf den Programmcode abgestellt werden. In den meisten Fällen ist die

[258] *Jaccard*, JuS-Letter IT 23, November 2017, S. 8.

[259] Vgl. *Singer*, in: Staudinger (2017), BGB, Vor §§ 116–144 Rn. 51 ff.

[260] *Söbbing*, ITRB 2018, 43 (45); für das angloamerikanische Recht *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (322 f.).

[261] *Kaulartz/Heckmann*, CR 2016, 618 (621), die jedoch dem Programmcode die Fähigkeit Willenserklärungen auszudrücken völlig absprechen. Dies ist jedenfalls ungenau. Möchte man eine Willenserklärung auf den Inhalt reduzieren, dass der Programmcode Geltung erlangen solle, so wäre der für die Vertragseinigung bedeutsame Inhalt nämlich im Code zu suchen. Einige, zum Beispiel *Jaccard*, JuS-Letter IT 23, November 2017, S. 23 raten jedenfalls davon ab.

[262] *Kaulartz/Heckmann*, CR 2016, 618 (621); *Söbbing*, ITRB 2018, 43 (45). Vgl. zur Auslegung näher unten S. 61 ff.

Abgabe völlig isoliert vom Smart Contract zu erwarten. Dies folgt insbesondere aus der Bewertung verschiedener Gestaltungsszenarien.

a) Szenarien

aa) Szenario 1 – Vertrag außerhalb des Systems Eine Möglichkeit wäre es, den Vertrag **außerhalb** des DL-Systems in konventioneller Form zu schließen und dessen Regelungen später in Form vollzugsfähigen Codes zu implementieren. Denkbar wäre auch eine nur teilweise Automatisierung, bei welcher lediglich ein Teilbereich der Vertragsbeziehung selbstvollziehend umgesetzt wird.

Die Interessenlage dürfte in der Regel dahingehend auszulegen sein, dass nur der außerhalb einer Blockchain geschlossene Vertrag letztverbindlich sein soll. Sonst würden Programmierfehler gleichzeitig ungewollte Rechtsfolgen herbeiführen. Stattdessen können in einem isolierten Vertrag besondere Regelungen für die Korrektur ungewollter Abläufe aufgenommen werden.[263]

Alternativ käme in Betracht, einen in Text gefassten, umfassenden **Rahmenvertrag** zu schließen, der nachfolgend durch zahlreiche in Codeform gefasste Einzelverträge konkretisiert werden soll. Der Rahmenvertrag müsste dabei die möglichen Gestaltungsvarianten abbilden und gewünschten Abläufe beschreiben, könnte die Details aber an das technische System auslagern, während er für mögliche Fehlabläufe, unvorhergesehene Umstände oder sonstige abstrakt regelungsbedürftige Umstände selbst den gewünschten Rahmen setzt.

bb) Szenario 2 – Code als Vertrag? Eine andere Möglichkeit bestünde darin, den Vertrag alleine als Programmcode bzw. Protokoll zu formulieren, während auf einen in natürlicher – also von Menschen verwendeter – Sprache gefassten Vertragstext vollständig verzichtet wird. Hierbei nähert man sich am ehesten dem Dogma „Code is Law“ an, wie es in einigen Diskussionen im DLT-Kontext (jenseits des juristischen Diskurses) auch weiterhin vertreten wird. Alle dem Code entgegenstehenden gesetzlichen Normen wären nach diesem Verständnis, soweit möglich, konkludent abbedungen.[264]

(1) Zulässigkeit Die Zulässigkeit einer Einigung in Programmiersprache wird dabei überwiegend bejaht.[265] Der Einwand, mangels allgemeiner Lesbarkeit eigne sich Programmiersprache nicht als Vertragssprache, kann nicht überzeugen. Aus dem Grundsatz der **Vertragsfreiheit** (§ 311 Abs. 1

[263] Vgl. zu den Hintergründen bereits die Vermeidungsstrategien S. 44 ff.

[264] Alternativ könnte in einer solchen Vereinbarung auch der Verzicht auf jegliches Vertragsverhältnis zu lesen sein, so, jedoch mit Bedenken, *Mann,* NZG 2017, 1014 (1017).

[265] *Kaulartz/Heckmann*, CR 2016, 618 (622); *Söbbing*, ITRB 2018, 43 (46); *Heckelmann*, NJW 2018, 504 (506); *Djazayeri*, jurisPR-BKR 12/2016, Anm. 1; für das schweizerische Recht *Jaccard*, JuS-Letter IT 23, November 2017, S. 22.

BGB) folgt eine weite Gestaltungsmacht der Parteien hinsichtlich der Fassung ihrer rechtsgeschäftlichen Einigung.[266] Hinzu kommt, dass das deutsche Recht auch sonst keine bestimmte Sprache vorschreibt.[267] Vorbehaltlich später zu behandelnder AGB-rechtlicher Implikationen[268] ist daher die Vereinbarung eines Vertrags in Code-Form zulässig.

(2) Schwierigkeiten und Mittelwege Problematisch erscheint jedoch, dass nur wenige in der Lage sein dürften, den in Programmiersprache verfassten Vertrag vollends zu erfassen.[269] Hinweise und Erläuterungen in den Code einzubetten ist zwar möglich, jedoch weder übersichtlich noch für die meisten transparent. Je nach Netzwerkarchitektur könnten sich bei öffentlichen DL-Systemen aufgrund des erhöhten Speicherbedarfs u.U. Skalierungsprobleme ergeben.

Einen Mittelweg gehen Konzepte, die man als „***dual integration***" bezeichnen könnte.[270] Hierbei wird in der Außenwelt ein Vertragsdokument erstellt, dass die im Code getroffenen Regelungen vollständig widerspiegelt und die Adresse des Smart Contract wiedergibt. Gleichzeitig wird in der jeweiligen Systemarchitektur, bei Smart Contracts der Blockchain, eine verschlüsselte Version dieses Dokuments hinterlegt, sodass eine untrennbare und jederzeit verifizierbare Verbindung entsteht. Übersetzungsprobleme sollen hierdurch soweit wie möglich vermieden werden, während davon abgesehen wird, den Vertragstext ausschließlich in Code-Form auszudrücken.

Eine ähnliche Idee verfolgt der Erfinder des Ricardianischen Systems *Grigg*, der Smart Contracts mit seinem ursprünglichen Projekt zusammenführen möchte.[271] Das in natürlicher Sprache gefasste Vertragsdokument soll unter Zuhilfenahme einer besonderen **Markup-Sprache** in maschinenlesbare Form gebracht und gehashte Referenzen eine untrennbare Verknüpfung von Vertrag und Code herstellen.[272] Wie sich eine solche Markup-Sprache oder sonstige Parameter zur Verknüpfung von Recht und Code fassen lassen, wird derzeit auch von zahlreichen anderen Projekten untersucht.[273]

(3) Zwischenfazit Ausschließlich codierte Verträge erweisen sich aus Transparenzgesichtspunkten als problematisch. Auch wenn sich der Vertrag meist schon aus den äußeren Umständen ergibt, erscheint eine **textgebundene**, in natürlicher Sprache verfasste Version vorzugswürdig. Der

---

[266] *Kaulartz/Heckmann*, CR 2016, 618 (622).

[267] *Djazayeri*, jurisPR-BKR 12/2016, Anm. 1; *Singer*, in: Staudinger (2017) BGB § 119, Rn. 18.

[268] Vgl. S. 72 f.

[269] Vgl. *Jaccard*, JuS-Letter IT 23, November 2017, S. 22.

[270] Vgl. zum Konzept *Christidis/Devetsiokiotis*, IEEE Access 2016, 2292 (2300 f.). Begriff erstmals verwendet Monax Industries für ihr entsprechendes Produkt, Dual Integration, 2016, abrufbar unter: https://monax.io/learn/dual_integration/.

[271] *Grigg*, On the intersection of ricardian and smart contracts, 2015, abrufbar: http://iang.org/papers/intersection_ricardian_smart.html

[272] Vgl. *Clack/Bakshi/Braine*, Smart Contract Templates I, S. 7 ff.; *dies.*, Smart Contract Templates II, S. 3 ff.

[273] Nennenswert etwa das Accord-Projekt, vgl. https://www.accordproject.org, oder die Working Group 3 unter dem ISO/TC 307 "Smart contracts and their applications", https://www.iso.org/standard/75095.html, jedoch beide bislang ohne Ergebnisse.

Code kann daran anküpfend mit dem Vertragstext (digital) verlinkt werden, wobei idealiter der Vertragstext eine "Übersetzung"des Codes (in anderen Worten eine Beschreibung des gewünschten Funktionsablaufs) enthält.[274] Statt zu versuchen, den gesamten Vertrag in Programmiersprache zu zwängen, könnte sich der Vertrag dabei auf eine möglichst präzise Beschreibung der gewünschten Programmabläufe konzentrieren, während für unvorhergesehe Umstände bewährte, abstrakt gehaltene Regelungen festgehalten sind.

b) Praktische Perspektiven?

Nach alledem erweist sich das Szenario 1 als die effizientere Lösung – insbesondere in der Variante des **Rahmenvertrags**. Damit unterscheidet sich die Herangehensweise jedoch nicht besonders von herkömmlichen automatisierten Abwicklungsinstrumenten: Der auf herkömmlichen Wege geschlossene Vertrag erfährt eine teilweise automatisierte Abwicklung, indem etwa einzelne Schritte einer Warenlieferung mit einer automatisierten Zahlungsüberweisung verknüpft sind. Die entsprechenden Modalitäten sind als Nebenpunkte im Vertrag geregelt.

Die gesteigerte Komplexität in Verbindung mit den im Einzelfall benötigten Ressourcen werden dafür sorgen, dass ein vollständig codierter Vertrag regelmäßig nicht in Frage kommt. Es dürfte insbesondere die Ausnahme sein, dass beide Parteien das entsprechende Hintergrundwissen besitzen, um selbst eine möglichst fehlerfreie codierte Fassung des Vertrags zu erstellen. Sie müssten nicht nur rechtliche wie wirtschaftliche Risiken hinreichend berücksichtigen können, sondern zudem ein hinreichendes Verständnis für das Programmieren mitbringen.

Mit der Zeit könnten sich stattdessen **Datenbanken** entwickeln, in welchen (ggf. bestimmte Anbieter) Musterverträge mit dem korrespondierenden Smart Contract bereitstellen und diese ggf. nach Bedarf konfigurieren.[275] Bei der sorgsamen Entwicklung von Vorlagen ist eine enge Zusammenarbeit zwischen Juristen und Programmierern unvermeidlich. Sollte bei der Gestaltung des Vertragstextes eine individuelle, einzelfallbezogene juristische Prüfung erfolgen, ist darauf zu achten, dass möglicherweise eine erlaubnispflichtige Rechtsdienstleistung gem. § 2 Abs. 1 RDG vorliegt.[276]

Welche typischen Risiken oder Fehlerursachen sich bei selbstvollziehenden Verträgen, insbesondere unter Verwendung der Blockchain-Technologie, ergeben können, wird im Folgenden untersucht.

2. Wirksamkeit automatisierter Willenserklärungen

Der automatisierte Vertragsumsetzung durch einen Smart Contract kann es mit sich bringen, dass Willenserklärungen bereits im Code vorgesehen sind und durch das technische System abgegeben werden sollen. Denkbar ist etwa die vorweggenommene Erklärung eines Zurückbehaltungsrechts

[274] So auch Best-practices-Vorschlag von *Jaccard*, JuS-Letter IT 23, November 2017, S. 23.
[275] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 16.
[276] Vgl. *Römermann/Günther*, NJW 2019, 551 (552).

oder Rücktritts bei fehlendem Zahlungseingang. Immer dann, wenn künstliche Systeme bzw. Maschinen rechtsgeschäftliche Handlungen ausführen, ohne selbst Träger von Rechten und Pflichten sein zu können, wirft dies **Zurechnungsfragen** auf.

a) Unterscheidung automatisiert bzw. autonomisiert

Die Zurechnungsfrage stellt sich dabei in unterschiedlicher Intensität, je nachdem, ob eine Automatisierung oder eine Autonomisierung vorliegt. **Automatisierung** bedeutet, dass der Nutzer die Regeln, nach denen das System agiert, in vollem Umfang vorgibt und damit dessen Handlungsspielraum vollständig determiniert.[277] Die delegierten Arbeitsschritte beziehungsweise Entscheidungsfindungen werden entsprechend vorher bestimmter Parameter ausgeführt und sind damit hinsichtlich ihrer Ergebnisse in vollem Umfang vorhersehbar. Das System kann jedoch nicht selbständig tätig werden bzw. nach eigenen Kriterien entscheiden. Unabhängigkeit und Indeterminiertheit zeichnen hingegen ein **autonomes System** aus.[278] Entsprechend der griechischen Wortherkunft (*auto* = selbst, unabhängig und *nomos* = Gesetz, Regel) kann dieses ohne spezifische Veranlassung nach seinen eigenen Regeln tätig werden, diese auf Basis neuer Informationen verändern oder neue Regeln schaffen.[279] Diese Differenzierung ist notwendig, da in Zurechnungsfragen bei autonomen Systemen aufgrund des marginalisierten Einflusses natürlicher Personen (ggf.) andere Maßstäbe anzulegen sind.[280]

b) Einordnung der Rechtshandlungen eines selbstvollziehenden Vertrags

Bei selbstvollziehenden Verträgen übernimmt das System entsprechend seines Programmcodes teilweise Handlungen, die sonst von natürlichen bzw. juristischen Personen ausgeführt würden. Da alle möglichen Handlungsschritte bereits im Code enthalten sind und dieser ohne Wertungsspielraum ausgeführt wird, ist das System in jeder Hinsicht vom Menschen **determiniert** und damit grundsätzlich als **Automatisierungsvorgang** einzuordnen. Das gilt auch, wenn das System noch innerhalb vorgegebener Wertungsspielräume tätig wird. Auf absehbare Zeit kann von einem selbständigen Tätigwerden oder der Fähigkeit zur autonomen Regeländerung noch nicht im relevanten Maße ausgegangen werden.

Die Diskussion um die generelle Wirksamkeit eines von einem autonomen künstlichen System geschlossenen Vertrags bzw. die Rechtsfähigkeit von Robotern muss daher hier nicht ausgeführt werden.[281] Es handelt sich um

[277] Vgl. *Sosnitza*, CR 2016, 764 (765).

[278] In Abweichung zum selbstvollziehenden Vertrag, der seine eigenen Regeln von der einzelnen Vertragspartei unbeeinflusst durchsetzen kann.

[279] Vgl. *Sosnitza*, CR 2016, 764 (765).

[280] Jedenfalls sind andere Begründungsansätze erforderlich, vgl. überblicksweise *Paulus/Matzke,* ZfPW 2018, 431 (442 ff.).

[281] Vgl. hierzu etwa *Specht/Herold*, MMR 2018, 40 (41 ff.); *Paulus/Matzke,* ZfPW 2018, 431 (441 ff.).

eine nicht DL-spezifische Frage, die aufgrund der alsbald nicht zu erwartenden Autonomie der Systeme hier nicht vertieft werden muss.[282]

c) Wirksamkeit von Willenserklärungen mittels eines Smart Contracts

Soweit die Parteien also Willenserklärungen mittels eines Smart Contract abgeben, handelt es sich um einen **automatisierten Rechtsvorgang**. Hierzu zählt bspw. die Auslösung eines Gestaltungsrechts durch das Programm entsprechend vorher festgelegter Bedingungen. Die Zurechnung und Wirksamkeit solcher – häufig als Computererklärung bezeichneter[283] – automatisiert generierter Willenserklärungen wird heute unter dem Gesichtspunkt des arbeitsteiligen Zusammenwirkens und Bestehen eines generellen Erklärungswillens als unproblematisch angesehen.[284]

d) Bedingungsfeindlichkeit einseitiger Rechtsgeschäfte

Einseitige Rechtsgeschäfte sind in der Regel bedingungsfeindlich (vgl. insb. § 388 S. 2 BGB).[285] Eine rechtsgestaltende Wirkung soll final eintreten; der Vertragspartner nicht in eine unzumutbare Schwebelage gebracht werden. Eine Schwebelage ist grundsätzlich nur zumutbar, soweit die Bedingung nicht der Willkür des Erklärenden unterliegt und sich der Vertragspartner entsprechend darauf einstellen kann.[286] Auch beseitigt das Einverständnis der anderen Partei eine etwaige Unzumutbarkeit.[287]

Smart Contracts geraten mit ihrer Automatisierung hierzu nicht in Konflikt. Die Fixierung der Bedingungen im Programmcode führt dazu, dass dem Eintritt der **objektiven Parameter** garantiert die Ausführung der Transaktion folgt. Entweder sieht man erst in der auslösenden Transaktion die Erklärung des Gestaltungsrechts, dann läge kein bedingtes Rechtsgeschäft vor, oder man verneint grundsätzlich eine Schwebelage, da die Bedingungen objektiv gefasst sind und ihr Eintritt stets objektiv nachvollziehbar ist.

Selbst wenn einer Partei das Recht überlassen sein soll, sich nach freiem Belieben mittels einer Transaktion vom Vertrag lösen zu können, liegt in dieser Vereinbarung kein bedingtes Gestaltungsrecht, sondern die Vereinbarung eines vertraglichen Rücktritts- (§ 346 Var. 1 BGB) bzw. Widerrufsrechts.

e) Zugangsfragen

Schließlich bringt die Einschaltung eines technischen Systems einige **Zugangsfragen** mit sich.

---

[282] Mit diesem Hinweis auch *Paulus/Matzke*, ZfPW 2018, 431 (465).
[283] Vgl. *Singer*, in: Staudinger (2017), BGB, Vor §§ 116 – 144, Rn. 57.
[284] Statt vieler *Singer*, in: Staudinger (2017), BGB, Vor §§ 116–144, Rn. 57; *Specht/Herold*, MMR 2018, 40 (41); abweichend teilweise ältere Literatur, vgl. *Clemens*, NJW 1985, 1998 (2001 f.).
[285] Vgl. *Westermann*, in: MüKo-BGB; § 158 Rn. 28.
[286] *Westermann*, in: MüKo-BGB; § 158 Rn. 29.
[287] *Mansel*, in: Jauernig, BGB, § 158 Rn. 11.

aa) Grundsätze Eine Willenserklärung unter Abwesenden wird wirksam, wenn sie zugeht, § 130 S. 1 BGB. Hierfür muss die Erklärung dergestalt in den **Machtbereich** des Erklärungsempfängers gelangen, dass dieser unter normalen Umständen die **Möglichkeit zur Kenntnisnahme** hat.[288] Wird eine Willenserklärung durch das technische System generiert, muss das Design folglich sicherstellen, dass die gegnerische Partei hiervon Kenntnis erlangen kann. Auch wenn es sich bei einer Blockchain um ein öffentliches Register handelt, ist jedenfalls der Node, den der Empfänger über seinen Client adressiert, seinem gewählten Machtbereich zuzuordnen. Die Möglichkeit der Kenntnisnahme wäre anschließend nach allgemeinen Grundsätzen zu beurteilen.

Im Rahmen der Privatautonomie ist der Zugang als Wirksamkeitserfordernis zudem grundsätzlich disponibel und kann durch alternative Anknüpfungspunkte ersetzt werden, etwa die Abgabe der Erklärung oder die Übernahme der entsprechenden Transaktion in eine Blockchain mit X bestätigten Blöcken.[289] Die Parteien könnten insoweit, bei allgemeinen Geschäftsbedingungen in den Grenzen von § 309 Nr. 13 lit. c BGB, auch eine eigene Regelung treffen.

bb) Risiko eines Fork Fraglich ist aber, wie sich die Möglichkeit sog. **Forks** auswirkt. Durch einen Fork könnte sich der Inhalt der Kette nachträglich verändern, möglicherweise eine Transaktion wieder herausfallen und erst später wieder übernommen werden. Forks sind zumindest nach einigen bestätigenden Blöcken relativ unwahrscheinlich; zudem sorgen sie in der Regel nur für eine verspätete Übernahme der Transaktion.[290] Daher wird teilweise befürwortet, schon beim Anhängen eines Blocks an die Blockchain rechtliche Relevanz zu bejahen.[291]

Tatsächlich bereitet es Schwierigkeiten, einen fixen Zeitpunkt für eine letztverbindlich gültige Kette zu definieren. Es wäre jederzeit möglich, dass ein besonders **tiefer Fork** die aktuelle Version überholt, wenn nur ausreichend Rechenkraft konzentriert wird. Angezeigt scheint eine Differenzierung im Einzelfall:

cc) Differenzierung Gelangte eine Information dergestalt in die Kette, dass der Empfänger unter normalen Umständen Kenntnis nehmen konnte und verblieb sie auch während dieser Zeit in der Kette, so ist von einem Zugang der enthaltenen Willenserklärung auszugehen.

Ist für den Empfänger hingegen ersichtlich, dass der Absender seine Erklärung an die Übernahme in den Ledger binden wollte, könnte man eine auflösende Bedingung annehmen (§ 158 Abs. 2 BGB). Das wäre insbesondere der Fall, wenn die entsprechende Transaktion **Bedingung** eines Smart Contracts ist, der daraufhin weitere Folgen auslösen soll. Nach Auslegungsgesichtspunkten müsste dabei feststehen, dass die Erklärung für den Absender ohne Verbleib in der Blockchain keinen Bestand haben soll.

---

[288] Statt vieler *Mansel*, in: Jauernig, BGB, § 130 Rn. 4.

[289] BGH, NJW 1995, 2217 (m. zust. Anm. *Armbrüster*, NJW 1996, 438); *Einsele*, in: MüKo-BGB; § 130 Rn. 12.

[290] Ein relevantes Szenario wäre allerdings das Double-Spending, dazu sogleich.

[291] *Heckelmann*, NJW 2018, 504 (506).

Werden alle **Folgen On-Chain** ausgelöst, stellt dieses Vorgehen für den Gegenüber kein Problem dar. Im Übrigen verzögern Forks eine Transaktion meist nur für kurze Zeit, da sie aus dem Pool offener Transaktionen erneut herausgegriffen und so in einem späteren Block übernommen werden.

dd) Fazit **Grundsätzlich** sollte nach allgemeinen Regeln beurteilt werden, ob der Empfänger Kenntnis nahm oder unter normalen Umständen Kenntnis hätte nehmen müssen, selbst wenn eine Transaktion (zunächst wieder) aus einer geforkten Chain entfällt. Ein besonders tiefer Fork wäre, außer in Fällen des § 158 Abs. 2 BGB, unbeachtlich.

Eine andere Frage ist es, wie lange man in der Praxis bei werthaltigen Transaktionen warten sollte, bis auf deren Endgültigkeit vertraut und ein Double-Spending möglichst ausgeschlossen werden kann.[292] Mit jedem Block wird der vorige bestätigt und ein tiefer Fork unwahrscheinlicher. Während man in großen Netzwerken wie Bitcoin in der Regel **sechs Blöcke** als ausreichend erachtet, sollten bei kleineren Netzwerken mit einer geringeren Gesamtrechenkraft deutlich mehr Bestätigungen abgewartet werden.

3. Abbildbarkeit rechtlicher Begriffe und Wertungen im Programmcode

Besondere Probleme entstehen dort, wo digitale Systeme nicht an rechtliche Wertungen angepasst werden können. Das Konzept eines selbstvollziehenden, ggf. unaufhaltbaren und unabänderlichen Vertrags führt nur dann zu sinnvollen Ergebnissen, wenn der Programmcode die Rechtslage korrekt wiedergibt. Die **korrekte Übersetzung** rechtlicher Begriffe und Wertungen erweist sich jedoch als problematisch.

a) Übersetzungsschwierigkeiten im Hinblick auf Rechtssprache, Rechtsnormen und gesetzliche Wertentscheidungen

aa) Problemstellung Ein Algorithmus bzw. ein Programm arbeitet stets strikt seine im Protokoll bzw. Code festgesetzten Arbeitsanweisungen ab. Durch ein komplexes System aus logischen Regeln (Wenn-Dann, XOR, etc.) und mathematischen Formeln wird ein Regelwerk etabliert, das keinerlei Abwägungsspielraum bietet.[293] Der die **Protokolle** bzw. **Algorithmen** definierende Code muss dabei stets eindeutig gefasst und vollständig sein, andernfalls nimmt ihn das System nicht fehlerfrei auf.[294] Es kann dadurch auch mit absoluter Sicherheit gewährleistet werden, dass ein spezifischer Input der Form X stets den Output der Form Y ergeben wird.[295] Dem System ist damit jede Ambiguität fremd; ganz anders jedoch das Rechtsystem:

[292] Im Bitcoin Netzwerk erachtet man in der Regel sechs Bestätigungen als ausreichend.
[293] *Wright/De Filippi*, S. 26.
[294] Vgl. *Szabo*, Formalizing and Securing Relationships on Public Networks, *First Monday*, Volume 2, Number 9.
[295] Beispiel etwa https://www.elinext.com/industries/financial/trends/smart-vs-ricardian-contracts/, der sich darauf fokussiert, dass Ambiguität nur dazu diene, sich aus der eigentlichen Vereinbarung herauszuwinden.

Das Recht greift auf **natürliche Sprache** zurück, die in der Regel mehrdeutig und unscharf ist.[296] Rechtsnormen enthalten grundsätzlich Wertungs- und Auslegungsspielräume, die Einzelfallgerechtigkeit ermöglichen sollen, aber einem deterministisch agierenden System nicht zugänglich sind.[297] Erst durch einen Konkretisierungsvorgang durch den Rechtsanwender wird im Rahmen methodischer Argumentation ein Auslegungsergebnis für den Einzelfall gefunden. Nicht umsonst ist die richtige Antwort auf die meisten Rechtsfragen: „Es kommt darauf an.“, nicht ein richtig und falsch – true oder false, wie es die Parameter des Codes erfordern. Schwierigkeiten bereiten insbesondere unbestimmte Rechtsbegriffe wie „angemessen“ oder „schuldhaft“ und Generalklauseln, z.B. das Gebot von Treu und Glauben (§ 242 BGB).

Die **Ambiguität** der Rechtssprache ist dabei kein Versehen, sondern ein ein bedeutendes Merkmal unseres Rechtssystems.[298] Die abstrakte Formulierung der Rechtsnormen ermöglicht eine große Bandbreite von Fällen zu erfassen und Spielraum für die Berücksichtigung der Umstände und Interessenlagen im Einzelfall zu erhalten.[299] Die in § 241 Abs. 2 BGB referenzierte Verpflichtung, Rechte und Rechtsgüter des Gegenübers zu achten, kann je nach Art des Schuldverhältnisses und der sonstigen Umstände extrem unterschiedlich ausfallen; nicht zuletzt, da auch auf die individuelle Erkennbarkeit und Zumutbarkeit von Gefahren Rücksicht genommen werden muss. Aufgrund der Unüberschaubarkeit tatsächlicher Gegebenheiten und Fallkonstellationen muss hier und auch in anderen Fällen ein Interpretationsspielraum bestehen.[300]

bb) Ausprägungen Die **allgemein gehaltenen Formulierungen** und **unbestimmten Rechtsbegriffe** können und sollen vielfältig sowie einzelfallbezogen, insbesondere unter Berücksichtigung der *ratio legis* verstanden werden.[301] Man haftet gerade nicht in strikter Weise am Wortlaut der Norm und kommt so in jedem Fall zum selben Auslegungsergebnis, sondern bezieht weitere Umstände mit ein.

Deskriptive Begriffe, die auf tatsächliche Umstände Bezug nehmen (Sache, Grundstück,...) und meist nach dem allgemeinen Sprachgebrauchs zu deuten sind, erweisen sich aufgrund ihrer teilweise abstrakten Beschreibungen bereits als problemträchtig; noch schwieriger gestaltet sich die Übersetzung **normativer Begriffe**, die eine Wertung durch den Rechtsanwender verlangen. Hierzu zählen beispielsweise der wichtige Grund für

[296] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 17; *Wright/De Filippi*, S. 25 f. Prägend hierfür auch *Szabo*, der die natürliche Sprache des Rechts als „wet code“ und die formalisierte der Software als “dry code” bezeichnete, vgl. *Szabo*, Wet code and dry, 2006, abrufbar unter: http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html.

[297] Vgl *Kaulartz/Heckmann*, CR 2016, 618 (621); *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (13). Ähnliche Schwierigkeiten ergeben sich dabei, die abstrakte Rechtssetzung in Common Law-Systemen nach dem Billigkeitsrecht (*equity*) zu erfassen, *Guggenberger*, in: Schulze/Staudenmayer/Lohsse (Hrsg.), 83 (96).

[298] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 23.

[299] *Honsell*, in: Staudinger (2013), Einleitung zum BGB, Rn. 117.

[300] *Honsell*, in: Staudinger (2013), Einleitung zum BGB, Rn. 114.

[301] *Honsell*, in: Staudinger (2013), Einleitung zum BGB, Rn. 114; *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (13).

eine außerordentliche Kündigung (§ 314 Abs. 1 BGB) oder das Merkmal des Vertretenmüssens (§ 280 Abs. 1 S. 2 BGB).[302] Insbesondere Generalklauseln, wie etwa § 242 BGB, entziehen sich einem festen Bedeutungsgehalt und können je nach Einzelfall völlig abweichende Bewertungen verlangen.[303] Hinzu kommt die Notwendigkeit der Rechtsfortbildung, um auf vom Gesetzgeber unvorhergesehene Umstände reagieren und zum Beispiel eine planwidrige Regelungslücke im Wege der Analogiebildung schließen zu können.[304]

b) Auslegung rechtsgeschäftlicher Erklärungen

aa) Auslegungsgrundsätze Die Ermittlung des rechtlich maßgeblichen Inhalts einer Willenserklärung vollzieht sich gem. §§ 133, 157 BGB. Nach dem dort enthaltenen Dogma der **objektiv-normativen Auslegung** ist grundsätzlich danach zu fragen, wie der Erklärungsempfänger das Erklärungszeichen nach Treu und Glauben mit Rücksicht auf die Verkehrssitte verstehen durfte, § 157 BGB.[305] Nur wenn die Parteien **übereinstimmend** von einem bestimmten Bedeutungsgehalt ausgehen, gilt das tatsächlich Gewollte (§ 133). Im Übrigen sind bei der Bestimmung des Empfängerhorizonts grundsätzlich sämtliche Umstände in die Deutung einzubeziehen, während sich ein starres Festhalten am Wortsinn verbietet.[306]

Selbst wenn alle Erklärungen bzw. Vertragsbedingungen in Code-Form ausgedrückt werden, führt das nicht zu einer unbedingten Geltung der Programmlogik. Ob und inwieweit der programmierte Inhalt Geltung erlangen soll, ist nicht dem Code des Smart Contract, sondern den nach Auslegungsgrundsätzen zu deutenden Willenserklärungen zu entnehmen.[307] Dogmen wie „Code is law“ haben für das Recht keine Bedeutung.

bb) Einigung auf strikten Vollzug der Programmlogik? Freilich könnten die Parteien auch **vereinbaren**, dass sie eine Vertragsbeziehung begründen wollen, deren Inhalt sich vollständig aus den codierten Programmlogiken ergibt (Formel: Code = privatautonom gesetztes Recht).

Eine solche Einigung wäre im Lichte der Vertragsfreiheit wohl grundsätzlich zulässig, jedenfalls im B2B-Bereich und soweit kein zwingendes Recht entgegensteht;[308] gleichwohl überginge eine solche **Pauschalisierung**, dass hierdurch selbst krasseste Programmierfehler rechtliche Legitimation erfahren würden.[309] Handelt es sich um ein wirtschaftlich unbedeutendes Geschäft oder ein solches, das durch einen extrem simplen Code reduziert werden kann, erscheint das Fehlerpotential noch vertretbar. Im Übrigen

[302] Vgl. *Honsell*, in: Staudinger (2013), Einleitung zum BGB, Rn. 114.
[303] *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (13).
[304] Vgl. *Säcker*, in: MüKo-BGB, Einleitung, Rn. 150 f.
[305] BGHZ 103, 275 (280) = NJW 1988, 1378; BGHZ 47, 75 (78) = NJW 1967, 673; *Singer*, in: Staudinger (2017), BGB, § 133 Rn. 18 m.w.N.
[306] *Singer*, in: Staudinger (2017), BGB, § 133 Rn. 9.
[307] *Kaulartz/Heckmann*, CR 2016, 618 (621); für das österreichische Recht ebenso *Buchleitner/Rabl*, ecolex 2017, 4 (9).
[308] Vgl. zur Zulässigkeit der Vereinbarung eines gemeinsamen Begriffsverständnisses *Singer*, in: Staudinger (2017), BGB, § 133 Rn. 45.
[309] Zum Fehlerpotential siehe bereits S. 45 ff.

aber würden die fehlende Berücksichtigung der Begleitumstände und gegenseitigen Interessenlagen sowie der nach diesem Verständnis notwendige Verzicht auf etwaige gesetzliche Schutzrechte schwere Folgen haben.

Grundsätzlich dürfte aus der **Interessenlage** der Parteien daher abzuleiten sein, dass diese zwar einen Vertrag automatisiert und unter Verzicht auf eine vertrauensstiftende Institution abwickeln wollen; hingegen nicht den Vollzug des Programmcodes unter allen Umständen. Übersahen die Parteien zum Beispiel, dass eine im Vertrag enthaltene Regelung eine Partei weitestgehend rechtlos stellt oder das Vertragsziel mit dieser verfehlt wird, so wäre nach allgemeinen Auslegungsgrundsätzen die Nichtanwendung dieser Klausel angezeigt (teleologische Auslegung).[310] Liegt eine einseitige Divergenz zwischen Gewolltem und Erklärtem vor, ist hingegen nach allgemeinen Grundsätzen an eine Anfechtung zu denken.[311]

c) Zwischenfazit

Während das Recht also einen gewissen Spielraum bei der Deutung vertraglicher Regelungen und Rechtsnormen einfordert, ist der programmierte Vertrag vollständig durch logische Regeln determiniert. Häufig wird selbst in weniger komplexen Fällen erst ein letztinstanzliches Gerichtsurteil finale Klärung herbeiführen, ohne dass diese Interpretation von allgemeiner Gültigkeit für zukünftige Prozesse wäre. Dieselbe Formulierung kann in zwei bis auf Nuancen ähnlichen oder sogar in identischen Fällen unterschiedlich interpretiert werden.[312] Soweit codierte Verträge über kein Mittel verfügen, um die hermeneutische Ausrichtung der Rechtssprache zu adaptieren, ist das sich hieraus ergebende Divergenzrisiko ein **wesentlicher Einwand** gegen ihren Einsatz zur selbstvollziehenden Umsetzung zumindest im Ansatz komplexer Sachverhalte.[313]

Bei der Betrachtung selbstvollziehender Verträge müssen so in der Regel drei Ebenen auseinandergehalten werden, die jeweils ihr eigenes Risikopotential mit sich bringen:

- Der **rechtlich maßgebliche Inhalt** der Vereinbarung der Parteien, wie er nach §§ 133, 157 BGB unter Berücksichtigung des gegenseitigen Verständnishorizonts zu ermitteln ist,
- der in natürlicher Sprache gefasste **Vertragstext**, welcher die Parteivereinbarung festhält und vom Programmierer übersetzt werden soll und
- schließlich der **Vertragscode**, der weder erweitert noch verändert werden kann und unaufhaltbar seine Befehle ausführen wird.[314]

[310] Vorbehaltlich eines expliziten Willens, vgl. *Singer*, in: Staudinger (2017), BGB, § 133 Rn. 53 f.

[311] Siehe S. 74 f.

[312] Zur Bedeutung von Gerichtsentscheidungen und Richterrecht im Zivilrechtssystem *Honsell*, in: Staudinger (2013), Einleitung zum BGB, Rn. 117.

[313] Optimistischer hingegen *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (312 ff.), der allerdings die Arbeit eines Richters auf die strikte Anwendung konditionaler Bestimmungen auf einen festgelegten Sachverhalt beschränkt.

[314] *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 18.

Die zwischen den **Ebenen** bestehenden Zusammenhänge sorgen dafür, dass Fehler auf der einen Seite auch auf die anderen durchschlagen. Missverständnisse bei der Kommunikation zwischen den Parteien und dem Programmierer sind leicht vorstellbar.

Hierdurch besteht die Gefahr, dass selbst kleinste Verständnisdefizite auf der einen Ebene trotz fehlerfreier Übersetzung der beiden anderen das Gesamtsystem zum Fallen bringen.[315] Im Hinblick auf selbstvollziehende Verträge stellt die Synchronisation der Ebenen die wohl gravierendste rechtliche Herausforderung dar.

d) Unvollständigkeit eines Vertrags und soziale Dimension

Bevor auf Gegenstrategien eingegangen wird, zeigen die folgenden Überlegungen, warum es auch aus anderen Gründen sinnvoll sein kann, auf einen vollständig automatisierten Vollzug einer Vertragsbeziehung zu verzichten.

Beachtenswert ist in diesem Zusammenhang zum einen die Untersuchung *Oliver Harts*, wonach Verträge ihrer Natur nach zumindest teilweise **unvollständig** seien und das auch so sein müsse.[316] Tatsächlich ist es bei Verträgen überhaupt nicht möglich, sämtliche Details und noch so entfernten Szenarien in einer Vertragsurkunde zu berücksichtigen. Die Vertragsfreiheit erlaubt es den Parteien, sich nicht einem festgesetzten Schema unterwerfen zu müssen, sondern ihre Rechtsbeziehung frei und dynamisch zu gestalten. Eine gewisse Unwägbarkeit und Flexibilität bilden häufig erst die Grundlage für eine langfristige, stabile Zusammenarbeit.[317] So ist es gängige Praxis, dass einzelne Klauseln im Laufe der Vertragsbeziehung modifiziert werden.[318] Offen gelassene Punkte, der stets enthaltene Wertungsspielraum zur Berücksichtigung des Vertragszwecks, aber auch die Wahrscheinlichkeit unbeabsichtigter Lücken machen es höchst unwahrscheinlich, dass es gelingt, eine Vertragsbeziehung in all ihren Dimensionen in Codeform abzubilden.[319]

Ferner darf die **soziale Dimension** der Vertragspraxis nicht außer Acht gelassen werden. Verträge sind viel mehr als eine schlichte Durchsetzungsgrundlage. Die Parteien gestalten ihr Miteinander, ihre soziale Beziehung, wobei offene Definitionen und Regelungen Raum für sich ereignende Fehler, aber auch gemeinsames Wachsen bieten und selbst Ausdruck des gegenseitigen Vertrauens sind.[320] Damit verbunden ist der Aspekt, dass zahlreiche Verträge nie vollständig durchgesetzt werden. Häufig einigen sich

[315] Eine gute Übersicht zu den sich aufdrängenden Fragen liefern auch *Clack/Bakshi/Braine*, Smart Contract Templates, S. 10 f.

[316] Theorie der „Incomplete Contracts", vgl. *Hart/Moore*, Review of Economic Studies (66), 1999, 115 ff. sowie *Hart*, Incomplete Contracts and Control, American Economic Review 107 (7), 2017, 1371 (1372 ff.).

[317] *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (5).

[318] *Clack/Bakshi/Braine*, Smart Contract Templates, S. 4.

[319] Kritisch zur Formalisierung von Vertragssprache in starrer Code-Form auch *Szabo*, A Formal Language for Analyzing Contracts, abrufbar unter: https://nakamotoinstitute.org/contract-language/.

[320] Zu den sozialen Aspekten von Vertragsbeziehungen *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (7 f.).

die Parteien anderweitig oder lassen es „auch einmal gut sein". Smart Contracts und andere automatisierte Abwicklungsinstrumente haben hingegen eine Null-Fehler-Toleranz.[321] Der sofortige und strikte Vollzug lässt das vorige Entscheidungsmoment und damit die Chance, von der Durchsetzung abzusehen, entfallen.[322]

e) Folgen für die Parteien und Strategien zur Divergenzvermeidung

Nach alledem muss daher sorgfältig abgewogen werden, welche Bestandteile einer Vertragsbeziehung selbstvollziehend durch ein Programm durchgesetzt werden können und sollen. Völlig unproblematische Fälle dürfte es kaum geben. Stets könnte eine Eventualität eintreten, die das Konzept des selbstvollziehenden Vertrags an seine Grenzen bringt. Die Frage muss daher sein, wie es gelingen kann, die Risiken derart zu minimieren, dass die Vorteile der Automatisierung überwiegen.

aa) Limitierung des Übersetzungsgegenstands Der Übersetzungsgegenstand sollte zunächst auf eine **Konkretisierung einer Vertragsbeziehung** bzw. den Ausschnitt eines Business-Prozesses limitiert werden. Wie bereits im Rahmen der technischen Divergenzrisiken zeigt sich auch hier, dass es sinnvoller ist, sich nur einen strukturierten Teil einer Rechtsbeziehung zur Automatisierung herauszugreifen.

Dabei sollte sich der relevante Aspekt der Vertragsbeziehung auf ein **formales und logisches Muster** aus Bedingungen und Folgen herunterbrechen lassen.[323] Die Tatbestandsvoraussetzungen sollten dabei möglichst eindeutig definiert und frei von Wertungsspielräumen sein.[324] Von vornherein ausscheiden müssen alle normativen Kriterien, es sei denn, man lagert deren Auslegung an gesonderte Programme oder Dienstleister aus.[325]

Da die möglichen Inputs und Outputs bereits beim Schreiben des Codes bekannt sein sollten, können diese im Vertrag referenziert und eindeutig beschrieben werden. Eine **eindeutige Bezugnahme** z.B. auf Produktmerkmale beugt Missverständnissen oder Auslegungsstreitigkeiten vor.[326] Insoweit kann die durch Verknüpfung von Vertrag und Code bewirkte Rechtsformalisierung auch als Chance zur Streitvermeidung begriffen werden.

bb) Vertragsform und zusätzliche Inhalte Weiterhin sollte nicht auf eine außerhalb des Codes gefasste **vertragliche Einigung** verzichtet werden. Diese sollte möglichst präzise beschreiben, welcher Aspekt der Vertragsbeziehung auf welche Weise vom Programm umgesetzt werden soll.

[321] *Wright/De Filippi*, S. 25.
[322] *Wright/De Filippi*, S. 26.
[323] Vgl. *Szabo*, First Monday, Volume 2, Number 9 (1997).
[324] *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (13).
[325] Vgl. *Mik*, Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 16.
[326] So kann durch das Erfordernis der präzisen Zuordnung im Code etwa vermieden werden, dass die Parteien ähnlich benannte Produkte, Dienstleister, etc. verwechseln, vgl. *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (324).

Idealerweise ist die Beschreibung so passgenau, dass nur von einem übereinstimmenden Verständnis und damit nur einer entsprechenden Auslegung (§ 133 BGB) ausgegangen werden kann.

Für den Fall von **Programmier-** oder **Übersetzungsfehlern** oder -lücken erscheint eine eindeutige Regelung sinnvoll. Andernfalls überließe man die Folgen den Unwägbarkeiten der ergänzenden Vertragsauslegung.[327]

Immer dann, wenn der Code an seine Grenzen stößt oder dem übereinstimmenden Parteiwillen zuwiderläuft, ist das Recht als Mediator und Korrektiv gefragt. Für die **gerichtliche Klärung** ist daher auch hier zu betonen, dass die Kenntnis der Identität des Vertragspartners ein entscheidender Vorteil ist.

cc) Fokus auf Vertragsgestaltung Im Übrigen sollte der Fokus auf der **Vertragsgestaltung** liegen. Hier muss versucht werden, durch privatautonome Gestaltung die Rechtslage weitestgehend mit der beabsichtigten Funktionsweise des Smart Contract zu **synchronisieren**.[328] Es sollte sich daher möglichst sich um ein Regelungsgebiet handeln, auf dem eine möglichst große Vertragsfreiheit herrscht. In strenger regulierten Bereichen ist eine Automatisierung gleichwohl denkbar, solange das Regelungskorsett eine formale Beschreibung erlaubt.

Dabei liegt es auf der Hand, sowohl Programmierer als auch Juristen an der Entwicklung von Smart Contracts zu beteiligen, um den tatsächlich durch den Code erfüllbaren Vertragsteil zu validieren und andererseits Divergenzen zwischen Vertrag bzw. geschriebenem Recht und durch den Code geschaffenen Tatsachen zu vermeiden.

Rechtliche Tatbestandsmerkmale und rechtserhebliche Tatsachen wie auch sonstige bedingungsrelevante Umstände müssen möglichst präzise erfasst und beschrieben werden.[329] Es dürfte dabei nicht nötig sein, jede noch so kleine Eventualität mit einzubeziehen. Entfernte Szenarien mit überschaubaren und wirtschaftlich vertretbaren Risiken können auch außen vorgelassen werden. Generalklauseln wie etwa § 242 BGB lassen sich ohnehin nicht abbedingen.[330]

Auf diesem Wege unberücksichtigt gelassenen Rechtsnormen liegen gleichwohl häufig spezifische Schutzfunktionen zugrunde, sodass ein Abbedingen gut überlegt sein will.

dd) Beispiel für einen unproblematischen Fall Ein häufig genannter, angeblich **unproblematischer** Fall sind **Derivate**. Hierbei könnte die Kurswette ohne Einschaltung einer Bank automatisiert vollzogen werden, indem eine Schnittstelle zur Börse die entsprechenden Daten liefert und die entsprechenden Beträge freigegeben werden.[331]

---

[327] Vgl. zur ergänzenden Vertragsauslegung *Busche*, in: MüKo-BGB, § 157 Rn. 26 ff.

[328] *Clack*, Smart Contract Templates III, S. 2.

[329] *Clack/Bakshi/Braine*, Smart Contract Templates, S. 10.

[330] *Jacobs/Lange-Hausstein*, ITRB 2017, 10 (13).

[331] So *Kaulartz/Heckmann*, CR 2016, 618 (619). Hinzugefügt werden müssten ferner ein Basiswert, eine Knock-Out-Schwelle und eine Laufzeit. Vgl. auch *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (337).

ee) Alleinige Bezugnahme auf Rechtszustände und Rechtszuweisungen Alternativ bliebe die Möglichkeit, in dem Ledger überhaupt keine schuldrechtlichen Vereinbarungen abzubilden, sondern allein **Rechtszustände** und **Rechtszuweisungen**. Eigentums- oder Pfandrechte, Inhaberschaften, usw. lassen sich einfach formal beschreiben und hängen nicht in gleichem Maße von Auslegungs- und Wertungsfragen ab, wie die dazugehörigen Kausalgeschäfte. Das Trennungsprinzip des deutschen Rechtssystems bringt zudem den Vorteil mit sich, dass Fehler beim Kausalgeschäft (in der Regel) keine unmittelbare Auswirkung auf die dingliche Rechtslage haben. Eine rückwirkende Korrektur des Ledger wäre nicht nötig; man kann vielmehr die Registerlage hin zur wahren Rechtslage fortschreiben. Entsprechend könnten die Parteien bei Uneinigkeiten vor Gericht über die Rechtslage streiten und dabei die Zustimmung zur Anpassung des Ledger zum Streitgegenstand erheben. Mit der vertraglichen Regelung verständigen sich die Netzwerkteilnehmer auf bestimmte Abläufe und Rechtszuweisungen, wodurch mit dem Ledger ein eigener Mikrokosmos geschaffen wird, in welchem die eigentlich schuldrechtlichen Verbindungen gegenüber dem anderen Teilnehmer absolute Wirkung entfalten.

f) Mögliche Entwicklungen

Teilweise wird davon ausgegangen, dass es gegenwärtig keinen Weg gibt, eine hinreichende Übereinstimmung von „rechtlicher Sprache“ und „technischer Sprache“ (Computercode) herbeizuführen bzw. ein gemeinsames Verständnis von Programmierern und Rechtspraktikern herzustellen, da es an einer vermittelnden Kommunikationsterminologie oder Logik fehle.[332]

Verschiedene Projekte untersuchen indes, inwiefern rechtliche Wertungen in einer **formalisierten Sprache** abgebildet werden können (Frage der sog. denotationellen Semantik).[333] Einige versuchen eine neue (Programmier-)Sprache zu entwickeln, die rechtliche Begriffe in ihrer Mehrdeutigkeit abzubilden und so einen technischen Wertungsspielraum zu schaffen vermag.[334] Maschinelles Lernen könnte hierbei eine große Rolle spielen, indem die Bedeutung bestimmter Formulierungen anhand eines umfangreichen Datenabgleichs ermittelt wird. Bis dato sind solche Entwicklungen und Modelle jedoch nicht ausgereift und die getesteten Verfahren mit zu vielen Fehlern behaftet.[335] Verlässliche Aussagen zu zukünftigen Strategien können daher noch nicht getroffen werden.

Dennoch muss man sich fragen, inwieweit eine neue Sprache bei der Übersetzung zwischen Programmiersprache und natürlicher Sprache überhaupt den Anforderungen gerecht werden kann. Mehrdeutigkeit und Unschärfe juristischer Regelungen sind entscheidend für die bisherige Flexibilität und Dynamik unseres Rechtssystems. Versuche, einen möglichst hohen Formalisierungsgrad zu erreichen, um maschinenlesbare und -analysierbare Verträ-

[332] *Al Khalil et al.*, 2017, S. 8.

[333] Etwa das Accord Projetc (https://docs.accordproject.org/) oder die Ansätze von Legalese, https://legalese.com/.

[334] Vgl. zur Idee einer sog. „Symbolic Discourse Language“ anstelle von natürlicher Sprache, *Wolfram*, Computational Law, Symbolic Discourse and the AI Constitution.

[335] Die nötigen Entwicklungsschritte beschreiben *Clack/Bakshi/Braine*, Smart Contract Templates, S. 11 f.

ge zu schaffen, mögen in einigen Fällen zu sinnvollen Ergebnissen führen, sind jedoch als Patentlösung für ein völlig verändertes Rechtsverständnis in Frage zu stellen. Selbst wenn sich Sachverhalte formal darstellen lassen, entbindet dies nicht davon, weiter eine Ausdifferenzierung, Wertung und Auslegung rechtlicher Normen vorzunehmen und den Umständen des Einzelfalls Rechnung zu tragen.[336]

4. Anpassungsfähigkeit digitaler Systeme an zwingendes Recht

Besonderes Potential für Divergenzen weisen **zwingende Rechtsnormen** auf. Hier kann nicht einfach durch Vertragsgestaltung versucht werden, das Recht der Funktionslogik des Ledger zu unterwerfen. Vielmehr muss sich der Ledger in diesen Fällen dem Recht beugen.

a) Verbraucherschutzinstrumente

In zahlreichen Rechtsmaterien finden sich besondere **Schutzinstrumente** zugunsten von **Verbrauchern**, die in der Regel einseitig zwingend ausgestaltet sind (vgl. §§ 312k Abs. 1, 476, 512 S. 1 BGB). Es kann somit nicht verhindert werden, dass ein Smart Contract etwa wegen der Ausübung eines verbraucherschützenden Widerrufsrechts (vgl. §§ 312 ff., 355 ff. BGB) anzuhalten ist bzw. Formvorschriften Anpassungen nötig werden lassen (vgl. § 494 Abs. 2 BGB).

Dies muss bei der Konstruktion bedacht und evaluiert werden, ob sich der jeweilige Anwendungsfall hinreichend verlässlich durch das technische System selbstvollziehend abwickeln lässt.

Die Beteiligung von Verbrauchern bereitet aber noch aus einem anderen Grund Schwierigkeiten: Während im unternehmerischen und erst recht im kaufmännischen Geschäftsverkehr Rechtsbeziehungen weitgehend frei gestaltet werden können, bestehen bei Verträgen zwischen Unternehmen und Verbrauchern erhebliche **Einschränkungen** der **Vertragsgestaltungsfreiheit**, die häufig auch unionsrechtlich determiniertet sind.[337] Das sonst flexible Recht kann nur eingeschränkt angepasst werden, während zahlreiche zwingende Rechtsvorschriften sowie Informations-, Widerrufsrechte, etc. die Gestaltung eines rechtskonformen technischen Abwicklungssystems erschweren. Besonders deutlich wird dies im AGB-Recht: Gemäß § 310 Abs. 1 S. 1 BGB findet eine vollständige Inhaltskontrolle nur zugunsten von Verbrauchern statt; zwischen Kaufleuten ist zudem auf die im Handelsverkehr geltenden Gewohnheiten und Gebräuche angemessen Rücksicht zu nehmen (Satz 2 2. Halbsatz). In Verbindung mit den zahlreichen Formvorschriften, Informations- sowie Belehrungspflichten erweist sich die Beteiligung eines Verbrauchers daher in der Regel als potentiell problematisch.

[336] Eine kritische Auseinandersetzung mit einigen Ansätzen findet sich bei *Funk*, S. 239 ff.

[337] Vgl. *Emmerich*, in: MüKo-BGB, § 311 Rn. 4; *Olzen/Looschelders*, in: Staudinger (2015), BGB, § 242 Rn. 456 ff.

Möchte man sicherstellen, dass das Recht auch tatsächlich der Funktionsweise des DL-Systems folgt und nicht höherrangige Schutzzwecke eine privatautonome Regelung überstimmen, sollte der Teilnehmerkreis möglichst auf kaufmännische Beteiligte begrenzt werden.

b) Berücksichtigung gesetzlicher Verbote

Gesetzliche Verbote können sich in zweierlei Hinsicht problematisch auf selbstvollziehende Verträge auswirken:

Einerseits sind Rechtsgeschäfte, die gegen ein solches Verbot verstoßen, gemäß § 134 BGB **nichtig**, soweit sich aus dem Verbotsgesetz nichts anderes ergibt.[338] Eine getroffene und mittels eines selbstvollziehenden Vertrags durchgesetzte Verpflichtung könnte damit ihre Grundlage verlieren, falls das Rechtsgeschäft etwa gegen ein Strafgesetz verstößt. Zudem besteht die Gefahr, dass der Abwicklungsmechanismus die Gesetzesverletzung perpetuiert. Bei der Ausarbeitung des Smart Contract bzw. dem Entwurf des Vertrags müssen etwaige entgegenstehende Rechtsvorschriften daher beachtet werden, was jedoch aufgrund der Auslegungsbedürftigkeit und Einzelfallabhängigkeit Schwierigkeiten mit sich bringt.[339]

Die zweite Dimension ist Blockchain-spezifischer Natur: Eine Studie von *Mazutt* et. al. zeigte bereits die Gefahr auf, dass **strafrechtlich relevante Inhalte** selbst auf einer limitierten Blockchain wie der Bitcoin-Chain hinterlegt werden können.[340] Viel diskutiert wird dabei eine Strafbarkeit wegen des Besitzes kinderpornographischer Schriften gem. § 184b Abs. 3 2. Alt. StGB. Dies erweist sich insbesondere für Full-Node-Betreibern als problematisch, da diese stets die vollständige Kette abspeichern und verifizieren.[341] Um eine Strafbarkeit auf Fälle positiver Kenntnis beschränken zu können, wird teilweise die Heranziehung der Privilegierungsvorschrift für Host-Provider nach § 10 S. 1 TMG gefordert.[342] Eine vergleichbare Interessenlage liegt aber nur bei fremden, also nicht vom Betreiber des Node selbst stammenden Informationen vor.[343]

Doch selbst dann besteht gem. § 10 S. 2 TMG eine Löschungspflicht, sobald der Betreiber Kenntnis von den Inhalten erlangt. Ein Alleingang löst dabei das Problem nur bedingt: Die übrigen Teilnehmer würden weiterhin der Originalkette folgen und damit weiter den strafrechtlich relevanten Inhalt verbreiten; der belangte Node wäre wiederum faktisch zum Ausscheiden aus dem Netzwerk gezwungen, da er mit seiner abweichenden Kette nicht mehr als legitimer Teilnehmer betrachtet werden würde. Wenn nach und nach immer mehr Nodes dem Beispiel folgen würden, könnte das zu einem schrittweisen Ausfall des Integritäts- und Sicherheitsversprechen der Blockchain führen, da in dem verkleinerten Netzwerk 51-Prozenz-Attacken leich-

[338] Vgl. zu den Kriterien *Mansel*, in: Jauernig, BGB, § 134 Rn. 14.
[339] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Schrey/Thalhofer*, NJW 2017, 1431 (1435 f.).
[340] Vgl. den Möglichkeiten, derartige Inhalte auf einer Blockchain zu hinterlegen *Matzutt* et. al, A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin.
[341] Vgl. *Beaucamp/Henningsen/Florian*, MMR 2018, 498 (503).
[342] Dafür *Beaucamp/Henningsen/Florian*, MMR 2018, 498 (504 f.).
[343] Auch insgesamt zur Einordnung der Blockchain im Lichte des TMG *Saive*, CR 2018, 186 (191).

ter umzusetzen wären.[344] Abhilfe schaffen würde nur ein gemeinsames Vorgehen aller Teilnehmer mit einem sog. Hard Fork. Wie man das Netzwerk entsprechen koordinieren oder durch andere technische Lösungsansätze das Problem von vorneherein vermeiden kann, ist offen. Dabei könnten auch urheberrechtliche Normen entsprechende Löschungsverpflichtungen formulieren. Einige Autoren fordern mit Rücksicht auf die Situation der Full-Nodes-Betreiber eine Anpassung des TMG, zumindest im Hinblick auf die Privilegierungsvorschrift.[345] Eine solche muss jedoch sorgfältig mit den Schutzwecken der strafrechtlichen Normen abgewogen werden und entbindet die Entwickler nicht davon, technische Lösungen zu implementieren.

c) Sittenwidrigkeit

Im Falle des Nichtigkeitsdogmas für **sittenwidrige Rechtsgeschäfte** des § 138 Abs. 1 BGB treffen die zuvor besprochenen Auslegungsschwierigkeiten bei **Generalklauseln** mit den Folgen von Strafgesetzen zusammen. Da allerdings grundsätzlich nur bei besonders schwerwiegenden Umständen von einer Sittenwidrigkeit auszugehen ist, dürften sich entsprechende Konsequenzen noch eher vermeiden lassen. Gleichwohl wäre ein sittenwidriges Vollzugssystem, das nicht einfach aufgehalten oder rückgängig gemacht werden kann, in rechtspraktischer Hinsicht problematisch.

d) Minderjährigenschutz

Rechtsgeschäfte eines **Minderjährigen** können im Falle seiner Geschäftsunfähigkeit bereits nichtig sein (§ 105 Abs. 1 BGB); im Übrigen ist grundsätzlich die Zustimmung der gesetzlichen Vertreter erforderlich (§§ 2, 106, 107, 108 BGB). Eine (schwebende) Unwirksamkeit kann jedoch von einem Smart Contract bzw. der Blockchain nur schwer berücksichtigt werden. Für bedeutsamere Transaktionen könnte deshalb mit der ohnehin ratsamen Identifikation auch eine Altersverifikation von Vorteil sein.[346] Soll der Ledger einen verlässliches Abbild der Rechtslage ergeben, erweist sich ein unerkannter Minderjähriger (ebenso wie ein unerkannt Geisteskranker) als fatal. Die Entwicklungen auf dem Gebiet digitaler Identitäten könnten jedoch zumindest im Hinblick auf das Alter eine verlässliche Infrastruktur liefern.

Ein Blick auf den Online-Handel zeigt jedoch, wie in der Praxis häufig auf einen Altersnachweis verzichtet wird. Zu Effizienzzwecken wird die Angabe des Alters ohne Überprüfung hingenommen. Wer keine Vorkehrungen zur Altersverifikation treffen möchte, sollte zumindest darauf achten, in später offenbar werdenden Fällen die geschaffenen Tatsachen auch korrigieren zu können. Erneut wird deutlich, wie wichtig Schnittstellen zur Korrektur von Registerlagen in einem Distributed-Ledger sind.

---

[344] *Beaucamp/Henningsen/Florian*, MMR 2018, 498 (505). Vgl. vertiefend die Ausführungen zum Datenschutzrecht S. 94 ff.

[345] Vgl. *Beaucamp/Henningsen/Florian*, MMR 2018, 498 (507).

[346] Vgl. *Schrey/Thalhofer*, NJW 2017, 1431 (1436).

e) Gesetzliche Formvorgaben

Wollen die Parteien die rechtsgeschäftlichen Erklärungen alleine durch Transaktionen im digitalen Register und dessen Einträgen ausdrücken, könnte dies zum Konflikt mit **gesetzlichen Formvorschriften** führen.[347] Der Textform (§ 126b BGB) unterliegende Rechtsgeschäfte können noch ohne weiteres ausschließlich in einer Blockchain ausgedrückt werden, da diese die Daten auf einem bzw. hier mehreren dauerhaften Datenträgern speichert. Strengere Formvorgaben wie die Schriftform oder notarielle Beurkundung erweisen sich hingegen als problematisch.[348] Ein Rechtsgeschäft, das die gesetzliche Form nicht einhält, ist gem. § 125 S. 1 BGB nichtig. In den meisten Fällen wird man daher die notwendigen Erklärungen außerhalb der Blockchain abschließen müssen. De lege ferenda könnte die Signatur einer Transaktion mit einer nachgewiesenen ID als qualifizierte Signatur anerkannt und der Schriftform gleichgestellt werden (§ 126a BGB).

Im Rahmen der Privatautonomie ist es freilich möglich, die Eintragung einer Information in eine bestimmte Blockchain materiell-rechtlich als gewillkürte Form zu vereinbaren (§ 125 S. 2 BGB).[349]

f) Berücksichtigung von Nichtigkeitsfolgen und Rückabwicklungsfragen

Neben den bereits genannten **Nichtigkeitsgründen** ist insbesondere die Anfechtung (§ 142 BGB) zu nennen. Betreffen die Folgen das Verpflichtungsgeschäft, ist in der Regel an eine Kondiktion zu denken. Dabei stellt sich die Frage, ob und wie die „unabänderliche" Blockchain darauf reagieren kann. Das gleiche gilt auch für das **Rechtsfolgenregime** von Rücktritt (§§ 346 ff. BGB) und Widerruf (§§ 357 ff. BGB).

Ein wesentlicher Vorzug der Blockchain-Technologie ist die **Unveränderlichkeit** des Registers. Hieraus scheint sich teilweise das Missverständnis entwickelt zu haben, Smart Contracts bzw. über eine Blockchain abgewickelte Transaktionen könnten nicht rückabgewickelt werden.[350] Dies ist aus folgenden Gründen falsch:

Zum einen betrifft die Unveränderbarkeit nicht das Recht: Die Blockchain selbst protokolliert nur Ereignisse und Tatsachen; deren rechtliche Wertung findet hingegen auf einer anderen Ebene statt. Ist der Ledger also – von Anfang an oder erst durch nachträgliche Erklärung – unrichtig, so ist die Korrektur eine Tatsachenfrage, nicht anders als bei anderen Registern auch.[351] Die Verantwortung dafür leitet sich aus dem jeweiligen Rechtsgrund ab. Erlangte Positionen sind grundsätzlich zurückzugewähren (§§ 812 ff. BGB oder §§ 346 ff. BGB bzw. §§ 357 ff. BGB).

---

[347] *Heckelmann*, NJW 2018, 504 (507).
[348] *Heckelmann*, NJW 2018, 504 (507); *Paulus/Matzke*, ZfPW 2018, 431 (457).
[349] *Paulus/Matzke*, ZfPW 2018, 431 (458)
[350] In diese Richtung *Schrey/Thalhofer*, NJW 2017, 1431 (1435 f.)
[351] *Heckelmann*, NJW 2018, 504 (507); *Buchleitner/Rabl*, ecolex 2017, 4 (10).

Zum anderen bedeutet Unveränderbarkeit in diesem Sinne eher Manipulationssicherheit: Die Technologie verhindert lediglich Eingriffe in abgeschlossene Transaktionen. Eine Transaktion kann so zwar (ohne besondere Vorkehrung) nicht nachträglich gelöscht werden, es bleibt jedoch die Möglichkeit, mit einer **neuen Transaktion** ein Spiegelbild der wahren Rechtslage herzustellen (sog. ***Reverse Transactions***).[352] Nach der Anfechtung eines Geschäfts können beispielsweise gesendete Coins einfach zurücktransferiert werden. Der Rücktransfer kann dabei den Grund der Rückabwicklung transparent machen. Als problematisch erweisen sich alleine Löschungspflichten oder die Notwendigkeit nachträglicher Anpassungen des Codes. Das kommt im klassischen Fall einer Rückabwicklung jedoch kaum vor. Selbst für den Fall der Unmöglichkeit (§ 275 Abs. 1 BGB) hält das Recht entsprechende Regelungen bereit, welche dann eine Rückabwicklung nach anderen Maßstäben vollziehen (etwa § 812 Abs. 2 BGB). Allgemeine Fragen der Rechtsdurchsetzung, wie insbesondere die Kenntnis der Identität des Vertragspartners, stehen auf einem anderen Blatt.

g) Recht der allgemeinen Geschäftsbedingungen

Sollte sich die Entwicklung von Smart Contracts und selbstvollziehenden Verträgen durchsetzen, werden sich insbesondere Muster als besonders ökonomisch erweisen. Bei diesen **Musterverträgen** wirft jedoch das Recht der **allgemeinen Geschäftsbedingungen** (§§ 305 ff. BGB) zahlreiche Fragen auf.

aa) Vorliegen von AGB In der Regel handelt es sich bei dem Code eines Smart Contracts, der als vorgefertigtes Programm eingebunden wurde, um **vorformulierte Bedingungen**. Sieht man bereits den Code als Vertrag oder wird dem Muster ein korrespondierender Vertragstext beigefügt, handelt es sich um vorformulierte Vertragsbedingungen iSv. § 305 Abs. 1 BGB.[353]

Ob jedoch eine Kontrolle nach den §§ 305 ff. BGB erfolgt, hängt davon ab, ob ein **Verwender** auszumachen ist. Gemäß § 305 Abs. 1 BGB müssen die Bedingungen von einer Seite „**gestellt**“ werden.[354] Hierunter ist ein einseitiges Auferlegen der Klauseln bereitstellen in Verbindung damit, dass zu erkennen gegeben wird, diese nicht ernsthaft zur Disposition zu stellen.[355] Nicht erfasst ist hingegen das Unterbreiten einer Vorlage auf gegenseitige Vereinbarung hin.[356] Noch unproblematisch kann der Partei, die den Vertrag selbst in der Blockchain hinterlegt oder ihn sonst eingebracht hat, dies als SStellenßugerechnet werden. Schwieriger wird es, sollten die Transaktionskonditionen bereits vom Netzwerk bzw. einer Plattform vorgegeben sein, auf die sich die Parteien mit der Nutzung des Smart Contract einlassen. Hier dürfte ein SStellenßu verneinen sein.[357] Die Bedingungen wür-

[352] Vgl. *Schrey/Thalhofer*, NJW 2017, 1431 (1436).
[353] *Kaulartz/Heckmann*, CR 2016, 618 (622).
[354] Es handelt sich um eine Zurechnungsfrage, vgl. *Basedow*, in: MüKo-BGB, § 305 Rn. 21.
[355] BGH, Urt. v. 20.3.2013, VII ZR 248/13
[356] Vgl. nur BGH, Urt. v. 17.2.2010 - VIII ZR 67/09 = NJW 2010, 1131.
[357] *Heckelmann*, NJW 2018, 504 (507).

den dann nach allgemeinen Grundsätzen Wirksamkeit entfalten.[358] Das gilt auch, wenn die Nutzer gemeinsam einen individuellen Vertragstext erstellen und sich dabei auf vom System gesetzte Auswahlmöglichkeiten verlassen.[359]

Bei Verträgen zwischen einem Unternehmer und einem Verbraucher ist hingegen stets von einem SStellen"durh den Unternehmer auszugehen, da die **Fiktion** des § 310 Abs. 3 Nr. 1 BGB Anwendung findet.

bb) Einbeziehung, insb. Sprachregelungen Die wirksame **Einbeziehung** der AGB in den Vertrag setzt grundsätzlich die Einhaltung von § 305 Abs. 2 BGB voraus. Fraglich erscheint insbesondere, ob allgemeine Geschäftsbedingungen, die ausschließlich in Form von Programmcode übermittelt werden, Vertragsbestandteil werden können.

Grundsätzlich stellt § 305 Abs. 2 Nr. 2 BGB die Anforderung auf, dass sich der Vertragspartner vom Inhalt der AGB in zumutbarer Weise Kenntnis verschaffen können muss. Ist er der Programmiersprache nicht mächtig, wovon bei Verbrauchern in der Regel auszugehen ist,[360] so erscheint die Übermittlung des Codes nicht als ausreichend.[361] Der Inhalt wäre dann dem Verbraucher in der jeweiligen Verhandlungssprache zugänglich zu machen.[362]

Teilweise wird eine Ähnlichkeit von Smart Contracts zu Formularverträgen behauptet, weshalb die Sprachfrage allein in den Grenzen von § 305c Abs. 2 BGB und § 307 Abs. 1 BGB zu prüfen sei.[363] Bei einem sog. Formularvertrag sind alle wesentliche Vertragsregelungen im vorformulierten Regelwerk enthalten, während in der klassischen AGB-Konstellation ein individueller Vertrag durch in Code gefasste Nebenbestimmungen ergänzt wird. Die generell für Formularverträge anerkannte[364] Ausnahme rechtfertigt sich nur dadurch, dass bei diesen Hauptvertrag und vorformulierte Nebenabreden in einem einheitlichen Dokument gefasst und ein gesonderter Hinweis (Nr. 1) bzw. die Verschaffung der Kenntnisnahmemöglichkeit (Nr. 2) aufgrund der einheitlichen Darstellung obsolet sind.[365] Die Situation bei Smart Contracts liegt insofern anders, als dass es nicht um einen gesonderten Hinweis, sondern um die Verständlichkeit des Vertrags als solchen geht. Die eigentliche rechtsgeschäftliche Einigung wird aber aufgrund der Verständnisdefizite nicht am Quellcode, sondern der Kommunikation der Parteien und den übrigen Umständen festzumachen sein. Wenn diese und ggf. auch die sonstige Kontaktaufnahme bzw. Darstellung des Rechtsgeschäfts in natürlicher Sprache erfolgen, muss auch der Vertragstext in dieser Form übermittelt werden.

---

[358] Ausnahmen wären nur einschlägig, wenn die eine Seite üblicherweise nur zu den jeweiligen Bedingungen kontrahiert oder eine entsprechende Marktmacht hat, sodass der Gegenseite letztlich keine andere Wahl verblieb, *Basedow*, in: MüKo-BGB, § 305 Rn. 25.

[359] *Heckelmann*, NJW 2018, 504 (507).

[360] Vgl. *Kaulartz/Heckmann*, CR 2016, 618 (622).

[361] *Söbbing*, ITRB 2018, 43 (46).

[362] *Kaulartz*, InTeR 2016, 202 (205). Vgl. allgemein *Wurmnest*, in: MüKo-BGB, § 307 Rn. 251.

[363] *Kaulartz*, InTeR 2016, 202 (206); ähnlich im Hinblick auf das Transparenzgebot *Heckmann/Schmid*, S. 27 f.

[364] Vgl. nur *Basedow*, in: MüKo-BGB, § 305 Rn. 72.

[365] *Basedow*, in: MüKo-BGB, § 305 Rn. 65.

Etwas anderes würde nur gelten, wenn bereits eine zulässige[366] privatautonome **Einigung** darauf stattgefunden hat, dass der jeweilige Code die Rechtsbeziehung vollständig abbilden solle. Erfolgt Vertragsschluss selbst in einer bestimmten Sprache und kann diese als Vertragssprache angesehen werden, ist grundsätzlich auch die Übersendung der AGB als zumutbar erachtet.[367] Im Hinblick auf den Schutzbedarf des Verbrauchers scheint in solchen Fällen jedoch Zurückhaltung geboten.

cc) Inhaltsschranken Wie bereits hervorgehoben, ist es grundsätzlich zu empfehlen, eine möglichst intensive Synchronisation der Rechtslage mit der Logik des Ledgers anzustreben. Etwaige Versuche, beispielsweise potentielle Gestaltungsrechte einer Partei einzuschränken, könnten jedoch häufig mit den besonderen **Inhaltsschranken** kollidieren.[368] Beispielhaft genannt seien Ausschlüsse mangelbedingter Rücktrittsrechte (§ 309 Nr. 8 BGB) oder Beschränkungen von Zurückbehaltungsrechten (§ 309 Nr. 2 BGB). Werden Zahlungen abgewickelt, führt die garantierte Leistungsausführung zwar zu einem faktischen Verlust des Zurückbehaltungsrechts; allerdings liegt hierin wertungsmäßig eine Vorleistung, die nicht von § 309 Nr. 2 BGB sondern allenfalls im Einzelfall von § 307 Abs. 1 BGB erfasst sein soll.[369]

Unwirksame Klauseln führen zu fehlerhaften Vollzugshandlungen. Um jede Kollision zu vermeiden, müsste das System von vorneherein in jeder Hinsicht AGB-rechtskonform ausgestaltet werden. Insbesondere im Hinblick auf die Generalklausel (§ 307 BGB) dürfte es sich als schwierig erweisen, alle denkbaren Varianten angemessen zu berücksichtigen.[370] Hieran zeigen sich erneut die Vorteile, hält man den einem selbstvollziehenden System überlassenen Anteil des Vertrags möglichst gering.

h) Umgang mit teilnichtigen Verträgen

Erweisen sich einzelne Klauseln des Vertrags, etwa gem. § 134 Abs. 1 BGB, als unwirksam, richtet sich die Wirksamkeit des übrigen Vertrags nach dem Parteiwillen (vgl. § 139 Abs. 1 BGB). Im Falle von AGB berührt die Unwirksamkeit einzelner Bestimmungen die Wirksamkeit des Vertrags nicht, § 306 Abs. 1 BGB.[371] Im Hinblick auf Smart Contracts sollte nicht nur an einen technischen Mechanismus zur nachträglichen Anpassung des Codes gedacht werden. Es dürfte darüber hinaus auch sinnvoll sein, bereits *ex ante* bestimmte modifizierbare Vertragsinhalte, etwa Fälligkeiten, vorzusehen, um späterem Streit vorzubeugen und sich gegenseitig zur Anpassung zu verpflichten.[372] Ein solches Bedürfnis kann bereits bei geänderter höchstrichterlicher Rechtsprechung entstehen.[373]

[366] Siehe zuvor S. 53 f.
[367] *Schlosser*, in: Staudinger (2013), BGB, § 305 Rn. 141.
[368] *Schrey/Thalhofer*, NJW 2017, 1431 (1436).
[369] Vgl. ausführlich Fraunhofer FIT, S. 116 ff.
[370] Vgl. auch *Schrey/Thalhofer*, NJW 2017, 1431 (1436).
[371] Vgl. auch *Basedow*, in: MüKo-BGB, § 306 Rn. 11.
[372] *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (327).
[373] Für das US-amerikanische Recht *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (328).

5. Anfechtung bei selbstvollziehenden Verträgen

a) Zusammenspiel mit Auslegungsfragen

Die Grundsätze zur **Anfechtung** finden wie auch sonst Anwendung, wobei ein enger Zusammenhang mit den bereits besprochenen Auslegungsfragen besteht.

Sollten die Parteien etwa übereinstimmend den Vertragsgegenstand falsch bezeichnen, zum Beispiel ein Grafikkartenmodell mit der Modellnummer eines Arbeitsspeichers, so liegt nach § 133 BGB eine Einigung über den Vertragsgegenstand Grafikkarte vor, soweit dieses bestimmbar ist (falsa demonstratio non nocet). Gleichwohl könnte die falsche Modellbezeichnung in den Smart Contract aufgenommen worden sein. Sollte sich, wovon grundsätzlich auszugehen ist, ein Bindungswille der Parteien ergeben, wäre ein wirksamer Vertrag zustande gekommen, von dem der Smart Contract abweicht.[374] Unterliegt nur eine Partei dem (Inhalts-)Irrtum, wäre sie nach § 119 Abs. 1 BGB anfechtungsberechtigt und könnte durch nachträgliche Gestaltungserklärung (§ 142 Abs. 1 BGB) die Rechtslage rückwirkend umgestalten.

Grundsätzlich ist die rechtsgeschäftliche Einigung dabei zwar mit Rücksicht auf den Programmcode auszulegen. Eine größere Bedeutung kommt aber, schon alleine aufgrund des teilweise fehlendem Verständnisses der Programmiersprache, dem durch die sonstigen Handlungen und Umstände zum Ausdruck kommenden Parteiwillen zu.[375]

b) Grundsätze

Ein nach § 119 Abs. 1 BGB zur Anfechtung berechtigender **Irrtum** liegt nur dann vor, wenn der jeweilige Umstand auch Niederschlag in der rechtsverbindlichen Erklärung gefunden hat. Das Erklärungszeichen muss vom gedachten Inhalt abweichen. Rechenfehler und Programmierfehler bleiben als Motivirrtümer außen vor,[376] während nach dem Rechtsgedanken des § 120 BGB die falsche Übermittlung zu einer Anfechtung berechtigt.[377]

An diesen Grundsätzen ändert sich nichts, soweit Teile der Erklärung nur durch den **Quellcode** des Smart Contract zum Ausdruck kommen. Entscheidend ist, ob die jeweilige Programmzeile als Bestandteil der rechtsverbindlichen Erklärung aufgefasst werden darf.[378] Sollte der Anfechtende jedoch in dem Bewusstsein handeln, die Erklärung bzw. den Quellcode nicht zu verstehen, kommt keine Anfechtung in Betracht: Wer sich keine Vorstellung vom Inhalt seiner Erklärung macht kann auch nicht irren.[379]

[374] In ergänzender Vertragsauslegung dürftet sich aber eine Korrekturpflicht ergeben.
[375] *Söbbing*, ITRB 2018, 43 (45).
[376] *Singer*, in: Staudinger (2017), BGB, § 119 Rn. 36 f.
[377] Ähnlich *Paulus/Matzke*, ZfPW 2018, 431 (456).
[378] *Singer*, in: Staudinger (2017), BGB, § 119 Rn. 36.
[379] *Kaulartz*, InTeR 2016, 201 (205).

Hinsichtlich sonstiger Anfechtungskonstellationen sind keine Besonderheiten ersichtlich. Insbesondere für computergenerierte Erklärungen gelten die dafür anerkannten Grundsätze.[380]

6. Sicherstellung des korrekten Leistungsaustauschs (Erfüllung)

Die Problematik der **Sicherstellung** des korrekten **Leistungsaustauschs** als **Schnittstellenproblematik** wurde bereits angedeutet.[381] Damit verbunden ist die Schwierigkeit, genau zu definieren, was die zu erbringende Leistungshandlung ist. Gemäß § 362 Abs. 1 BGB ist die Leistung wie geschuldet zu bewirken, um Erfüllung herbeizuführen. Während im Falle einer Gattungsschuld grundsätzlich Sachen mittlerer Art und Güte zu liefern sind (vgl. § 243 Abs. 1 BGB), lässt die Vertragsfreiheit den Parteien große Spielräume, die Modalitäten der Leistungserbringung näher auszugestalten. Verwenden die Parteien einen Smart Contract, liegt es nahe, die getroffene Vereinbarung dahingehend auszulegen, dass die Leistungshandlung sowohl entsprechend der codierten Vorgaben als auch für die Oracles eines Smart Contracts wahrnehmbar erbracht werden müsse. Der Parteiwille oder besondere gesetzliche Vorgaben können freilich zu einem anderen Ergebnis führen.[382]

Zu berücksichtigen ist auch, ob und inwieweit die Parteien auf ein **Erfüllungssurrogat** zurückgreifen können. Beispielhaft genannt sei hier die Aufrechnung, §§ 387 ff. BGB.[383] Liegen die Voraussetzungen vor und wurde insbesondere kein Aufrechnungsverbot vereinbart, kann sich die berechtigte Partei mit einer entsprechenden Erklärung von einer Zahlungsverpflichtung befreien. Gem. § 389 BGB erlischt damit die Forderung, ggf. auch nur teilweise, was dem Smart Contract jedoch verborgen bliebe.

Der Smart Contract würde in solchen Fällen, wenn also rechtlich Erfüllung eingetreten ist, jedoch die codierte Bedingung unerfüllt blieb, möglicherweise die Freigabe der bedingten (Gegen-)Leistung verweigern. Es ist daher in jedem Fall sinnvoll, als **Alternativbedingung** stets eine Bestätigungstransaktion der Empfängerpartei zu definieren. Hierdurch kann diese gegebenenfalls die fällige Leistung freigeben bzw. hierzu durch gerichtliches Urteil gezwungen werden. Die digitale Überprüfbarkeit als solche ist zudem Grundvoraussetzung, damit eine Leistung überhaupt als Bedingung eines Smart Contracts herangezogen werden kann.

7. Eigenmächtige Rechtsdurchsetzung

a) Zulässigkeit sog. elektronischer Selbsthilfe

Mit der Diskussion zu Smart Contracts eng verwandt ist die Debatte zur sog. **elektronischen Selbsthilfe**, also der eigenmächtigen Durchsetzung

[380] Vgl. etwa *Söbbing*, ITRB 2018, 43 (45 f.).
[381] Siehe S. 32 ff.
[382] Letzteren Aspekt für das US-Recht hervorhebend *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (326).
[383] Weitere Erfüllungssurrogate sind etwa die Hinterlegung (§§ 233 ff. BGB) oder die Leistung an Erfüllungs statt (§ 365 BGB).

vertraglicher Rechte durch technische Zwangsmittel. Hierzu gehört etwa das ferngesteuerte Unterbinden des Motorstarts bei Leasingwagen, sollten eine Rate nicht gezahlt oder Verkehrsverstöße registriert werden.[384] Obschon es noch an einer flächendeckenden praktischen Umsetzung fehlt, sind die notwendigen Systeme (fernsteuerbare Startunterbrecher, etc.) bereits verfügbar. Aufgrund erwartbarer Effizienzsteigerungen ist ein solches System für die Gläubigerseite durchaus attraktiv. Man bewege sich jedoch, so einige Stimmen, zwischen verbotener Eigenmacht und erlaubter Sicherungsabrede.[385] Problematisch ist dabei, dass die eigentliche Klägerrollenverteilung, nach welcher der Gläubiger zunächst vor Gericht ziehen müsste, um seinen Anspruch geltend zu machen, umgekehrt wird. Greift der Vermieter eigenmächtig zu Zwangsmitteln, um seinen angeblichen Anspruch durchzusetzen, muss sich nun der ausgesperrte Mieter zur Wehr setzen. Grundsätzlich steht dem Gläubiger gerade kein Recht zur Selbsthilfe zu (vgl. § 227 BGB); vielmehr bezwecken das staatliche Gewaltmonopol und der damit verbundene Vorrang des Rechtswegs neben einer Verhinderung des Faustrechts nicht zuletzt effektiven Rechtsschutz.[386]

Der wesentliche Regelungskomplex zur Umsetzung dieses Anliegens ist der **possessorischen Besitzschutz** (§§ 858 ff. BGB). Problematisch erweist sich für Schuldner, dass nicht alle Fälle elektronischer Selbsthilfe davon erfasst sind:

Bei **Wohnungen** sorgt einschlägige Rechtsprechung noch für Klarheit: Dem BGH zufolge entzieht ein Vermieter, der einen Mieter eigenmächtig aus der Wohnung aussperrt, diesem den Besitz und begeht damit verbotene Eigenmacht i.S.v. § 858 BGB.[387] Hierauf darf mit Besitzkehr gem. § 859 Abs. 3 BGB reagiert werden. Zudem komme die Erfüllung der Straftatbestände §§ 123 Abs. 1, 240 Abs. 1, 253 Abs. 1 StGB in Betracht.[388]

Der **Besitz** ist insoweit unstrittig im Hinblick auf **Einwirkungs- und Ausschlussmacht** geschützt, sodass der Ausschluss aus der Wohnung unmittelbar erfasst ist. Für den Gläubiger kann ein ähnliches Druckmittel aber auch im Gebrauchsentzug zu finden sein, indem der Schuldner beispielsweise nicht aus dem Mietwagen ausgesperrt wird, sondern lediglich eine Abschaltvorrichtung vorgesehen ist. Ob und unter welchen Voraussetzungen eine eigenmächtige Rechtsdurchsetzung insoweit zulässig sein soll, ist im Detail noch offen.[389] Der BGH wollte bislang jedenfalls den **Gebrauchsentzug** nicht dem Besitzentzug gleichstellen.[390] Für das Abschalten eines Mietwagens würde das bedeuten, dass zumindest die §§ 858 ff. BGB nicht entgegenstünden.[391]

Die Abschaltung der zum Gebrauch erforderlichen Software ist bei vielen vernetzten Gegenständen in der Theorie möglich, während sich aus

[384] Vgl. *Paulus/Matzke*, CR 2017, 769 (772 ff.); *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (329 ff.).
[385] So *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Wendehorst*, NJW 2016, 2609.
[386] Vgl. auch *Paulus/Matzke*, CR 2017, 769 (770, 772 ff.).
[387] BGH v. 14.7.2010 – VIII ZR 45/09, NJW 2010, 3434.
[388] OLG Köln v. 25.7.1995 – Ss 340/95, NJW 1996, 472.
[389] Vgl. zur Diskussion in den USA *Raskin*, 1 Geo. L. Tech. Rev. 2017, 305 (329 ff.).
[390] BGH, NJW 2009, 1947.
[391] *Paulus/Matzke*, CR 2017, 769 (775).

dem einschlägigen **Immaterialgüterrecht** weit weniger Hindernisse ergeben. Eine eindeutige vertragliche Grundlage kann dabei schon genügen, soweit keine höchstpersönlichen Rechtsgüter tangiert sind.[392] Dass nur die sachenrechtlichen Vorschriften effektiv zur Durchführung eines Zwangsvollstreckungsverfahrens anhalten, die fragliche Steuerungssoftware in Abgrenzungsfragen hingegen höchstrichterlich vermehrt dem rein immaterialgüterrechtlichen Bereich zugeordnet wird, bedeutet für viele potentielle Fälle eine Aushebelung des Schuldnerschutzes.[393] Gerade im Interesse eines effektiven Verbraucherschutzes gilt es hier in Zukunft Antworten zu finden.

Ein gangbarer Weg wäre, jene Software, die den Gebrauch eines Gegenstands sicherstellt (**Firmware**), künftig ebenfalls dem **Sachbegriff** zu unterstellen, um so den Vorrang des Zwangsvollstreckungsverfahrens und die Anwendbarkeit des Besitzschutzes sicherzustellen.[394] Das erscheint konsequent, da ein vollständiger Gebrauchsentzug sich letztlich nicht wesentlich von einem fremdbestimmten Ausschluss von der Einwirkungsmacht auf die Sache als solche unterscheidet. Zudem stellen die §§ 858 ff. BGB nicht auf Gewaltanwendung, sondern lediglich den unberechtigten Besitzentzug bzw. die Besitzstörung ab. Ein digitales Faustrecht erscheint nicht erstrebenswert.

b) Realistisches Bedrohungspotential im Rahmen der Blockchain-Technologie

Elektronische Selbsthilfe ist zwar nicht notwendigerweise auf Smart Contracts angewiesen. Es liegt jedoch nicht nur aus Zweckmäßigkeitsgründen nahe, die Auslösung der Sperre einem unaufhaltbaren Programmcode zu überlassen. Einerseits entsteht der Anschein, eine objektiv entscheidende Stelle könne nur zu richtigen Ergebnissen kommen (unbestechlicher Code), andererseits wird gerade durch diese **angebliche Objektivierung des Verfahrens** psychischer Druck auf den Schuldner ausgeübt, der sich sicher sein kann, dass sein Handeln entsprechende Konsequenzen nach sich ziehen wird. Der Code würde damit selbständig Recht oder eben Unrecht durchsetzen. Für letzteres müsste nicht einmal die elektronische Selbsthilfe an sich unzulässig sein. Es würde schon genügen, wenn die geschuldete Leistung, im Beispielsfall die Zahlung der Miete, auf andere Weise erbracht worden wäre. Man nehme an, das Programm würde zunächst den Zugriff auf das Auto sperren, später eine Strafzahlung verhängen und dann den Schuldner gar einer „schwarzen Liste“ zahlungsunwilliger Kunden melden. Ein Erlöschen der Forderung wegen Aufrechnung oder aufgrund einer mangelbedingten Minderung (vgl. § 536 Abs. 1 BGB) sind durchaus realistische Szenarien. Ein Programm, das auf solche Umstände keine Rücksicht nehmen kann, könnte schnell einen „Amoklauf“ begehen.

[392] Vgl. *Paulus/Matzke*, CR 2017, 769 (772 ff.), die vergleichend auf die Programmsperre-Rechtsprechung des BGH abstellen.

[393] *Paulus/Matzke*, CR 2017, 769 (776).

[394] *Paulus/Matzke*, CR 2017, 769 (776 ff.), die aber eine Ausnahme für kurzfristige Gebrauchsüberlassung im Rahmen der Sharing Economy erwägen.

8. Zivilprozessuale Durchsetzbarkeit

Im Hinblick auf die **zivilprozessuale Durchsetzbarkeit** von Ansprüchen im Kontext einer Blockchain sind zwei Aspekte hervorzuheben.

a) Richtiger Vollstreckungsantrag

Ein erfolgreiches Begehren setzt das Stellen des **richtigen Vollstreckungsantrags** voraus. Einerseits ist der Fall problematisch, wenn Gegenstand des Anspruchs die **Änderung eines Datenbankeintrags** bzw. eine Transaktion ist. Beides setzt eine entsprechende Berechtigung, in der Regel die Signatur mit dem passenden privaten Schlüssel voraus. Soll ein digitales Asset übertragen werden, ist deshalb die Mitwirkung des Schuldners unumgänglich. Nur ihm sollte der Schlüssel bekannt sein, weshalb in einem autonomen, dezentralen Netzwerk die meisten Transaktionen bzw. sonstige Datenbankänderungen auch nur von ihm selbst autorisiert werden können. Die Vornahme eines Datenbankeintrags ist daher grundsätzlich als unvertretbare Handlungen einzuordnen, die nach Maßgabe des § 888 ZPO notfalls mit Zwangsgeld bzw. Zwangshaft durchgesetzt werden muss.[395]

Schwieriger zu beurteilen ist ein Begehren gerichtet auf die **(Rück-)Gewähr von Kryptowährungen**, insb. Bitcoins, bzw. **digitaler Assets**. Mangels Geld-, Rechts- oder Sacheigenschaft ist grundsätzlich weder ein Vorgehen nach den §§ 802a ff. ZPO noch §§ 883 – 887 ZPO statthaft.[396] Hingegen in jedem Falle auf § 888 ZPO abzustellen,[397] erscheint zu pauschal: Zunächst ist zu fragen, ob tatsächlich die Summe einer Kryptowährung oder vielmehr eine Wertsumme (gemessen am aktuellen Kurswert) geschuldet ist.[398] Verkauft etwa eine Bar ihre Getränke wahlweise in Euro oder zum aktuell geltenden BTC-Kurs, könnte die Parteivereinbarung u.U. erlauben, primär oder stattdessen eine Geldforderung zu titulieren.

Steht (wie regelmäßig) eine **Leistungsverpflichtung zur Zahlung** bzw. Rückzahlung einer bestimmten Summe Bitcoins fest, scheint auch hier eine Differenzierung angezeigt. Es könnte sich dabei nämlich um eine vertretbare Handlung gem. § 887 Abs. 1 ZPO handeln, wenn sie auch von einem Dritten vorgenommen werden kann.[399] Dies scheidet nur aus, wenn der private Schlüssel des Schuldners erforderlich ist, indem nicht nur ein Zufluss beim Gläubiger sondern gleichzeitig ein Abfluss vom Konto des Schuldners Leistungsgestand ist. Soll etwa ein rechtsgrundlos erlangter Datenbankeintrag bzw. eine bestimmte digitale Münze herausgegeben werden, wäre für die geschuldete Naturalrestitution (§§ 812 Abs. 1 S. 1, 818 ff. BGB) demnach der private Schlüssel nötig und § 888 ZPO die richtige Norm. In anderen Fällen, wenn es den Parteien überhaupt nicht auf die Leistung einer bestimmten digitalen Münze ankommt, sondern allein eine Summenzuschreibung in der Datenbank begehrt wird, liegt eine Handlung nach § 887 Abs. 1

[395] *Paulus/Matzke*, ZfPW 2018, 431 (464). Vgl. allgemein *Gruber*, in: MüKo-ZPO, § 888 Rn. 2.

[396] *Kütük/Sorge*, MMR 2014, 643 (644 f.). Etwas anderes gilt für die nach § 857 ZPO mögliche Pfändung eines Anspruchs gegen einen dritten Verwahrer, vgl. ebd.

[397] So *Kütük/Sorge*, MMR 2014, 643 (644 f.); *Mössner*, in: BeckOGK-BGB, § 90 Rn. 104.4 (Stand: 01.08.2018); ähnlich *Paulus/Matzke*, ZfPW 2018, 431 (464) („i.d.R.“).

[398] Bei ausländischen Währungen wird dies idR als gegeben gesehen (sog. unechte Fremdwährungsschuld), vgl. *Gruber*, in: MüKo-ZPO, § 803 Rn. 3 ff. (auch zu Kursverlusten).

[399] *Gruber*, in: MüKo-ZPO, § 887 Rn. 3.

ZPO vor. Anstelle des Schuldners kann nämlich jeder Dritte seinem öffentlichen Schlüssel zugeordnete Bitcoins transferieren, notfalls, nachdem er diese an einem der zahlreichen Handelsplätze erworben hat.[400] Aus Sicht des Gläubigers hängt die wirtschaftliche Bedeutung und der Charakter der Leistung gerade nicht davon ab, dass der Schuldner sie selbst vornimmt.[401] Während es sich so bei Rückabwicklungsfragen in der Regel um einen Fall des § 888 ZPO handelt, ist bei den meisten Leistungsbegehren im Kontext von Kryptowährungen § 887 Abs. 1 ZPO die treffende Norm.

b) Beweisfragen

Um Schwierigkeiten bei der **Beweisführung** vorzubeugen, sollten Parteien, die miteinander ohnehin in vertraglicher Beziehung stehen, über eine **Beweisvereinbarung** nachdenken. Beispielsweise könnte vereinbart werden, dass jene Partei die Beweislast trägt, die sich gegen die im Ledger dargestellte Rechtslage stellt. Eine solche Vereinbarung wäre jedenfalls unter Unternehmern ohne weiteres zulässig.[402] Dies überbrückt auch eine weitere Schwierigkeit: Einträgen im Ledger haben gegenwärtig nicht die Qualität einer (Privat-)Urkunde (vgl. § 416 ZPO); ebenso wenig entspricht eine Signatur mittels privatem Schlüssel den Anforderungen an ein Privaturkunden gleichgestelltes elektronisches Dokument nach § 371a ZPO. Die Beweiskraft von Ledgereinträgen (Sicherheit und Nachvollziehbarkeit der gespeicherten Informationen) müsste daher im Verfahren u.U. gutachterlich überprüft werden, was entsprechend Kosten verursacht.

Möchte man *de lege ferenda* über eine Gleichstellung nachdenken, sollte als Anforderung zumindest ein hinreichend sicherer Distributed-Ledger gefordert sowie bedacht werden, dass mit der Signatur in der Regel nur die Urheberschaft des Eintrags, nicht aber dessen inhaltliche Richtigkeit bezogen auf Tatsachen oder Zustände der Außenwelt nachvollzogen werden kann. Zu beobachten bleibt in diesem Zusammenhang eine **mögliche Regulierung** elektronischer Wertpapiere und Krypto-Token, wie sie in einem Eckpunktepapier des Bundesministeriums der Finanzen und des Bundesministeriums der Justiz und für Verbraucherschutz bereits in ersten Ansätzen erwogen wird.[403]

9. Rechtsvergleichender Überblick

Gesetzliche Regelungen im Bezug auf Blockchain/DLT und Smart Contracts wurden u.a. in den U.S.-Bundesstaaten Arizona und Vermont erlassen. Beide erkannten an, dass auf einer Blockchain gespeicherte Informationen auch rechtliche Folgen auslösen können bzw. dass Informationen oder Rechten nicht allein wegen ihres Speicherorts die Anerkennung versagt

[400] Unklar insbesondere das Argument von *Kütük/Sorge*, MMR 2014, 643 (644 f.), die Übertragung durch einen Dritten sei aufgrund der Dezentralität ausgeschlossen.

[401] *Gruber*, in: MüKo-ZPO, § 887 Rn. 9.

[402] So schon RGZ 106, 295 (298 f.); 145, 322 (327). Beachte in AGB gegenüber Verbrauchern § 309 Nr. 12 BGB, der jedoch einer Beweislastumkehr nicht grundsätzlich entgegensteht, vgl. zum Anwendungsbereich *Wurmnest*, in: MüKo-BGB, § 309 Nr. 12 Rn. 9 ff.

[403] Eckpunktepapier vom 07. März 2019, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Eckpunkte_Krypto_Blockchain.pdf?__blob=publicationFile&v=2.

werden dürfe.[404] Diese Betonung der Auswirkungen technischer Systeme auf das Rechtssystem[405] spricht aus Sicht des deutschen Rechts freilich nur eine Selbstverständlichkeit aus, die allenfalls in beweisrechtlicher Hinsicht Bedeutung entfaltet.[406] Der Staat Vermont geht darüber sogar hinaus, indem eine Vermutung der Authentizität auf einer Blockchain gespeicherten Informationen im Hinblick auf Eigentum, Erklärungsurheberschaft und Vertragsinhalte aufgestellt wird.[407] Auch wenn hinzukommen muss, dass ein Sachverständiger die Integrität des Eintrags bestätigt, scheinen Zweifel angebracht. So fehlt ein besonderes Verfahren sowie eine Legitimationsbildung dafür, DL-Systeme grundsätzlich mit Geltung für alle (erga omnes) aufzuwerten.[408] Nicht jedes DL weist per se dieselbe Sicherheit auf; würde man diese jedoch in jedem Fall gutachterlich prüfen lassen, erscheint die Vorzugswürdigkeit des Ansatzes zweifelhaft. Eine vertragliche Regelung der Beweisfrage erscheint daher weiterhin vorzugswürdig.

10. Anwendbares Recht[409]

Das **internationale Privatrecht** sieht sich mit seiner Fixierung auf den Sitz eines Rechtsverhältnisses, also dem Schwerpunkt eines Lebenssachverhaltes, dezentralen Strukturen gegenüber offensichtlichen Schwierigkeiten ausgesetzt.[410] Die Suche nach einem tauglichen Anknüpfungspunkt fällt jedoch zumindest bei den hier interessierenden Vertragsabwicklungsfragen deutlich einfacher, da an ein konkretes, zwischen den Parteien bestehendes Rechtsverhältnis angeknüpft werden kann. Da es sich bei dem Smart Contract um ein Abwicklungsinstrument handelt, findet Art. 12 Abs. 1 lit. b Rom-I-VO Anwendung, sodass die Beurteilung des Distributed Ledgers insoweit akzessorisch zur Beurteilung des zugrundeliegenden Schuldverhältnisses ist (vgl. auch Art. 4 Abs. 3 Rom-II-VO).[411] Maßgeblich ist daher das jeweilige Vertragsstatut, das, soweit die Parteien keine Rechtswahl vorgenommen haben (Art. 3 Rom-I-VO), nach den Art. 4 ff. Rom-I-VO zu bestimmen ist. Für Verbraucherverträge ist dabei grundsätzlich gemäß Art. 6 Rom-I-VO der gewöhnliche Aufenthaltsort des Verbrauchers entscheidend.

[404] In Arizona Section 44-7061 D, Arizona Revised Statute, Bill HB 2417, abrufbar https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf; in Vermont 12 V.S.A. § 1913, abrubar unter: https://legislature.vermont.gov/statutes/section/12/081/01913.

[405] *Jaccard*, JuS-Letter IT 23, November 2017, S. 10 f.

[406] *Jaccard*, JuS-Letter IT 23, November 2017, S. 11.

[407] Vermont Section I.1. 12 V.S.A. § 1913 b u. c, Bill H.868.

[408] In dieser Hinsicht insb. *Jaccard*, JuS-Letter IT 23, November 2017, S. 12, nach dem allenfalls Zugangsrechte, nicht aber Eigentumsrechte verkörpert werden sollten.

[409] Mit Blick auf die Schweiz *Jaccard*, JuS-Letter IT 23, November 2017, S. 20 f.

[410] Vgl. *Zimmermann,* IPRax 2018, 566.

[411] *Zimmermann,* IPRax 2018, 566 (568 f.).

VII. Fazit zur rechtssicheren Einbettung von Smart Contracts

An sich bereiten Smart Contracts dem BGB **keine besonderen Schwierigkeiten**.[412] Damit sich selbstvollziehende Verträge – in einer Blockchain oder einem sonstigen System implementiert – jedoch tatsächlich als „smartes“ Hilfsmittel erweisen, sollten einige Empfehlungen beachtet werden, die sich aus dem dem zuvor Gesagten ableiten:

Grundsätzlich...

- sollte die vertragliche Einigung nicht in Codeform, sondern außerhalb eines digitalen Systems geschlossen und formgerecht festgehalten werden.
- sollten sich die Parteien kennen bzw. identifizieren.
- sollte die limitierte Darstellbarkeit rechtlicher Normen und Wertungen bzw. die mangelnde Auslegungsfähigkeit technischer Systeme berücksichtigt werden.[413]
- sollten im Ledger lediglich Konkretisierungen bzw. Auszüge einzelner vertraglicher Regelungsgegenstände und Abläufe abgebildet oder bloße Rechtszustände bzw. -zuweisungen dokumentiert werden.

Im Einzelnen...

- müssen alle vom Code nachvollzogenen Regelungen, Parameter und Inhalte digital abgebildet werden können, d.h. der jeweilige Umstand muss in einem 1/0-Schema (true oder false) darstellbar sein. Definitionsmerkmale mit Wertungsspielraum sind grundsätzlich ungeeignet, sodass diese Aspekte wie auch andere Wertungsfragen einem Oracle überantwortet werden müssten.
- sollte eine Schnittstelle implementiert sein, die den Parteien erlaubt durch beiderseitige Signatur den Programmablauf zum einen anhalten, zum anderen den Ledger für die Zukunft zur wahren Rechtslage hin korrigieren zu können (Korrekturschnittstellen). Dass der Ledger dann weiterhin Fehler dokumentiert, dürfte hingegen unschädlich sein. Entscheidend ist, dass der auslesende Client die korrigierte Fassung als die aktuelle erkennt.
- sollte versucht werden, das Recht weitestgehend mit der Prozesslogik des Smart Contract bzw. des Ledger zu synchronisieren. Die Rechtslage sollte durch privatautonome Gestaltung weitestgehend den Zwängen der Technik angepasst werden. Verstöße gegen zwingendes Recht, insbesondere gesetzliche Verbote, sind selbstredend zu vermeiden, während Auswirkungen des Minderjährigenschutzes durch Identifizierungssysteme vermieden werden könnten.

[412] So auch *Paulus/Matzke*, ZfPW 2018, 431 (465); *Heckelmann*, NJW 2018, 504.
[413] Vgl. zu den konkret hieraus resultierenden Empfehlungen S. 64 ff.

- sind Einschränkungen der Vertragsfreiheit weitestgehend zu vermeiden, um eine passgenaue und mit wenigen Risiken behaftete Synchronisierung der Rechtslage erreichen zu können. Kollisionen mit dem AGB-Recht können so ebenfalls besser vermieden werden. Smart Contracts sind daher besser für das unternehmerische bzw. kaufmännischen Umfeld geeignet.
- sollte im Hinblick auf spätere Rechtsstreitigkeiten eine vertragliche Beweisvereinbarung getroffen werden, die den im Ledger dargestellten Inhalten eine Richtigkeitsvermutung verleiht.

Eine völlig andere Frage ist, ob die mit dem Smart Contract bezweckte garantierte Rechtsdurchsetzung auch **sozialverträglich** ist. *Levy* weist etwa darauf hin, dass in einigen Bereichen die Nichtdurchsetzung bestimmter Rechte, etwa aus Kulanz, für das soziale Miteinander oder aber auch das Funktionieren eines Systems entscheidend sein können.[414]

[414] *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (11). Vgl. auch S. 63 f.

VIII. Rechtliche Aufladung von Blockchain-Einträgen, insb. sog. Token

Im Rahmen der **Privatautonomie** steht es den Parteien grundsätzlich frei ihr Miteinander eigenen Regeln zu unterwerfen. Durch Vereinbarung (§ 311 Abs. 1 BGB) könnten damit auch Blockchain-Einträge rechtlich „aufgeladen" werden. Es käme zum Beispiel in Betracht, die Wirksamkeit von Rechtsgeschäften an die Vornahme einer Transaktion zu binden (§ 158 Abs. 1 BGB). In ähnlicher Weise könnte die Eintragung mittels Transaktion als gewillkürte Formvorgabe festgeschrieben werden (§ 125 S. 2 BGB).[415]

Ein besonderer Ansatz, rechtliche Bedeutung in Blockchain-Einträge zu legen, ist die Verwendung von Token. Ein Token ist ein **digitaler Wertbehälter**, der entweder ein Faktum dokumentiert oder eine Berechtigung im Sinne einer technischen Möglichkeit verkörpert.[416] Wie der Token im Einzelnen ausgestaltet ist, wie viele ausgegeben werden und alle sonstigen Modalitäten werden vom Ersteller (i.d.R. dem Entwickler des Netzwerkprotokolls) festgelegt.[417] Welche Arten von Token regelmäßig verwendet werden, wurde bereits aufgezeigt. Im Folgenden sollen einige grundlegende rechtliche Überlegungen angestellt werden.

Im Rahmen einer rechtlichen Prüfung ist dabei sorgfältig zu unterscheiden: Geht es um den **Datenbankeintrag** als solchen, der mit einer bestimmten technischen Ausgestaltung bzw. Inhaltsbeschreibung eindeutig einem Inhaber zugewiesen ist, oder sollen (gesetzliche oder vertragliche) **Rechte** hergeleitet oder untersucht werden, für die der Token allenfalls ein digitaler Repräsentationskörper **(Visualisierung)** ist. Mit der Inhaberschaft des Tokens muss nicht notwendigerweise eine **darüberhinausgehende Rechtsinhaberschaft** verknüpft sein. Ob dem Inhaber des Tokens etwa eine Beteiligung, ein Anspruch übertragen bzw. verliehen wurde, bedarf stets einer isolierten Betrachtung im Einzelfall.[418]

1. Token als solcher

a) Einordnung im Kontext vertraglicher Schuldverhältnisse

Welchen Rechtscharakter hat die bloße Inhaberschaft eines Tokens bzw. der schuldrechtliche Vertrag, um einen Token zu erwerben? Die Fragen stellen sich insbesondere, wenn dem verkörperten Inhalt keine eindeutige Rechtsposition zugeordnet werden kann. Hierzu zählen vor allem die sog. **Kryptowährungen**. Die Currency Token (Ether, IOTA-Coin, Ripple Coin, etc.) werden als Datenbankeintrag einem Kontoinhaber zugeordnet und können von diesem durch Signierung einer Transaktion übertragen werden. Mangels staatlicher Emission handelt es sich zunächst nicht um Geld.[419]

[415] *Paulus/Matzke*, ZfPW 2018, 431 (457f.).
[416] Nach *Borkert*, ITRB 2018, 91 (92) ein digitaler Blankogutschein.
[417] Dabei kann im Rahmen der Ethereum-Plattform auf eine Reihe Vorlagen zurückgegriffen werden.
[418] *Jaccard*, JuS-Letter IT 23, November 2017, S. 13.
[419] Vgl. nur *Engelhardt/Klein*, MMR 2014, 355 (358); *Schlund/Pongratz*, DStR 2018, 598 (599); *Mössner*, in: BeckOGK-BGB, § 90 Rn. 104.3 (Stand: 01.08.2018).

Auch die Einordnung als Sache i.S.v. § 90 BGB scheitert, da ein digitaler Registereintrag nicht das Merkmal der Körperlichkeit erfüllt.[420] Token, insb. Kryptowährungen, sind daher nicht eigentumsfähig. Da es sich damit nicht um einen Sachkauf gem. (§ 433 Abs. 1 BGB) handelt, könnte man an einen Rechtskauf denken, § 453 Abs. 1 Alt. 1 BGB.

Dafür müsste sich aus einem Rechtsgeschäft oder der Rechtsordnung eine unmittelbare Befugnis des Tokeninhabers herleiten lassen.[421] Ein Datenbankeintrag begründet jedoch als solcher keine rechtliche Verpflichtung. Im Falle der genannten Kryptowährungen ist keine Person oder Stelle dem Inhaber gegenüber zu einer Leistung verpflichtet. Es fehlt an einem mit der Visualisierung einhergehenden Recht bzw. einer Forderung im Sinne von § 241 Abs. 1 S. 1 BGB, .[422] Kryptowährungen bzw. Token als solche sind daher nicht als Recht i.S.v. § 453 Abs. 1 Alt. 1 BGB einzuordnen.

Demzufolge hat eine Einordnung als **sonstiger Gegenstand** (§ 453 Abs. 1 Alt. 2 BGB) zu erfolgen.[423] Der Vorschrift kommt eine Auffangfunktion für jedes übertragbare Gut, das weder Sache noch Recht ist, zu.[424] Für den Erwerb des Tokens bzw. der Kryptowährung finden daher gem. § 453 Abs. 1 Alt. 2 BGB die Vorschriften über den Kaufvertrag Anwendung.[425] Wird mit einer Kryptoeinheit eine Sache, ein Recht oder ein sonstiger Gegenstand **erworben**, muss dies konsequenterweise als **Tauschvertrag** (§ 480 BGB) eingeordnet werden.[426]

In anderen Vertragsverhältnissen, die lediglich die Zahlung eines Entgelts, einer Vergütung oder Miete vorsehen, kann die Zahlung in Kryptowährungen unproblematisch als Erbringung einer sonstigen Leistung gesehen werden.[427] Genaueres Augenmerk ist jedoch im Einzelfall darauf zu richten, in welcher **Einheit** die Parteien den geschuldeten Wert definieren: Ist eine Mietzahlung in Euro bedungen, käme, soweit von den Parteien als zulässig erachtet, die Begleichung einer entsprechenden Summe Bitcoin einer Leistung an Erfüllungs statt gleich.[428] Auch sonst kommt es für das vereinbarte Wertverhältnis darauf an, ob die Parteivereinbarung tatsächlich

[420] *Borkert*, ITRB 2018, 91 (92).

[421] *Berger*, in: Jauernig, BGB, § 453 Rn. 2; *Westermann*, in: MüKo-BGB, § 453 Rn. 3.

[422] Vgl. *Roth/Kieninger*, in: MüKo-BGB, § 413 Rn. 2; *Langenbucher*, AcP 218 (2018), 385 (405 f.); a.A. *Spindler/Bille*, WM 2014, 1357 (1362 f.): der Inhaber müsse „ein wie immer geartetes „Recht" auf den „Gegenstand" [sic!] Bitcoin haben".

[423] *Borkert*, ITRB 2018, 91 (92); *Schlund/Pongratz*, DStR 2018, 598 (600); diese Variante übersehend *Engelhardt/Klein*, MMR 2014, 355 (359).

[424] *Berger*, in: Jauernig, BGB, § 453 Rn. 11.

[425] *Borkert*, ITRB 2018, 91 (92); *Schlund/Pongratz*, DStR 2018, 598 (600); *Shmatenko/Möllenkamp*, MMR 2018, 495 (499); a.A. für die Bezahlung in Bitcoins *Schneider*, Interview, Legal Tribune Online, abrufbar unter: http://www.lto.de/recht/hintergruende/h/bitcoins-waehrung-rechnungseinheit-umsatzsteuer: „atypischer Werkvertrag"; zustimmend *Boehm/Pesch* , MMR 2014, 75 (78); Verweis auf angebliche werkvertragliche Dimension *Langenbucher*, AcP 218 (2018), 385 (411). Es fehlt allerdings an einer schöpferischen Eigenleistung des Absenders; insoweit bestehen keine wesentlichen Unterschiede zwischen dem Absenden einer Ware beim Versendungskauf und dem Absenden einer Transaktion im Netzwerk, *Beck/König*, JZ 2015, 130 (132). Ein Werkvertrag liegt nur dann vor, sofern die Generierung von (Currency) Token geschuldet wird, vgl. *Shmatenko/Möllenkamp*, MMR 2018, 495 (499).

[426] *Spindler/Bille*, WM 2014, 1357 (1362); Engelhardt/Klein, MMR 2014, 355 (359); *Westermann*, in: MüKo-BGB, § 433 Rn. 16, § 480 Rn. 1; a.A. *Beck/König*, JZ 2015, 130 (133); *Ammann*, CR 2018, 379 (380 f.).

[427] *Paulus/Matzke*, ZfPW 2018, 431 (451) m.w.N.

[428] Vgl. *Langenbucher*, AcP 218 (2018), 385 (415).

allein auf den Kurs der Kryptowährung, trotz dessen Volatilität, abzielte – entscheidend ist dies insbesondere bei Darlehensverträgen.

b) Rechtscharakter der Übertragung eines Tokens

Die **Übertragung** des Tokens vollzieht sich aufgrund der fehlenden Körperlichkeit nicht nach §§ 929 ff. BGB. Es handelt sich schlicht um einen verschlüsselten Datenbankeintrag, dessen Zugriff allein mittels eines bestimmten Schlüssels möglich ist. Damit sind weder § 413 BGB noch sonstige Sonderregeln einschlägig. Ein Token wird als unkörperlicher Gegenstand daher allein durch **Realakt** übertragen; ein gutgläubiger Erwerb findet nicht statt.[429] Überzeugende Gründe dafür, sich mit Analogien zu sachenrechtlichen Vorschriften zu behelfen, finden sich nicht.[430]

Mangels abzuschließendem Rechtsgeschäft kann auch ein Minderjähriger oder Geschäftsunfähiger stets wirksam mit einer Kryptowährung bezahlen.[431] Schutzlücken entstehen hierdurch jedoch nicht. Ein Rechtsgrund kann nur nach Maßgabe der §§ 105 ff. BGB begründet werden, sodass – bei fehlender Zustimmung der Eltern – eine bereicherungsrechtliche Rückabwicklung angezeigt ist. Ist das zugrundeliegende Kausalgeschäft dagegen wirksam, kann der Empfänger grundsätzlich auf den Bestand des Erwerbs vertrauen, während auf Rechte Dritter keine Rücksicht genommen werden muss.

Dieselben Regeln gelten für sonstige **virtuelle Gegenstände**, denen kein Sonderrecht oder eine Forderung zugrunde liegt. Wird demgegenüber bei anderen Tokenarten eine Berechtigung visualisiert, folgt diese aus dem zugrundeliegenden Vertrag. Der Anspruch (i.S.v. § 194 BGB) wird durch den Token lediglich in Form einer digitalen Urkunde visualisiert (quasi technisch verbrieft).[432] Das jeweilige Recht muss demzufolge selbständig übertragen werden, was, soweit keine sachen- oder immaterialgüterrechtlichen Sonderregelungen bestehen, durch Abtretung (§ 398 BGB, ggf. i.V.m. § 413 BGB) zu vollziehen ist.[433] Unter Umständen kann daher zwar eine technische Übertragung des Tokens erfolgen, der Rechtsübergang hingegen (etwa aufgrund der Minderjährigkeit des Teilnehmers) scheitern.

2. Durch den Token verkörperte Rechte

Anders liegen die Dinge, wenn mit dem Token tatsächlich ein rechtliches Können verkörpert wird. Das betrifft zum einen die Visualisierung von **An-**

[429] *Engelhardt/Klein*, MMR 2014, 355 (359); *Heckelmann,* NJW 2018, 504 (507); *Langenbucher*, AcP 218 (2018), 385 (407); insofern zutreffend auch *Borkert*, ITRB 2018, 91 (92); *Shmatenko/Möllenkamp*, MMR 2018, 495 (499) mwN; a.A. *Mössner*, in: BeckOGK-BGB, § 90 Rn. 104.4 (Stand: 01.08.2018).

[430] *Schlund/Pongratz*, DStR 2018, 598 (600): §§ 929 ff. BGB analog; in diese Richtung auch *Spindler/Bille*, WM 2014, 1357 (1363). Wiederum anders *Ammann*, CR 2018, 379 (381): §§ 873 ff., 925 BGB analog.

[431] *Paulus/Matzke*, ZfPW 2018, 431 (452).

[432] *Borkert*, ITRB 2018, 91 (92); *Engelhardt/Klein*, MMR 2014, 355 (359).

[433] Irreführend insofern *Borkert*, ITRB 2018, 91 (92), der von einer Übertragung durch Verpflichtungsgeschäft spricht. Dies betrifft aber nur Fälle, in denen kein Recht im Sinne eines Anspruchs visualisiert wird.

teilen, insb. bei der Gewährung von Stimm- und sonstigen Beteiligungsrechten, die ggf. als **gesellschaftsrechtliche Mitgliedschaft** einzuordnen sind (sog. Equity Token).[434] Zum anderen muss bei sog. Debt Token der vereinbarte **Rückzahlungsanspruch** entsprechend betrachtet und anhand besonderer darlehensrechtlicher Schutzvorschriften überprüft werden. Ebenfalls muss im Einzelfall untersucht werden, ob und inwieweit das mithilfe eines Utility Token visualisierte **Leistungsversprechen** auch rechtliche Bindung haben soll. Die unterschiedliche Einordnung von Token und Recht kann zu einem Auseinanderfallen von Registerlage und Rechtslage führen.

Der *numerus clausus* dinglicher Rechte verbietet es, alleine auf Basis eines Tokens neue absolut wirkende Rechte zu begründen. Im Gegensatz dazu können **schuldrechtliche Rechtsbeziehungen** grundsätzlich frei geformt werden. Der Token selbst kann anstelle des Eigentumsrechts möglicherweise einen darauf gerichteten Verschaffungsanspruch verkörpern.[435] Bei Asset-Backed Token könnte so etwa durch Abtretung des Herausgabeanspruchs gem. §§ 929 S. 1, 931 BGB Eigentum an beweglichen Sachen verschafft werden, wenn der Veräußerer mittelbarer Besitzer der Sache ist. Denkbar wäre auch, den physischen Besitz (tatsächlichen Zugriff, § 854 Abs. 1 BGB) technisch an den Ledger zu knüpfen, indem das Schloss nur von dem oder mit Genehmigung des Tokeninhabers geöffnet werden kann. In diesem Fall läge in der Übertragung des Tokens auch eine Übergabe i.S.v. § 929 S. 1 BGB. Gleichwohl müsste in jedem Fall zum einen die abgebildete Sache auch tatsächlich existieren, zum anderen dürften keine Rechte Dritter entgegenstehen – jedenfalls solange kein gutgläubiger lastenfreier Erwerb nach Maßgabe der §§ 932 ff., 936 BGB erfolgt. Vorstellbar ist auch, dass Token eine wertpapierähnliche Funktion erfüllen, so insb. das sog. Security Token, wenn digitale Beteiligungsansprüche an einem Projekt, ggf. auch Gewinnansprüche oder Stimmrechte, abgebildet werden.

Insgesamt ergeben sich, von der aufsichtsrechtlichen Dimension[436] abgesehen, verschiedene Divergenzrisiken, von denen einige im Folgenden angesprochen werden sollen.

a) Isolierte Übertragung von Token und Recht

Die unterschiedliche Einordnung von Token und dem damit verkörperten Recht macht sich zunächst bei der Übertragung bemerkbar. Eine Abtretung kann aus verschiedenen Gründen scheitern, etwa bei Bestehen eines Abtretungsverbots (§ 399 Alt. 2 BGB) oder bei einer mit der Abtretung verbundenen Inhaltsänderung (§ 399 Alt. 1 BGB). Hat der Tokeninhaber das Token dennoch an einen Dritten übertragen, kann es nicht ohne dessen Mitwirkung zurückgeholt werden, sodass die Rechtslage und die tatsächlich geschaffene Situation auseinanderfallen würden. Dasselbe gilt, wenn der Tokeninhaber nicht der eigentliche Rechtsinhaber war. Hier kann § 405 BGB **mangels Urkundenqualität** nicht direkt zur Anwendung kommen.[437]

[434] Mögliche Ausgestaltungsvarianten zu Umgehung gesellschaftsrechtlicher Formvorschriften andeutend *Borkert*, ITRB 2018, 91 (93).
[435] Mit schweizer Perspektive *Jaccard*, JuS-Letter IT 23, November 2017, S. 13, 18 f.
[436] Vgl. S. 90 ff. sowie *Langenbucher*, AcP 218 (2018), 385 (416 ff.).
[437] Vgl. *Roth/Kieninger*, in: MüKo-BGB, § 405 Rn. 5.

Ob sich unter Heranziehung der Regeln zur Rechtsscheinhaftung oder in Analogie zu bestimmten Normen[438] ein anderes Ergebnis finden lässt, ist bislang noch nicht geklärt. Zu bedenken ist im Einzelfall, ob mit der Inhaberschaft eines Tokens ein entsprechend vertrauenswürdiger Rechtsschein verbunden ist, dass dem Inhaber auch die dort beschriebene Berechtigung zukommt. Hierfür spielt nicht nur die jeweilige Systemarchitektur, die Stabilität des Netzwerks und die Beziehung der Mitglieder untereinander eine Rolle. Insbesondere ist zu bedenken, weshalb im Einzelfall der ins Ledger geschriebenen Information mit Bezug zur rechtlichen Außenwelt Vertrauen geschenkt werden soll; warum also alleine sie die korrekte Rechtslage darstellt.[439] Der Gesetzgeber könnte freilich Blockchain-Einträgen Rechtswirkung zuerkennen, ggf. ähnlich den §§ 371a, 416a ZPO. Aufgrund der unterschiedlichen Systeme scheint jedoch zumindest eine pauschale Vermutung zu undifferenziert.[440] Den Parteien ist es freilich unbenommen, sich durch schuldrechtliche Vereinbarung an die Abbildung in der Datenbank zu binden, indem sie eine entsprechende Beweislastverteilung vereinbaren.[441]

b) Rechtsgestaltende Mittel zur Koppelung von Recht und Token

Freilich kann man sich bemühen, von vorneherein Recht und Token so aneinander zu **koppeln**, dass eine isolierte Übertragung scheitert. Die Emittenten könnten hierfür ein Regelungswerk bereitstellen, dass technische wie rechtliche Vorkehrungen trifft. In praktischer Hinsicht sollte das Recht dem grundsätzlich unveränderlichen Ledger folgen, um dessen Integrität nicht in Frage zu stellen. So könnte einerseits die Abtretung an die Zustimmung des Emittenten gekoppelt werden (§ 399 Alt. 2 BGB), die dann automatisiert bei bestätigter Tokenübertragung im Ledger erteilt wird. Möchte man hierauf nicht zurückgreifen, ließe sich nur an die Vereinbarung einer gewillkürten Form (§ 127 BGB)[442] oder eine entsprechende Bedingungskonstruktion denken, die vorsieht, dass eine Erstübertragung nur mit bestätigter Tokentransaktion wirksam ist und bei einer Zweitübertragung ohne bestätigte Tokenübertragung (auflösende Bedingung gem. § 158 Abs. 2 BGB) ihre Wirksamkeit wieder verliert.[443] Eine isolierte Übertragung des Tokens hindert das freilich nicht; jedoch dürfte der Emmittent keinem Risiko ausgesetzt sein, solange man die Tokentransaktion im Netzwerk konsequent als Abtretungsanzeige einordnet (vgl. § 409 Abs. 1 S. 1 BGB). Jedenfalls dann, wenn alle Teilnehmer untereinander dem Ledger eine entsprechende Beweiswirkung zugesprochen haben und die Geltung akzeptieren, dürfte hieran kein Zweifel bestehen, ja eventuell sogar eine schuldrechtliche Vereinbarung einer Befreiungswirkung zu sehen sein.[444]

---

[438] Vgl. zur Anwendbarkeit von §§ 793 ff. BGB *Kaulartz/Matzke,* NJW 2018, 3278 (3282 ff.); *Krüger/Lampert*, BB 2018, 1154 (1156).

[439] Kritisch *Heckelmann*, NJW 2018, 504 (507).

[440] Vgl. aber die erwähnte Regelung des US-Staates Vermont, 12 V.S.A. § 1913, siehe S. 79.

[441] Siehe S. 79.

[442] Vgl. zum möglichen Konflikt bei AGB mit § 309 Nr. Nr. 13 lit. b *Kaulartz/Matzke,* NJW 2018, 3278 (3281).

[443] *Kaulartz/Matzke,* NJW 2018, 3278 (3281).

[444] Damit die gleichen Folgen wie §§ 793 ff. BGB herbeiführend *Kaulartz/Matzke,* NJW 2018, 3278 (3283).

c) Gesellschaftsrechtliche Implikationen

Im Rahmen von ICOs[445] stellen sich einige **gesellschaftsrechtliche Probleme**, welche die Praktikabilität von Unternehmensbeteiligungen in Form von Equity Token erschweren. Eine unbeschränkte Haftung aller Gesellschafter dürfte unerwünscht sein, jedoch zeigen sich die Gesellschaften mit beschränkter Haftung als nur wenig praktikabel. Die Übertragung von Anteilen einer GmbH (§ 15 Abs. 3 GmbHG) oder von Geschäftsguthaben einer Genossenschaft (§ 76 Abs. 1 GenG) ist formbedürftig, AG-Anteile müssen in der Regel zumindest in einer Globalurkunde wertpapiermäßig verbrieft werden.[446] Bei einer KG sind Kommanditisten zum Handelsregister anzumelden (§§ 162 Abs. 1, 3, 106 Abs. 2 Nr. 1 HGB). Um einer unbeschränkte Haftung zu entgehen, bliebe nur die Gestaltung eines Treuhandverhältnisses mit den jeweiligen Komplikationen.[447]

3. Deliktischer Schutz

Ein weiterer Diskussionspunkt ist der **deliktische Schutz** von reinen Token bzw. Kryptowährungen. In Betracht kommt wohl nur die Einordnung als „**sonstiges Recht**“ im Sinne von § 823 Abs. 1 BGB. Hierfür wird teilweise auf Ansätze zum „Recht am eigenen Datenbestand“ Bezug genommen. Ob ein körperlicher oder unkörperlicher Gegenstand vorliegt, könne nicht entscheidend sein.[448] Stattdessen könne ein Recht des Inhabers des privaten Schlüssels anerkannt werden, da durch die alleinige Signaturbefugnis ein hinreichender Zuweisungsgehalt und gegenüber Dritten eine Ausschließungsmöglichkeit gegeben sei.[449] Mangels physischem Besitz könnte man zwar an dieser Einordnung zweifeln, zumal das Deliktsrecht gerade keine reinen Vermögenswerte schützen soll. Gleichwohl überzeugt es, auf Basis der Schlüsseltechnologie eine hinreichende faktische Ausschließungsbefugnis anzunehmen, die sich – ähnlich dem berechtigten Besitz nach §§ 854 ff. BGB – durch die tatsächliche Zugriffsmöglichkeit auszeichnet.[450] Die Gefahr eines uferlosen Deliktsschutzes ist nicht gegeben. Vielmehr erfolgt eine Gleichbehandlung von virtuellem mit physischen „Besitz“.[451] Somit können wertverkörpernde Token, insb. Currency Coins, aber auch Bitcoins, unter den genannten Bedingungen als sonstiges Recht im Sinne von § 823 Abs. 1 BGB zu betrachten sein.[452]

Sind **personenbezogene Daten** gespeichert, vermitteln sie ein sonstiges

[445] Siehe S. 34.
[446] Vgl. zu den Beispielen *Krüger/Lampert*, BB 2018, 1154 (1156).
[447] *Krüger/Lampert*, BB 2018, 1154 (1156) mit Verweis auf steuerrechtliche Bedenken.
[448] *Spindler/Bille*, WM 2014, 1357 (1363).
[449] Dafür auch *Spindler/Bille*, WM 2014, 1357 (1363); *Paulus/Matzke*, ZfPW 2018, 431 (453 f.).
[450] *Shmatenko/Möllenkamp*, MMR 2018, 495 (498), die ferner auf das strafrechtliche Verbot des unbefugten Zugriffs auf besonders gesicherte Daten nach § 202a StGB abstellen.
[451] *Spindler/Bille*, WM 2014, 1357 (1363). Die Argumente, beim Besitz lediglich den berechtigten Besitz zu schützen (vgl. *Wagner*, in: MüKo-BGB; § 823 Rn. 289) können mangels Eigentümer-Besitzer-Verhältnis nicht auf die Behandlung von Token übertragen werden.
[452] *Spindler/Bille*, WM 2014, 1357 (1363); *Langenbucher*, AcP 218 (2018), 385 (409); *Shmatenko/Möllenkamp*, MMR 2018, 495 (498); a.A. *Engelhardt/Klein*, MMR 2014, 355 (358): nur bei Zerstörung eines Datenträgers oder gem. § 823 Abs. 2 i.V.m. § 303a StGB.

Recht schon kraft des grundrechtlich gesicherten Rechts auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts.[453]

Hinzu kommt der (lückenhafte) Schutz nach § 823 Abs. 2 BGB i.V.m. § 303a StGB (sowie ggf. § 202a StGB).[454]

[453] *Shmatenko/Möllenkamp*, MMR 2018, 495 (498).
[454] *Shmatenko/Möllenkamp*, MMR 2018, 495 (498); *Paulus/Matzke*, ZfPW 2018, 431 (453).

IX. Regulierungsfragen (Überblick)

1. Know Your Costumer (KYC) und Anti Money Laundering (AML)

Einige Regelungsbereiche machen es erforderlich, dass zumindest einem der Netzwerkteilnehmer die Identitäten der anderen bekannt sind. Insbesondere bei größeren Anlage- und Finanzprodukten sind in der Regel die Intermediäre verpflichtet, die Identität ihrer Kunden zu überprüfen und diese zu speichern (**Know Your Customer** – KYC).[455] Solche Pflichten ergeben sich etwa aus der unionsrechtlichen **Geldwäsche-Richtlinie**[456] (Art. 2 Abs. 1, Art. 13 Abs. 1 lit. a–c) und werden durch Überprüfungs- (Art. 13 lit. d) und Meldepflichten (Art. 33, 34) ergänzt, sog. Customer Due Diligence. Nach dem deutschen Geldwäschegesetz (GwG) treffen die fraglichen Pflichten (§§ 10 ff.) alle Emittenten von Token, die als Finanzdienstleistungsinstitute zu qualifizieren sind (§ 2 Abs. 1 Nr. 2 GwG i.V.m. § 1 Abs. 1a KWG).[457] Die KYC-Prozesse können und sollten dabei bereits von vorneherein in ein DL-System integriert werden. Hierfür bedarf es jedoch besonderer vertrauenswürdiger Stellen, welche die Identität bzw. Integrität validieren können.[458] Werden öffentliche Stellen eingebunden, könnten sich die Nutzer schlicht diesen gegenüber ausweisen. Am besten ließen sich die geseztlichen Vorgaben jedoch gewährleisten, wenn es gelingt, eine sichere digitale Identität zu entwickeln, die mit hinreichender Vertraulichkeit entsprechende Nachweise plattformübergreifend erbringen kann.

In jedem Fall müssen die geltenden Regularien beachtet und ein Austausch mit den zuständigen Behörden betrieben werden, um **rechtskonforme Systeme** zu errichten. Sollte ein System etwa auch die Option beinhalten müssen, dass eine staatliche Autorität oder ein Intermediär auf deren Anweisung verdächtige Zahlungen einfrieren kann, wie es die Geldwäsche-Richtlinie in Art. 35 vorsieht, könnte das seine Vorteile gegenüber den heutigen Systemen allerdings in Frage stellen.[459]

2. Aufsichtsrechtliche Fragestellungen

Wie bereits erwähnt werfen sog. Kryptowährungen wie auch der Verkauf verschiedentlicher Token im Rahmen von ICOs zahlreiche **aufsichtsrechtliche Fragen** auf. Es ist etwa umstritten, ob Kryptowährungen als **Finanzinstrumente** in Form von Rechnungseinheiten (§ 1 Abs. 11 Nr. 7 KWG) zu qualifizieren sind, was u.a. eine Erlaubnispflicht für den gewerblichen Han-

[455] *Reed/Sathyanarayan/Ruan/Collins*, S. 12.
[456] Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.
[457] *Weitnauer*, BKR 2018, 231 (235).
[458] *Reed/Sathyanarayan/Ruan/Collins*, S. 14.
[459] *Reed/Sathyanarayan/Ruan/Collins*, S. 20.

del oder Betrieb einer Plattform nach sich zöge.[460] Sowohl die **BaFin**[461] wie auch mittlerweile die Bundesregierung nahmen eine entsprechende Einordnung vor.[462] In einem viel beachteten Urteil vertrat das KG Berlin eine ablehnende Auffassung. Nach dem KG fehle es insbesondere an der Vergleichbarkeit mit Devisen, da keine staatliche Garantie für die Stabilität der Werte existiert.[463] Für die Praxis ist jedoch zu beachten, dass es sich um eine strafrechtliche Entscheidung handelte, die im Lichte des Bestimmtheitsgebots (Art. 103 Abs. 2 GG) bei strafrechtlichen Sanktionen getroffen wurde und für die Verwaltungspraxis der BaFin keine Bindung hat. Die BaFin hat bereits signalisiert, weiter an ihrer Rechtsauffassung festhalten zu wollen.[464] Wirkliche Klarheit herrscht daher nach wie vor nicht, auch wenn die wohl herrschende Meinung in der Literatur bislang den Erwägungen der BaFin folgt.[465] Sollten jedoch Anteile verkauft oder mit dem Token Genussrechte als Vermögensanlage verkörpert werden, wurde darauf hingewiesen, dass u.U. abweichende Maßstäbe anzulegen wären.[466]

Damit verwandt sind einige **kapitalmarktrechtliche Fragen**, insb. zur regulatorischen Einordnung von ICOs. Hierbei ist insbesondere entscheidend, ob sich das jeweilige Token als Wertpapier i.S.v. § 2 Abs. 1 WpHG sowie § 2 Nr. 1 WpPG einordnen lässt, wobei das zumindest für Currency Token einhellig abgelehnt wird.[467] Die Einordnung als Wertpapier hätte dabei gleichsam die Anwendbarkeit des KWG zur Folge, da diese als Finanzinstrument i.S.v. § 1 Abs. 11 Nr. 1 bis 4 KWG gelten.[468] Schließlich sind die besonderen Anlegerschutzvorschriften des KAGB wie auch subsidiär des VermAnlG zu prüfen.[469]

---

[460] Vgl. zur Übersicht *Weitnauer*, BKR 2018, 231 (233 f.) sowie die Hinweise der BaFin unter https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html.

[461] BaFin Journal, Mitteilungen der Bundesanstalt für Finanzdienstleistungsaufsicht, 2016, abrufbar unter https://www.bafin.de/DE/PublikationenDaten/BaFinJournal/AlleAusgaben/bafinjournal_alle_node.html.

[462] BT-Drs. 19/2452, S. 5; BT-Drs. 17/14530, S. 41.

[463] KG, Urteil vom 25.9.2018 – (4) 161 Ss 28/18 (35/18) = NJW 2018, 3734 ff., mit zust. Anm. *Lehmann*; i.E. ebenso *Froitzheim*, BKR 2018, 473 (476); krit. etwa *Patz*, MMR 2018, 828 (830 ff.).

[464] Vgl. *Holtermann,* abrufbar unter: www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrungen-bitcoin-laut-olg-urteil-keine-rechnungseinheit-bafin-ueberschritt-kompetenzen/23192036.html%3fticket=ST-1570639-T1ezGsLzuFiVWSZBeVlk-ap2.

[465] Vgl. nur *Spindler/Bille*, WM 2014, 1357 (1361 f.); *Weitnauer*, BKR 2018, 231 (233); *Patz*, MMR 2018, 828 (830) m.w.N.

[466] *Lehmann*, NJW 2018, 3734 (3737) (Anm. zu BGH, NJW 2018, 3734).

[467] Vgl. zum Ganzen *Langenbucher*, AcP 218 (2018), 385 (418 ff.); *Weitnauer*, BKR 2018, 231 (233 f.).

[468] *Weitnauer*, BKR 2018, 231 (233).

[469] Vgl. *Weitnauer*, BKR 2018, 231 (234 f.).

X. DLT-Systeme und das Gesellschaftsrecht

An der Schnittstelle zwischen Blockchain und dem **Gesellschaftsrecht** stellen sich zahlreiche Rechtsfragen, von denen hier nur einige wenige angedeutet werden können. Diskutiert wurde insbesondere, ob der Verbund der Blockchain-Teilnehmer selbst eine Gesellschaft darstellt.

1. Öffentliche und zulassungsfreie Blockchain

In einer öffentlichen, zulassungsfreien Blockchain wird das Netzwerk der Öffentlichkeit vom Entwickler zur Verfügung gestellt, ohne dass er sich oder einer zentralen Stelle Einfluss über die Teilnahme und Inhalte vorbehält. Jeder kann als gleichberechtigter Teilhaber beitreten und das Netzwerk nutzen. Eine **Gesellschaft** würde in der einfachsten Form der GbR (§§ 705 ff. BGB) nach herrschender Auffassung erfordern, dass von den Teilnehmern ein gemeinsamer Zweck verfolgt und dessen Förderung durch Rechtsgeschäft als verbindliche Aufgabe aller Teilnehmer festgeschrieben wird.[470] Die Teilnehmer eines Blockchain-Netzwerks verfolgen jedoch weder einen gemeinsamen Zweck noch besteht ein übereinstimmender Wille zur verbindlichen Förderung. Sie sind sich weder gegenseitig bekannt noch liegt, über die Nutzung des Netzwerks im eigenen Interesse hinaus, ein verbindender Faktor vor, der es zuließe, eine rechtsverbindliche Vereinbarung anzunehmen.[471] Damit ist das Netzwerk keine Gesellschaft im Sinne des § 705 BGB.

2. Konsortial-Blockchain

Differenzierter gestaltet sich die Rechtslage, wenn sich mehrere Unternehmen zu einem Konsortium zusammenschließen und als gleichberechtigte Teilnehmer einer Blockchain mitwirken. Ein verbindendes Band bzw. ein gemeinsamer Wille scheinen hier vorhanden zu sein. Doch letztlich ist es vom Einzelfall abhängig, inwieweit über die bloße Nutzung des Netzwerks heraus gesellschaftsrechtliche Pflichten im Außenverhältnis begründet werden sollen. Insbesondere wenn die Unternehmen nach außen weiter nur für sich auftreten, die Konsortial-Blockchain hingegen als eigenständiges, dezentrales Netzwerk ohne feststehende Entscheidungsgewalt einsetzen, könnte es auch völlig an einer Gesellschaft fehlen. Anstelle einer Innengesellschaft könnte möglicherweise auch nur ein multipolar-mehrseitiger Vertrag vorliegen.[472]

3. „The DAO"

Die Frage nach der Einordnung der **DAO** stellt sich nur hypothetisch.[473] Mangels der Bestellung eines organschaftlichen Vertreters, der Eintragung

[470] *Schäfer,* in: MüKo-BGB, § 705 Rn. 1, ggf. auch durch schlüssiges Handeln.

[471] *Schwintowski/Klausmann/Kadgien*, NJOZ 2018, 1401 (1404) mit dem Vergleich zur Nutzung eines öffentlichen Guts.

[472] Vgl. zum Begriff *Zwanzger*, Der mehrseitige Vertrag, S. 9 ff. bzw. zur Abgrenzung zum Gesellschaftsrecht S. 99 ff.

[473] Vgl. hierzu bereits S. 37 f.

im Handelsregister oder der Einhaltung eines besonderen Gründungsverfahrens dürfte in der Regel zumindest keine Kapital-, sondern alleine eine Personengesellschaft in Betracht kommen; es sei denn, man schaltet zwischen DAO und Kapitalgeber eine weitere Gesellschaft.[474] Im schon erwähnten Fall von „The DAO" griffen die Initiatoren auf eine schweizer Gesellschaft zurück, die im Außenverhältnis als Treunehmer tätig werden sollte.[475]

Käme erneut ein Projekt einer DAO zustande, wäre die Beurteilung des Falles schwierig. Ob schon in einer Zahlungsleistung an die Gesellschaft der Schluss eines Gesellschaftsvertrags gesehen werden kann, erscheint zumindest zweifelhaft; insb. dürfte ein Wille zur verbindlichen Übernahme von Förderpflichten über die einmalige Zahlung hinaus fehlen.[476] Das Risiko, mit allen Folgen als eine Gesellschaft bürgerlichen Rechts eingeordnet zu werden, muss von den Teilnehmern dennoch ebenso sorgfältig bedacht werden, wie von den Gründern bzw. Initiatoren.[477]

4. Anwendbares Recht

Eine übergeordnete Frage bildet die Suche nach dem **anwendbaren Recht**. Die herkömmlichen Theorien werden dabei insbesondere durch die angestrebte Dezentralität an ihre Grenzen gebracht.[478] In das eigentliche Spannungsverhältnis zwischen Gründungs- und Sitztheorie, die jeweils an den Ort der Gründung bzw. den Sitz einer Gesellschaft anknüpfen,[479] kann ein dezentral agierender, ohne rechtliche Fixierung in einem Gründungsstaat errichteter Verbund nicht ohne weiteres eingeordnet und damit einem Gesellschaftsrechtsstatut unterstellt werden.[480] Diese Schwierigkeiten stellen sich freilich nur bei echten dezentralen Netzwerken. Erfolgt eine zentralisierte Verwaltung oder Koordinierung im Rahmen eines Konsortiums, kann auf die eine oder andere Weise an diesen Punkt angeknüpft werden.[481] Ob sich der Tätigkeitsbereich eines dezentralen Verbunds einem Unternehmen und dessen Rechtsstatus zurechnen lässt oder welche Anknüpfungspunkte sonst gefunden werden können, sind Fragen des Einzelfalls. Während in Netzwerken wie beim Bitcoin eine Zergliederung auf einzelne Streitfälle möglich ist, wird ein völlig dezentraler Ansatz nach dem Vorbild der „DAO" völlig eigene Fragen aufwerfen. Nach dem prominenten Scheitern von „The DAO" sind noch keine erfolgreichen Umsetzungen bekannt. Jedenfalls dürfte letztlich mit dem Rechtsverweigerungsverbot jedenfalls auf die Auffangregelung des *lex fori* zurückzugreifen sein.[482]

[474] *Mann*, NZG 2017, 1014 (1017 f.).
[475] *Mann*, NZG 2017, 1014 (1018).
[476] Dafür *Mann*, NZG 2017, 1014 (1018); zweifelnd *Langenbucher*, AcP 218 (2018), 385 (422 f.).
[477] Zu weiteren Fragen bei der Gründung und Kapitalaufbringung *Langenbucher*, AcP 218 (2018), 385 (423 ff.).
[478] Vgl. *Simmchen*, MMR 2017, 162 (165).
[479] Zum grundsätzlichen Vorrang der Sitztheorie nach deutschem Recht statt vieler BGHZ 97, 269, 272 = NJW 1986, 2194 (2195).
[480] *Simmchen*, MMR 2017, 162 (164 f.); *Zimmermann,* IPRax 2018, 566 (568 ff.).
[481] Vgl. *Zimmermann,* IPRax 2018, 566 (569 f.).
[482] So *Zimmermann,* IPRax 2018, 566 (56 ff.).

XI. Datenschutz und Blockchain

Trotz der von der DS-GVO ausdrücklich (vgl. Erwägungsgrund 15) angestrebten Technologieneutralität offenbart die Gegenüberstellung mit der Distributed-Ledger-Technologie einige Schwierigkeiten.

1. Sachlicher Anwendungsbereich (Art. 2 Abs. 1 DS-GVO)

Der **sachliche Anwendungsbereich** der DS-GVO[483] ist gem. Art. 2 Abs. 1 auf die Verarbeitung personenbezogener Daten beschränkt.

a) Verarbeitung (Art. 4 Nr. 2 DS-GVO)

Eine **Verarbeitung** liegt bei jedem Vorgang im Zusammenhang mit personenbezogenen Daten, von der Erhebung bis zur Löschung, vor.[484] Der Anwendungsbereich ist in dieser Hinsicht denkbar weit gefasst. Jedes Abspeichern in einem DL, jedes Auslesen sowie bereits weiterverarbeitende Schritte wie das Bündeln in Blöcken fällt darunter.[485]

b) Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)

Nach Art. 4 Nr. 1 DS-GVO ist ein **Personenbezug** gegeben, wenn sich die Daten auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl. auch Erwägungsgrund 26). Enthält ein Ledger dementsprechend reine Unternehmensdaten, die keinerlei Rückschlüsse auf daran beteiligte Personen erlauben, etwa reine Maschinendaten oder organisatorische Details, findet die DS-GVO keine Anwendung.

Umstritten ist, auf wessen Erkenntnismöglichkeiten es dabei ankommen soll. Nach der absoluten Theorie reicht es aus, dass irgendjemand den Personenbezug herstellen kann. Die **relative Theorie** bezieht sich demgegenüber auf die verantwortliche Stelle.[486] Der EuGH hat sich letzterer Ansicht angeschlossen.[487] Grundsätzlich sind nach dem Urteil auch Daten Dritter einzubeziehen, falls der Verantwortliche diesen gegenüber einen Rechtsanspruch hat, die Informationen einzusehen. Hierzu zählen auch staatliche Auskunftsansprüche, zum Beispiel im Fall von Urheberrechtsverletzungen oder Straftaten.[488] Gemäß Erwägungsgrund 26 sollen bei der Ermittlung der Identifizierungsmöglichkeiten der verantwortlichen Stelle objektivierte Maßstäbe angelegt werden.[489] Zusammengefasst liegt für denjenigen ein

[483] Vgl. zum weit gefassten räumlichen Anwendungsbereich Art. 3 DS-GVO.
[484] *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO, Art. 2 Rn. 13.
[485] Vgl. auch Fraunhofer FIT, S. 126 f.
[486] Zum Meinungsstreit *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO, Art. 4 Nr. 1 Rn. 25 f.
[487] *EuGH*, ECLI:EU:C:2016:779 = ZD 2017, 24 m. Anm. *Kühling/Klar* – Breyer im Hinblick auf IP-Adressen.
[488] Vgl. *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO, Art. 4 Nr. Rn. 28.
[489] *Erbguth/Fasching*, ZD 2017, 560 (562).

Personenbezug vor, der „über das notwendige Zusatzwissen verfügt, um sie mit verhältnismäßigen Mitteln einer bestimmten Person zuzuordnen.“[490]

Bei einer zulassungsbeschränkten Blockchain existiert von vorneherein eine Stelle, die über die Vergabe der Nutzer-ID entscheidet und somit eine Zuordnung zur dahinterstehenden Person vornehmen kann.[491]

In der Regel sind Teilnehmer einer öffentlichen Blockchain demgegenüber zunächst nur über ihren öffentlichen Schlüssel zu identifizieren (pseudonym).[492] Diese Pseudonymität kann jedoch in der Regel mit verhältnismäßigen Mitteln überwunden werden. Imn vielen Fällen wird die Pseudonymisierung bereits durch den Nutzer selbst aufgehoben, indem er seine Identität freiwillig Vertragspartnern oder anderen Teilnehmern bekannt gibt. Die jeweilige Stelle kann dann auch spätere Transaktionen ohne weiteres dem jeweiligen Nutzer zuordnen.[493] Greift der Nutzer auf Kryptowährungstausch oder -börsen zurück, führt die damit verbundene Identifizierungspflicht (Know-Your-Customer) auch zu einer Identifizierbarkeit.[494] In den übrigen Fällen besteht die praktische Erreichbarkeit häufig über technische oder rechtliche Hilfsmittel. Neben Transaktionstracking[495] oder der Datenanalyse, insb. unter Zuhilfenahme bestimmter Big-Data-Analysetools,[496] ermöglichen zudem rechtliche Auskunftsansprüche (bei der Durchsetzung von Verträgen) potentiell die spätere Zuordnung der Daten zur Person.[497] Eine ausreichende mittelbare Identifikation erscheint daher in vielen Fällen möglich.

Die Überlegungen zeigen, dass ein Personenbezug auch trotz Pseudonymisierung in vielen Fällen in Betracht kommen wird. Aufgrund der Relativität muss die Frage aber im Einzelfall beantwortet werden, wobei auch die Leseberechtigung der jeweiligen Stelle sowie die Unterschiede zwischen den Distributed-Ledger-Modellen Berücksichtigung finden müssen. Neuere Blockchains wie Monero und Zcash verwenden Protokolle, bei denen die Identität einer Adresse angeblich gänzlich anonymisiert ist.[498] Enthält eine Blockchain andererseits überhaupt keine auslesbaren Informationen, dürfte ebenfalls kein Personenbezug gegeben sein. Dies wäre etwa der Fall, wenn man anstelle der Daten nur deren Hash-Werte speichert. Mithilfe der Hash-Funktion könnte man so zwar als Besitzer des Originaldokuments

[490] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253) mit Verweis auf *EuGH*, ECLI:EU:C:2016:779 = ZD 2017, 24 m. Anm. *Kühling/Klar* – Breyer.

[491] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).

[492] Aus diesem Grund eher gegen Personenbezug bei *permissionless* Blockchains *Schrey/Thalhofer*, NJW 2017, 1431 (1433).

[493] *Bechtolf/Vogt*, ZD 2018, 66 (69).

[494] *Bechtolf/Vogt*, ZD 2018, 66 (69). Aktuelle Pläne der EU-Kommission, die Börsen zur Erfassung und Speicherung der Nutzeridentität zu verpflichten, könnten sich unmittelbar auswirken vgl. *Erbguth/Fasching*, ZD 2017, 560 (562).

[495] Da z.B. ein *Node* stets eine feste Zusammensetzung benachbarter Teilnehmer (i.d.R. acht, sog. *entry Nodes*) hat, kann über diese ein digitaler Fingerabdruck erstellt werden, vgl. hierzu und bezüglich technischer Verfahren des Trackings *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2103 ff.).

[496] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2107). Allgemein zu Big-Data-Analysen *Brisch/Pieper*, CR 2015, 724 (727 ff.).

[497] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253); *Bechtolf/Vogt*, ZD 2018, 66 (69). Es sind Fälle bekannt, in denen Ermittlungsbehörden den Nutzer hinter einer Bitcoin-Adresse herausfinden konnten, *Voshmgir*, S. 13.

[498] *Voshmgir*, S. 13.

dessen Echtheit verifizieren, nicht aber den gehashten Text zurückübersetzen.[499]

2. Verantwortliche Stelle

Der **persönliche Anwendungsbereich** im Hinblick auf die Erfüllung der in der DS-GVO beschriebenen Pflichten wird definiert durch den Begriff des **Verantwortlichen** (Art. 4 Nr. 7 DS-GVO): Verantwortlicher ist, wer eine faktische Bestimmungsmacht innehat, indem er allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.[500] Zweck bedeutet die Festlegung des erwarteten Ereignisses als Ziel der Verarbeitung oder Speicherung, Mittel die Art und Weise, wie das Ziel erreicht werden soll.[501] Von zentraler Bedeutung ist daher die Entscheidungsgewalt.

Soweit ein Personenbezug gegeben ist, treffen die verantwortliche Stelle zahlreiche **Pflichten**: Art. 5 DS-GVO regelt die Grundsätze für die Verarbeitung personenbezogener Daten. Nach Art. 6 DS-GVO bedarf jede Verarbeitung und Speicherung durch eine verantwortliche Stelle einer entsprechenden Verarbeitungsgrundlage,[502] was auch die für den Betrieb einer Blockchain erforderliche Verarbeitung durch Miner und Nodes erfasst.[503] Zudem müssen mit anderen die Daten verarbeitenden Stellen ggf. Auftragsverarbeitungsverträge geschlossen werden, Art. 28 Abs. 3 DS-GVO. Ferner stehen dem Nutzer diverse Rechte nach den Art. 12 ff., insb. das sog. Recht auf Vergessenwerden aus Art. 17 DS-GVO zu.

Der Unionsgesetzgeber nahm an, die Verantwortung für die Datenverarbeitung lasse sich stets einer Person oder gemeinschaftlich handelnden Personengruppe zuschreiben (Erwägungsgrund 79).[504]

Dabei erweist sich weniger das Eingeben von Daten als problematisch: Entweder betreffen die jeweiligen Daten bereits die sie speichernde Person oder die Stelle benötigt eine entsprechende Rechtfertigung.[505] Schwieriger zu beurteilen sind die Verarbeitungsvorgänge im Ledger selbst, also die Gestaltung der Blöcke sowie der Blockkette und ähnliche Vorgänge. Die dezentrale Struktur, insbesondere zulassungsfreier Blockchains, werfen dabei einige Fragen auf.

---

[499] Ob in einigen Fällen doch personenbezogene Daten vorliegen, ist offen und zudem systemabhängig. Größere Sicherheit erhält man mit „Salted Hashes“: Zu den Eingabedaten wird eine zufällige Zeichenfolge (salt) zu den zu verschlüsselnden hinzugefügt, um so auszuschließen, dass jemand, der mögliche Eingaben kennt, im „Trial and Error“-Verfahren die richtigen Daten errät.

[500] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253).

[501] *Wagner*, ZD 2018, 307 (309).

[502] Vgl. zur Verarbeitung von Daten Dritter Fraunhofer FIT, S. 142 f.

[503] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253); *Hofert*, ZD 2017, 161 (164 ff.), der jedoch nur auf die Verarbeitung durch Miner abstellt und die Speicherung durch die *Nodes* übersieht.

[504] *Bechtolf/Vogt*, ZD 2018, 66 (69).

[505] Fraunhofer FIT, S. 133.

a) Zulassungsfreie Blockchains

Die **Verantwortlichkeit für eine zulassungsfreie Blockchain** ist in der Literatur hoch umstritten. Im Folgenden sollen vor allem einige Kritikpunkte an gegenwärtig in der Literatur zu findenden Auffassungen aufgezeigt werden; eine finale Klärung wird es (wenn) nur durch den EuGH oder den Unionsgesetzgeber geben.

aa) Entwickler Der **Entwickler** der Blockchain initiiert und programmiert das System, gibt den Betrieb des Netzwerks anschließend jedoch aus der Hand. Der Betrieb und damit die eigentlichen Datenverarbeitungsvorgänge haben mit der eigentlichen Entwicklung nichts mehr zu tun. Auf die später zu speichernden und verarbeitenden Inhalte nehmen Entwickler keinen Einfluss, sodass eine Einorndung als Verantwortlicher ausscheidet.[506]

bb) Miner Die **Miner** sind zwar für die Errechnung neuer Blöcke zuständig, nehmen aber auf deren Inhalt keinen Einfluss. Selbst wenn ein Miner wollte, könnte er allein den Inhalt eines Blocks nicht modifizieren, da er von den übrigen Teilnehmern verworfen werden würde.[507] Sie nehmen damit faktisch dieselbe Rolle wie ein Telekommunikationsdienste-Anbieter ein, die ebenfalls nicht als verantwortliche Stelle gelten.[508]

cc) Nodes

(1) Einzelner Node Jedoch könnte nach einer Ansicht schon grundsätzlich **jeder vollwertig teilnehmende Rechner** (*Full*-Node)[509] Verantwortlicher sein, indem er Transaktionen vornimmt (Verarbeitung vorhandener und Verteilung neuer Daten) oder die veränderte Blockchain als lokale Kopie abspeichert und dabei auch Veränderungen vornehmen kann.[510] Als

[506] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253). Ein Hard Fork, also eine vom Entwickler vorgeschlagene Änderung der alten Chain, ändert nicht die gespeicherten Daten, sondern beginnt einen völlig neuen Datensatz. Zudem wäre das Fortleben abhängig davon, welcher Blockchain-Version die Teilnehmer folgen. Unklar ist hingegen die Argumentation der französischen Datenschutzbehörde CNIL, La Blockchain, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, dazu nachfolgend.

[507] *Erbguth/Fasching*, ZD 2017, 560 (563).

[508] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253); *Janicki/Saive*, ZD 2019, 251 (253). Andere Auffassung wohl nur Hofert, ZD 2017, 161 (164) im Hinblick auf die Verantwortlichkeit nach dem BDSG, der letztlich jedoch die Ausnahme nach § 28 Abs. 1 BDSG für einschlägig erachtet.

[509] *Light-Nodes* speichern lediglich Referenzen (*Hashes*) und nehmen keine eigenen Verarbeitungsschritte vor.

[510] *Schrey/Thalhofer*, NJW 2017, 1431 (1433 f.); *Pesch/*Sillaber, CRi 2017, 166 (169 f.); *Martini/Weinzierl*, NVwZ 2017, 1251 (1253) mit weiterem Vergleich zur EuGH-Rechtsprechung zur Funktion von Suchmaschinen. Ebenso, wenn auch kritisch zur Zweckhaftigkeit *Bechtolf/Vogt*, ZD 2018, 66 (69).

eigenes Interesse sei dabei zumindest die Teilnahme am Netzwerk zu nennen.[511] Dies gehe jedenfalls über das bloße – nicht für die Qualifikation als Verantwortlicher ausreichende – Betreiben eines Servers hinaus.[512]

Dabei ist aber schon grundsätzlich zwischen Node und Nutzer zu unterscheiden. Auch ist zu berücksichtigen, dass nach der Funktionslogik eines Blockchain-Netzwerks ein Rechner, der inhaltlich von der Mehrheit der übrigen Nodes abweicht, ignoriert wird. Eine Einflussnahme auf die gespeicherten Daten käme dem Abschalten des Knoten gleich.[513] Er kann damit nicht über die Zwecke und Mittel der Verarbeitung der auf der Blockchain gespeicherten Daten entscheiden. Als Teilnehmer des Peer-to-Peer-Netzwerks ist er dessen Konsensmechanismus unterworfen, der für alle Teilnehmer festlegt, welche Zwecke und Mittel die Verarbeitung hat. Solange er dem Netzwerk folgt, kann er also nicht Mittel und Zweck der Verarbeitung bestimmen.[514]

Freilich könnte man auch umgekehrt argumentieren, dass gerade die Entscheidung für die Verarbeitung entsprechend der Netzwerkregeln eine Bestimmung über Zwecke und Mittel darstelle.[515] Jeder Nutzer wäre demnach für sich gesehen Verantwortlicher. Erwägungsgrund 79 der DS-GVO hilft – mit seiner Betonung des Ziels klare Verantwortlichkeiten festzuschreiben – nur weiter, wenn man ihn so versteht, dass jeder Verarbeitungsvorgang zwanghaft einer Person zugeordnet werden muss und die Verantwortungsfrage nicht offen blieben darf.[516] In einem dezentralen Netzwerk ohne zentrale Verantwortlichkeit hieße das, man müsste stets die noch am ehesten mit dem Vorgang zusammenhängende Stelle verantwortlich machen, selbst wenn ihr kein bestimmender Einfluss zukommt.[517]

Diese Herangehensweise erscheint zweifelhaft, zumal nicht zwangsläufig ein besserer Schutz personenbezogener Daten erreicht wird. Es entstünde wohl keine auf die Person des Nodes-Betreibers bezogene Schutzlücke. Soweit dieser nämlich die Daten noch zu anderen Zwecken ausliest, speichert oder verarbeitet, bestimmt er über diesen Verarbeitungsvorgang und gerät ohne weiteres in der Rolle des Verantwortlichen i.S.d. DS-GVO.[518] Im Übrigen sollte der bloß teilnehmende Node jedoch nicht als Verantwortlicher angesehen werden.[519] Letztverbindlich wird die Frage jedoch nur der EuGH beantworten können, wenn keine Anpassung der Verordnung erfolgt.

(2) Gemeinsame Verantwortlichkeit Dennoch könnte die Einordnung der Gesamtheit der Nodes-Betreiber als **gemeinsam Verantwortliche** im

[511] *Martini/Weinzierl*, NVwZ 2017, 1251 (1253). Nach Art. 2 II Buchst. c DS-GVO finden jedoch für ihn die Regeln der DS-GVO keine Anwendung, soweit die Teilnahme rein persönlichen oder familiären Zwecken dient.
[512] Vgl. *Erbguth/Fasching*, ZD 2017, 560 (563).
[513] *Erbguth/Fasching*, ZD 2017, 560 (563).
[514] *Erbguth/Fasching*, ZD 2017, 560 (563); *Böhme/Pesch*, DuD 2017, 473 (475, 478 f.).
[515] Fraunhofer FIT, S. 135
[516] Mit diesem Verständnis *Janicki/Saive*, ZD 2019, 251 (253).
[517] *Erbguth/Fasching*, ZD 2017, 560 (563).
[518] *Wagner/Groß*, S. 19; *Böhme/Pesch*, DuD 2017, 473 (479) sowie sogleich.
[519] So auch noch *Janicki/Saive*, ZD 2019, 251 (254); a.A. Fraunhofer FIT, S. 135.

Sinne von Art. 26, Art. 4 Nr. 7 DS-GVO in Betracht kommen.[520] Nach Art. 26 Abs. 1 S. 1 DS-GVO ist dabei allerdings erforderlich, dass sich die Nodes gemeinsam auf einen bestimmten Zweck der Teilnahme verständigen.[521] An einer solchen Absprache dürfte es in der Regel fehlen; vielmehr folgt der Konsens aus einem selbständigen Verhalten der einzelnen Knoten bzw. ist auf den Konsensmechanismus des Netzwerksprotokolls zurückzuführen.[522] Allein ein Mining-Pool, also ein Verbund von Minern, dessen Netzbeteiligung 50 % übersteigt, könnte den Inhalt frei verändern und dementsprechend als verantwortliche Stelle einzustufen sein.[523] Gleichwohl würde das dem Netzwerkvertrauen und damit der Grundidee von DLT-Systemen zuwiderlaufen, sodass ein solche Zusammenschluss praktisch nicht zu erwarten ist.[524]

dd) Individueller Nutzer infolge einer Transaktion Schließlich wird vertreten, man solle alleine auf den Transaktionsvorgang abstellen und dabei jeden Nutzer, der eine **Transaktion auslöst**, als für diesen bzw. die folgenden Vorgänge Verantwortlichen i.S.d. DS-GVO einstufen.[525] Er leite durch seine Signatur der Transaktion einen Vorgang ein, der die Blockchain inhaltlich beeinflusst und, soweit er über ein entsprechendes Guthaben verfügt, auch nicht von den Nodes oder Minern verworfen werden kann. Hierdurch bestimme er den Zweck und die Mittel der Datenverarbeitung. Soweit daher die Ausnahme der rein zu privaten oder familiären Zwecken erfolgenden Nutzung (Art. 2 II Buchst. c DS-GVO) nicht einschlägig ist, wäre nach dieser Ansicht jeder Nutzer gleichzeitig Verantwortlicher. Eine gemeinsame Verantwortlichkeit liege aber auch hier nicht vor, da es an einer entsprechenden Absprache grundsätzlich fehle, während eine mögliche Weiterverarbeitung in einem eigenen Verantwortungsbereich erfolge.[526]

(1) Kritik Sofern eine Stelle weder rechtlichen noch tatsächlichen Einfluss auf die Art und Weise der Verarbeitung der Daten hat, kann sie laut der Artikel-29-Datenschutzgruppe hierfür keine datenschutzrechtliche Verantwortung tragen.[527] Der Nutzer beeinflusst nur einen Teil der Blockchain, nämlich die eigene Transaktionshistorie und die des Empfängers. Er setzt zwar den Ursprung für die Schaffung eines neuen Blockinhalts; sein Beitrag erschöpft sich insoweit jedoch in der Nutzung des bereitgestellten Systems.[528] Er handelt letztlich nicht anders als jemand, der bei einem automatisierten Bestellsystem eine Ware anfragt oder als Nutzer eines sozialen Netzwerks einen Status postet. Auch hier löst er durch seinen Input eine

[520] In diese Richtung *Bechtolf/Vogt*, ZD 2018, 66 (69); *Beck,* DVP 2018, 251 (254); *Pesch/*Sillaber, CRi 2017, 166 (170), die im Folgenden (171) jedoch wesentliche Teile der Rechtsfolgen als unverhältnismäßig einschränken.

[521] *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO, Art. 26 Rn. 12 u. 20: Notwendig ist zwar nicht einer Vereinbarung iSv Art. 26 Abs. 1 S. 2, wohl aber irgendeine Form kollaborativen Entscheidung.

[522] *Erbguth/Fasching*, ZD 2017, 560 (563); *Böhme/Pesch*, DuD 2017, 473 (479); *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO, Art. 26 Rn. 15.

[523] *Erbguth/Fasching*, ZD 2017, 560 (564).

[524] *Erbguth/Fasching*, ZD 2017, 560 (564).

[525] *Erbguth/Fasching*, ZD 2017, 560 (564); ähnlich *Janicki/Saive*, ZD 2019, 251 (254).

[526] *Janicki/Saive*, ZD 2019, 251 (254).

[527] Vgl. *Artikel-29-Datenschutzgruppe*, WP 169, S. 15 f.

[528] Vgl. zu den Bedenken *Wagner*, ZD 2018, 307 (309).

Berechnung (Transaktion) aus. Die Verarbeitung der Daten erfolgt hingegen durch den Betreiber des Bestellsystems und nach dessen Regeln. Im Falle der Blockchain tritt an diese Position die Gesamtheit des Netzwerks. Dem Netzwerk kann jedoch nicht als solchem die Verantwortlichkeit zugeschrieben werden. Der Nutzer hat weder die notwendige Kontrollmöglichkeit, um auf die rechnenden Nodes einzuwirken, noch delegiert er eine eigene Kompetenz, sodass auch nicht von einer Auftragsverarbeitung gesprochen werden kann.[529] Die Konsequenzen der soeben beschriebenen Ansicht muten auch merkwürdig an: Dass sich die Miner tatsächlich dem Nutzer unterordnen, entspricht nicht der Funktionslogik dezentraler Systeme. Dennoch müsste man eine Art Auftragsverarbeitungsvertrag mit ständig wechselnder Rollenverteilung auf Basis des Systemcodes fingieren, um die nachfolgende Verarbeitung durch die Miner und die Validierung durch andere Nodes zu rechtfertigen.[530] Offen bleibt die Frage: Sind die Transaktionsauslöser dann tatsächlich nur für den jeweiligen Teil eines Blockes (bzw. dessen Berechnung und Speicherung) verantwortlich, sodass schon für einen Block bei Bitcoin bis zu 2.500 Verantwortliche auszumachen wären?

(2) Berücksichtigung der EuGH-Rechtsprechung? Auch der EuGH betonte in seinem Urteil zu Facebook-Fanseiten, dass die bloße Nutzung eines Netzwerks den Nutzer nicht für die Verarbeitung durch den Netzwerkbetreiber mitverantwortlich macht.[531] Etwas anderes könne ausnahmsweise gelten, wenn der Nutzer eine eigenständige Verarbeitungsebene schafft. Betreibt ein Nutzer eine Fanseite, so schafft er einen vom Netzwerkbetreiber abgrenzbaren Verantwortungsbereich.[532] Auf die Regeln innerhalb des Bereichs kann er unmittelbaren Einfluss nehmen, indem er Mittel und Ziele der Datenverarbeitung durch den Netzwerkbetreiber anhand von Konfigurationsparametern bestimmt.[533] Diese Option fehlt einem Blockchain-Nutzer vollständig. Er schafft auch keine eigenständige Verarbeitungsebene, sondern nutzt nur die Gesamtstruktur des Netzwerkes.

(3) Zwischenfazit Der Unionsgesetzgeber hat die Möglichkeit eines dezentralen Netzwerks nicht bedacht bzw. wollte bewusst keine besondere Regelung integrieren. Er ging davon aus, dass für jede Verarbeitung stets eine natürliche Person oder Stelle verantwortlich ist (vgl. Erwägungsgrund 79).[534] Nur wer diese Aussage ernst nimmt, kommt zu einer anteiligen Verantwortlichkeit des Nutzers für den nachfolgenden Verarbeitungsvorgang durch das Netzwerk.[535] Dem Nutzer eine **seltsam geartete Teilverantwortlichkeit** aufzubürden, erscheint hingegen weder sachgerecht (wie soll ein Nutzer mit jedem Node bzw. Miner einen Vertrag zur Auftragsdaten-

[529] Vgl. *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO, Art. 3 Nr. 8 Rn. 7.
[530] So *Janicki/Saive*, ZD 2019, 251 (255).
[531] *EuGH*, Urteil vom 5.6.2018 – C-210/16 – ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein, Rz. 36.
[532] *EuGH*, Urteil vom 5.6.2018 – C-210/16 – ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein.
[533] Vgl. *Wagner*, ZD 2018, 307 (309 ff.).
[534] Ebenso der BDSG-Gesetzgeber, vgl. *Böhme/Pesch*, DuD 2017, 473 (478).
[535] Vgl. *Janicki/Saive*, ZD 2019, 251 (253 f.).

verarbeitung gem. Art. 28 Abs. 3 DS-GVO abschließen)[536] noch rechtlich zielführend, da es an der notwendigen Entscheidungsgewalt und Durchsetzungsmacht im Hinblick auf Löschungs- und Informationspflichten fehlt.[537] Argumentationen können sowohl in die eine als auch die andere Richtung erfolgen, ohne dass sich ein klares Bild ergibt. Eine pauschale Antwort verbietet sich daher.

Es mag mit einer anderen Gewichtung des bestimmenden Einflusses auch möglich sein, jeden, der einen eigenen Verarbeitungsvorgang durchführt – etwa die Berechnung einer Transaktion, Speicherung des Ergebnisses, etc. – als eigenen Verantwortlichen anzusehen, wodurch untereinander mangels Unterordnung kein Auftragsverarbeitungsverhältnis zustande käme. Auch wenn sich eine Einwilligung des Nutzers zur entsprechenden Verarbeitung vermutlich noch konstruieren ließe, wirft diese Betrachtung im Übrigen nur weitere Fragen auf.

ee) Dritte (Art. 4 Nr. 10 DS-GVO) Folgt man daher der zunächst genannten Argumentation, kommen nur **„Dritte“** als Verantwortliche in Betracht. Dritte in diesem Sinne sind jene, die einen vor- oder nachgeschalteten Verarbeitungsvorgang vornehmen, der nicht unmittelbar den Betrieb der Blockchain bzw. einer Transaktion betrifft.[538] In anderen Worten kann jeder, der von außen auf Daten der Blockchain zugreift (Auslesen) und einen eigenen Verarbeitungszweck verfolgt, potentiell Verantwortlicher sein.[539] Während so zwar das bloße Betreiben eines Miners keine Verantwortlichkeit auslöst, wäre das Auslesen oder Abspeichern der Daten zu eigenen Zwecken (z.B. Verifizierungsvorgänge) ein relevanter Datenverarbeitungsvorgang. Das trifft insbesondere auf Handelsplätze bzw. Geldbörsendienstleister zu, die für ihre Kunden Transaktionen durchführen und dabei vorgeschaltet Informationen verarbeiten.[540]

Solche externen bzw. intermediären Nutzer erscheinen auch als die tatsächliche Gefahrenquelle, da durch die Verbindung mit anderen Datensätzen schnell ein umfassenderes Bild über eine Person geschaffen werden kann.[541]

ff) Erste Reaktionen von Datenschutzbehörden Erste Erwägungen stellte bereits die französische Datenschutzbehörde **CNIL** an.[542] Nach dieser sei jeder am Netzwerk beteiligte Nutzer eine verantwortliche Stelle, solange er nicht unter die Ausnahme der privaten bzw. familiären Nutzung fällt. Einzige Ausnahme seien Miner, da sie nicht über Ziel und Mittel der Datenverarbeitung bestimmen können, die jedoch als Auftragsverarbeiter

[536] *Böhme/Pesch*, DuD 2017, 473 (478 f.); insofern auch *Bechtolf/Vogt*, ZD 2018, 66 (69), wenn auch mit anderer rechtlicher Bewertung.
[537] Vgl. die oben referenzierte gegenteilige Wertung von Fraunhoft FIT, S. 135.
[538] So auch *Böhme/Pesch*, DuD 2017, 473 (479); *Wagner/Groß*, S. 19 f.
[539] *Erbguth/Fasching*, ZD 2017, 560 (562); Fraunhofer FIT, S. 134.
[540] Mit allerdings anderer Definition und Blickrichtung *Erbguth/Fasching*, ZD 2017, 560 (564).
[541] Vgl. auch *Bechtolf/Vogt*, ZD 2018, 66 (69).
[542] CNIL, La Blockchain, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf. Vgl. auch Zusammenfassung von *Kaulartz/Quiel*, https://www.cmshs-bloggt.de/tmc/datenschutzrecht/dsgvo-blockchain-cnil/ und die kritische Anmerkung von *Erbguth*, https://erbguth.ch/CNILonBlockchain.pdf.

zu qualifizieren seien. Unklar hieran ist, dass nach dem zuvor Gesagten allenfalls die Full-Nodes, welche die Blockchain bei sich speichern, ggf. auch Mining-Aufgaben übernehmen, als Verantwortliche in Betracht kommen. Warum Miner ausgenommen werden sollen, erschließt sich nicht. Zweifelhaft erscheint insbesondere die Einordnung der Entwickler von Smart Contracts als Auftragsverarbeiter, da diese überhaupt keine Daten verarbeiten, sondern lediglich den Programmcode bereitstellen.[543] Am Ende wird allein der EuGH letztverbindlich für Klärung sorgen können, sollte keine gesetzliche Klarstellung erfolgen.

b) Private Ledger

Deutlich einfacher ist die Regelungslage bei **privaten Ledger**. Entscheidet eine einzelne Stelle über die Zulassung zu einer Blockchain und verfolgt sie mit der Verarbeitung und Speicherung einen besonderen Zweck, ist sie Verantwortliche im Sinne der DS-GVO.[544] Selbst wenn die Stelle nicht die Identität hinter den einzelnen Netzwerkadressen kennt, verfügt sie jedenfalls über die IP-Adressen der Nutzer und kann in einer Vielzahl von Fällen sämtliche Aktivitäten zuordnen.[545] Entscheidend ist, dass sie über die Macht verfügt, Mittel und Zweck der Datenverarbeitung festzuschreiben. Die Nodes und Miner werden ihr gegenüber als Auftragsverarbeiter (Art. 4 Nr. 8, Art. 28 DS-GVO) tätig, indem sie als selbständige Teilnehmer Daten im Interesse der leitenden Stelle verarbeiten.[546]

Bei privaten Blockchains liegt ohnehin kein Unterschied zu einem klassischen zentralistischen Netzwerk vor. Die geteilte Verantwortung in konsortialen Systemen führt hingegen zu einer gemeinsamen Verantwortlichkeit, da in solchen Fällen Zwecke und Mittel der Datenverarbeitung absprachegemäß erfolgen (vgl. Art. 26, 4 Nr. 7 DS-GVO). Beide sind den datenschutzrechtlichen Pflichten eines Verantwortlichen unterworfen. Zudem können sich weitere Pflichten aus dem Telemediengesetz (TMG) ergeben, soweit geschäftsmäßig Telemedien angeboten werden.[547]

3. Recht auf Vergessenwerden

Die Architektur einer Blockchain zeichnet sich insbesondere durch die Unabänderlichkeit aus, was jedoch zu Konflikten mit dem sog. Recht auf Vergessenwerden führt.

a) Ausgestaltung

Art. 17 Abs. 1 DS-GVO gewährt Betroffenen ein **Recht auf Löschung**. Auf ihren Wunsch sind alle sie betreffenden personenbezogenen Daten durch

[543] Vgl. auch *Kaulartz/Quiel*, https://www.cmshs-bloggt.de/tmc/datenschutzrecht/DS-GVO-blockchain-cnil/#.
[544] *Martini/Weinzierl*, NVwZ 2017, 1251 (1254) mit Beispielen des Staats in der Verwaltung oder privater Banken, ggf. auch als Konsortium (vgl. Art. 26 DS-GVO).
[545] *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2103).
[546] *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).
[547] Vgl. *Heckmann/Schmidt*, vbw-Studie, S. 21 f.

den Verantwortlichen in seinem Verantwortungsbereich zu entfernen.[548]

Erfolgt eine Löschung, trifft den Verantwortlichen eine flankierende Informationspflicht gem. Art. 17 Abs. 2 DS-GVO. Bei öffentlich einsehbaren Daten muss diese Informationspflicht eigentlich auch öffentlich erfüllt werden, was in den meisten Netzwerkstrukturen erst besondere Funktionen und Eingabeformen voraussetzt. Gegenüber bekannten Teilnehmern trifft ihn die allgemeine Mitteilungspflicht gem. Art. 19 S. 1 DS-GVO.

Damit verwandt ist auch das Recht auf Berichtigung bzw. Korrektur (Art. 16 DS-GVO).

b) Herausforderung

Die Umsetzung gestaltet sich bei dezentralen und öffentlich organisierten Ledger schwierig. Alle Transaktionsdaten und Informationen, etwa Bitcoin-Transaktionen, werden grundsätzlich für immer[549] in der jeweiligen Blockchain gespeichert.[550] Nähme ein einzelner Node die Transaktion aus den gespeicherten Daten heraus, würde seine Kette von der mehrheitlich akzeptierten abweichen und wäre eventuell sogar unschlüssig. Das übrige Netzwerk würde dies unbeeindruckt lassen und weiterhin auf die jeweils längste valide Version zurückgreifen.

Eine Korrektur müsste daher entweder bewusst vom gesamten Netzwerk angestrebt werden, indem die Nodes bei einem sog. Hard Fork kollektiv eine neue Kette auswählen, oder ein entsprechender Mechanismus vorgesehen sein, der einen entsprechenden Eingriff ermöglicht.

c) Umsetzungsmöglichkeit und -pflicht

In den derzeit diskutierten Modellen öffentlicher zulassungsfreier Ledger wäre die **Durchsetzung der Löschungspflicht**, ebenso wie die der flankierenden Informationspflicht, aufgrund der Dezentralität, der ständig wechselnden Teilnehmer und nicht zuletzt der fehlenden territorialen Fixierung wohl praktisch nicht effektiv möglich.[551] Freilich besteht das Recht auf Vergessenwerden nur, wenn im Einzelfall ein Verantwortlicher im Sinne der DS-GVO auszumachen ist. Andernfalls liefe das Recht auf Vergessenwerden schlicht ins Leere.

Soweit man hingegen nur bei einer zulassungsbeschränkten Blockchain den Netzwerkbetreiber bzw. das Konsortium als Verantwortliche fasst, lassen sich die Vorgaben durch entsprechende technische Vorbehalte umsetzen.[552] Der Netzwerkbetreiber bzw. das Konsortium müsste dafür Sorge

[548] *Martini/Weinzierl*, NVwZ 2017, 1251 (1254).

[549] Hard Forks oder die Löschung der gesamten Blockchain außen vor gelassen.

[550] *Bechtolf/Vogt*, ZD 2018, 66 (69).

[551] Vgl. zu den Schwierigkeiten *Martini/Weinzierl*, NVwZ 2017, 1251 (1255); kritisch auch *Bechtolf/Vogt*, ZD 2018, 66 (70).

[552] Etwa einem Masterkey, der nachträglich einzelne Transaktionsinhalte anonymisieren kann, sodass nur noch die zu einem neueren Stichtag existierenden Salden ausgelesen werden können. Ebenso könnte nur ein besonderer Master-Node die gesamte Kette speichern, während andere Teilnehmer nur die zu Hash-Bäumen verschlüsselte Version herunterladen: Alle Teilnehmer können mit den Hash-Werten die Master-Kette validieren;

tragen, dass ihm die notwendige technische Verfügungsmacht zukommt, um Inhalte nachträglich zu verändern bzw. sich rechtliche Ansprüche gegen die Auftragsverarbeiter zu verschaffen (eine Pflicht, die ihn auch gem. Art. 28 DS-GVO trifft).[553]

4. Anonymisierungsstrategien und weitere Alternativen

a) Anonymisierungsstrategien

Angesichts der Unsicherheiten erscheint es ohnehin vorzugswürdig, von vorneherein auf eine bessere **Anonymisierung** der Nutzerdaten zu setzen. Können die Daten einer Person nicht mehr zugeordnet werden, ist die Datenschutzgrundverordnung auf die im Distributed-Ledger gespeicherten Daten nicht anwendbar. Geeignete Szenarien sind stark abhängig vom jeweiligen Anwendungsfall, sodass nachfolgend nur einige Ansätze veranschaulicht werden sollen.[554]

aa) Systemdesign Ein besonders einfacher Ansatz liegt darin, (personenbezogene) Daten nicht mehr in dem Ledger (on-chain) zu speichern, sondern **allein Hash-Werte** bzw. Merkle-Trees.[555] Alle in dem Block gespeicherten Transaktionen können so zwar anhand der Kette validiert, aber ohne eine Kopie der Originaldaten nicht ausgelesen werden. Ob alle Nutzer die Originaltransaktionen speichern oder nur eine einzige Stelle ist irrelevant: Die Validität kann weiter von jedem überprüft werden, den die betreffenden Daten etwas angehen und der sie deshalb unverschlüsselt gespeichert hat. Löschungsverlangen beträfen hingegen nicht die Blockchain.

Zusätzlich könnten zu den Hashwerten auch Links zum Speicherort der referenzierten Originaldokumente hinterlegt werden. So kann das Dokument aufgerufen und seine Integrität überprüft werden; mit dem Entfernen des Dokuments geht der Verweis schließlich ins Leere und die Löschungspflichten sind insoweit erfüllt.

Durch sog. *Salted Hashes* wird ein noch höheres Anonymisierungsniveau erreicht: die Zugabe einer zufälligen Information („salt“) zu einem Datensatz verhindert, dass ein Angreifer, der alle potentiellen Eingaben kennt, schlicht die in der Kette referenzierte errät.

Ähnlich wird bei den sog. Zero-Knowledgement-Proof-Verfahren vorgegangen.[556] Für die beteiligten Nodes sowie Außenstehende ist dabei anhand des Ledgers alleine nachvollziehbar, dass eine Transaktion stattgefunden hat, nicht aber die Urheberschaft oder der Adressat des Wertzuflusses.[557] Die übrigen Mechanismen müssen dann aber besonders transparent sein,

löscht der Masternode jedoch eine Information aus seiner Kette heraus, können die anderen ihren Inhalt nicht wiederherstellen. Ausführlich Fraunhofer FIT, S. 144 ff.

[553] *Martini/Weinzierl*, NVwZ 2017, 1251 (1255) mit Verweis auf einige diskutierte Verfahren.

[554] Vgl. zu weiteren Strategien Frauenhofer FIT, S. 137 ff.

[555] Siehe bereits S. 8.

[556] *Samman*, The Trend Towards Blockchain Privacy, http://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs.

[557] *Martini/Weinzierl*, NVwZ 2017, 1251 (1256).

um die Fähigkeit des Systems zu erhalten, um weiter auch von sich aus Vertrauen auszustrahlen. Diverse Identity-Management-Systeme erlauben etwa, verschiedenen Prozessbeteiligten Rollen zuzuschreiben und diese funktionsgemäß mit bestimmten Rechten auszustatten. Andere Parteien werden hingegen nur sehen, dass die jeweilige Rolle (etwa Verkäufer, Käufer, etc.) ihre Aufgaben wahrgenommen hat, nicht aber, wer hinter der Rolle steckt.

bb) Für die Nutzer Um **als Nutzer** einem Transaktionstracking zu entgehen, sind besondere Vorkehrungen nötig. Vorgeschlagen wurde beispielsweise die Verwendung immer neuer Schlüssel.[558] Dies ist für eine große Bandbreite von Nutzern jedoch wenig praktikabel. Zudem könnte das Verfahren möglicherweise durch Big Data bzw. IP-Tracking schnell an seine Grenzen gebracht werden.

b) Nachträgliche Eingriffe

Es werden viele neue Vorschläge unterbreitet, die eine **nachträgliche Löschung** ermöglichen sollen. Häufig wird etwa auf sog. Chameleon-Hashes verwiesen.[559] Hierbei handelt es sich letztlich erneut um ein zentral organisiertes Verfahren, bei dem eine besondere Stelle über eine Korrektur-Schnittstelle für nachträgliche Änderung verfügt. Dementsprechend muss das Vertrauen von der Stelle selbst ausgehen sowie eine hinreichende rechtliche Sicherheit bestehen, dass Änderungen auch nur nach den vorgegebenen Regeln oder Gesetzen erfolgen.

5. Regulierungsmöglichkeiten

a) EU-Ebene

Die DS-GVO lässt den Mitgliedstaaten wenig Spielraum. Änderungen gegenüber der aktuellen Regelungslage müssten demnach grundsätzlich auf **Unionsebene** angestrebt werden. Bis zu einer Entscheidung des EuGH über die Frage der Verantwortlichkeit – sollte es jemals zu einer kommen – oder einer gesetzlichen Klarstellung verbleiben jedenfalls große Rechtsunsicherheiten. Hinzu kommt, dass Blockchain nicht gleich Blockchain und DL nicht gleich DL ist.

Einige Autoren, welche die Nodes in zulassungsfreien und öffentlichen Blockchains als Verantwortliche ansehen, fordern in Zukunft eine implementierte Pseudonymisierung als hinreichende Erfüllung von Art. 17 DS-GVO einzustufen, sollte eine Löschung zu hohen technischen Hürden bzw.

[558] Exemplarisch für das System Bitcoin *Tschorsch/Scheuermann*, IEEE Commun. Surveys Tuts. 2016, 2084 (2107 ff.).

[559] *Martini/Weinzierl*, NVwZ 2017, 1251 (1256). Wenn nicht sogar rechtliche Anordnungsbefugnis bzw. Hoheitsschnittstelle, dies., 1157. Mit Blick auf andere Blockchain-Netzwerke, die eine solche Änderungsmöglichkeit vorsehen auch *Bechtolf/Vogt*, ZD 2018, 66 (70).

Unstimmigkeiten führen.[560] Es empfiehlt sich aber wohl eher, die datenschutzrechtlichen Fragen im Lichte dezentral organisierter Systeme generell zu überdenken. Dabei muss jedoch der besonders hohe Stellenwert des allgemeinen Persönlichkeitsrechts, dessen Schutz die DS-GVO dient (Art. 1 Abs. 2), beachtet werden. Während die Vorgaben aus Art. 28 DS-GVO nur schwer einzuhalten sind, könnten neue technische Lösungen in Verbindung mit rechtlichen Anpassungen einen gangbaren Weg darstellen.

b) Nationale Ebene

Art. 23 Abs. 1 lit. e eröffnet zusammen mit Erwägungsgrund 73 DS-GVO Möglichkeiten, für staatliche DL-Anwendungen einen Rechtsrahmen zu schaffen. Hiernach dürfen für „das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses“ Abweichungen von den Betroffenenrechten zugelassen werden. Im Übrigen haben die **Mitgliedstaaten** wenig nationale Spielräume.

6. Chancen

Der Distributed-Ledger-Technologie werden auch zahlreiche **Potentiale** zugeschrieben, künftig für einen besseren Datenschutz zu sorgen oder auch neue Formen der Datenkontrolle zu etablieren.[561]

Eine aktuelle Studie beschreibt ein System des **Datenmanagements**[562] unter Zuhilfenahme der Blockchain-Technologie.[563] Der Nutzer soll erstmalig Verfügungsgewalt über seine Daten erreichen, auch wenn er sie gegenüber einzelnen Stellen preisgibt, indem er präzise bestimmen kann, wer, wie lange und in welchem Umfang darauf zugreifen kann.[564] Technisch umsetzbar ist die Idee etwa durch Kanäle (sog. *Channel*). Der jedem zugängliche Hauptkanal enthält nur Hash-Werte zur Verifikation, während die einzelnen Inhalte in privaten *Channels* geteilt werden, die jeder flexibel gestalten und dadurch bestimmen kann, wer die jeweiligen Informationen einsehen und ggf. über sie verfügen darf. Mittels einer solchen selektiven Informationsverbreitung können auch Identitäten anonymisiert und so ggf. die Personenbeziehbarkeit von Daten in einem Kanal vermieden werden.

Alternativ können Rollenmodelle in Verbindung mit Identitätsmanagementsystemen helfen, eine relative Anonymität zu erhalten: Die Gegenüber im jeweiligen System sehen nur die Rolle, die ein Beteiligter in einem Businessprozess einnimmt, nicht aber den Namen, eine Nutzerkennung, o.ä. Dies schafft eine Balance zwischen Transparenz im Verfahren und dem Schutz personenbezogener Daten.

---

[560] *Martini/Weinzierl*, NVwZ 2017, 1251 (1257).
[561] Vgl. *Wright/De Filippi*, S. 12 f.
[562] Der Begriff Datensouveränität ist hingegen noch als Werbebegriff noch mit Vorsicht zu genießen.
[563] *Zyskind/Nathan/Pentland*, 2 ff.; vgl. zum Potential auch die Anmerkung von *Bechtolf/Vogt*, ZD 2018, 66 (71).
[564] Vgl. zum Modell auch die Grafik bei *Wagner/Groß*, S. 21.

Mit steigender Sicherheit und besser werdenden Verschlüsselungstechniken eröffnen dezentrale Clouddienste außerdem die Möglichkeit, nicht verwendeten Speicherplatz oder sogar die eigene Rechenleistung anderen Nutzern zur Verfügung zu stellen.[565]

[565] *Wright/De Filippi*, S. 13.

XII. Perspektiven konsortialer Netzwerke

1. Problemstellung

Wie gezeigt, bringen öffentliche dezentrale Netzwerke zahlreiche Schwierigkeiten mit sich. Die Jedermann zustehende Schreibberechtigung erfordert einen komplizierten und teils ressourcenintensiven Konsensmechanismus,[566] die Pseudonymität der Nutzer erschwert die Rechtsdurchsetzung und zahlreiche rechtliche Unklarheiten, insbesondere im Zusammenhang mit der DS-GVO, erschweren den Aufbau verlässlicher Strukturen. Zudem ist eine Information, nur weil sie in einem öffentlichen Netzwerk gespeichert ist nicht zugleich verlässlich, da die Vertrauenswürdigkeit des Schreibers meist nicht überprüft werden kann.

All diese beispielhaft genannten Schwierigkeiten lassen sich überbrücken, wenn sich die Teilnehmer aus einem festen Kreis zusammensetzen und durch Rechtsgestaltung einem einheitlichen Regelwerk unterwerfen. Verfahren für die Änderung oder Löschung sich später als falsch herausstellender Einträge können damit eingebettet und z.B. durch Abstimmungen vollzogen werden.[567]

2. Bedingte Relevanz interner Ledger?

Dezentrale Netzwerke sind gewissermaßen eine Antwort auf Vertrauensdefizite. Wofür also ein Netzwerk in Gestalt eines privaten Ledgers, dessen Teilnehmer aus demselben Unternehmen oder einer ähnlich gleichlaufenden Interessensphäre stammen? Interne Ledger sind letztlich wieder zentralisiert und erweisen sich daher als nur bedingt revolutionär. Der einzige Unterschied zu herkömmlichen verteilten Datenbanken ist, dass nachträgliche Änderungen transparent nachvollzogen werden können. Ob die Einträge selbst der Wahrheit entsprechen oder bestimmten qualitativen Ansprüchen genügen, kann nicht abgeleitet werden.[568] Der hohe Implementierungsaufwand und die notwendigen Abstimmungsverfahren führt dazu, dass dezentrale Systeme in der Regel weder kosteneffizienter noch schneller sind als herkömmliche Datenbanklösungen. Ohne Vertrauensdefizit kein Bedarf für ein DL.[569] Freilich mag auch innerhalb eines Unternehmensgeflechts nicht immer blindes Vertrauen herrschen oder es anderweitig von Vorteil sein, alle Änderungen transparent nachvollziehen zu können. Alle Nodes zentral zu halten erscheint jedoch auch dann nicht sinnvoll.

[566] Vgl. *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (141 f.).
[567] *Swanson*, S. 27 f.
[568] *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (142).
[569] Etwas schärfer *Horlacher*, 'Centralized' blockchain projects are doomed to failure, BankThink 2017, abrufbar unter: https://www.americanbanker.com/opinion/centralized-blockchain-projects-are-doomed-to-failure.

3. Multipolare dezentrale Netzwerksysteme

Deutlich interessanter sind hingegen Netzwerke, deren Teilnehmer ein **multipolares Interessengeflecht** aufweisen und sich damit gerade nicht vollständig vertrauen.[570] Mit ihnen wird die hinter dem Blockchain-Ansatz stehende Idee der Kollaboration weiter vorangetrieben, indem sich vorher gegeneinander arbeitende Akteure zu einem Miteinander inspiriert sehen. Überschneiden sich die Geschäftsbeziehungen mehrerer Akteure und besteht Interesse an einfacherem Austausch, einheitlichem Datenbestand oder etwa einem **Identitätsmanagementsystem**, kann vieles für die Einrichtung eines dezentralen Netzwerks sprechen. Dabei sind mehrere **Konstellationen** denkbar:

Einerseits kann das Netzwerk als **unabhängige Plattform** verstanden werden, die von verschiedenen Interessengruppen betrieben wird, grundsätzlich aber offen für interessierte Teilnehmer ist. So könnten etwa Branchenverbände, größere Marktteilnehmer oder auch staatliche Organisationen mit einem Interesse an der Förderung eines solchen Netzwerks Nodes bereitstellen, ohne dass der individuelle Nutzer hierzu verpflichtet wäre.[571] Es handelt sich in diesem Szenario um **zulassungsbeschränkte**, meist auch **private Ledger**, deren Nutzer einen KYC-Prozess (Identifizierung) durchlaufen und fortan anhand dieser digitalen Identität wiedererkannt werden können. Dies ermöglicht nicht nur eine rechtliche Durchsetzbarkeit von im Ledger referenzierten Rechten oder Pflichten, sondern erlaubt in Verbindung mit der Unveränderbarkeit der Ledger-Inhalte jedenfalls den finalen Beweis, dass ein Eintrag auch von einer bestimmten Person stammt. Wird ein solches Netzwerk etwa zur Abbildung von Vertragsbeziehungen oder einer Wertschöpfungskette unter Einbeziehung der Sacheigenschaften der gehandelten Ware verwendet, kann später jeder zweifelsfrei nachvollziehen, wer an welchem Prozess mit welchem Inhalt beteiligt war und wer für welche Information oder Aussage verantwortlich ist. Erneut zeigt sich die Herstellung von **Transparenz** und **Nachvollziehbarkeit** als der wesentliche Vorteil der Distributed Ledger Technologie. Hinzu kommen potentielle Einsparungen von Transaktionskosten durch digitalisierte Systeme, die mit entsprechend sicheren Identitätsmanagementsystemen vergrößert werden.

Andererseits kann auch eine deutlich **engere Zusammenarbeit** erfolgen, wenn sich die Beteiligten zu einem **Konsortium** zusammenschließen und die Kooperation sowie die Funktionsweise des Ledgers in einem **mehrseitigen Vertrag** regeln. Die einzelnen Beteiligten werden zwar vermutlich weiter eigene Datenbanken verwalten, um die Informationen besser in die bestehenden Systeme zu integrieren und eine u.U. notwendige Datenhoheit zu erhalten; sie können sich jedoch durch die Vernetzung völlig neue Formen des Austauschs und Miteinanders erschließen, wobei gerade die einheitlichen, für alle Teilnehmer verbindlichen Regeln der Plattform eine besondere Rechtswirkung verleihen.[572] Binden sich die Parteien an die Dar-

[570] *Swanson*, S. 21 ff. mit einigen Modellen.

[571] Branchenverbände könnten es etwa als Service an ihre Mitglieder verstehen, diesen Zugang zu bieten. Da der mittelbare Zugang jedoch Vertrauen an den Mittler voraussetzt, werden größere Unternehmen gleichwohl ein Interesse daran haben, selbst einen *Node* zu betreiben.

[572] *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (144).

stellung im konsortialen Ledger, haben die dargestellten Rechte für alle im Konsortialsystem Beteiligten absolute Wirkung.

Beiden Modellen gemeinsam ist, dass mittels programmierter Logiken (also Smart Contracts) den jeweils Beteiligten feste Rollen und Rechte zugewiesen werden können. Ein Auditor kann beispielsweise Geschäftsprozesse prüfen und genehmigen, ein Finanzierungsgeber eine Finanzierung bestätigen oder ein Verkäufer Angebote erstellen bzw. Verkaufszusagen aussprechen. Die Rollenmodelle erlauben es außerdem, dass die interne Besetzung (Identität der Person) nicht offengelegt werden muss, sondern stattdessen festgehalten wird, dass die zuständige Person die ihr zugewiesenen Rechte ausgeübt hat. Der Ledger kann so beliebig an das jeweilige Business-Modell angepasst und die Einhaltung individueller Rechte garantiert werden – eine ordnungsgemäße Programmierung vorausgesetzt. Soweit der Ledger dabei die Funktion eines transparenten Registers von Transaktionen und Handlungen erfüllt, stellt sich auch bei Fehlern die Unveränderbarkeit nicht als Problem dar: Korrekturen können mit einem Verweis auf die fehlerhafte Transaktion von der dafür vorgesehenen Stelle hinzugefügt werden, sodass eine transparente Korrektur erfolgt. Künftig kann das System dann schlicht den korrigierten Eintrag referenzieren, während der Konsensmechanismus den fehlerhaften nicht mehr akzeptieren wird.

Ersten Prognosen zufolge,[573] die von Beobachtungen in der Praxis bestätigt werden, sind private und konsortiale Systeme deutlich besser für die Abbildung von Businessprozessen, Accounting-Angelegenheiten oder Transaktionen entlang der Wertschöpfungskette geeignet, als öffentliche. Hierbei wird auch auf den Einsatz sog. cloud-basierter Blockchains verwiesen.[574] Die Idee dahinter ist, dass nicht jeder Nutzer die vollständige Blockchain speichern oder an dem Betrieb mitwirken können muss, um an den Vorzügen zu partizipieren. In ähnlicher Weise könnten auch kleineren Nutzern entsprechende Zugangspunkte durch einen Mittler bereitgestellt werden.

Solche Zusammenschlüsse werfen völlig neue Rechtsfragen auf, die an dieser Stelle nicht weiter vertieft werden können. Beispielsweise stellt sich bei den neuartigen Formen der Zusammenarbeit die Frage nach der rechtlichen Strukturierung bzw. ggf. nach der geeigneten Rechtsformen. Teilweise kommt die Gründung einer Gesellschaft in Betracht, womit jedoch eine Zentralisierung einhergeht, die bei DLT-Lösungen eigentlich vermieden werden soll. Alternativ kann ein mehrseitiger Vertrag die Eigenständigkeit der Systemteilnehmer erhalten, muss in diesem Fall als gemeinsames Regelwerk jedoch Verfahrensabläufe, Abstimmungsmodalitäten und gegenseitige Rechte und Pflichten erfassen, was ein komplexes Unterfangen sein kann. In beiden Fällen kann es sich um marktrelevante Absprachen bzw. Zusammenschlüsse handeln, sodass u.U. die Vorgaben des Kartellrechts Beachtung finden müssen.

Unabhängig davon muss eine Regelung getroffen werden, wer für den Erhalt des Netzwerks und dessen Betrieb verantwortlich ist. Gelingt es einen dezentralen Ansatz zu finden oder müssen doch wieder Mittelsmänner mit

[573] *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (139).
[574] *O´Leary*, Intell Sys Acc Fin Mgmt. 2017, 138 (140).

entsprechendem Einfluss zwischengeschaltet werden? Ein potentieller Mittelweg wäre es, die Verantwortung nicht den eigentlichen Netzwerkteilnehmern aufzuerlegen, sei es einem für alle oder allen gemeinsam, sondern diesen zuzuorndende Verbände und andere Interessengruppen für eine ausbalancierte Machtstruktur sorgen. In einem Netzwerk aus Verbrauchern, Unternehmen und Banken könnten der Betrieb beispielsweise aufgeteilt werden auf eine Verbraucherschutzorganisation, einen Interessenverband der Unternehmen und einen Interessenverband des Finanzgewerbes. Die Verbände können ihren jeweiligen Mitgliedern Zugang gewähren, während das Netzwerk über Beiträge oder die Erhebung von Transaktionsgebühren finanziert wird.

XIII. Aspekte des Verbraucherschutzes

Die DLT ermöglicht es potentiell, am Transaktionsprozess beteiligte Akteure unmittelbar in alle Abläufe einzubinden, wo es bislang noch eines Intermediärs bedurfte. Damit entfallen zwar Transaktionskosten, es steigen aber auch die Risiken der Teilnehmer, die nun nicht mehr auf einen Mittelsmann übertragen werden.

Noch sind wenige bis keine Projekte ersichtlich, die sich konkret an **Endverbraucher** richten bzw. diese als aktive Bestandteile einbinden und bereits die Phase des Proof of Concept überschritten haben.

Dies lässt sich vor allem mit dem gegenwärtigen **Entwicklungsstadium** der Technologie erklären: Die vorhandenen Systeme stecken meist noch in den Kinderschuhen und werden nicht an eine große Zahl Kunden herangetragen. Vielmehr prüft man zunächst die Vereinbarkeit der Technologie mit den jeweiligen Prozess- und Businesslogiken und erprobt ihre Grenzen (Learning Phase). Dies geschieht meist in größeren Konzernen oder innerhalb von Konsortien. Dabei kommt es entscheidend auf die noch sichere, abgeschirmte Umgebung an. Hinzu kommt, dass die Interaktion mit der Technologie ein gewisses Maß an technischem Know How sowie entsprechendes Interesse voraussetzt, was die breite Masse der Bevölkerung nicht mitbringt. Auch wenn Kryptowährungen immer wieder große Medienaufmerksamkeit auf sich ziehen, können nur verhältnismäßig wenige Menschen erklären, was unter einem Distributed-Ledger bzw. einer Blockchain zu verstehen ist.

Darüber hinaus bringt die Beteiligung von Verbrauchern an DL-Systemen rechtlich gesehen eine erhebliche **gesteigerte Komplexität** mit sich. Jedenfalls zu Beginn wird die eingeschränkte Gestaltungsfreiheit dazu führen, dass Testversuche im Bereich DLT eher den unternehmerischen Verkehr fokussieren werden.

Einige potentiellen Veränderungen sowie einige spezifische Risikolagen, die sich heute schon abzeichnen, werden im Folgenden betrachtet.

1. Neue Chancen durch Prosuming und im Bereich der Sharing Economy

Verbrauchern fällt es häufig schwer, die rechtlichen und wirtschaftlichen Implikationen einer Transaktion zu überblicken. In Szenarien, in welchen sie als Anbieter auftreten, fungiert deshalb bislang meist eine **zentrale Plattform** als Vermittler. Beispielhaft genannt sei Ebay, die als Handelsplattform einen Raum schafft, in dem sich gegenseitig unbekannte Käufer- und Verkäufer gegenübertreten können. Die Verbraucher können so selbst am Markt teilnehmen, ohne die notwendige Infrastruktur bereitstellen oder sich über die Rahmenbedingungen Gedanken machen zu müssen. Damit begegnet die Plattform zum einen dem Problem der fehlenden gegenseitigen Kenntnis, zum anderen schafft sie in Konfliktsituationen mittels eines Schlichtungsmechanismus‘ eine gewisse Transaktionssicherheit. Nicht die Plattform tritt dabei als letztverantwortlicher Akteur auf, sondern die Plattformnutzer selbst. Wie viele Risiken die Plattform dabei übernimmt

und wie viel Vertrauen sie damit stiftet, unterscheidet sich von Fall zu Fall. In einigen Fällen, etwa bei AirBNB, wird der vollständige Zahlungsverkehr kontrolliert, um so über entsprechende Eingriffsbefugnisse in Konfliktfällen zu verfügen, was in der Regel mit höheren Transaktions- bzw. Nutzungsgebühren einhergeht.

Bei **dezentralen, öffentlichen und zulassungsfreien Netzwerken** könnte die vermittelnde Plattform als eigenständiger Akteur wegfallen. Das Netzwerk selbst würde nicht mehr von einer zentralen Instanz gesteuert werden, sondern – in der Idealform – selbst eine hinreichende Gewähr für die Richtigkeit der dort hinterlegten Daten liefern. Ein entsprechend sicheres Design vorausgesetzt, könnten die Parteien einen Vertrag über ein DLT-System abwickeln und dabei mit Sicherheit davon ausgehen, dass die vorgegebenen Parameter auch ausgeführt werden. Dabei muss das Netzwerk einige Fragen beantworten, um dem Verbraucher das nötige Vertrauen zu vermitteln, damit er ohne Bedenken mit Unbekannten kontrahieren kann: Wer ist mein Vertragspartner? Wie komme ich an meine Gegenleistung? An wen kann ich mich bei Problemen wenden? Hierfür müsste zum einen Transparenz hergestellt werden, indem der an sich unverständliche Code des Netzwerks übersetzt wird. Zum anderen müsste sich das jeweilige System mit den Einschränkungen selbstvollziehender Verträge und weitergehenden Bedenken auseinandersetzen, die in den vorstehenden Kapiteln ausgeführt wurden. Für den Austausch von Leistungen, deren Erbringung nicht vollständig digital überprüfbar ist, muss zunächst ein funktionierendes System demonstriert werden, in welchem sich gegenseitig unbekannte Vertragspartner sich auf einen Vertrag einlassen können, ohne auf eine vertrauenswürdige Schlichtungsstelle angewiesen zu sein. Sind die Systeme wiederum zulassungsbeschränkt und zentral kontrolliert, liegen keine gewichtigen Unterschiede zu derzeitigen Plattformmodellen vor.

Neuerungen ergeben sich jedoch, wenn Verbraucher Anbieter von etwas werden, dass sie vorher nicht kommerzialisieren konnten und so völlig neue Märkte erschließen. Exemplarisch genannt seien insbesondere **Daten**. War es bisher der Fall, dass Daten (häufig) ohne Steuerungsmöglichkeit des Verbrauchers und jedenfalls ohne finanzielle Entlohnung erhoben und verarbeitet wurden, hält die Blockchain-Technologie zahlreichen Stimmen zufolge ein Werkzeug bereit, um dies zu ändern. Häufig wird von einer Rückgewinnung der Datensouveränität gesprochen. So können mithilfe der Blockchain Daten nur bestimmten Nutzern freigegeben und sogar nur zu begrenzten Rechten mitgeteilt werden. Ferner lässt sich leicht verifizieren, wem Zugriff zu entsprechenden Daten gewährt wurde. Ähnlich einem **Rechte-Management-System** könnten **Datenrechte** vergeben werden, im Gegenzug der Verbraucher ein Entgelt (in Form von Token) erhalten. Die Coins könnten dann entweder als Kryptowährung gegen Geld gehandelt werden oder als Utility Token andere Funktionalitäten freischalten. Ein anderes Feld, in dem Prosuming-Bestrebungen zu beobachten sind, ist der private Stromhandel. Verbraucher können dabei etwa überschüssigen Strom selbst über einen dezentralen Marktplatz anderen Nutzern oder Stromanbietern zur Verfügung stellen.

2. Perspektiven des Verbraucherschutzes

a) Chancen

Die veränderten Prozesslogiken eines verbindlichen und unabänderlichen Ledgers versprechen Effizienzsteigerungen und Transaktionskostenvorteile, die auch an Verbraucher weitergegeben werden sollen. Die Netzwerke sollen gleich zwei Institutionen obsolet machen: Sie sollen zum einen die **vertrauensstiftende Funktion** eines Notars einnehmen, indem Bedingungseintritte überwacht, verifiziert und Leistungen freigegeben werden; zum anderen sollen sie vermittelnde bzw. rechtsdurchsetzende Aufgaben erledigen und so an die Stelle von Gerichten und Anwälten treten.[575] Nicht zuletzt wird der Technologie das Potential zugeschrieben, **soziale Barrieren** zu überwinden und insbesondere Verbrauchern, die angesichts der Übermacht eines großen Unternehmens von der Klageerhebung abgesehen hätten oder sich schon aufgrund der Ressourcendivergenz in einer unausgeglichenen Lage befinden, besser zu ihrem Recht zu verhelfen.[576] Beispielhaft sei hier der Fall genannt, dass ein Smart Contract automatisierte Entschädigungszahlungen bei Flugverspätungen leistet und damit die Rechtsdurchsetzung fördert. Hierdurch würde die Technologie tatsächlich Verbraucherschutz verwirklichen. Ein „neutraler Code" soll in diesem Rahmen die Risiken von politischen, sozialen oder sonstigen Abhängigkeiten abfedern.

b) Risiken durch ungleiche Rollen bei der Systemgestaltung

Diese Annahme verfängt jedoch nur für den Fall, dass tatsächlich ein **„neutraler" Code** implementiert wurde. Neutralität wäre gegeben, wenn die Interessen von Verbrauchern und Unternehmern gleichermaßen berücksichtigt wurden und sich ein solches ausgeglichenes Verhältnis auch in der Gestaltung des Codes widerspiegelt. Schon heute nehmen Unternehmen jedoch eine deutlich stärkere Verhandlungsposition bei der Vertragsgestaltung ein, die es ihnen beispielsweise erlaubt, Nebenbestimmungen in der Regel einseitig durch AGB festzulegen. Auch bei Smart Contracts sind Musterverträge zu erwarten, die in der Regel von den Unternehmen selbst eingebracht werden. Vielen Verbrauchern wird bereits das Wissen fehlen, um die komplexen technischen Zusammenhänge zu überblicken, geschweige denn diese dem geltenden Recht gegenüber zu stellen. Die Gestaltung und wesentlichen Einflüsse eines Systems werden daher grundsätzlich einseitig von der Unternehmerseite ausgehen. Warum sollten diese bestimmten Einreden oder Einwendungen des Gegenübers einbeziehen und die eigene Geschäftszwecke gefährden? Neutralität kann nur dann erwartet werden, wenn sich entsprechende Standards etablieren und für Unternehmen ein Anreiz besteht, diese auch zu nutzen (Regulierung, Marktdruck, etc.). Verbrauchern hilft in erster Linie Transparenz und die Möglichkeit öffentlicher Kontrolle, wie es bereits heute bei Open Source Lösungen üblich ist.

---

[575] Vgl. *Wright/De Filippi*, S. 24; *Szabo*, First Monday, Volume 2, Number 9 (1997); krit. *Mik*, Law, Innovation and Technology 2017 (9.2), p. 269 ff., zitiert aus https://ssrn.com/abstract=3038406, S. 4 ff.

[576] *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (3).

Setzen Unternehmen einseitig zu Lasten des Verbrauchers oder einer sonst unterlegenen Verhandlungspartei einen selbstvollziehenden Vertrag ein, kann dies aber auch im Hinblick auf die späteren Prozessrollen gravierende Folgen haben.

3. Einschüchterungspotential selbstvollziehender Systeme

Für viele Unternehmen mag es immer noch reizvoll sein, auf Compliance mit dem (Verbraucherschutz-)Recht zu verzichten und darauf zu bauen, dass der risikoscheue Verbraucher von einem Prozess absehen wird.[577] Wo schon heute häufig ein rechtliches Vorgehen angesichts der **psychologischen Hemmschwelle**, welche die Klageerhebung mit all ihren Formalien und der Zahlung eines Prozesskostenvorschusses mit sich bringt, ausbleibt, dürfte ein solches unter dem häufig proklamierten „Code is law"-Dogma und dem Anschein der Unnachgiebigkeit der „smarten Verträge" noch unwahrscheinlicher werden.

Der Selbstvollzug hat damit einerseits einen erheblichen Einschüchterungseffekt; der Verbraucher sieht sich gewissermaßen der **Macht des Faktischen** ausgesetzt und unterwirft sich der Logik des unbestechlichen Programmcodes. Andererseits besteht die Gefahr, dass ein Unternehmer hierdurch die Klagerolle faktisch einseitig auf die unterlegene Vertragspartei verlagert, ohne dass es zu einer generellen Verbesserung des Abwicklungssystems kommt.[578] Dies korreliert mit der zuvor angeführten Problematik, dass ein selbstvollziehendes System unter Umständen schuldnerschützende Regelungen (insb. Einwendungen und Einreden) schlicht übergeht.[579]

Man könnte der Technologie allerdings auch das Potential zugestehen, in einigen Feldern für **größeren Verbraucherschutz** zu sorgen, indem die Rechtsdurchsetzung nicht mehr in der Hand einflussreicher und ressourcenstarker Unternehmer liegt, sondern einem Smart Contract überlassen wird. Beispielhaft genannt wird in diesem Zusammenhang immer wieder die automatisierte Durchsetzung von **Entschädigungsleistungen bei Flugverspätungen** bzw. –ausfällen. Auch hier müsste jedoch ein „neutraler" Code implementiert sein.

Noch weitergehend lässt sich über Szenarien nachdenken, in welchen selbstvollziehende Verträge Unternehmen zur Einhaltung der Gesetze zwingen.[580] Marktmächtige Unternehmen werden sich darauf kaum oder nur bei einem besonders hohen Marktdruck einlassen. Daher werden bereits Überlegungen laut, Unternehmen zur Verwendung solcher Protokolle in Verbraucherverträgen zu zwingen.[581] Auch aufsichtsrechtlich könnte die Pflicht zur Verwendung eines transparenten und im Einklang mit geltenden Vorschriften stehenden Netzwerks mit selbstvollziehenden Logiken ein scharfes Schwert sein. Dies sei hier jedoch nur als Gedankenspiel angedeutet.

---

[577] *Fries*, Compliance Elliance Journal 2018, Vol. 4, 11 (13).
[578] Vgl. *Levy*, Engaging Science, Technology, and Society 3 (2017), 1 (11).
[579] Siehe S. 75 ff.
[580] Ob diese Annahme auch ökonomische Vorteile für die beteiligten Verbraucher bringt, erscheint nicht sicher, vgl. *Fries*, Compliance Elliance Journal 2018, Vol. 4, 11 (15 f.).
[581] Vgl. *Fries*, Compliance Elliance Journal 2018, Vol. 4, 11 (15).

4. Neue Hinweis- und Aufklärungspflichten bei selbstvollziehenden Verträgen?

Einer **potentiellen Einschüchterungswirkung** dürfte vor allem Aufklärung vorbeugen. Einerseits wäre darüber zu informieren, dass Recht und Technik getrennt voneinander zu beurteilen sind und mit dem Ledger gerade keine endgültigen Entscheidungen getroffen wird. Dies obliegt allein den Gerichten. Auch helfen transparente Systeme, bei welchen das Miteinander von Rechtslage und technischer Umsetzung verständlich erläutert wird. Hinzu kommen müssen Überlegungen, in welchen Fällen der Selbstvollzug (gleich einer elektronischen Selbsthilfe) zu einer problematischen Umgehung des Schuldnerschutzes führt.[582]

Generell bleibt zu beobachten, ob es einer **neuen Fallgruppe** im Verbraucherschutzrecht bedarf, die der zu erwartenden technischen oder rechtlichen Überforderung und der sich durch die Automatisierung und den Selbstvollzug ergebenen Zwangslage begegnet. Man könnte insbesondere Plattformbetreiber in die Pflicht nehmen und besondere Hinweise vorschreiben. Eine transparente Übersicht zu den Folgen des Programmcodes, Hilfestellung bei Fehlern oder Hinweise auf die mit der sofortigen Ausführung einhergehenden Risiken könnten hilfreich sein. Freilich bleibt die Gefahr einer „**information overload**“, wie sie aus dem Verbraucherkreditrecht bekannt ist. Noch ist die Technologie nicht praktisch umgesetzt und auch ihre künftige Verbreitung ungewiss. Die Folgewirkungen müssen daher zunächst abgewartet werden. Möglicherweise setzt die Industrie von vorneherein selbst auf ausreichend Transparenz, sodass überhaupt kein Bedarf für rechtliche Maßnahmen entsteht.

[582] Siehe bereits S. 75 ff.

XIV. Ergebnisse

Bei Distributed-Ledger-Systemen handelt es sich um Kombinationen aus einer auf viele Rechner verteilten Datenbank (dezentrales Transaktionsregister) und einem Netzwerk zum Austausch von digitalen Informationen oder Werten, dessen Teilnehmer unmittelbar miteinander verbunden sind. Anstelle einer zentralen, alle Daten sammelnden und verifizierenden Stelle tritt eine verteilte Verantwortung der Teilnehmer. Die Daten werden redundant auf allen (vollwertig) teilnehmenden Rechnern gespeichert, während ein Konsens- und Validierungssystem für ihre Integrität und Validität sorgt. In der Regel kann so zwar nicht die Richtigkeit der von außen eingetragenen Daten, zumindest aber deren Unverändertheit und die jeweilige Urheberschaft sicher verifiziert werden. Anders als bei herkömmlichen Datenbanken tritt so die Funktion des Abspeicherns hinter Aspekten der Nachvollziehbarkeit und Transparenz zurück. Die gegenwärtig prominenteste derartige Architektur ist das Blockchain-Modell, bei welchem die Informationen zu Blöcken verschlüsselt und anschließend linear miteinander verkettet werden, sodass eine Kette aus Blöcken entsteht.

Im Register (Ledger) werden Informationen, (Transaktions-)Ergebnisse und Inhaberschaften grundsätzlich eher in Form von Quittungen gespeichert; seltener weisen die Informationen als Token oder Kryptowährungen einen inhärenten Wert auf. Die Steuerung ist, jedenfalls bei öffentlichen Systemen, vom Einfluss einer zentralen Stelle entkoppelt, während die Abläufe des Netzwerks für alle Teilnehmer transparent sind. Ein Fälschungsversuch gilt bei einer entsprechenden Ausgestaltung als unwahrscheinlich bzw. jedenfalls wirtschaftlich unrentabel, jedenfalls würde eine Manipulation sofort bemerkt werden. Die Technologie ersetzt gewissermaßen das Vertrauen in eine zentrale Stelle, indem aus ihr heraus Konsens über die Richtigkeit eines Datensatzes hergestellt wird. Dies erlaubt eine direkte Zusammenarbeit von Parteien, die sich zwar gegenseitig nicht vertrauen, jedoch auf eine einheitliche Abbildung von Daten, Berechnungsergebnissen oder (insb. digitalen) Werten angewiesen sind.

Die im Vergleich zu anderen verteilt funktionierenden Datenbanken herausstehende Fälschungssicherheit und Transparenz zwingt jedoch, je nach Systemgestaltung, zu Konzessionen in Sachen Energieeffizienz, Geschwindigkeit oder Netzwerkgröße. In vielen Fällen wiegen die hervorgebrachten Nachteile bei öffentlichen Netzwerken (noch) schwerer als die potentiell zu erzielenden Gewinne. Zwar lässt sich das Fehlen herausstehender Erfolgsmodelle (jenseits der umstrittenen Kryptowährungen) noch mit dem frühen Entwicklungsstadium und der erforderlichen langen Lernphase erklären, gleichwohl wird hierdurch zumindest die Bedeutung in Frage gestellt, die der Technologie von vielen Stimmen zugeschrieben wird. Noch sind keine belastbaren Anhaltspunkte ersichtlich, welche die Distributed-Ledger-Technologie als Allheilmittel oder Wunderwerk bestätigen würden, das einen echten Kulturwandel hervorruft. Selbst für die erste Etablierung und Verknüpfung mit bestehenden Systemen sind noch einige Hürden zu meistern.

Öffentliche Netzwerke werden derzeit vor allem durch die Kryptowährungen getragen. Produktive Einsatzszenarien lassen sich hingegen zuneh-

mend bei einigen privaten oder konsortialen Netzwerke beobachten, die jedoch weit weniger revolutionäre Formen dezentraler Netzwerke darstellen. In vielen Fällen könnten auch andere Formen verteilter Datenbanken eingesetzt werden. Diesen fehlen jedoch die besondere Transparenz und Nachvollziehbarkeit. Ein weiterer positiver Aspekt der DLT-Diskussion ist zudem, dass alte Arbeitsläufe überdacht werden und die neue Technologie als Anreiz zum Aufbrechen alter Prozesse und Neustrukturierung betrachtet wird.

Eine besondere Eigenschaft der DLT ist die Möglichkeit, Prozess- und Businesslogiken in Form von Programmcode abzubilden, die später garantiert und transparent vollzogen werden. Dies trägt nicht nur in vielen Bereichen zu einer Automatisierung, sondern im Rahmen neuer Kollaborationsmodelle auch zu einem besonderen Vertrauen in die Ausführung der jeweiligen Regeln bei. Ein großes Missverständnispotential birgt jedoch die Bezeichnung des verwendeten Programmcodes als Smart Contract. Es handelt sich nämlich lediglich um in einem Distributed-Ledger implementierte Computerprogramme, die jedoch weder Verträge noch notwendigerweise intelligent sein müssen.

Dennoch ist die Frage berechtigt, ob sich Smart Contracts oder ähnliche Hilfsmittel zur Automatisierung von Vertragsbeziehungen eignen. Selbstvollziehende Verträge brächten sowohl Kosten- als auch Zeitersparnisse und könnten gleichzeitig die tatsächliche Rechtsdurchsetzung voranbringen. Jedoch ergeben sich zahlreiche technische Limitationen, insbesondere angesichts dereingeschränkten Fähigkeit von Programmcode, rechtliche Wertungen und Regelungsstrukturen nachzubilden und der Notwendigkeit von Schnittstellen, um Informationen der analogen Welt einzubinden oder auf Gegenstände der analogen Welt Einfluss nehmen zu können. Diese führen dazu, dass allenfalls Ausschnitte von Vertragsbeziehungen einem Selbstvollzug zugänglich sind. Gerade unabänderliche Smart Contracts verbieten sich für die meisten wirtschaftlich bedeutsamen Vertragsbeziehungen, insbesondere wenn die Parteien nicht über Korrekturschnittstellen verfügen. Einen vollständig automatisierten, sich selbst vollziehenden Vertrag wird es daher auf absehbare Zeit wohl nur in sehr eingeschränkten Fällen geben. Man sollte Smart Contracts daher als schlichte Programme verstehen, die als digitale Hilfsmittel zur Automatisierung von Businessprozessen beitragen, nicht aber als eigenständige und unfehlbare Identität die erfolgreiche Abwicklung jeder Geschäftsbeziehung garantieren. Digitale Hilfsmittel zur Automatisierung von Wirtschaftsprozessen sind freilich keine Novation, sondern ein unser Wirtschaftssystem seit vielen Jahrzehnten prägendes Phänomen. Wie Smart Contracts dazu einen Beitrag leisten und dabei möglichst rechtssicher implementiert werden können, wurde in Kapitel VII zusammengefasst.

Neben einer initialen Einordnung sog. Token, digitaler und meist handelbarer Verkörperungen von Rechten, Berechtigungen oder sonstiger Inhalte, wurden die verschiedenen Implikationen anderer Rechtsbereiche, u.a. des Gesellschafts- und Datenschutzrechts untersucht. Der frühe Entwicklungsstatus führt vor allem dazu, dass viele Fragen nur spekulativ beantwortet werden können und auch in praktischer Hinsicht noch wenige Anwendungsszenarien eine praktische Umsetzung erfahren haben. Wie sich die

Technologie auf große Wirtschaftsbereiche und insbesondere Verbraucher auswirken wird, bleibt demnach abzuwarten.

XV. Gesetzgeberischer Handlungsbedarf

Die vorstehenden Untersuchungen haben gezeigt, dass Smart Contracts bzw. selbstvollziehende Verträge bereits hinreichend vom geltenden Recht erfasst werden können.[583] Es sind keine Gründe ersichtlich, eine neue Kategorie oder Sonderregeln in das bewusst abstrakt gehaltene Regelungsgefüge des BGB zu implementieren.

Die einschlägigen Divergenzrisiken beim Einsatz selbstvollziehender Verträge sind im Wesentlichen auf technische Limitationen zurückzuführen, meist im Zusammenhang mit dem Versuch der Übersetzung zwischen digitaler und analoger Welt bzw. zwischen technischer und rechtlicher Ebene. Diese technischen Limitationen verlangen auch nach technischen Lösungen und erfordern ein wohl überlegtes Abwägen der Parteien, ob sich das Abwicklungsinstrument im Einzelfall auch für die jeweilige Anwendung eignet. Hieraus ergibt sich zwar weiterer Forschungsbedarf, insbesondere im Hinblick auf die technische Abbildbarkeit rechtlicher Sprache und Wertungen. Ein **gesetzgeberischer Handlungsbedarf** ist jedoch nicht ersichtlich.

Eine andere Frage ist es, ob *de lege ferenda* Sonderregelungen für Blockchain-Einträge bestehen sollten. Verschiedentlich wurde bereits vorgeschlagen, dem Ledger eine gewisse Autorität, sei es formelle Legitimationswirkung, die Eigenschaft als Rechtsscheinträger, o.ä. zuzuerkennen. Eine solche gesetzliche Regelung will jedoch gut überlegt sein. Einerseits können pauschale Regelungen der Variationsbreite an Netzwerken und Netzwerktechnologien nur schwer gerecht werden. Weder ist vorhersehbar, welche Architekturen sich durchsetzen, noch, inwiefern verallgemeinerungsfähige Aussagen über Sicherheitsstandards getroffen werden können. Bei kleineren Systemen besteht bei vielen Konsensverfahren zudem ein relevantes Fälschungsrisiko, insb. das einer 51%-Attacke. Schließlich ist selbst eine sichere Blockchain kein Garant für die Richtigkeit der gespeicherten Daten. Sie ist im Hinblick auf Einträge mit Bezug zu Blockchain-externen Ereignissen nur so vertrauenswürdig, wie die Personen oder Quellen, welche die Daten eintragen dürfen.

Letzteres ist nur dann nicht der Fall, wenn die Informationen auf einer Blockchain völlig von Zuständen der analogen Welt abgekoppelt sind. Hierunter fallen sog. Kryptowährungen, deren Zuweisung vollständig und autark vom DL-System verifiziert werden kann. Die Regulierung digitaler Währungen, ebenso wie die Schaffung digitaler Wertpapiere, Beteiligungs- oder Finanzierungsinstrumente oder sonstiger Formen von Krypto-Token werfen weitreichende Rechts- und Regulierungsfragen auf. Ob und inwiefern in dieser Hinsicht gesetzgeberischer Handlungsbedarf besteht, war nicht Gegenstand des Gutachtens und muss aufgrund der Vielschichtigkeit der Thematik eingehend betrachtet werden. Gleichwohl kann erwogen werden, die Blockchain als Regulierungsinstrument zu prüfen. Die Einbeziehung staatlicher Akteure in Echtzeit könnte die Transparenz und Auditierbarkeit der Ledger für einfachere und fälschungssicherere Kontrollsysteme zunutze machen, soweit ohnehin Offenlegungspflichten bestehen.

[583] So auch *Paulus/Matzke*, ZfPW 2018 2018, 431 (436).

Große regulatorische Unklarheiten, die schon jetzt einen dringenden Evaluations- und Handlungsbedarf hervorrufen, bestehen allerdings im Bereich Datenschutz. Die Pflichten eines Verantwortlichen (Art. 4 Nr. 7 DS-GVO) lassen sich nicht in sinnvoller Weise auf öffentliche dezentrale Systeme übertragen. Der diffuse Meinungsstand sowie die teilweise an der technischen Realität vorbeigehenden Einschätzungen der Datenschutzbehörden führen zu einer unklaren und daher unbefriedigenden Rechtslage für Entwickler bzw. die Rechtspraxis. Es bleiben damit die in der Praxis zu beobachtenden Bestrebungen, von vorneherein keine personenbezogenen Daten auf einem öffentlichen Ledger zu speichern und so die Anwendbarkeit der DS-GVO von vorneherein auszuschließen, alternativ der Rückgriff auf zulassungsbeschränkte Ledger. Eine gesetzgeberische Klarstellung, freilich auf Unionsebene, würde den Umgang mit dezentralen Systemen ohne steuernde und damit verantwortliche Stelle erleichtern.

Im Übrigen bleibt anzuregen, insbesondere im frühen Stadium einer Technologie aber auch sonst bei jedem Innovationsgewinn zu fragen, ob mit vorgeschlagenen rechtlichen Neuerungen nicht bedeutsame Instrumente oder gar unverzichtbare (rechtliche) Mechanismen verloren gehen. Eine formalisierte Rechtssprache etwa brächte in einigen Bereichen zwar Automatisierungspotential mit sich, kann jedoch schlicht nicht auf alle Umstände des Einzelfalls Rücksicht nehmen. Ob dies dem Anspruch einer Rechtsordnung genügt, die Lösungen für eine analoge Welt finden soll, deren Abläufe in keiner Weise formal und logisch stringent vonstatten gehen, erscheint zweifelhaft.

XVI. Ausblick

Noch scheint der Hype um die Distributed-Ledger-Technologie also überzogen; insbesondere das Versprechen, sie würde „disruptiv“ wirken und alsbald althergebrachte Arbeitsweisen ablösen. Doch wohin könnte der Weg gehen?

Sie verspricht vor allem die Herstellung von Transparenz bei Prozessabläufen, eine verbindliche Gewähr eines einheitlichen Datenbestands für mehrere Parteien und Automatisierungspotential unter Einbindung von Smart Contracts. Es handelt sich um eine Grundlagentechnologie, die auf der Anwendungsebene für die Nutzer häufig unbemerkt bleiben wird. Ob sich hieraus in den kommenden Jahren etablierte Systeme entwickeln können und die Technologie auch weiter vorangetrieben wird, dürfte im Wesentlichen von größeren Unternehmen abhängen. In im Rahmen des Projekts JUSTiCE durchgeführten Experteninterviews zeigte sich, dass aktuelle Projekte in der Regel private oder konsortiale Netzwerklösungen anstelle öffentlicher fokussieren. Der Technologie wird nach einer längeren Trainings- und Lernphase zwar durchaus Anwendungspotential zugeschrieben, dennoch sei zunächst in Produktivszenarien die versprochenen Effizienzgewinne bzw. Erschließung neuer Anwendungsfelder zu beweisen, um eine weitere Forschung zu rechtfertigen. Der Hype um öffentliche Netzwerke kam mit dem Crash des Bitcoin-Kurses Ende 2018 teilweise zum Erliegen. Von den Sonderfragen der sog. Kryptowährungen abgesehen wird es wohl zunächst an den privaten und zulassungsfreien Netzwerken hängen, ob die private Technologieforschung weiter vorangetrieben wird und damit Anwendungsszenarien für öffentlichen Ledger ermöglicht werden.

Die DLT wird nicht jeden Intermediär ausschalten können und sollte das in vielen Fällen auch nicht.[584] Gleichwohl schafft die Technologie in zweierlei Hinsicht einen Anreiz zur Kollaboration bisher gegeneinander arbeitender Akteure: Einerseits können gemeinsame Abläufe in einen gemeinsam verwalteten Prozessrahmen eingebettet und hierdurch transparent und möglicherweise kostensparender vollzogen werden; andererseits kann in vertrauenssensiblen Bereichen unter Umständen das System die vertrauensstiftende Rolle eines Mittlers übernehmen und damit eine unmittelbare Zusammenarbeit erst ermöglichen. Die heutige Konzentration vieler Angebote auf teilweise monopolistische Züge aufweisende Plattformen könnte perspektivisch durch neue kollaborative Modelle bzw. neue Formen der Zusammenarbeit abgelöst werden. Gelingt es, zahlreiche Akteure in einem (möglicherweise sehr groß gefassten) Geschäftsfeld oder Anwendungsbereich zu verbinden, könnten diese mithilfe eines Ledger-Netzwerks selbst die Regeln und Abläufe festlegen und damit die Gestaltung ihres zukünftigen Nachfragemarktes in die Hand nehmen. Erforderlich ist freilich ein Wille zu und eine Rechtfertigung von Transparenz. Weitere Entwicklungen, wie die Schaffung eines sicheren Netzwerks zur Abwicklung von Micro-Transaktionen,[585] Bestrebungen im Bereich des Datentrackings und Datenhandels oder einer Infrastruktur für eine zunehmende M2M-Vernetzung

[584] Mitunter bestehen etwa rechtliche Interessen an der Identifizierung beteiligter Personen durch eine verantwortliche Stelle, etwa im Rahmen der Geldwäscheprävention.

[585] *Wright/De Filippi*, S. 29 f.; etwa zur Einrichtung von Vergütungssystemen in Echtzeit, *Schütte* et. al., Fraunhofer Positionspapier Blockchain, S. 23.

und Kommunikation[586] müssen eventuell hinzukommen und Synergien mit der Zeit beobachtet werden.

Ein wesentlicher Schritt für die dauerhafte Etablierung der DLT in verschiedenen Lebensbereichen wäre die Entwicklung eines globalen Systems im Bereich des **Identitätsmanagements** bzw. von **Identitätsnachweisen**, sowohl im Hinblick auf Personen aber auch die Herkunft von Gütern (Assets).[587] In einer vernetzen Welt ist die Möglichkeit, sich durch eine unabänderlichen ID auszuweisen, von großer Bedeutung. Jeder könnte als Nutzer nacheigenem Ermessen Informationen über sich teilen (souveräne Identität) und diese mittels seines Schlüssels verifizieren.[588] Mit dem Begriff Identität ist dabei nicht nur die konkrete Identifizierung einer Person oder eines Assets gemeint sein. Vielmehr können mit diesen auch untrennbar bestimmte Eigenschaften verknüpft werden, etwa die Kreditwürdigkeit einer Person bzw. der Lebenszyklus und Wartungsaufwand einer Sache, etc.[589] Erst dann gelingt ein globaler Austausch von Werten bzw. eine sichere Vernetzung ohne vermittelnde Intermediäre.

[586] *Wright/De Filippi*, S. 33 f.
[587] *Reed/Sathyanarayan/Ruan/Collins*, S. 14 f.
[588] *Reed/Sathyanarayan/Ruan/Collins*, S. 15.
[589] *Reed/Sathyanarayan/Ruan/Collins*, S. 7.

XVII. Schlusswort

Die Blockchain bzw. DL-Technologie ist (jedenfalls noch) nicht so disruptiv, wie immer behauptet wird. Für einige Anwendungsfälle bringt sie tatsächlich grundlegende Neuerungen, in der Regel bestärkt sie hingegen die Fortentwicklungen des Bestehenden. Gerade im Bestreben um die Automatisierung kann sie als Triebfeder bezeichnet werden, indem sie potentiell eine sichere Kommunikation zwischen Maschinen ermöglicht oder zur Digitalisierung bislang noch papiergebundener Prozesse anregt. Neue kollaborative oder kooperative Modelle, sowohl im wirtschaftlichen wie auch nicht wirtschaftlichen Bereich, könnten durch die DLT hervorgebracht, getragen oder inspiriert werden. In transparenzsensiblen Bereichen verspricht schließlich die Authentizität und Transparenz Vorteile gegenüber herkömmlichen Verfahren.

Auf der anderen Seite ist die DLT weder ein Allheilmittel, noch in vielen Fällen die einzige Technologie, die vielversprechende Ergebnisse liefern kann. Man „braucht“ in der Regel keine Blockchain. Die Konsensverfahren in öffentlichen Systemen schaffen nicht notwendigerweise eine gleichberechtigte Beteiligung, während die optimale Systemaufstellung für offene Teilnehmerkreise erst noch gefunden werden muss. Wie auch im Hinblick auf Smart Contracts und selbstvollziehende Verträge ist die Frage nach dem richtigen Einsatz und dem richtigen technischen wie rechtlichen Rahmen entscheidend. Die Vereinbarkeit der Systemkreise Technik und Recht muss gewährleistet sein.

Der perspektivische Erfolg der DLT hängt vor allem davon ab, ob Produktivszenarien Anreiz für weitere Forschung und Entwicklung setzen. Neue Modelle der Zusammenarbeit, die insbesondere durch eine digitale Identität getragen werden, könnten sich als die Triebfeder erweisen. Deren Ausgestaltung, aber auch die derzeit stark im Aufwind befindliche „Tokenisierung“ werfen vielseitige Rechts- und Umsetzungsfragen auf. Erneut ist das frühe Entwicklungsstadium der Technologie hervorzuheben. Um gegenwärtig bereits en prognostizierten Wertewandel festzustellen, ist es noch zu früh. Die hinter dem Gedanken der Dezentralität stehenden Bestrebungen Machtkonzentrationen zu verhindern, den Einfluss großer Plattformen und anderer Intermediäre einzudämmen und neue Mitgestaltungsmöglichkeiten zu etablieren, können zukünftig auf vielerlei Art verfolgt und erreicht werden.Die Distributed-Ledger-Technologie kann hierzu einen Beitrag leisten. Ob ihr das nachhaltig gelingt, werden die kommenden Jahre zeigen.

Literaturverzeichnis

Ammann, Thorsten: Bitcoin als Zahlungsmittel im Internet, CR 2018, 379–386

Al Khalil, Firas / Ceci, Marcello / O´Brien, Leona / Butler, Tom: A Solution for the Problems and Transparency in Smart Contracts, GRTC, 2017, abrufbar unter: https://e9a5d5c6.stackpathcdn.com/wp-content/uploads/2017/06/GR3C-Smart-Contracts-White-Paper-2017.pdf

Beaucamp, Sophie / Henningsen, Sebastian / Florian, Martin: Strafbarkeit durch Speicherung der Bitcoin-Blockchain?, MMR 2018, 501–507

Bechtholf, Hans / Vogt, Niklas: Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66–71

Beck, Benjamin / König, Dominik: Der Versuch einer vertragstypologischen Einordnung von kryptographischem Geld, JZ 2015, 130–138

Beck, Wolfgang: Chancen und Risiken der Distributed-Ledger- und Blockchain-Technologien, DVP 2018, 251–255

Bertram, Ute: Smart Contracts, MDR 2018, 1416–1421

Blocher, Walter: The next big thing: Blockchain – Bitcoin – Smart Contracts, AnwBl. 2016, 612–618

Böhme, Rainer / Pesch, Paulina: Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD 2017, 473–481

Bonneau, Joseph / Miller, Andrew / Clark, Jeremy / Narayanan, Arvind / Kroll, Joshua / Felten, Edward: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, IEEE Security and Privacy, abrufbar unter: http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

Borkert, Kristian: Crowdfunding goes Blockchain, ITRB 2018, 39–43 und 91–95

Brisch, Klaus / Pieper, Fritz: Das Kriterium der „Bestimmbarkeit“ bei Big Data-Analyseverfahren, CR 2015, 724–729

Brown, Richard / Carlyle, James / Grigg, Ian / Hearn, Mike: Corda: An Introduction, 2016, abrufbar unter: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

Buchleitner, Christina / Rabl, Thomas: Blockchain und Smart Contracts, ecolex 2017, 4 ff.

Bundesamt für Sicherheit in der Informationstechnik: BSI – Technische Richtlinie – Kryptographische Verfahren, Stand: 22. Februar 2019, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=4)

Christidis, Konstantinos / Devetsiokiotis, *Michael*: Blockchains and Smart Contracts for the IoT, IEEE Access, 2016, 2292–2303

Clack, Christopher: Smart Contract Templates: legal semantics and code validation, 2018, abrufbar unter: https://arxiv.org/pdf/1612.04496.pdf (zitiert als: *Clack*, Smart Contract Templates III)

Clack, Christopher / Bakshi, Vikram / Braine, Lee: Smart Contract Templates: foundations, design landscape and research directions, 2016, abrufbar unter: https://arxiv.org/pdf/1608.00771.pdf (zitiert als: *Clack/Bakshi/Braine*, Smart Contract Templates I)

Clack, Christopher / Bakshi, Vikram / Braine, Lee: Smart Contract Templates: essential requirements and design options, 2016, abrufbar unter: https://arxiv.org/pdf/1608.00771.pdf (zitiert als: *Clack/Bakshi/Braine*, Smart Contract Templates II)

Djazayeri, Alexander: Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016, Anm. 1

Ekkenga, Jens, Bitcoin und andere Digitalwährungen – Spielzeug für Spekulanten oder Systemveränderung durch Privatisierung der Zahlungssysteme?, CR 2017, 762-768

Engelhardt, Christian / Klein, Sascha: Bitcoins – Geschäfte mit Geld, das keines ist - Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355–360

Eschenbruch, Klaus / Gerstberger, Robert, Smart Contracts – Planungs-, Bau- und Immobilienverträge als Programm?, NZBAU 2018, 3–8

Fazekas, *Zoltan*: Wie funktioniert eigentlich die Blockchain? Teil 2: Smart Contracts, die Businesslogik von Blockchain-Anwendungen, abrufbar unter: https://www.iteratec.de/tech-blog/artikel/news/wie-funktioniert-eigentlich-die-blockchain-teil-2-smart-contracts-die-businesslogik-von-blockchai/

Fraunhofer FIT, Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik, Mai 2019, abrufbar: https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile

Fries, Martin: Private Law Compliance through Smart Contracts?, Compliance Alliance 2018, Vol 4, 11–18

Froitzheim, Oliver, Anmerkung zu KG, Urt. v. 25.9.2018 – (4) 151 Ss 28/18 (35/18), BKR 2018, 473–477

Funk, Christian, Allgemeine Geschäftsbedingungen in Peer-to-Peer-Märkten, Karlsruhe 2010

Glatz, Florian: Blockchain – Ein Paradigmenwechsel, in: *Breidenbach/Glatz,* Rechtshandbuch Legal Tech, München 2018, 59–78

Grigg, Ian: The ricardian contract, In Proceedings of the First IEEE International Workshop on Electronic Contracting, 2004, 25–31, abrufbar unter: http://iang.org/papers/ricardian_contract.html.

Grigg, Ian: On the intersection of ricardian and Smart Contracts, 2015, abrufbar unter: http://iang.org/papers/intersection_ricardian_smart.html

Grigg, Ian: The sum of all chains – let's converge!, 2015, Presentation for Coinscrum and Proof-of-Work, abrufbar unter: https://financialcryptography.com/mt/archives/001556.html

Gsell, Beate / Krüger, Wolfgang / Lorenz, Stephan / Reymann, Christoph (Gesamthrsg.): Beck´scher Online Großkommentar zum BGB

Guggenberger, Nikolas: The Potential of Blockchain-Technology for the Conclusion of Contracts, in: Schulze/Staudenmayer/Lohsse (Hrsg.), Contracts for the Supply of Digital Contents: Regulatory Challenges and Gaps, München 2017, S. 83–96

Habersack, Mathias / Mülbert, Peter / Schlick, Michael (Hrsg.): Unternehmensfinanzierung am Kapitalmarkt, 4. Auflage, Köln 2018

Hart, *Oliver*: Incomplete Contracts and Control, American Economic Review 107 (7), 2017, 1371 ff.

Heckelmann, Martin: Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504–510

Heckmann, Dirk / Schmid, Alexander, Blockchain und Smart Contracts – Recht und Technik im Überblick, vbw Studie, Passau, Oktober 2017, abrufbar unter: https://bit.ly/2CUq4aE

Hofert, Eduard: Blockchain-Profiling, ZD 2017, 161–166

Hoppen, Peter: „The DAO-Hack" und der letzte Flug Otto Lilienthals am 09.08.1896, CR-Online.de Blog, abrufbar unter: https://www.cr-online.de/blog/2016/06/21/thedao-hack-und-der-letzte-flug-otto-lilienthals-am-09-08-1896/

Jaccard, Gabriel: Smart Contracts and the Role of Law, Jusletter IT 23, November 2017

Janicki, Thomas / Saive, David: Privacy by Design in Blockchain-Netzwerken, ZD 2019, 251–256

Jauernig, Othmar (Hrsg.): Bürgerliches Gesetzbuch, 17. Auflage, München 2018

Kaulartz, Markus: Herausforderungen bei der Gestaltung von Smart Contracts, InTeR 2016, 201–206

Kaulartz, Markus / Heckmann, Jörn: Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, 618– 624

Kaulartz, Markus / Matzke, Robin: Die Tokenisierung des Rechts, NJW 2018, 3278–3283

Kolain, Michael / Wirth, Christian, Multichain-Governance, DSRI Tagungsband 2017, 845–852

Krüger, Fabian / Lampert, Michael: Augen auf bei der Token-Wahl - privatrechtliche und steuerliche Herausforderungen im Rahmen eines Initial Coin Offering, BB 2018, 1154–1160

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

Kütük, Merih/ Sorge, Christoph, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie“ zur „Bitcoinmanie“, MMR 2014, 643–646

Kuhlmann, Nico: Bitcoins, Funktionsweise und rechtliche Einordnung der digitalen Währung, CR 2014, 691–696

Langenbucher, Katja: Digitales Finanzwesen, AcP 218 (2018), 385–429

Lauslathi, Kristian /Mattila, Juri / Sepällä, Timo: Smart Contracts – How will Blockchain Technology Affect Contractual Practices, ESLA Reports No. 68, 2017, abrufbar unter: https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-68.pdf

Lessig, Lawrence: Code: And other Laws of Cyberspace, New York 1999

Levy, Karen: Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law, Engaging Science, Technology, and Society 3 (2017), 1–15

Mainelli, Michael /Milne, Alistair, The Impact and Potential of Blockchain on the Securities Transaction Lifecycle, SWIFT Institute Working Paper No. 2015-007, abrufbar unter: http://www.smallake.kr/wp-content/uploads/2016/09/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL-1.pdf

Mann, Maximilian, Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp?, NZG 2017, 1014–1020

Matzutt, Roman / Hiller, Jens / Henze, Martin / Ziegeldorf, Jan Hernik / Müllmann, Dirk / Hohlfeld, Oliver / Wehrle, Klaus: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, RWTH Aachen/Goethe-Universität Frankfurt/Main, 2018, abrufbar unter: https://fc18.ifca.ai/preproceedings/6.pdf

Martini, Mario / Weinzierl, Quirin: Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251–1259

Mik, Eliza: Law, Innovation and Technology 2017 (9.2), 269 ff., zitiert nach https://ssrn.com/abstract=3038406

Müller, Martin: Bitcoin, Blockchain und Smart Contracts, ZfIR 2017, 600–611

Münchener Kommentar Bürgerliches Gesetzbuch
Band 1: Allgemeiner Teil, 7. Auflage 2015
Band 2: Schuldrecht Allgemeiner Teil, 7. Auflage, München 2016
Band 3: Schuldrecht Besonderer Teil I, 7. Auflage 2016
Band 6: Schuldrecht Besonderer Teil IV, 7. Auflage 2017
Band 7: Sachenrecht, 7. Auflage 2017

Münchener Kommentar zur Zivilprozessordnung
Band 2: §§ 355 – 945b, 5. Auflage 2016

O´Leary, David: Configuring Blockchain Architectures for Transaction Information in Blockchain Consortiums: The Case of Accounting and Supply Chain Systems, Intelligent Systems in Accounting, Finance and Management 24 (2017), 138 – 147, abrufbar unter: https://onlinelibrary.wiley.com/doi/full/10.1002/isaf.1417

Patz, Anika: Anmerkung KG, Urteil vom 25.9.2018 – (4) 161 Ss 28/18 (35/18), MMR 2018, 828–833

Paulus, Christoph / Matzke, Robin: Digitalisierung und private Rechtsdurchsetzung – Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?, CR 2017, 769 – 778

Paulus, Christoph / Matzke, Robin: Smart Contracts und Smart Meter – Versorgungssperre per Fernzugriff, NJW 2018, 1905–1911

Paulus, David / Matzke, Robin: Smart Contracts und das BGB – Viel Lärm um nichts? –, ZfPW 2018, 431–465

Pesch, Paulina / Sillaber, Christian: Distributed-Ledger, Joint Control? – Blockchains and the GDPR´s Transparency Requirements, Cri 2017, 166–172

Raskin, Max: The law and legality of Smart Contracts, Georgetown Law Technology Review, Vol. 1:2 (2017), 305–341

Reed, Chris / Sathyanarayan, Umamahesh / Ruan, Shuhui / Collins, Justine: Beyond Bitcoin – legal impurities and off-chain assets, Queen Mary University of London, School of Law Legal Studies Research Paper No. 260/2017, abrufbar unter: https://ssrn.com/abstract=2154404

Saive, David: Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 183–196

Samman, *George*: The Trend Towards Blockchain Privacy: Zero Knowledge Proofs, 2016, abrufbar unter: http://www.Coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs.

Sattler, Andreas: Der Einfluss der Digitalisierung auf das Gesellschaftsrecht, BB 2018, 2243– 2253

Schlund, Albert / Pongratz, Hans: Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, DStR 2018, 598–604

Schrey, Joachim / Thalhofer, Thomas: Rechtliche Aspekte der Blockchain, NJW 2017, 1431–1436

Schütte, Julian et. al.: Fraunhofer Gesellschaft, Positionspapier Blockchain und Smart Contracts, 2017, abrufbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf?_=1516641660

Schulz, Hajo: Vertrag denkt mit – Smart Contracts in der Ethereum-Blockchain, c´t 2017, 108–112

Schwintowski, Hans-Peter / Klausmann, Nikolas / Kadgien, Michael: Das Verhältnis von Blockchain-Governance und Gesellschaftsrecht, NJOZ 2018, 1401–1406

Shmatenko, Leonid /Möllenkamp, Joachim: Digitale Zahlungsmittel in einer analog geprägten Rechtsordnung, MMR 2018, 495–501

Simmchen, Christoph: Blockchain (R)Evolution – Verwendungsmöglichkeiten und Risiken, MMR 2017, 162–165

Söbbing, Thomas: Smart Contracts und die Blockchain-Technologie, ITRB 2018, 43–46

Sosnitza, Olaf: Das Internet der Dinge – Herausforderung oder gewohntes Terrain für das Zivilrecht?, CR 2016, 764–772

Spalink, Joachim: Ethereum Smart Contracts: Eine technische Einführung, RI 2018, 95–99

Specht, Louisa / Herold, Sophie: Roboter als Vertragspartner?, MMR 2018, 40–44

Spindler, Gerald / Bille, Martin: Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357–1369

Staudinger, *Julius von*: Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetzen und Nebengesetzen, Berlin

Swanson, Tim: Consensus-as-a-service: a brief report on the emergence of permissioned, Distributed-Ledger systems, 2015, abrufbar unter: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

Szabo, Nick: Smart Contracts: Formalizing and Securing Relationships on Public Networks, First Monday, Volume 2, Number 9 (1997), abrufbar unter: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html

Szabo, Nick: Wet code and dry, 2006, abrufbar unter: https://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html

Tschorsch, Florian /Scheuermann, Björn: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Commun. Surveys Tuts. 2016, 2084–2123

Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web, Technologiestiftung Berlin, 2016, abrufbar unter: https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf

Wagner, Bernd: Disruption der Verantwortlichkeit, ZD 2018, 307–312

Wagner, Jens: Legal Tech und Legal Robots in Unternehmen und den sie beratenden Kanzleien, BB 2017, 898–905

Wagner, Axel-Michael / Groß, Stefan: White Paper Blockchain und Smart Contracts, München 2018, abrufbar unter: https://www.psp.eu/media/allgemein/white_paper_blockchain.pdf

Walport, Mark: Government Office for Science: Distributed-Ledger Technology: beyond block chain – A report by the UK Government Chief Scientific Adviser, 2015, abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Weitnauer, Wolfgang: Initial Coin Offerings (ICOs): Rechtliche Rahmenbedingungen und regulatorische Grenzen, BKR 2018, 231–236

Wilsch, Harald: Die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts, DNotZ 2017, 761–787

Wright Aaron / De Filippi, Primavera: Decentralized Blockchain Technology and the rise of *Lex Cryptographia*, 2015, abrufbar unter: https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf

Zickgraf, Peter: Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?, AG 2018, 293–308

Zimmermann, Anton: Blockchain-Netzwerke und internationales Privatrecht – oder: der Sitz dezentraler Rechtsverhältnisse, IPRax 2018, 566–573

Zwanzger, Michael: Der mehrseitige Vertrag, Tübingen 2013 (zugl. Diss. Bayreuth 2012)

Zyskind, Guy / Nathan, Oz / Pentland, Alex: Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015, abrufbar unter: https://enigma.co/ZNP15.pdf

Abbildungsverzeichnis

Impressum

Der Autor weiß um die Bedeutung einer geschlechtergerechten Sprache und befürwortet grundsätzlich ihren Gebrauch. Von einer durchgehenden Bennenung beider Geschlechter bzw. der konsequenten Verwendung geschlechterneutraler Bezeichnungen wurde im vorliegenden Text dennoch zumeist abgesehen, weil dies die Lesbarkeit deutlich erschwert werden würde.

Besonderer Dank gilt Frau Katrin Rentzsch und Herrn Lorenz Dudew für die kritische Durchsicht, Herrn Dudew zudem für die Gestaltung des Titelblattes und umfangreiche Formatierungshilfe.

Verfasser:
Ref. iur. Nico Bilski

Betreuer:
Prof. Dr. Michael Zwanzger

Lehrstuhl für Bürgerliches Recht,
Rechtsgeschichte und
Europäische Rechtsharmonisierung
Universität Leipzig

Juristenfakultät, Burgstraße 27,
04109 Leipzig

Telefon: +49 341 97 35 140
nico.bilski@uni-leipzig.de
sekretariatzwanzger@uni-leipzig.de