Bundesministerium
für Verkehr und
digitale Infrastruktur

Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik

Fraunhofer FIT

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE INFORMATIONSTECHNIK FIT

CHANCEN UND HERAUSFORDERUNGEN VON DLT (BLOCKCHAIN) IN MOBILITÄT UND LOGISTIK

Prof. Dr. Gilbert Fridgen
Prof. Dr. Nikolas Guggenberger
Prof. Dr. Thomas Hoeren
Prof. Wolfgang Prinz (PhD)
Prof. Dr. Nils Urbach

Johannes Baur, Henning Brockmeyer, Wolfgang Gräther, Elisaweta Rabovskaja,
Vincent Schlatt, André Schweizer, Johannes Sedlmeir, Lars Wederhake

Vielen Dank den weiteren Mitwirkenden:
Matthias Babel, Martin Brennecke, Patrick Camus, Benedict Drasch, Tobias Guggenberger,
Luis Lämmermann, Jannik Lockl, Sven Radszuwill, Alexander Rieger, Marco Schmidt, Nico Thanner,
Patrick Troglauer, Florian Vogt, Malte Weißert, Felix Würmseher

Inhalt

1 Management Summary

1.1 Zielsetzung des Gutachtens

Das vorliegende Grundgutachten stellt die ökonomischen Potenziale, die rechtlichen Rahmenbedingungen und die für das Verständnis notwendigen technischen Grundlagen der Distributed-Ledger- bzw. Blockchain-Technologie vor, um die Chancen und Herausforderungen dieser Technologien insbesondere im Mobilitäts- und Logistiksektor zu verdeutlichen. Das Grundgutachten wurde im Auftrag des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) durch das Blockchain-Labor des Fraunhofer FIT erarbeitet.

Es richtet sich an junge Unternehmen, die bspw. eine rechtliche Einschätzung bezüglich Fragen des Datenschutzes im Bereich DLT/Blockchain suchen, an Entscheider aus der Privatwirtschaft, die bspw. anhand konkreter Beispiele verstehen wollen, wie diese Technologie auf bestehende sowie entstehende Märkte wirkt und welche Handlungsoptionen aus unternehmerischer Perspektive sinnvoll sein könnten, an Entscheider aus der Politik, welche bspw. Implikationen für ihre Positionierung zu diesem Thema insbesondere im Hinblick auf die Sektoren Mobilität und Logistik gewinnen möchten sowie an die an der Technologie und ihren Potenzialen interessierte Öffentlichkeit. Nicht im Fokus der Zielleserschaft stehen rein wissenschaftlich fokussierte Interessenten, wenngleich einige Beiträge des Gutachtens den Status quo des akademischen Diskurses widerspiegeln.

Die schnell voranschreitende Digitalisierung betrifft mittlerweile nahezu alle Bereiche unserer Gesellschaft. Grundlagen dieser Entwicklung sind dabei insbesondere der allgegenwärtige Einsatz von digitaler Informationstechnologie (IT) (Ubiquitous Computing), immer kürzere Innovationszyklen und die Konvergenz – also das Zusammenwachsen – der digitalen Technologien bzw. Innovationen. Eine dieser Technologien, der besonderes Potenzial zugesprochen wird, ist die Distributed-Ledger-Technologie (DLT). Im Jahr 2009 fand die DLT in Form einer Blockchain für die Kryptowährung Bitcoin erstmalig eine breite Anwendung. Seitdem hat sich die DLT zu einer vielseitig einsetzbaren Technologie weiterentwickelt: In praktisch jeder Branche existieren bereits prototypische Anwendungen von DLT-Lösungen. Diese Anwendungen zeigen u. a. die Potenziale von sogenannten Smart Contracts zur Abbildung von Geschäftslogik. Vermehrt zeichnet sich ab, dass die DLT als Innovationstreiber potenziell disruptive Veränderungen in vielen Wirtschafts-, Rechts- und Gesellschaftsfeldern sowie der öffentlichen Verwaltung hervorbringen könnte. DLT als ein transparentes, elektronisches Register für Informationen, das durch die Teilnehmer eines verteilten Rechnernetzes verwaltet wird, bietet eine Antwort auf bisher unerfüllt gebliebene Anforderungen an die Informations- und Kommunikationstechnik: Sichere Verarbeitung von Informationen und Transaktionen, Manipulationsresistenz und dezentrale Konsensbildung sind ihre inhärenten Eigenschaften. DLT ermöglicht als höherwertige digitale Infrastruktur eine Fortentwicklung vom heutigen „Internet der Informationen“ zum „Internet der Werte und des Vertrauens“.

Insbesondere die Sektoren Mobilität und Logistik weisen eine Vielzahl an Eigenschaften auf, welche diese beiden Sektoren für die DLT als besonders geeignet erscheinen lassen. Im Mobilitätssektor tragen hierzu besonders jüngste Entwicklungen bei: die Kommunikation vernetzter Fahrzeuge mit ihrer Umwelt, intermodale Verkehrskonzepte und der Aufbau kleinteiliger Elektroladeinfrastruktur. Im Logistiksektor existieren zahlreiche organisationsübergreifende Prozesse, die aktuell nur sehr ineffizient (bspw. mit enormem Papierverbrauch) ablaufen und dringend digitale Unterstützung benötigen. Diese digitale Unterstützung könnte durch DLT erstmalig praktisch umsetzbar werden.

DLT adressiert die Kompetenzbereiche des BMVI auf zweierlei Art. Erstens, zur Umsetzung von vielversprechenden Anwendungen im Mobilitäts- und Logistiksektor. Zweitens, zur Schaffung und Bereitstellung von digitalen Infrastrukturen. Lediglich durch den proaktiven Umgang mit DLT kann sichergestellt werden, dass die Technologie dem deutschen Rechts- und Wertesystem entsprechend weiterentwickelt wird und der deutschen Wirtschaft und Gesellschaft den erhofften Mehrwert stiften kann. Deutschland verfügt über eine hervorragende Ausgangslage, da die Entwicklung bei DLT aktuell sehr stark durch Start-ups und Forschung aus Deutschland heraus erfolgt. Somit ist es folgerichtig und wichtig, dass der Staat in diesem Kontext aktiv wird, um das Momentum zu nutzen und die Entwicklung von DLT in seinem Sinne zu prägen. Dieses Grundgutachten fungiert somit als Grundlage für die Formulierung weiterführender Handlungsempfehlungen, damit die politische Zielsetzung – den Einsatz von DLT zur Steigerung der Wohlfahrt und Stärkung der deutschen Wirtschaft proaktiv und rechtssicher zu gestalten – erfüllt werden kann.

Im Rahmen des Grundgutachtens werden ökonomische, rechtliche und, wo es relevant ist, auch technische Fragestellungen identifiziert, analysiert und je nach Fragestellung disziplinär oder interdisziplinär bearbeitet. Die Analysen aus verschiedenen Perspektiven erfolgten dabei nicht unabhängig voneinander, sondern durch kontinuierlichen Austausch unter Experten aus Forschung, Wirtschaft, Verbänden und Politik.

1.2 Allgemeine Analyse

1.2.1 Technische Betrachtung

Der Begriff Distributed-Ledger-Technologie bezeichnet eine Form von Datenbanksystemen, welche sich durch gemeinsame und synchronisierte Datenhaltung in einem Peer-to-peer-Netzwerk sowie fortlaufende, kryptografische Verkettung der Daten auszeichnen. Blockchain stellt eine konkrete Ausgestaltungsform dieser Technologie dar. Andere Ausgestaltungsformen sind bspw. gerichtete, azyklische Graphen. Die Informationen werden dabei in Blöcken gespeichert („Block“), über kryptografische Methoden miteinander verkettet („Chain“) und in jedem Knoten des Netzwerks mittels Peer-to-peer-Protokollen redundant gespeichert, d. h., bei jedem Teilnehmer am Netzwerk liegen dieselben Informationen bzw. Daten vor. Das verteilte Netzwerk unabhängiger Rechner (Knoten), die dafür miteinander kommunizieren und sich synchronisieren, verifiziert und bestätigt diese Blöcke über einen sogenannten Konsensmechanismus. Der derzeit gebräuchlichste Konsensmechanismus, der in der Bitcoin- und Ethereum-Blockchain verwendet wird, wird als „Proof of Work“ bezeichnet. Daneben existieren mittlerweile mehrere alternative Konsensmechanismen, die jeweils abhängig von der spezifischen Ausgestaltung des DLT-Netzwerks gewisse Vor- und Nachteile mit sich bringen. Zudem bieten DLT-Lösungen der zweiten Generation meist die Möglichkeit, sogenannte Smart Contracts zu definieren und zu nutzen. Als Smart Contracts wird Programmcode bezeichnet, der in die DLT geschrieben und entsprechend von allen Teilnehmern am DLT-Netzwerk redundant bzw. verifizierbar ausgeführt werden kann. Dadurch können DLT nicht nur zur sicheren Speicherung von Daten genutzt werden, sondern darüber hinaus Geschäftslogiken abbilden und ausführen. Wegen des breiten Spektrums an Anwendungsmöglichkeiten steigen jedoch die Anforderungen hinsichtlich der Skalierbarkeit und Energieeffizienz von DLT-Systemen. Um den aktuellen Entwicklungen gerecht zu werden, wird an innovativen, skalierbaren und energieeffizienten Systemen geforscht. Diese Forschungsarbeiten haben auch bereits erste Erfolge vorzuweisen, sodass gängige Kritik über Ineffizienz und hohen Energieverbrauch nur bereits überholte Systeme betrifft.

Neben der zeitlichen Entwicklung der DLT können diese u. a. auch nach dem Grad der Öffentlichkeit in öffentliche und private sowie nach dem Grad der Zugriffsbeschränkung

in permissioned und permissionless Systeme unterteilt werden. An öffentlichen Systemen, wie bspw. der Bitcoin-Blockchain, kann prinzipiell jeder teilnehmen und sehen, welche Transaktionen hinzugefügt werden. Ein solches System organisiert sich somit selbst, da es ohne zentrale Instanz (vgl. Bank) konzipiert ist und die Netzwerkteilnehmer Entscheidungen via Konsensmechanismus dezentral treffen. In diesem Zusammenhang ist es wichtig, dass es für die Teilnehmer des Netzwerks genügend Anreize gibt, sich an der Konsensfindung zu beteiligen. Geschieht dies nicht, kann es leicht zu einer Dominanz von einigen wenigen Mitgliedern kommen, was dem Grundgedanken von DLT widerspricht und Manipulationen ermöglichen kann. In privaten Systemen existieren Zugangsbeschränkungen, d. h., Teilnehmer müssen sich registrieren, um in das Netzwerk aufgenommen zu werden. In permissionless Systemen können Netzwerkteilnehmer ohne Beschränkungen alle Aktionen ausführen. Ist das System hingegen permissioned, gibt es Rollenprofile, sodass bestimmte Teilnehmer nur bestimmte Aktionen ausführen können. Beispielsweise kann festgelegt werden, dass nur bestimmte Teilnehmer in den Prozess der Konsensfindung eingebunden werden. Da bei einer privaten (auch konsortialen) DLT-Anwendung häufig bereits ein gewisser Grad an Vertrauen zwischen den Netzwerkmitgliedern vorhanden ist, können hier effizientere Konsensmechanismen im Vergleich zu „Proof of Work" verwendet werden. Beispielsweise genügt in privaten DLT-Systemen oft eine geringe Anzahl von Akteuren, die aktiv an der Konsensfindung teilnehmen.

Beispiele bekannter DLT sind Bitcoin (öffentlich, permissionless), Ethereum (öffentlich, permissionless – geeignet für die Entwicklung von massentauglichen Smart Contracts), Hyperledger Fabric (privat, permissioned – modularer Aufbau), Sovrin (öffentlich, permissioned – speziell für digitale Identitäten) oder IOTA (öffentlich, permissioned – unterstützt Mikrozahlungen). Zwar basieren all diese auf demselben Basiskonzept, eine direkte Interaktion und Kommunikation zwischen den unterschiedlichen Systemen, die über das Lesen hinausgeht, ist jedoch bislang nicht möglich. Ferner liegen für die Entwicklung von DLT-Infrastrukturen noch keine standardisierten Richtlinien vor. Allerdings befassen sich verschiedene Organisationen damit, Transaktionen zwischen verschiedenen DLTs zu ermöglichen. Zudem werden derzeit von der International Organisation for Standardization (ISO) elf Normen für DLT entwickelt. In der EU haben sich 21 Mitgliedstaaten zusammengeschlossen und die European Blockchain Partnership gegründet, um die Etablierung einer europäischen DLT-Infrastruktur zu fördern.

Um DLT-Systeme in bestehende IT-Systeme zu integrieren, bedarf es der Interaktion mit herkömmlichen Systemen sowie der Integration von externen Daten. Aktuell bestehen zu Letzterem zwei grundlegende Möglichkeiten: 1) Die Integration basiert auf der Verwendung von Hashwerten als „Fingerabdrücke" von externen Daten wie Textdokumenten, Bildern, Videos oder Auszügen von multimedialen Datenbanken. Dieses Verfahren kann auch zur Prüfung der Integrität der externen Daten genutzt werden. Zu diesem Zweck wird der Hashwert des externen Datums mit dem im DLT-System gespeicherten Hashwert verglichen. Jede Manipulation eines externen Datums würde direkt aufgedeckt werden, da dann der Hashwert des externen Datums nicht mit dem im DLT-System gespeicherten identisch wäre. 2) Die Integration von Daten geschieht durch Teilnehmer, die externe Daten protokollieren, verifizieren und in das DLT-System einspielen bzw. Smart Contracts für diesen Prozess zur Verfügung stellen (sogenannte Orakel). Um die Korrektheit von Orakeln und deren Daten sicherzustellen, werden diese häufig auf Basis des Inputs anderer Orakel plausibilisiert oder müssen sich diese zertifizieren lassen.

1.2.2 Gesellschaftlich-ökonomische Perspektive

1.2.2.1 Status quo

DLT werden aufgrund ihres infrastrukturellen Charakters als Basisinnovationen eingestuft. Durch die (Weiter-)Entwicklung der einzelnen Komponenten wie bspw. des Kon-

sensmechanismus sind DLT-basierte IT-Lösungen für eine zunehmende Zahl an Anwendungsfällen geeignet. Allerdings wird vermehrt deutlich, dass für viele bereits untersuchte und perspektivische Anwendungsfälle Kombinationen verschiedener emergenter, digitaler Technologien nötig sind. Als besonders vielversprechend gelten die Kombinationen von DLT mit dem Internet der Dinge (IoT), der Künstlichen Intelligenz (KI) und Methoden des Privacy-Preserving Computings.
In den letzten Jahren und Monaten haben Unternehmen hohe Summen in die Entwicklung von DLT-Lösungen investiert, um die in Aussicht gestellten Potenziale zu heben und ihre Innovationskraft zu stärken. Gemäß Zahlen des Marktforschungsunternehmens IDC wurden im Jahr 2017 weltweit etwa 950 Millionen US-Dollar und im Jahr 2018 etwa 1,5 Milliarden US-Dollar in DLT-Lösungen investiert. Hinsichtlich des zukünftig zu erwartenden Blockchain-Marktvolumens divergieren die Einschätzungen indes stark. Während das Marktforschungsinstitut Tractica das weltweite Marktvolumen von DLT im Jahr 2025 auf 20,3 Milliarden US-Dollar schätzt, prognostiziert WinterGreen Research das Marktvolumen bereits im Jahr 2024 auf 60 Milliarden US-Dollar. Analysen von MarketsandMarkets hingegen erwarten im Jahr 2023 einen weltweiten Blockchain-Markt von 20,3 Milliarden US-Dollar. Die Entwicklung der Zahl von Blockchain-bezogenen Patentanmeldungen zeigt ebenso, dass unternehmensseitig ein hohes Interesse an der Technologie sowie eine hohe Innovationskraft bestehen. Auch das Interesse an sogenannten Initial Coin Offerings, die ein Mittel zur Unternehmensfinanzierung anhand von Kryptowährungen darstellen, steigt. Kumuliert wurde bis 2019 durch ICOs Kapital in Höhe von etwa 14,2 Milliarden US-Dollar beschafft.

In Deutschland hat sich mittlerweile sowohl in der Forschung als auch in der Wirtschaft ein umfangreiches Ökosystem im Bereich der DLT entwickelt. Dabei sind die meisten Initiativen mit der Erstellung von Proofs-of-Concept oder der Entwicklung von Prototypen beschäftigt. Es sind seltener Lösungen existent, die sich bereits im produktiven Einsatz befinden. Entsprechend diesen Entwicklungen herrscht auf dem Arbeitsmarkt ein hoher Bedarf an DLT-Fachkräften. Darüber hinaus entstehen weltweit aktuell sowohl auf Unternehmensebene als auch auf Regierungsebene zahlreiche Initiativen zur Förderung und Erforschung der DLT: Start-ups ergründen innovative Geschäftsideen, etablierte Unternehmen evaluieren intern oder in Konsortien mögliche Anwendungen der Technologie – innerhalb ihrer Branche oder branchenübergreifend.

DLT bietet potenziell einen weiteren Evolutionsschritt des Internets als digitaler Infrastruktur. Der erste Schritt war dabei das Internet in seiner heute bekannten Funktion als „Internet der Informationen". Darauf basierend hat sich in den vergangenen Jahren durch die zunehmende Vernetzung intelligenter Geräte das „Internet der Dinge" entwickelt. Aufgrund der grundsätzlichen Kopierbarkeit sämtlicher digitaler Daten konnten allerdings bislang nur Informationen übertragen werden. Eine Übertragung von Werten war nur durch Einbindung einer vertrauenswürdigen dritten Partei möglich. Mit der Einführung der DLT sind nun auch Werttransaktionen ohne Abhängigkeit von bzw. Vertrauen in eine dritte Partei möglich geworden. In diesem Rahmen wird daher häufig auch das „Internet der Werte und des Vertrauens" genannt. DLT muss daher als höherwertige digitale Infrastrukturtechnologie verstanden und weiterentwickelt werden.

1.2.2.2 Generische Rollen und Anwendungsmuster

Grundsätzlich kann die DLT in Form von drei generischen Rollen eingesetzt werden. Erstens als Verbesserer zur Optimierung bestehender Prozesse, die bereits ohne Intermediäre über bilaterale (Peer-to-peer-)Schnittstellen digital oder nicht-digital abgewickelt werden. Zweitens als Transformator zur Verschlankung von Abläufen, die zuvor unter Einbindung klassischer Intermediäre durchgeführt wurden. Drittens, als Befähiger, um Systeme zu ermöglichen, die zuvor technisch nicht realisierbar waren. Die Möglichkeiten zur Umsetzung verschiedener Dienstleistungen und Anwendungen sind sehr vielfältig, jedoch lassen sich bestimmte Anwendungsmuster erkennen. Diese umfassen die Bereiche

„Neutrale Plattform“, „Fälschungssichere Dokumentation“, „Zahlungsverkehr“, „Management organisationsübergreifender Prozesse“, „Digitale Identität“, „Digitale Urkunden“, „Dienstleistungen ohne Dienstleister“, und „Ökonomisch autonome Maschinen“.

In den meisten Fällen ist die Nutzung einer DLT-basierten IT-Lösung nicht technisch, sondern vielmehr wirtschaftlich bzw. organisatorisch motiviert. Wegen der redundanten Datenhaltung und Programmausführung (Smart Contracts) ist die Performanz und die Skalierbarkeit einer DLT-Lösung zumindest bislang einem zentral organisierten System technisch unterlegen. Vielmehr bietet die DLT die Möglichkeit, Prozesse, die bislang nur durch Einbindung einer vertrauenswürdigen dritten Partei umsetzbar waren, digital umzusetzen.

Auf Plattformmärkten steigt der Nutzen aufgrund von Netzwerkeffekten für alle Beteiligten typischerweise, je mehr Teilnehmer es sowohl auf der Anbieter- als auch auf der Nachfragerseite gibt. Dadurch konsolidiert sich der Markt meist auf wenige oder gar einen Plattformanbieter („winner-takes-all“). Als Konsequenz können die monopolistischen Plattformen dann erfahrungsgemäß ihre Vormachtstellung nutzen, um Markteintrittsbarrieren für neue Mitbewerber zu schaffen („Datensilos“) oder Nutzungsentgelte unangemessen hoch anzusetzen. Insbesondere im B2B-Bereich besteht demnach eine grundlegende Skepsis gegenüber Plattformlösungen jener Art. Die Motivation für den Einsatz von DLT ist hier klar ökonomischer Art, nämlich die Vermeidung eines monopolistischen Plattformbetreibers zugunsten einer dezentralen Plattformlösung. Nicht immer ist es jedoch notwendig oder sinnvoll, gänzlich auf zentrale Strukturen zu verzichten. Hierbei ist es wichtig zu untersuchen, wie das Zusammenspiel von bereits existenten, Vertrauen stiftenden Mechanismen mit DLT wirkt.

1.2.2.3 Diffusion und Förderpolitik

In Bezug auf die strukturellen und finanziellen Rahmenbedingungen ist zu verzeichnen, dass in Deutschland derzeit zu wenige Absolventen mit entsprechender DLT-Expertise aus den Universitäten auf den Arbeitsmarkt kommen. Nötig wäre hier aufgrund des Charakters der Technologie insbesondere eine Förderung von Programmen, welche die Schnittstelle mindestens zweier der Disziplinen Wirtschaft, Recht, Informatik und gegebenenfalls Ingenieurwissenschaften bedienen. Zudem bedarf es projektbezogener Förderprogramme durch die Ministerien, die sich explizit auf den Aufbau von DLT-Infrastrukturlösungen beziehen, welche ohne diese Technologien nicht denkbar wären. Zudem scheint für die Innovationsdiffusion eine Doppelstrategie ratsam. Zum einen sollten KMUs gezielt mit verschiedenen Förderprogrammen wie angewandten Forschungsprojekten angesprochen werden. Zum anderen sollten bestehende niederschwellige Instrumente wie der mFUND und Förderung von strategischen Leuchtturmprojekten genutzt werden. Derartige Förderprogramme müssten in der Zusammensetzung der Konsortien ebenfalls den interdisziplinären Charakter von DLT betonen. Ferner ist zu eruieren, inwieweit förderungspolitisch Anreize gesetzt werden können, um – bei gleichzeitiger regulatorischer Überwachung – insbesondere solche Marktakteure zur Partizipation zu motivieren, welche in Konkurrenzverhältnissen stehen. Zudem ist eine langfristige und vorausschauende Förderpolitik zu DLT, die über den aktuellen Hype hinausgeht, kurzfristigen Investitionen vorzuziehen. Die bereits über Ländergrenzen hinweg existierenden Start-ups, Konsortien, Initiativen und Organisationen sind zur Orientierung auf einen einheitlichen Rechts- und Handelsraum angewiesen. Wie andere technologische Neuentwicklungen kann auch DLT davon profitieren, in zeitlich und räumlich sowie gegebenenfalls hinsichtlich weiterer Parameter beschränkten Testräumen (sogenannten Sandboxes und Reallaboren) wertvolle Erfahrungen zu sammeln. Da sich das Technologiefeld nichtlinear entwickelt, ist es ferner geboten, regelmäßig Nutzen und Umsetzungsstand zu prüfen.

Da die DLT noch vergleichsweise jung ist, weist sie stellenweise noch gewisse Defizite bspw. hinsichtlich Transaktionsgeschwindigkeit und Energieverbrauch auf. Darüber hinaus hat die DLT insbesondere im Rahmen ihrer verbreitetsten Anwendungen in Form von Kryptowährungen für negative Schlagzeilen gesorgt, bspw. im Zusammenhang mit Geldwäsche oder Diebstahl. Zudem bedürfen DLT-Systeme und deren Entwicklung nicht nur selbst implementierter Governance-Regeln, sondern können potenziell auch mittels ihrer Eigenschaften und Möglichkeiten zur Implementierung verbesserter Governance-Mechanismen beitragen. Hierzu beruhen die bisherigen Überlegungen hauptsächlich auf zwei zentralen Konzepten: zum einen auf dem Transparenzprinzip in DLT-Systemen, auf Basis dessen sich viele Vorteile auch hinsichtlich Manipulationssicherheit erhofft werden. Zum anderen auf den sogenannten demokratischen Strukturen von DLT, die bspw. in Dezentralen Autonomen Organisationen (DAO) umgesetzt werden können.

1.2.2.4 DLT im Mobilitätssektor

Im Mobilitätsbereich können die Anwendungsmöglichkeiten für DLT in vier Anwendungsfelder unterteilt werden. Dabei weisen die Anwendungsfälle in den einzelnen Bereichen unterschiedliche Reifegrade auf. Das Anwendungsfeld Transport und Logistik beinhaltet Initiativen, deren Ziel es ist, durch DLT-Lösungen insbesondere Prozesse und Zusammenarbeit verschiedener Transport- und Logistikanbieter transparenter und effizienter zu gestalten. Das Anwendungsfeld Mobilitätsinfrastruktur subsumiert sämtliche Initiativen mit infrastrukturellem Charakter, wie z. B. die elektrische Ladeinfrastruktur. Initiativen im Anwendungsfeld Mobilitätsplattform haben zum Ziel, unterschiedliche Mobilitätsservices (intermodale Mobilität) in einer einzigen Plattform zu integrieren, um diese den Kunden mithilfe eines einheitlichen Portals oder einer einzigen App zugänglich zu machen. Das Anwendungsfeld Vollautonome Mobilität beinhaltet Initiativen, welche die Vision der vollautomatisierten Mobilität verfolgen, worin der Anwendungsfall der autonomen Fahrzeuge eine zentrale Bedeutung einnimmt.

1.2.3 Rechtliche Betrachtung

1.2.3.1 Zivilrecht

Aus zivilrechtlicher Sicht ist insbesondere der Einsatz sogenannter Smart Contracts interessant. Dabei handelt es sich um Software, die eine Automatisierung der Vertragsabwicklung ermöglicht. Die Bezeichnung als „Contract" suggeriert dabei, dass diese Software einen Vertrag im Rechtssinne darstellt. Wendet man allerdings die allgemeinen Regeln zu Vertragsschluss und Auslegung von Willenserklärungen an, so wird ersichtlich, dass der Smart Contract in den meisten Fällen nur der Abwicklung des (unabhängig von der DLT-Ebene) Vereinbarten dienen wird. Daneben ist zwar denkbar, dass Willenserklärungen durch Softwarecode ausgedrückt werden, sodass der Smart Contract einem Vertragsdokument ähnelt. Aus Gründen der Verständlichkeit ist diese Möglichkeit allerdings stark beschränkt.

Wie alle Verträge unterliegen auch solche, die den Einsatz eines Smart Contracts beinhalten, dem geltenden Recht. Das betrifft sowohl die Wirksamkeit des Vertrags als auch die Einhaltung von zwingendem Recht.

Soweit eine Rückabwicklung einer stattgefundenen Transaktion notwendig wird, bildet die Immutabilität von DLT aus zivilrechtlicher Sicht keine besondere Herausforderung. Es ist keinesfalls ungewöhnlich, dass eine Übertragung eines Werts stattfindet, die später rückgängig gemacht werden muss. Dies geschieht durch eine wirtschaftliche Wiederherstellung des ursprünglichen Zustands, im Falle von DLT also durch eine rückwärtsgerichtete Transaktion. Unveränderlich ist lediglich die Aufzeichnung darüber, dass ursprünglich eine Transaktion stattgefunden hat, was allerdings unschädlich ist.

Aus vertragsrechtlicher Sicht bildet das existierende Zivilrecht also einen angemessenen Rechtsrahmen, um den Einsatz von Smart Contracts zu erfassen. In praktischer Hinsicht ist zu beachten, dass der aktuelle Stand der Technik eine vollständige Automatisierung von Vertragsverhältnissen nicht zulässt. Software arbeitet nach vordefinierten Parametern und ist bisher nicht in der Lage, wertende Entscheidungen zu treffen. Rechtsnormen hingegen enthalten unbestimmte Rechtsbegriffe, die gerade von solchen Einzelfallwertungen abhängen.

1.2.3.2 Datenschutzrecht

Eine rechtliche Herausforderung für den Einsatz von DLT begründet das geltende Datenschutzrecht. Während DLT eine verteilte Speicherung der Daten auf mehrere Knoten immanent ist, folgt die Datenschutz-Grundverordnung dem Prinzip eines zentral Verantwortlichen. Was zunächst einen Widersprich darstellt, lässt sich teilweise durch entsprechende Gestaltung der Architektur auflösen. Es zeigt sich jedoch, dass hierfür nicht gänzlich auf den Einsatz von Intermediären verzichtet werden kann. Durch Einrichtung koordinierender Zentralstellen kann ein Ansprechpartner und Anspruchsgegner für den von der Datenverarbeitung Betroffenen geschaffen werden. Der offene Austausch von Daten ohne eine solche Zentralstelle kann nur dann datenschutzkonform gestaltet werden, wenn auf dem DLT-Layer auf personenbezogene Daten gänzlich verzichtet wird. Was zunächst einfach erscheinen mag, entpuppt sich in der konkreten Umsetzung jedoch häufig als beachtliche Herausforderung. Während die Daten von Dritten oftmals auch außerhalb des DLT-Layers (off-Chain) gespeichert werden können, befinden sich durch den öffentlichen Schlüssel regelmäßig personenbeziehbare Informationen der unmittelbaren Nutzer auf dem DLT-Layer. Hier bedarf es einer Anonymisierung der Nutzerkennungen, die nicht nur technisch vorbereitet, sondern auch in der praktischen Anwendung gesichert sein muss.

Ein weiterer datenschutzrechtlicher Konflikt besteht zwischen der Immutabilität der DLT und den Betroffenenrechten auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten. Während in gewöhnlichen Datenbanken der Verantwortliche nachträgliche Änderungen vornehmen kann, ist dies bei einer DLT-Plattform grundsätzlich weder möglich noch gewünscht. Als Lösungsansätze kommt die Implementierung technischer Vorkehrungen zur Ermöglichung einer nachträglichen Manipulation durch einen Berechtigten oder abermals der Verzicht auf die Speicherung personenbezogener Daten auf dem DLT-Layer in Betracht, welcher eine nachträgliche Veränderung obsolet machen würde.

Allgemein bleibt zu konstatieren, dass mit Blick auf die rasante technische Entwicklung und die Potenziale neuer Technologien, zukünftige gesetzliche Regelungen möglichst technologieneutral ausgestaltet sein sollten.

1.3 Anwendungsfallbeispiele

Basierend auf den vier zuvor benannten Anwendungsfeldern von DLT im Mobilitätssektor wird deren Rolle im Grundgutachten an konkreten Anwendungsfallbeispielen detailliert untersucht. Dabei wurde aus jedem der vier Anwendungsfelder je ein repräsentativer Vertreter ausgewählt, detailliert beschrieben und hinsichtlich seiner Potenziale analysiert. Bei der Auswahl wurden nicht nur die Anwendungsfelder, sondern auch ein ausgewogener Mix verschiedener Reifegrade sowie von öffentlichkeits- und unternehmensrelevanten Themen berücksichtigt. Die zentralen Gedanken und Erkenntnisse hinsichtlich der möglichen Rolle von DLT in diesen vier Anwendungsfallbeispielen sollen im Folgenden skizziert werden.

1.3.1 Frachtpapiere

Der erste Anwendungsfall ist im Bereich Transport & Logistik angesiedelt und besteht in einer Digitalisierung des sogenannten Bill of Lading (BoL, deutsch: Konnossement) und der damit verbundenen Bank- und Supply-Chain-Prozesse im internationalen Seehandel. Das BoL ist ein Warenwertpapier, welches die verschiffte Ware repräsentiert und insbesondere während der Verschiffung der Ware handelbar ist. Allgemein für Frachtpapiere, aber insbesondere für das im Anwendungsfall näher betrachtete BoL kann DLT als Befähiger dienen und zuvor aus ökonomisch-gesellschaftlichen Gründen nicht digitalisierbare Prozesse auf einer IT-Plattform abbilden. Da diese Thematik bereits vor der Verbreitung von DLT wegen seines enormen Potenzials häufig in der Praxis diskutiert worden ist, weist dieses Anwendungsfallbeispiel bereits einen sehr hohen Reifegrad auf. Es können daher im Gutachten mehrere Initiativen beschrieben sowie eine quantitative Potenzialanalyse durchgeführt werden. Zudem wird aufgezeigt, dass die hierzu in Deutschland bestehende Regulierung durch die Aufnahme von digitalen Öffnungsklauseln in das Handelsgesetzbuch (HGB) bereits fortgeschritten ist.

Ein Großteil der heutzutage international gehandelten Waren wird nach wie vor mittels traditioneller Papierdokumente wie BoL dokumentiert. Die Verwendung papierbasierter Dokumente weist dabei verschiedene Nachteile auf. Der stark papierbasierte Prozess verlangsamt nahezu alle Arbeitsschritte und verursacht zudem eine hohe Fehleranfälligkeit durch das häufige, manuelle Übertragen von Informationen. Schätzungen zufolge verursacht das heutige analoge System Kosten in Höhe von 5-10 Prozent des Werts der jährlich international gehandelten Waren und liegt somit in der Größenordnung von etwa einer Billion US-Dollar pro Jahr. Heruntergerechnet auf den Anteil deutscher Waren am internationalen Handel ergeben sich so aus diesem Prozess Einsparpotenziale im zweistelligen Milliardenbereich. Ungeachtet grundsätzlich verfügbarer technischer Möglichkeiten war bislang keiner der Digitalisierungsversuche dieses Prozesses erfolgreich, da sich die entsprechenden zentralen Ansätze, die ein Monopol für den jeweiligen Plattformbetreiber bedeuten würden, bislang nicht flächendeckend etablieren konnten. DLT

kann die genannten Herausforderungen adressieren und als grundlegende IT-Infrastruktur die Kooperation von Unternehmen ermöglichen. Basis für die Implementierung bildet eine Smart-Contract-fähige DLT-Plattform. Die in den letzten Monaten in starkem Maße zunehmenden Bemühungen, DLT-basierte Lösungen am Markt zu etablieren, bestätigen die These, dass DLT neue, von den beteiligten Akteuren als vielversprechend angesehene Möglichkeiten schaffen kann.

Wie bereits angedeutet, treffen bisherige Frachtpapier-Digitalisierungsinitiativen in Bezug auf die Regulierung in Deutschland auf technologieneutrale und damit flexible digitale Öffnungsklauseln im HGB. Gegenstand dieser ist die schlichte Gleichstellung analoger und digitaler Warenwertpapiere durch ein Äquivalenzerfordernis, d. h., das digitale (i. S. d. Gutachtens DLT-basierte) Abbild muss alle Funktionen erfüllen, die ein papiergebundenes Pendant verkörpern würde.

Bei sämtlichen derzeitigen Initiativen sollte dabei jedoch nicht ausschließlich das BoL betrachtet werden. Dieses sollte eher als exemplarisches, wichtiges Dokument angesehen werden. Auch weitere Dokumente, etwa Versicherungspapiere oder Echtheitszertifikate, die in diesem und ähnlichen Prozessen von Wichtigkeit sind, sollten einbezogen werden. Gesetzesanpassungen oder Klarstellungen müssen gegebenenfalls sowohl hinsichtlich der Gültigkeit elektronischer Signaturen und digitaler Zertifikate als auch hinsichtlich der Zugänglichkeit und Beweiskraft elektronischer Transaktionen vor Gericht sowie der Unterscheidung von verhandelbaren Papieren (Konnossements) und nicht-verhandelbaren Papieren stattfinden. Die digitalen Öffnungsklauseln sind eine Rechtssetzungstechnik, die der Gesetzgeber perspektivisch auch in anderen Bereichen fruchtbar machen könnte.

1.3.2 Elektrisches Laden

Die Elektromobilität bzw. die elektrifizierte Mobilität haben in den letzten Jahren eine rasante technische Entwicklung durchlaufen. Unabdingbare Voraussetzung für eine schnelle Akzeptanz und Marktdurchdringung ist die Bereitstellung öffentlich zugänglicher (Schnell-)Ladeinfrastruktur insbesondere für das Laden unterwegs. Physische, IT-seitige und abrechnungsbezogene Unterschiede von Ladeinfrastruktur haben zur Partitionierung von (Schnell-)Ladeinfrastruktur, d. h. insbesondere zu einer Anbieterzersplitterung, geführt. Plattformbetreiber – spezielle Mobilitätsdienstleister – versuchen, vergleichbar mit dem Roaming im Mobilfunk, diesem Hemmnis der Elektromobilität entgegenzuwirken. Konkret hat das Hemmnis zur Folge, dass Kunden eines Anbieters nicht auf alle theoretisch verfügbaren Ladesäulen bequem zugreifen können. Dabei besteht ein erhebliches Interesse, dass Kunden eines Anbieters an möglichst vielen (schnellladefähigen) Ladesäulen Strom zu transparenten und für sie geeigneten Konditionen beziehen können und dass der dazugehörige Lade- und Abrechnungsvorgang reibungslos und mit minimalem Einsatz des Fahrers erfolgt. Zu diesem könnte eine DLT-basierte Lösung einen Beitrag leisten. DLT können mindestens drei potenzielle Funktionen wahrnehmen, um die Herausforderungen im Bereich elektrisches Laden zu adressieren: erstens, Authentifizierungs- und Autorisierungsfunktionen über DLT-basierte Identitätslösungen; zweitens, manipulationssichere Dokumentation und Nachhaltung der Ladevorgänge; drittens, Abrechnung und Werttransfer der Ladevorgänge mittels Token.

Auf diese Weise kann eine DLT-Lösung durch Disintermediation, d. h. die teilweise Substitution und Reduktion der Beteiligten, die Risiken einer Konzentration von Marktmacht einzelner Akteure „by design“ ausschließen. Zudem könnte neuen Teilnehmern schneller und vergleichsweise einfacher Zugang und Partizipation ermöglicht werden. Es bleibt jedoch fraglich, inwieweit eine DLT-basierte Lösung signifikante Marktanteile erzielen kann, nachdem insbesondere in Deutschland der Markt bereits verteilt erscheint und Ladeinfrastrukturbetreiber zudem häufig selbst mit Unternehmensanteilen an (zentralen) Plattformlösungen beteiligt sind. Hinzu kommt, dass Bürgern im Allgemeinen nicht zuzumuten ist, jedes Detail einer Technologie zu verstehen. Es ist daher zu eruieren, ob DLT

gemeinsam mit Verbraucherschutzportalen bzw. TÜV etc. Technologieverständnis & -akzeptanz im Privatkundenbereich erwirken kann. Falls eine Blockchain-basierte Lösung etabliert würde, könnte diese um das Aufteilen der Ladeleistung über mehrere E-Fahrzeuge und um Herkunftsnachweise für Grün- und Lokalstrom erweitert werden. Zudem ist eine Anwendung bei eigentumsrechtlich komplizierteren Ladesituationen (z. B. bei Wohneigentümergemeinschaften) interessant. Dadurch würde sich ein neues Bild abzeichnen, und die DLT-Lösung könnte einem neuen bisher noch nicht verteilten Markt als neutrale Plattform dienen. Perspektivisch gilt es, nicht nur das DLT-basierte Laden, sondern auch das Entladen, d. h. die Einbeziehung der Elektrofahrzeuge in Stromnetze (bspw. Microgrids), zu fördern. Hierfür bedarf es allerdings zunächst der Lösung energierechtlicher Herausforderungen.

1.3.3 Ridesharing

Die Personenbeförderungsbranche in Deutschland steht aktuell im Zwiespalt zwischen der traditionell stark regulierten und genossenschaftlich organisierten Taxibranche, dem ÖPNV sowie neuen digitalen Mobilitätsplattformen, die Gelegenheiten zum Ridesharing anbieten. Als Ridesharing wird die geteilte Nutzung eines Fahrzeugs durch mehrere Personen mit ähnlichen Reiseanforderungen bezeichnet. Den Potenzialen hinsichtlich verbesserter Auslastungen von Fahrzeugen, verringerter Emissionen und niedrigerem Gesamtverkehrsaufkommen stehen große Herausforderungen gegenüber. Am relevantesten ist hierbei die Gefahr der Monopolbildung, aber auch auf der operativen Ebene, etwa in Bezug auf das Identitätsmanagement und das Vermitteln von Vertrauen zwischen den involvierten Parteien, sowie bei der Bezahlung bestehen Probleme. Beispielsweise muss für die Fahrten das erforderliche Vertrauen zwischen den sich gegenseitig meist unbekannten Reisenden gebildet werden. Zudem muss gewährleistet werden, dass nur für tatsächlich und wie vereinbart stattgefundene Dienstleistungen bezahlt wird, um Betrug zu vermeiden.

Um die Bildung von Monopolen und den damit einhergehenden Datensilos zu verhindern, ist die Schaffung einer offenen und geteilten Ridesharing-Plattform notwendig, die weder Nachfrager noch Anbieter von der Teilnahme ausschließt. Hierzu sollten die Umsetzungsmöglichkeiten und Implikationen offener und dezentraler Plattformen (technologieagnostisch) untersucht werden. Prinzipiell ist DLT aufgrund ihrer dezentralen Natur und ihrer Möglichkeiten zur Automatisierung von Geschäftsprozessen mittels Smart Contracts gut geeignet, um einzelne Institutionen als Intermediäre für bilaterale Beziehungen obsolet zu werden zu lassen und der Gefahr einer Monopolbildung entgegenzuwirken. Bei der Novellierung des PBefG wäre insoweit zu beachten, dass Genehmigungserfordernisse nicht nur große heutige Intermediäre betreffen, sondern perspektivisch insbesondere auch den Fahrer einschließen. Jedoch ist im konkreten Kontext von Ridesharing die mehrwertschaffende konzeptionelle und technische Umsetzbarkeit wegen technischer Eigenschaften wie Latenz und Energieverbrauch fraglich. Hintergrund ist, dass für das Matching von Fahrtanbietern und Mitfahrern große Datenmengen kontinuierlich analysiert, aktualisiert und verarbeitet werden müssen, deren manipulationssichere Speicherung jedoch nicht notwendig ist, da erst nach einem Matching die entsprechende Dokumentation und Abwicklung des Vertrags vertrauensvoll geschehen muss. Bei Ridesharing-Plattformen für regelmäßige Strecken (Pendler-Angebote) und für Angebote mit langer Vorlaufzeit (Mitfahrgelegenheits-Angebote) können hingegen dezentrale Marktplätze auf Basis von DLT genutzt werden, um Angebote und Nachfrage zu koordinieren.

Wird der Anwendungsfall erweitert, bspw. um die Integration von Anbietern unterschiedlicher Transportmittel zusätzlich zu Ridesharing-Angeboten in einer offenen, multimodalen Plattform, könnte die DLT überdies potenziell wiederum Mehrwert stiften. In diesem Szenario müssen bereits bestehende Beziehungen mehrerer Anbieter abgebildet

werden, z. B. um die garantierte Abrechnung bereitgestellter Dienstleistungen im multimodalen Transport zu erleichtern. Beispielhafte Ansätze finden sich u. a. in der durch das mFund-Programm des BMVI geförderten Initiative zur Schaffung eines offenen und dezentralen Mobilitätssystems OMOS und der Forderung nach einem Deutschlandticket. Eine Integration in multimodale Angebote könnte überdies generell die Verbreitung von Ridesharing positiv beeinflussen. Hinsichtlich des Identitätsmanagements und der Schaffung von Vertrauen kann DLT zur selektiven und die Privatsphäre erhaltenden Identifikation und Authentifizierung einzelner Parteien eingesetzt werden. Neben der Nutzung von Kryptowährungen bzw. Token für die Bezahlung von Ridesharing-Angeboten erscheint insbesondere die Nutzung von Smart Contracts zur Umsetzung sogenannter Treuhandverträge ohne die Einbindung intermediärer Parteien möglich. Die DLT kann somit in verschiedenen generischen und unterstützenden Funktionen einen Mehrwert im Bereich Ridesharing schaffen.

1.3.4 Platooning

Unter Platooning – auch als elektronische Deichsel bezeichnet – wird ein techno-ökonomisches System für den Straßenverkehr verstanden, bei dem zwei oder mehrere Fahrzeuge in sehr geringem Abstand hintereinanderfahren, um Treibstoff zu sparen („Windschattenfahren"). Voraussetzung für das Platooning sind zahlreiche Technologien, die typischerweise auch beim (voll-)automatisierten Fahren zum Einsatz gelangen, etwa Abstandssensoren oder automatische Steuerungssysteme für Lenkrad und Gaspedal. Aktivitäten im Bereich des Platoonings sind momentan auf Lkw beschränkt und befinden sich heute (noch) im vorwettbewerblichen Bereich. Daneben setzt Platooning digitale Infrastrukturen voraus, um technische Abläufe koordinieren zu können. In diesem Anwendungsfall sind voraussichtlich Hardware-Nachrüstungen von Lkw nötig, um eine Verbreitung des Platoonings zu erleichtern. Damit Platooning Realität werden kann, gilt es jedoch – abgesehen von der technischen Weiterentwicklung – noch ökonomische Fragestellungen zu adressieren. Aus ökonomischer Sicht besteht beim Platooning grundsätzlich kein Anreiz, die Führung des Platoons zu übernehmen: Die Ersparnisse durch geringeren Treibstoffverbrauch sind für die hinteren Fahrzeuge höher als für das führende Fahrzeug. Falls zukünftig auch eine Reduktion von Lenkzeiten im Platoon möglich sein sollte, betreffen damit verbundene Einsparungen ebenfalls nicht das führende Fahrzeug bzw. dessen zugehöriges Unternehmen. Fahren Fahrzeuge eines Unternehmens häufiger vorn, so ergibt dies einen Wettbewerbsnachteil gegenüber den im Platoon hinterherfahrenden und dadurch Kosten sparenden Konkurrenten.

Die Hauptherausforderung einer breiten Anwendung von Platooning ist die Verrechnung der dadurch erzielten Vorteile unter den Beteiligten eines Platoons. Sobald ein Platoon aus Fahrzeugen unterschiedlicher Speditionen besteht, sind Zahlungsvorgänge nötig, die mit bisherigen Zahlverfahren kaum abbildbar sind. Ein monetäres Anreizsystem, das den führenden Lkw im Platoon für die ermöglichten Kosteneinsparungen während der Platoon-Fahrt vergütet, scheint die logische Konsequenz. In einem solchen Szenario bietet sich zunächst eine zentrale Plattform an, die als Intermediär zwischen den einzelnen Speditionen fungiert und die Zahlungsabwicklung koordiniert. Das Problem einer solchen Entwicklung besteht wiederum darin, dass sich einzelne Plattformen langfristig zu einem Monopolanbieter entwickeln könnten.

DLT könnte als dezentral organisierte Zahlinfrastruktur zum Ausgleich von erzielten (Treibstoff-)Einsparungen dazu beitragen, Platooning in der Breite zu etablieren. Da eine DLT-basierte Zahlungsabwicklung beim Platooning bereits vorhandene Fahrten in der Logistikbranche effizienter gestalten würde, kann man hier wiederum eine quantitative Potenzialanalyse durchführen. Diese ergibt, dass bei einer flächendeckenden Nutzung in Deutschland pro Jahr Treibstoffersparnisse in einer Größenordnung von 500 Millionen Euro und CO_2-Einsparungen von etwa 1,39 Millionen Tonnen realisiert werden könnten.

In Zukunft sind daneben weitere Einsparungen in den Kostenarten Personal und Versicherung sowie eine erhöhte Verkehrssicherheit denkbar.

DLT kann also für das Platooning insbesondere für die Verrechnung der gegenseitigen Kompensationen der Platooning-Teilnehmer von Nutzen sein. Sie bietet dabei neben der Monopolvermeidung die Vorteile, dass die Echtzeitverrechnung von Mikrotransaktionen automatisiert möglich ist und durch ihre Peer-to-peer-Struktur kein nachträgliches Clearing notwendig wird. Weiter könnte eine Dokumentation Schutz vor Betrug bei der Bezahlung sowie eine Nachweisbarkeit in der Schuldfrage bei Fahr- oder technischen Fehlern eines der am Platoon beteiligten Fahrzeuge gewährleisten. DLT-Systeme können somit das nötige Vertrauen schaffen, damit sich der Fahrer des im Platoon führenden Fahrzeugs sicher sein kann, auch eine faire Kompensation für die Leistung zu erhalten, auch wenn er mit direkten Konkurrenten (d. h. anderen Spediteuren) ein Platoon bildet. Grundlage hierfür ist ein durchdachter Ausbau des Internets bzw. dessen Zugänglichkeit, um insbesondere realwirtschaftliche Anwendungsfallbeispiele zu ermöglichen.

Aus rechtlicher Perspektive erfordert das flächendeckende Rollout des Platoonings eine Anpassung der Abstandsregelung (Lkw >3,5 t, 50 m) des § 4 Abs. 3 StVO. Zuvor sollte eine Möglichkeit für die Ordnungsbehörden gefunden werden, wie diese zuverlässig erkennen können, ob ein geringer Abstand aus einem Platoon herrührt oder nicht. Naheliegend erscheint es hierfür auf die nach § 63a Abs. 1 StVG zu speichernden Orts- und Zeitangaben, die einen Rückschluss auf den Fahrmodus (manuell/automatisiert) ermöglichen, zurückzugreifen. Obwohl es über § 63a Abs. 2 S. 1 StVG möglich ist, diese Daten Ordnungsbehörden zu übermitteln, stellt diese Lösung nur bei weiterer normativer Konkretisierung insbesondere des Adressaten und des Datenspeicherorts eine konkrete Alternative dar. Insoweit wäre der Gebrauch der Ermächtigungsgrundlage des § 63b StVG angezeigt.

Die Einstufung von Platooning als Lenkzeitunterbrechung i. S. d. Art. 7 Abs. 1, Art. 4 lit. d) VO (EG) Nr. 561/2006 erscheint rechtlich nicht gänzlich ausgeschlossen. Jedoch ist bisher wohl noch nicht abschließend erforscht, ob die Verpflichtung des Fahrers aus § 1b Abs. 1 i. V. m. Abs. 2 StVG wahrnehmungs- und übernahmebereit für die Fahraufgabe zu sein, eine vertretbare Erholung zulässt. Insoweit bestünde daher weiterer Forschungsbedarf. Im Weiteren gründet Platooning mit DLT-basierter Zahlungsabwicklung auf einer BGB-Innengesellschaft.

Datenschutzrechtlich ergeben sich ebenfalls Herausforderungen. Oftmals werden als Nutzer der Platooning-Plattform Unternehmen auftreten, bei denen die Kenntnis des Unternehmens auch Kenntnis über dahinterstehende natürliche Personen (Unternehmensinhaber, Fahrer etc.) beinhaltet. Werden diese mit einer Nutzerkennung auf einer öffentlichen DLT-Plattform aktiv, so können datenschutzrechtlich relevante Verarbeitungsvorgänge vorliegen. Es bedarf dann einer Anpassung der Architektur. Diese kann durch Implementierung einer Zentralstelle, welche Einfluss auf die Datenverarbeitungen nehmen kann („zentrale Lösung"), geschaffen werden. Alternativ könnten Techniken angewandt werden, um die Verbindung zwischen Nutzerkennung und Identität der Teilnehmer aufzuheben („Anonymisierungslösung"). Für den Fall, dass es sich bei den Teilnehmern ausschließlich um Unternehmen handelt, bei denen Rückschlüsse auf die hinter den Unternehmen stehenden natürlichen Personen nicht möglich sind, genügt es, auf die Speicherung personenbezogener Daten auf dem DLT-Layer zu verzichten. Die Informationen sind off-Chain zu speichern und mittels eines Hashwerts auf der DLT-Plattform zu verlinken. Eine derartige Lösung erfordert jedoch eine vorherige Prüfung der Teilnehmer dahingehend, ob diese die voranstehenden Herausforderungen erfüllen. Insbesondere kleinere Unternehmen könnten dann wohl nicht am System teilnehmen.

1.4 Fazit

Das vorliegende interdisziplinäre Grundgutachten beantwortet aktuelle Fragestellungen zu Chancen und Herausforderungen von DLT in Mobilität und Logistik aus den Perspektiven Ökonomie, Technologie und Recht.

Die allgemeine, aber auch die spezifische und anwendungsfallbasierte Untersuchung von DLT verdeutlichen, dass es sich um eine vergleichsweise junge Technologie mit großem Potenzial handelt. Nach ihrem ersten Einsatzzweck als Technologie zur technischen Umsetzung der Kryptowährung Bitcoin hat sich die DLT zu einer generisch nutzbaren digitalen Basislösung für ökonomische Infrastrukturaufgaben weiterentwickelt, die aktuell auf dem Weg zur Marktreife ist. Hinsichtlich der vier Anwendungsfälle Frachtpapiere, elektrisches Laden, Ridesharing und Platooning zeigen die Analysen, dass differierende Reifegrade und Potenziale vorherrschen. Im Fall der Frachtpapiere ist die technische Entwicklung und Implementierung schon fortgeschritten und die finanziellen Potenziale sind signifikant. Die länderübergreifende Integration unterschiedlicher rechtlicher Perspektiven stellt hierbei jedoch aktuell ein Hemmnis dar. Hinsichtlich des elektrischen Ladens haben sich bereits erste DLT-basierte Lösungen entwickelt, allerdings scheinen diese mehr als Marktkorrektiv aufzutreten, anstatt bestehende zentrale Plattformen zu verdrängen. Im Bereich des Ridesharing zeigt sich, dass aufgrund der nötigen Echtzeitverarbeitung von Massendaten der Einsatz von DLT nur in Servicefunktionen wie dem Bereich des Identitätsmanagements sinnvoll und vorteilhaft erscheint. Hinsichtlich des Platoonings erscheint der dezentrale Ansatz von DLT zielführend und einer zentralen Lösung überlegen.

Ferner ist nicht zu erwarten, dass DLT neue Monopole hervorbringen wird. Allerdings lässt sich festhalten, dass DLT-Lösungen und -Systeme aktiv nach freiheitlich-demokratischen Idealen durch den Staat mitgestaltet werden sollten. Sinnvoll erscheint hier insbesondere eine Förderung von Programmen, welche die Schnittstelle mindestens zweier der Disziplinen Wirtschaft, Recht, Informatik und gegebenenfalls Ingenieurwissenschaften bedienen. Solche Förderprogramme müssten in der Zusammensetzung der Konsortien ebenfalls den interdisziplinären Charakter von DLT betonen. Ferner sind die bereits über Ländergrenzen hinweg existierenden Start-ups, Konsortien, Initiativen und Organisationen darauf angewiesen, einen einheitlichen Rechts- und Handelsraum zu haben und sich an klaren Rahmenbedingungen orientieren zu können (z. B. durch Sandboxes und Reallabore).

2 Management Summary [English]

2.1 Purpose of this report

This report presents the economic potentials, the legal framework, and the necessary technical foundations for understanding distributed ledger (DL) / blockchain technology in order to illustrate the opportunities and challenges of these technologies, especially in the mobility and logistics sector. This basic assessment was compiled on behalf of the German Federal Ministry of Transport and Digital Infrastructure (BMVI) by the blockchain laboratory at Fraunhofer FIT. Its intended audience is start-ups that, for example, seek a legal assessment regarding data protection issues relating to DL / blockchain technologies; decision-makers from the private sector who, for example, want concrete examples to help them understand how this technology affects existing and emerging markets and which measures might be sensible from an entrepreneurial perspective; to deciders, policymakers and politicians who, for example, would like to know the implications of their positions on this topic, particularly with regard to the mobility and logistics sectors; as well as the general public interested in the technology and its potential. The report is not intended for those with a purely academic interest in these topics, although some of the contributions in the report do reflect the current state of the academic discussion.

The fast-moving pace of digitalization is now affecting almost all areas of our society. This development is the result of ubiquitous computing, ever shorter innovation cycles, and the convergence of digital technologies and innovations. One of these technologies with particular potential is distributed ledger technology (DLT). DLT had its first widespread use in 2009 in the form of a blockchain for the crypto-currency Bitcoin. Since then, DLT has evolved into a versatile technology: Prototypical applications of DLT solutions already exist in virtually every industry. Among other things, these applications show the potential of so-called smart contracts for mapping business logic. It is increasingly becoming apparent that DLT, as a driver of innovation, could potentially bring about disruptive changes in many fields of business, law, society, and public administration. DLT as a transparent, electronic register for information managed by the participants of a distributed computer network, offers a response to previously unfulfilled demands on information and communication technology for the secure processing of information and transactions, resistance to manipulation, and decentralized consensus building. As a high-level digital infrastructure, DLT enables a progression from today's internet of information to the internet of trust and value.

In particular, the mobility and logistics sectors have significant characteristics that make them especially suitable for DLT. For the mobility sector, these include connected vehicles communicating with their environment, intermodal transport concepts, and the development of electric charging infrastructure. While in the logistics sector, there are numerous cross-organizational processes that currently run only inefficiently (e.g. requiring a tremendous amount of paper consumption) and urgently require digital support. For the first time, this digital support could practically be implemented by DLT.

DLT addresses the BMVI's areas of competence in two ways: by implementing promising applications in the mobility and logistics sector and creating and delivering digital infrastructures. Only by proactively addressing DLT, one can ensure that the technology develops in line with the German legal and value systems and that it can provide the German economy and society with the desired added value. Germany has an excellent starting position, since start-ups and research organizations in Germany are currently actively pursuing the development of DLT. It is thus logical and important that the state become active in this context in order to harness the momentum and shape the development of DLT appropriately. This basic assessment thus serves as the basis for the formulation of

further recommendations for action in order to fulfill the policy objective of proactively ensuring that DLT will increase the well-being of German society and strengthen its economy in a legally secure manner.

This assessment report will identify, analyze, and address economic, legal and, where relevant, technical issues both within the respective disciplines and/or in an interdisciplinary manner. The analyses from different perspectives offered here were not created independently of each other, but are instead the product of continuous exchange among experts from research, industry, associations, and policymakers.

2.2 General analysis

2.2.1 Technical consideration

The term "distributed ledger technology" refers to a type of database systems characterized by shared and synchronized data management in a peer-to-peer network as well as continuous, cryptographic concatenation of the data. Blockchain represents one concrete example of this technology. Others include, for example, directed acyclic graphs. The information is stored in blocks, concatenated into chains via cryptographic methods, and redundantly stored in each node of the network by means of peer-to-peer protocols, which means that each participant in the network has the same information or data. The distributed network of independent hosts (nodes) that communicate and synchronize with each other verifies and validates these blocks through a so-called consensus mechanism. The most common consensus mechanism currently used in the Bitcoin and Ethereum blockchain is called "proof of work". In addition, there are now several alternative consensus mechanisms which, depending on the specific design of the DLT network, bring with them both certain advantages and also disadvantages. In addition, second-generation DLT solutions usually offer the option of defining and using so-called smart contracts. Smart contracts are program codes that can be written to the DLT and executed by all participants in the DLT network in a redundant or verifiable manner. As a result, DLTs can be used not only for the secure storage of data, but can also map and execute business logic. However, because of the wide range of applications, the scalability and energy efficiency requirements of DLT systems are increasing. In order to do justice to the latest developments, research is currently under way into innovative, scalable, and energy-efficient systems. This research has already shown initial successes, such that common criticisms of inefficiency and high energy consumption only affect obsolete systems.

In addition to the age of the DLT, these systems can also be divided into public and private and also permissioned and permissionless systems. In principle, anyone can participate in public systems, such as the Bitcoin blockchain, and see which transactions are added. Such a system thus organizes itself, since it is designed without a central authority (such as a bank) and the network participants make decisions decentrally via a consensus mechanism. In this context, it is important that there must be enough incentives for participants in the network to participate in the consensus process. If this does not happen, it can easily devolve into a few members' dominating, which contradicts the basic idea of DLT and makes manipulation more readily possible. Private systems, meanwhile, have access restrictions, meaning participants must register to join the network. In permissionless systems, all network participants can perform any action without restriction. However, if the system is permissioned, there are role profiles allowing certain participants to perform only certain actions. For example, it can specify that only certain participants be involved in the process of consensus finding. Since a private (even consortium-based) DLT application often already has some degree of trust between the network members, more efficient consensus mechanisms can be used here compared to proof of work. For example, in private DLT systems, often a small number of actors actively participate in finding consensus.

Examples of well-known DLT are Bitcoin (public, permissionless), Ethereum (public, permissionless, suitable for the development of widely usable smart contracts), Hyperledger Fabric (private, permissioned, modular design), Sovrin (public, permissioned, especially designed for digital identities), and IOTA (public, permissioned, supports micro payments). Although these are all based on the same basic concept, direct interaction and communication between the different systems that goes beyond reading is, to date, not possible. Furthermore, there are no standardized guidelines for the development of DLT infrastructures. However, different organizations are working on finding ways to allow transactions between different DLTs. In addition, eleven DLT standards are currently being developed by the International Organization for Standardization (ISO). In the EU, 21 member states have joined forces to form the European Blockchain Partnership to promote the establishment of a European DLT infrastructure.

Integrating DLT systems into existing IT systems requires interaction with traditional systems and the integration of external data. Currently there are two basic options for the latter: 1) The integration is based on the use of hash values as "fingerprints" on external data such as text documents, images, videos, or excerpts from multimedia databases. This method can also be used to test the integrity of the external data. For this purpose, the hash value of the external date is compared with the hash value stored in the DLT system. Any manipulation of external data would be revealed directly, since then the hash value of the external data would not be identical to that stored in the DLT system. 2) The integration of data is done by participants who log external data, verifying and importing into the DLT system, or provide smart contracts for this process (the so-called "oracle"). To ensure the correctness of oracles and their data, these are often made plausible based on input from other oracles or have to allow themselves to be certified.

2.2.2 Socio-economic perspective

2.2.2.1 Current situation

Due to their infrastructure character, DLTs are classified as basic innovations. Due to the (further) development of the individual components, such as the consensus mechanism, DLT-based IT solutions are suitable for an increasing number of applications. However, it is becoming increasingly clear that many use cases, both those already investigated as well as prospective ones, require combinations of different emergent, digital technologies. Particularly promising are the combinations of DLT with the Internet of Things (IoT), artificial intelligence (AI), and methods of privacy-preserving computing.
In recent years and months, companies have been investing heavily in the development of DLT solutions to unlock the potential they have to offer and to strengthen their innovative power. According to figures from market research firm IDC, global investment in DLT solutions was approx. $950 million in 2017 and approx. $1.5 billion in 2018. The forecasts for the blockchain market volume expected for the future diverge sharply, however. While the market research institute Tractica estimates the global market volume for DLT to reach $20.3 billion by 2025, WinterGreen Research estimates the market volume will reach $60 billion by 2024. In contrast, MarketsandMarkets analyses suggest a global blockchain market of $20.3 billion by 2023. The development of the number of blockchain-related patent applications also shows that there is a high level of corporate interest in the technology and a high level of innovation. The interest in so-called initial coin offerings, which represent a means of corporate financing based on cryptocurrencies, is also increasing. Cumulatively, ICOs are expected to raise $14.2 billion in capital by 2019.

In Germany, an extensive ecosystem relating to DLT has developed in both research and business. Most initiatives are involved in proof-of-concept or prototype development. There are fewer existing solutions that are already in productive use. Given these developments, there is a high demand on the labor market for DLT specialists. In addition,

numerous initiatives are currently under way around the world at both corporate and government levels to promote and explore DLT. Start-ups are exploring innovative business ideas, while established companies are evaluating potential applications of the technology either individually or as part of industry-based or interdisciplinary consortia.

DLT potentially is helping the internet to progress to a new developmental stage as a digital infrastructure. The first stage was the internet in its current, well-known function as a source of information. This has since evolved into the Internet of Things in recent years as a result of the increased networking of intelligent devices. Given the inherent ability to copy digital data, so far only information is being transmitted. A transfer of values was only possible through the involvement of a trusted third party. With the introduction of DLT, value transactions without dependence on or trust in a third party have now become possible. This is why the "internet of values and trust" is often mentioned in this context. DLT must therefore be understood and developed as a higher-level digital infrastructure.

2.2.2.2 Generic roles and patterns of application

Basically, the DLT can be used in the form of three generic roles: to optimize existing processes that are already handled without intermediaries via bilateral (peer-to-peer) interfaces digitally or non-digitally; to streamline operations previously carried out with the involvement of conventional intermediaries; to enable systems that were previously technically infeasible. The possibilities for implementing various services and applications are quite varied, although certain application patterns can be identified. These include neutral platforms, forgery-proof documentation, payment transactions, management of inter-organizational processes, digital identities, digital certificate, services without service providers, and economically autonomous machines.

In most cases, the use of a DLT-based IT solution is not motivated by the technology itself, but instead out of economic or organizational reasons. The redundant data management and execution of programs (smart contracts) makes the performance and scalability of a DLT solution technically inferior to a centrally organized system, at least for the time being. Rather, DLT offers the possibility of digitally implementing processes that were previously only possible through the involvement of a trustworthy third party.

In platform markets, the benefits of network effects typically increase for all participants as more people participate on both the provider and the demand sides. As a result, the market is usually consolidated to a few or even one platform provider ("winner-takes-all"). As a consequence, experience shows that the monopolistic platforms can use their supremacy to create market entry barriers (data silos) for new competitors or to set disproportionately high user fees. As a result, there is a fundamental skepticism about such platform solutions, especially in the B2B sector. The motivation for the use of DLT is clearly of an economic nature, namely avoiding a monopolistic platform operator in favor of a decentralized platform solution. However, it is not always necessary or sensible to completely renounce central structures. It is important to investigate how the interaction of already existing mechanisms for creating trust can work with DLT.

2.2.2.3 Diffusion and funding policy

With regard to the structural and financial framework conditions, it is noticeable that German universities are not producing enough graduates with the DLT expertise required by the labor market. Due to the nature of the technology, it would be necessary in particular to promote programs that serve the interface of at least two of the disciplines of business, law, computer science, and, possibly, engineering. In addition, ministries need to start funding projects related to the development of DLT infrastructure solutions,

which would not be conceivable without these technologies. A dual strategy seems advisable for diffusion of these innovations. On the one hand, SMEs should be targeted with different support programs, such as applied research projects. On the other hand, existing low-threshold instruments such as the mFUND and the promotion of strategic flagship projects should be used. Such funding programs should also emphasize the interdisciplinary nature of DLT by establishing consortia. The state must also determine the extent to which incentive measures can be used to motivate competing market players to participate, while also providing concomitant regulatory monitoring. A long-term, forward-looking policy that promotes DLT beyond the current hype is preferable to short-term investment. The start-ups, consortia, initiatives, and organizations that already exist across national boundaries are dependent on a uniform legal and commercial framework. Like other new technological developments, DLT can benefit from gaining valuable experience under different temporal and geographical constraints as well as other test spaces (so-called sandboxes and real laboratories) constrained by other parameters. Since the technology is undergoing a non-linear development, it is also advisable to check its implementation and continued usefulness on a regular basis.

As DLT is comparatively young, it still has some deficits, for example with regard to transaction speed and energy consumption. In addition, DLT has received negative press for such matters as money laundering and theft, particularly in the context of its most widespread cryptocurrency applications. DLT systems and their development not only require rules for self-governance developed internally, but they can also potentially contribute to implementing improved governance mechanisms. To this end, the previous considerations are mainly based on two central concepts: the transparency principle in DLT systems which offer many advantages, including security against manipulation; and the so-called democratic structures of DLT, which can be implemented in decentralized autonomous organizations (DAO), for example.

2.2.2.4 DLT in the mobility sector

DLT could be applied to any of four aspects of the mobility sector. The use cases for each are at different stages of development. The field of transport and logistics includes initiatives using DLT to make the processes and cooperation of various transport and logistics providers more transparent and efficient. Mobility infrastructure includes all infrastructure-related initiatives, such as chargers for electric vehicles. Mobility platform initiatives aim to integrate different mobility services (intermodal mobility) into a single platform, making them accessible to customers through a single portal or app. The field of fully autonomous mobility includes initiatives that pursue the vision of fully automated mobility, in which the use of autonomous vehicles plays a central role.

2.2.3 Legal considerations

2.2.3.1 Civil law

From a civil law perspective, the use of so-called smart contracts is particularly interesting. Smart Contracts are software that enables the automation of contract processing. The term "contract" suggests that this software represents a contract in the legal sense. However, if one applies the general rules on the conclusion of a contract and the interpretation of declarations of intent, it becomes clear that in most cases the smart contract will only serve to process that which has already been agreed (regardless of the DLT level). In addition, it is conceivable that declarations of intent are expressed by software code, so that the smart contract would then be similar to a contract document. For the sake of clarity, however, this possibility is severely limited.

Like all contracts, those that involve the use of a smart contract are subject to applicable law. This concerns both the validity of the contract and its compliance with mandatory law.

Insofar as it is necessary to reverse a transaction that has taken place, the immutability of DLT does not present a particular challenge from a civil law perspective. It is by no means unusual that transfers of value may need to be reversed later. This is done by a restoration to the original state, in the case of DLT, a reverse transaction. It is immutable only in the sense that the record shows the original transaction's taking place, which is harmless.

From a contract law perspective, existing civil law thus provides an appropriate legal framework to cover the use of smart contracts. In practical terms, it should be noted that the current state of the technology does not allow the complete automation of contractual relationships. Software works according to pre-defined parameters and, to date, is unable to make evaluative decisions. By contrast, legal norms contain indefinite legal concepts that depend precisely on such evaluations of the individual situation.

2.2.3.2 Data privacy law

Existing data protection law poses a legal challenge for the use of DLT. While a distributed storage of data on several nodes is immanent to DLT, the EU General Data Protection Regulation (GDPR) follows the principle of a centrally responsible person (data controller). What initially represents a contradiction can be partially resolved by appropriate design of the architecture. It turns out, however, that this cannot entirely be done without the use of intermediaries. The establishment of coordinating central offices could serve as a contact person and as claim opponent to those affected by the data processing. The open exchange of data without such a central office would only comply with GDPR if all personal data were completely avoided on the DLT layer. However, what may initially seem simple turns out to be a considerable challenge in actual implementation. While third-party data can often be stored outside the DLT layer (off-chain), the public key regularly contains personally identifiable information for the direct users on the DLT layer. Anonymization of user identities is required; this must be not only technically possible, but also ensured in practical application.

Another data protection conflict exists between the immutability of the DLT and data subject rights to the correction or deletion of personal data concerning them. While in ordinary databases, the data controller can make subsequent changes, this is basically neither possible nor desired in the case of a DLT platform. Possible solutions are the implementation of technical provisions to enable subsequent manipulation by an authorized party or otherwise avoiding the storage of any personal data on the DLT layer, which would make a subsequent change obsolete.

In general, it should be noted that in view of the rapid technological development and the potential of new technologies, future legal regulations should be as technology-neutral as possible.

2.3 Sample applications

Based on the four types of DLT application in the mobility sector mentioned above, its role will be examined in detail in this basic assessment report using case studies as examples. For each of the four fields of application, a representative application has been selected, described in detail, and analyzed for its potential. Not only the fields of application were taken into consideration when choosing the examples, but also a balanced mix of different levels of maturity as well as topics relevant to public and business concerns. The central thoughts and insights regarding the possible role of DLT in these four use case studies will be outlined below.

2.3.1 Shipping documents

The first application is in the field of transport & logistics: digitalizing bills of lading (BoL) and the related banking and supply chain processes in international maritime trade. The BoL acts as a security, which represents the value of the shipped goods and is tradable especially during the shipment of the goods. For shipping documents in general, but especially for the BoL considered in more detail in the case study, DLT can enable processes previously non-digitalizable for economic or social reasons to be mapped on an IT platform. Since this topic was already a frequent topic of discussion in the sector due to its large potential, even before the dissemination of DLT, this sample application is already quite mature. Therefore, the report can describe several initiatives as well as a quantitative potential analysis. It also shows that the existing regulations in Germany by the inclusion of digital opening clauses ("Digitale Öffnungsklauseln") in the Commercial Code (HGB) is already advanced.

Much of today's internationally traded goods are still documented using traditional paper documents such as BoL. The use of paper-based documents has several disadvantages. A process that is largely paper-based slows down almost all work steps and also causes a high error rate due to the frequent, manual transmission of information. It is estimated that today's analogue system costs about one trillion dollars or 5-10% of the value of the goods traded internationally each year. Calculated in terms of the share of German goods in international trade, this process could result in potential savings in the double-digit billions. Regardless of the fundamentally available technical possibilities, none of the attempts to digitalize this process have to date been successful, since the corresponding central approaches which would mean a monopoly for the respective platform operator could not yet be widely established. DLT can address these challenges and, as a basic IT infrastructure, enable business cooperation. The implementation is based on a smart contract-enabled DLT platform. The increasing efforts in recent months to establish DLT-based solutions on the market confirm the hypothesis that DLT can create new opportunities which participating players see as promising.

As already indicated, previous initiatives for the digitalization of shipping documents in Germany face technology-neutral and thus flexible digital opening clauses in the HGB. They require the simple equivalence of analog and digital securities, i.e. the digital image must fulfill all the functions that a paper-based counterpart would offer.

Current initiatives should not, however, focus exclusively on the BoL. This should be seen merely as an essential, yet exemplary document. Other documents, such as insurance papers or certificates of authenticity, which are of importance in this and similar processes, should also be included. Legal adjustments or clarifications may need to be made

regarding the validity of electronic signatures and digital certificates, as well as the accessibility and probative value of electronic transactions in court, and the distinction between negotiable and non-negotiable papers. The digital opening clauses are a law-making technique that legislators could fruitfully apply to other areas as well.

2.3.2 Electric charging

Electromobility and electrified mobility have undergone rapid technical development in recent years. An indispensable prerequisite for rapid acceptance and market penetration is the provision of publicly accessible, (fast) charging infrastructure, especially for charging on the go. Physical, IT, and billing-related differences in charging infrastructure have led to a partitioning of (fast) charging infrastructure, i.e. a splintering of suppliers. Platform operators (special mobility service providers) are trying to counteract this barrier to electromobility that can be compared to mobile service roaming. Specifically, the barrier means that a mobility service provider's customers cannot easily access all theoretically available charging stations. There is considerable interest in finding a way for the customers of one supplier to purchase electricity from as many (fast-charging) charging stations as possible under transparent and suitable conditions and that the associated charging and billing process takes place smoothly and with minimal input from the driver. A DLT-based solution could contribute to this. DLTs can perform at least three potential functions that would address the challenges of electrical charging: authentication and authorization capabilities through DLT-based identity solutions; tamper-proof documentation and maintenance of the charging process; billing and value transfer for the charging sessions using tokens.

In this way, a DLT solution can allow for disintermediation, i.e. the partial substitution and reduction of the participants to preclude the risks of individual actors' concentrating market power by design. In addition, new participants could be given access and allowed to participate more readily. However, it remains questionable to what extent a DLT-based solution might achieve significant market shares, especially since in Germany the market already appears to be maturing fast and charging infrastructure operators are also frequently holders of shares in (central) platform solutions. In addition, citizens generally cannot be expected to understand every detail of a technology. It must be determined whether DLT together with consumer protection portals or TÜV, etc. could enable an understanding and acceptance of the technology among private customers. If a blockchain-based solution were established, this could be extended by splitting the charging power across several electric vehicles and providing proof of origin for green and local electricity. In addition, an application for charging situations with complicated ownership structures (e.g. in homeowners associations) would also be interesting. This would create new opportunities for DLT solutions as a neutral platform for a new, as yet fairly undeveloped, market. Prospectively, not only DLT-based charging but also discharging (i.e. inclusion of electric vehicles in electricity grids such as microgrids) should be promoted. However, this first requires a solution of the challenges under energy legislation.

2.3.3 Ride sharing

The passenger transport industry in Germany is currently undergoing significant conflict between the traditionally heavily regulated, cooperatively organized taxi industry and public transport as well as novel digital mobility platforms offering opportunities for ride sharing. Ride sharing describes the shared use of a vehicle by several people with similar travel requirements. The potential for improved vehicle utilization, reduced emissions, and lower overall traffic volumes is facing major challenges. The most relevant here is the risk of emerging monopolies, but challenges exist also at the operational level, for example in terms of identity management and the conveyance of trust between the parties involved, as well as issues with processing payments. For example, there is a need to establish trust among fellow travelers largely unknown to each other. In addition, there

must be a way to ensure that only those services actually agreed and utilized are billed in order to avoid fraud.

To prevent the formation of monopolies and the associated data silos, it is necessary to create an open and shared ride sharing platform that excludes neither buyers nor providers from participating. To this end, the opportunities and implications of open and decentralized (technology-neutral) platforms should be examined. In principle, due to its decentralized nature and its ability to automate business processes through smart contracts, DLT is well suited to make individual institutions obsolete as intermediaries for such bilateral transactions and to counteract the risk of monopoly. In the amendment to the German Personal Transport Act (PBefG), it should be noted in this respect that permitting requirements not only affect the major current intermediaries, but also include the drivers in particular. However, in the specific context of ride sharing, the value-adding conceptual and technical feasibility due to technical characteristics such as latency and energy consumption is questionable. The background to this is that for providers and passengers to be matched, large quantities of data have to be continuously analyzed, updated, and processed, but their tamper-proof storage is not necessary, because the corresponding documentation and processing of the contract take place only after a match is found. However, for regular ride sharing (for commuters) and deals with long lead times, DLT based marketplaces can be used to coordinate offers and demand.

If the case study is extended, for example by the integration of providers of different means of transport in addition to ride sharing in an open, multimodal platform, the DLT could also potentially add value. In this scenario, existing relationships of multiple vendors must be mapped to facilitate the guaranteed billing of provided services in multimodal transport. Exemplary approaches can be found for example in the initiative funded by the BMVI mFund program for the creation of an open and decentralized mobility system "OMOS" and the demand for a "Germany Ticket." Furthermore, integration into multimodal services could generally have a positive impact on the popularity of ride sharing. In terms of identity management and trust creation, DLT can be used for selective and privacy-preserving identification and authentication of individual parties. In addition to the use of cryptocurrencies or tokens to pay for ride sharing, the use of smart contracts to implement trust agreements without the involvement of intermediary parties seems possible. DLT can thus create added value in the field of ride sharing in various generic and supporting functions.

2.3.4 Platooning

Platooning is a road traffic management system where two or more vehicles travel at a very close distance behind each other to save fuel ("slipstreaming"). The requirements for platooning are numerous technologies that are typically used in (fully) automated driving, such as distance sensors or automatic control systems for the steering wheel and accelerator pedal. Platooning activities are currently limited to trucks and are (still) in the pre-competitive phase of development. In addition, platooning requires digital infrastructures to coordinate technical processes. This case study shows that hardware retrofits of trucks are likely to be required to facilitate the dissemination of the platooning. In order for platooning to become reality, however, apart from the technical advancement, it is still necessary to address economic issues. From an economic perspective, there is basically no incentive to be the lead vehicle in a platoon. The savings from lower fuel consumption are higher for the vehicles in the rear than for the lead vehicle. If, in the future, a platoon can reduce driving times, the associated savings would also not affect the lead vehicle and its operator. If an operator's vehicles take the lead more often, this would result in a competitive disadvantage compared to those in the rear, resulting in cost savings for the lead vehicle operator's competitors.

The main challenge to a broad application of platooning is settling the benefits achieved by those involved in a platoon. As soon as a platoon consists of vehicles from different freight companies, payment transactions that have barely no equivalent with standard payment methods are required. A monetary incentive system that rewards the leading truck in the platoon for the cost savings achieved by the vehicles in the rear seems the logical consequence. In such a scenario, a central platform would act as an intermediary between the individual carriers and coordinate payment processing. The problem with such a development is that individual platforms could eventually become a monopoly provider.

As a decentrally organized payment infrastructure to offset realized (fuel) savings, DLT could help establish a broad base for platooning. Since DLT-based payment processing for platooning would make already existing trips in the logistics industry more efficient, one can again carry out a quantitative potential analysis here. This results in the fact that a nationwide use of platooning in Germany could save up to € 500 million in fuel and 1.39 million tons of CO_2 each year. In the future, further savings in personnel and insurance costs as well as increased road safety are also conceivable.

Thus, DLT can be useful for platooning, in particular for offsetting the mutual compensations payable by platooning participants. In addition to avoiding a monopoly, it offers the advantages of automating real-time billing of micro-transaction with a peer-to-peer structure that makes subsequent clearing unnecessary. Further, documentation could provide protection against fraud during payment as well as traceability in the question of blame in case of driving or technical errors of one of the vehicles involved in the platoon. DLT systems can thus provide the necessary confidence for the driver of the lead vehicle to be sure of fair compensation, even if the platoon contains direct rivals (i.e. other carriers). The basis for this is a sophisticated expansion of the internet or its accessibility, in particular to enable real-world case studies.

From a legal perspective, the nationwide roll-out of platooning requires an adjustment of the distance control (trucks > 3.5 t, 50 m) in §4(3) of the German Traffic Code (StVO). There needs to be an instrument for police authority to determine, if a short distance between two vehicles is caused by a platoon or by a human driver not adhering to required safety standards. It might be apparent to draw back on the time and location data which are required to store in accordance with §63a (1) StVG. These allow the inference on the driving mode (manual / automatized). Although it is possible via §63a(2)(1) StVG to transmit this data to police authorities, this solution represents an actionable alternative only with further normative preciseness in particular of the addressee and the data storage location. To that end, §63b StvG could likely represent the basis of authorization.

Deeming platooning to be driver downtime i.e. Art. 7(1), Art. 4d of Regulation (EC) No. 561/2006 does not appear to be legally completely ruled out. However, it has probably not yet been conclusively explored whether the driver's obligation under §1b(1) and (2) StVG to be aware of and ready to take on the task of driving permits such to be classified as downtime. This indicates a need for further research. In addition, platooning with DLT-based payment processing creates an undisclosed partnership per the BGB.

Data protection law also presents challenges. Often the users of the platooning platform will be companies in which the knowledge of the company also includes information about natural persons (business owners, drivers, etc.). If these are activated with a user ID on a public DLT platform, data protection-relevant processing operations may be present. This would then require an adaptation of the architecture. This can be created by implementing a central office to control the data processing. Alternatively, techniques could be used to break the link between user ID and participant identities, i.e. anonymization. In the event that the participants are exclusively companies for which the natural persons behind the companies cannot be identified, it is sufficient to forego the

storage of personal data on the DLT layer. The information must be stored off-chain and linked to the DLT platform via a hash value. However, such a solution requires a prior examination of the participants as to whether they meet the above challenges. Smaller companies in particular would probably not be able to participate in the system.

2.4 Summary

The present interdisciplinary basic assessment report addresses current questions on the opportunities and challenges facing the use of DLT in mobility and logistics from the perspectives of economics, technology, and law.

The general, but also the specific and application-based study of DLT shows that it is a comparatively young technology with great potential. After its initial use as a technology for the technical implementation of the cryptocurrency Bitcoin, DLT has evolved into a generically usable digital basic solution for economic infrastructure tasks, which is currently moving toward to market readiness. With regard to the four case studies examined here (shipping documents, electrical charging, ride sharing, and platooning), the analyses show differing levels of maturity and potential. In the case of shipping documents, the technical maturity and implementation is already advanced and the financial potential is very significant. However, transnational integration of different legal perspectives is currently an obstacle. With regard to electrical charging, first DLT-based solutions have already been developed, but they seem to be more market-corrective than replacing existing centralized platforms. In the field of ride sharing, it becomes apparent that due to the necessary real-time processing of mass data, the use of DLT only appears useful and advantageous in service functions such as the field of identity management. With regard to platooning, the decentralized approach of DLT appears to be purposeful and superior to a central solution.

Furthermore, it is unlikely that DLT will establish new monopolies. However, it can be stated that DLT solutions and systems should be actively shaped by the government in accord with free, democratic ideals. In particular, the promotion of programs which serve the interface of at least two of the disciplines of economics, law, computer science and, if applicable, engineering sciences seems to make sense. Such funding programs should also emphasize the interdisciplinary nature of DLT by establishing consortia. Furthermore, start-ups, consortia, initiatives and organizations that already exist across national borders are dependent on having a uniform legal and commercial framework which they can orient themselves to (e.g. through sandboxes and real laboratories).

3 Einleitung

3.1 Inhaltliche Einführung

Die Basis-Funktionalität der Distributed-Ledger-Technologie (DLT) kann durch die Analogie eines „besonderen" Notizbuchs veranschaulicht werden: Jeder Teilnehmer des DLT-Netzwerks besitzt ein solches Notizbuch, wobei all diese Notizbücher „synchronisiert" sind, d. h., sobald ein Akteur einen Eintrag in sein Notizbuch schreibt, taucht dieser Eintrag auch in allen anderen Notizbüchern auf. Die einzelnen Seiten des Notizbuchs („Blöcke") sind durch die Bindung („Chain") miteinander verbunden. Die kryptografische Verknüpfung der einzelnen Blöcke stellt eine unzertrennliche Verkettung her. Dadurch sind Einträge nicht nachträglich löschbar oder veränderbar, auch einzelne Seiten können nicht aus dem Notizbuch herausgerissen werden. Sämtliche Teilnehmer an dem DLT besitzen zu jedem Zeitpunkt eine vollständige Historie der dort enthaltenen Informationen und können sich auch sicher sein, dass diese nie manipuliert worden sind.

Werden in dieses Notizbuch etwa Transaktionen einer digitalen Geldeinheit inklusive der initialen „Kontostände" eingetragen, so kann aus dieser Eigenschaft ein Währungssystem geschaffen werden, das ähnlich der Buchhaltung einer Bank gesteuert wird. Das DLT-basierte Währungssystem funktioniert allerdings ohne einen Intermediär, der in diesem Fall traditionell durch eine Bank gegeben wäre. So können nicht nur Währungen, sondern auch jegliche anderen Dokumente als „Unikate" digitalisiert werden. Allgemein ersetzt die Kombination aus Transparenz, Nachvollziehbarkeit und Manipulationsresistenz ein Vertrauen zwischen den Teilnehmern. Dies wird erreicht, ohne eine besonders privilegierte Partei zu benötigen, die sich um die Einhaltung der Regeln kümmert. Die DLT wirft neben technischen und rechtlichen Fragen ebenfalls die Frage auf, wer die Implementierung solcher neutralen Plattformen übernehmen könnte. Da die Plattform per Konstruktion neutral ist d. h., kein Unternehmen die Plattform „besitzt", gibt es keine Betreiber mehr, die ihr Geschäftsmodell auf den Betrieb der Plattform auslegen könnten. Vielmehr wird DLT zur Infrastruktur, die darauf aufbauende Geschäftsmodelle ermöglicht. Da Infrastrukturen in den Aufgabenbereich des Staats und insbesondere in den Verantwortungsbereich des BMVI fallen, ist es nachvollziehbar, dass dieses eine wissenschaftlich fundierte erste Einschätzung der Potenziale der DLT insbesondere im Mobilitätsbereich anstrebt, um für die Zukunft gerüstet zu sein.

Das vorliegende Grundgutachten richtet sich an politische Entscheidungsträger auf verschiedenen Ebenen unseres föderalen Systems, die ein Verständnis über die möglichen Potenziale und Auswirkungen der Technologie erlangen und auf aktuelle Herausforderungen auch aus regulatorischer Sicht hingewiesen werden möchten. Weiter soll das Grundgutachten etablierte Unternehmen und Verbände ansprechen, die sich mit der DLT beschäftigen, die Auswirkungen der Technologie auf ihren Bereich noch nicht einordnen können oder deren Fokus auf den Sektoren Mobilität und Logistik liegt. Schließlich richtet sich das Gutachten auch an Start-ups, die oft besonders angewiesen sind auf einen präzisen regulatorischen Rahmen. Das BMVI will damit auch deutlich machen, dass die Türen für Nachfragen hinsichtlich regulatorischer Hürden immer offenstehen. Natürlich sind auch interessierte Bürger herzlich eingeladen, das Grundgutachten ganz oder in Teilen zu lesen. Das Grundgutachten richtet sich explizit nicht an die wissenschaftliche Forschungsgemeinschaft, da die angestrebte Behandlung der gesamten Breite des Spektrums von DLT eine akademische Auseinandersetzung in der Tiefe nicht zulässt.

Das Anliegen dieses Grundgutachtens ist es, einen einfachen und kompakten Einstieg in die Technologie zu ermöglichen. Was ist DLT? Was kann die Technologie schon heute – was ist in Zukunft denkbar? Welche zentralen Handlungsfelder ergeben sich aus sozialer,

welche aus ökonomischer Sicht? Aber auch: Welche rechtlichen oder technischen Herausforderungen bestehen – z. B. bezüglich des Datenschutzes oder einer stabilen digitalen Infrastruktur? Anhand praktischer Fallbeispiele zu dezentralen Energiesystemen, Identitätsmanagement und autonomer Mobilität werden einige bereits heute wirksame Anwendungsbereiche skizziert – inklusive der damit verbundenen Veränderungen und der existierenden Potenziale. Die Herausforderungen der digitalen Transformation erfassen mittlerweile sämtliche Lebensbereiche und stoßen durch digitale Innovationen wichtige Veränderungen in immer kürzeren Innovationszyklen entscheidend an. Um den tiefgreifenden Wandel von Anfang an gestalten zu können, ist es essenziell, sich frühzeitig mit digitalen Neuerungen und deren Potenzialen zu befassen. Zu diesen gehört nicht zuletzt auch die DLT. Diese stellt eine infrastrukturelle Basistechnologie dar und ermöglicht nicht zuletzt vielversprechende Anwendungen im Mobilitätssektor. Damit adressiert sie sogar zwei Kerngebiete des BMVI. Durch die umfassende und zielgerichtete Analyse von DLT kann sichergestellt werden, dass die Technologie dem deutschen Rechts- und Wertesystem entsprechend weiterentwickelt wird und der deutschen Wirtschaft und Gesellschaft den erhofften Mehrwert stiften kann. Das Grundgutachten fungiert zudem als Grundlage für die Formulierung weiterführender Handlungsempfehlungen, damit die politische Zielsetzung – den Einsatz von DLT zur Steigerung der Wohlfahrt und Stärkung der deutschen Wirtschaft proaktiv und rechtssicher zu gestalten – erfüllt werden kann.

Aus den Adressaten und der Zielsetzung des Grundgutachtens ergeben sich Einschränkungen in Bezug auf die inhaltliche Granularität des Grundgutachtens. So können die vier Anwendungsfallbeispiele, die im Rahmen dieses Grundgutachtens betrachtet werden (siehe 3.2), zwar individuell auf die Implikationen der DLT untersucht werden. Eine detaillierte Auseinandersetzung mit konkreten Prototypen auf Protokollebene konnte dabei jedoch nicht erfolgen. Zudem richtet sich der Fokus bei den Anwendungsbeispielen in erster Linie auf Veränderungen, die sich aus der Verbreitung und Anwendung der DLT ergeben, nicht aber durch die Effekte der Digitalisierung im Allgemeinen. Auf ökonomisch-gesellschaftlicher Seite kann zwar eine qualitative Einschätzung der Potenziale der Technologie gegeben werden, eine quantitative Betrachtung, etwa in Form von Transaktionskostentheorie und Implikationen hinsichtlich Wohlfahrt, Arbeitsplätzen etc. kann jedoch nicht erfolgen.

Die fachlichen Methoden, die für die Erstellung des Gutachtens eingesetzt worden sind, entstammen entsprechend der interdisziplinären Eigenschaft von DLT unterschiedlichen Disziplinen. Aus ökonomischer Sicht erfolgte die Aggregation von Wissen aus der Aufarbeitung bestehender wissenschaftlicher Fachliteratur, semi-strukturierten Experteninterviews sowie bisherigen Praxisprojekten und prototypischen Implementierungen in Industrie und öffentlicher Verwaltung. Auf der technischen Seite wurden realweltliche Implementierungen untersucht. Aus rechtlicher Perspektive fand eine Untersuchung des existierenden Rechtsrahmens und eine Auswertung vorhandener Fachliteratur zu Fragen von DLT, Mobilität, Verkehr und Infrastruktur sowie Datenschutzrecht statt. Zusätzlich wurden aktuelle und geplante Regulierungsansätze betrachtet. Daneben wurde im Oktober 2018 ein interdisziplinärer Fachworkshop mit zahlreichen DLT-Experten aus Industrie, Start-ups, Foundations und Forschung durchgeführt. Im Rahmen dieses Workshops wurden zahlreiche Diskussionsrunden geführt und als Ergebnisse in das Gutachten überführt. Durch die interdisziplinäre Auseinandersetzung mit technischen, ökonomischen und rechtlichen Themen, die eng mit der DLT verbunden sind, wurden auch neue Zusammenhänge und stellenweise Pionierarbeit im Rahmen des Gutachtens geleistet. Eine detaillierte Auseinandersetzung mit den vier Anwendungsfallbeispielen ermöglichte zudem die praktische Bestätigung zahlreicher Annahmen.

3.2 Aufbau des Grundgutachtens

Das vorliegende Grundgutachten besteht aus einem allgemeinen sowie einem speziellen Teil. Die allgemeine Analyse beginnt mit einer technischen Einführung in die der DLT

zugrunde liegenden Konzepte. Hier werden Konzepte der Kryptografie und der dezentralen Systeme sowie Begriffe wie Konsensmechanismen, Transaktionen und Smart Contracts erläutert. Zudem werden erste Einblicke in Anwendungsmöglichkeiten eröffnet. Daran wird deutlich, dass es sich keineswegs um eine vollkommen homogene Technologie mit charakteristischen Eigenschaften, sondern um ein diverses Gebiet mit vielen Ausprägungen und mit einer Vielzahl von kreativen Ideen handelt. Diese werden strukturiert und hinsichtlich ihrer grundlegenden Eigenschaften charakterisiert. Schließlich wird die DLT noch anderen Technologien gegenübergestellt, wie etwa der Künstlichen Intelligenz und dem Internet der Dinge (IoT). Dabei wird zudem das Potenzial der Kombination von Blockchain mit diesen Technologien untersucht.

Im darauffolgenden Abschnitt wird aufgezeigt, welche Bedeutung die DLT für unser Wirtschaftssystem und die Gesellschaft haben kann. Zunächst werden ökonomische Muster für die Anwendung der DLT-spezifischen Eigenschaften aufgezeigt und anhand von Beispielen veranschaulicht. Dabei wird insbesondere auf den Charakter der DLT als eines manipulationssicheren Datenspeichers, als neutraler Plattform und als Übermittler von Werten (Kryptowährungen und Token) eingegangen. Danach folgt eine Analyse der Diffusion der DLT, im Rahmen derer untersucht wird, wie die DLT sich in Deutschland und der Welt voraussichtlich etablieren kann. Hierbei liegt der Fokus insbesondere auf den Implikationen für den Standort Deutschland und auf geeigneten Fördermaßnahmen. Dabei werden intensiv Kritikpunkte sowie Chancen und Risiken der Technologie adressiert. Unter diese fallen etwa Angriffsmöglichkeiten auf DLT, private Schlüssel und eine Einschätzung der Auswirkungen von Quantencomputern.

Aus der Analyse der Risiken geht hervor, dass die DLT auch eine Reihe von Eigenschaften aufweist, die bei falscher oder böswilliger Verwendung Potenzial für Missbrauch haben. In diesem Sinne ist ebenfalls eine rechtliche Einordung der Technologie unabdingbar. Besonders im Zusammenhang der zivilrechtlichen Einordnung von automatisierten Vertragsabwicklungen durch Smart Contracts sowie der Bewertung der DSGVO-Konformität der DLT stellt sich eine Reihe von Fragen, die im Grundgutachten de lege lata analysiert und beantwortet werden. Zudem werden die Aspekte herausgearbeitet, an denen aus juristischer Perspektive noch Änderungsbedarf besteht, sofern in den jeweiligen Anwendungsfällen eine DLT-basierte Lösung angestrebt ist.

Im zweiten Teil des Grundgutachtens werden die allgemeinen Aussagen aus der allgemeinen Analyse durch eine Reihe von Anwendungsfallbeispielen bestätigt und veranschaulicht. Dabei wurde aus jedem der vier Anwendungsfelder im Mobilitätsbereich (Transport & Logistik, Mobilitätsinfrastruktur, Intermodale Mobilität und Autonomes Fahren) ein konkreter Anwendungsfall gewählt und untersucht, ob die DLT für den jeweiligen Anwendungsfall einen Mehrwert stiften kann. Diesbezüglich stellte sich heraus, dass nicht nur eine große Bandbreite an Anwendungspotenzialen, sondern auch in der Reife von DLT sehr große Unterschiede besteht. So ist etwa das Potenzial der Blockchain für eine Ridesharing-Plattform fundamental anders zu bewerten als im Zusammenhang mit einer neutralen Plattform, die digitale Frachtpapiere zulässt. Die vier Anwendungsfälle werden von ökonomisch-technischer Seite beschrieben, die mögliche Rolle der DLT analysiert und schließlich hinsichtlich ihrer Eignung mit einem Fazit sowie Handlungsempfehlungen bewertet. Anschließend erfolgt jeweils eine Beschreibung der rechtlichen Fragestellung und Hürden im Zusammenhang mit diesen Anwendungsfallbeispielen.

An dieser Stelle soll noch ein Lesehinweis formuliert werden: Das Kapitel 4 dient als Basiseinführung in das komplexe Thema der DLT. Für ein Verständnis des Grundgutachtens ist bei fehlenden Vorkenntnissen eine Lektüre der technischen Grundlagen empfehlenswert. Jedoch ist dieser allgemeine, technische Teil für ein Verständnis der weiteren Teile des Grundgutachtens nicht zwingend erforderlich. Auch die allgemeinen gesellschaftlich-ökonomischen und die allgemeinen rechtlichen Grundlagen weisen zwar ge-

genseitige Bezüge sowie Bezüge zum allgemeinen technischen Teil auf, sind aber durchaus so konzipiert, dass sie auch isoliert gelesen und verstanden werden können. Selbiges gilt für den speziellen Teil des Gutachtens, in welchem jedes der Anwendungsfallbeispiele auch selektiv gelesen werden kann. Viele Aussagen, die im Rahmen der Anwendungsfallbeispiele getroffen werden, sind verallgemeinerbar, sodass die verallgemeinerten Aussagen sich in der allgemeinen Analyse wiederfinden.

4 Technische Grundlagen

Verträge, Transaktionen und die dazugehörigen Daten sind unverzichtbar in unserem täglichen Leben. Eigentum an Anlagen, Vermögenswerten oder Ähnlichem werden dokumentiert und sind zu Teilen öffentlich einsehbar. Die Digitalisierung bietet für diese Prozesse einerseits neue Möglichkeiten, generiert andererseits aber auch neue Herausforderungen, die gelöst werden müssen. Die Grundlagentechnologie DLT stellt sich diesen Herausforderungen und ermöglicht Datensicherheit sowie Transparenz durch die Dokumentation von Transaktionen in einer dezentralen, sicheren, transparenten und unabänderlichen Weise.

Die Entwicklung der DLT erfolgte in verschiedenen Phasen. „Satoshi Nakamoto“[1] entwickelte 2008 das Konzept für die Kryptowährung Bitcoin. Die daraufhin entsprechend entwickelte Software wurde 2009 freigegeben und es entstand das Bitcoin-Netzwerk. Die der Bitcoin zugrunde liegende technische Infrastruktur wird als DLT 1.0 bezeichnet. Sie wird primär in der Finanzbranche und bei der Überprüfung von Herkunftsnachweisen eingesetzt. Im Jahre 2014 wurde die Ethereum-Blockchain entwickelt. Die Hauptinnovation im Vergleich zu Bitcoin sind dabei sogenannte Smart Contracts. Sie ermöglichen bspw. Geschäftslogik abzubilden, um Prozesse zu automatisieren. Bekanntestes Beispiel einer als DLT 2.0 bezeichneten Technologie ist Ethereum. DLT-2.0-Plattformen werden in Anwendungsfeldern wie dem Internet der Dinge, Supply-Chain-Management, Smart Grids oder im Mobilitätssektor genutzt. Abbildung 1 visualisiert die zeitliche Entwicklung von Blockchain und DLT (Distributed Ledger Technology).

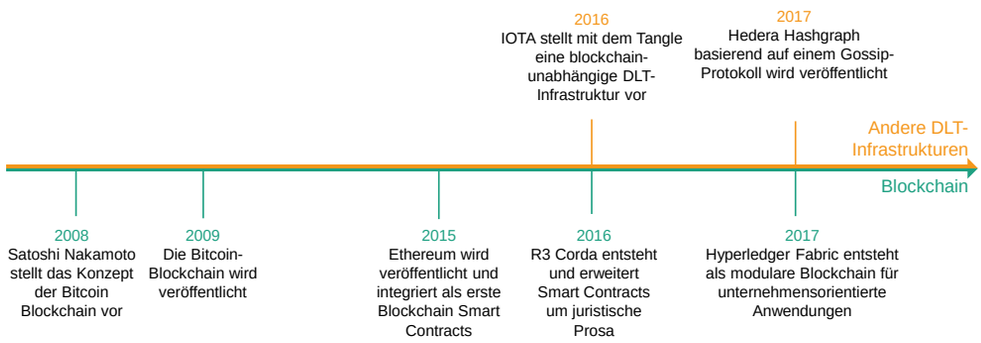


Abbildung 1: Blockchain im zeitlichen Verlauf

Die Grundlagentechnologie DLT kombiniert aus technischer Sicht Methoden aus den Forschungsfeldern Verteilte Systeme und Kryptografie. Die DLT ist organisiert als Netzwerk aus Computern, das ein dezentral geführtes Verzeichnis (DL, Kontenbuch) verwaltet. Dieses wiederum ist in Blöcke aufgeteilt. Jeder Block umfasst signierte Transaktionen. Die Blöcke sind untereinander in einer Kette kryptografisch verbunden; diese Kette wird als Blockchain bezeichnet. Das Vertrauen in die Blockchain entsteht durch die kryptografischen Verfahren, die eine nachträgliche Änderung des Kontenbuchs nach heutigem Stand der Technik praktisch unmöglich machen[2]. In den nachfolgenden Erläuterungen werden die grundlegenden Konzepte von DLT hauptsächlich am Beispiel der Blockchain-Technologie erörtert.

[1] Satoshi Nakamoto ist ein Pseudonym. Zum aktuellen Zeitpunkt ist jedoch nicht geklärt, welche Person oder Personengruppe sich hinter diesem Pseudonym verbirgt.

[2] Unter bestimmten Umständen sind nachträgliche Änderungen dennoch möglich, nämlich dann, wenn ein substanzieller Teil des Netzwerks sich verbündet und gezielt gegen die Regeln verstößt. Zu diesen sogenannten 51-Prozent-Attacken siehe auch Abschnitt 5.3.2.2.

4.1 Grundlegende Konzepte

Die Identifikation von potenziellen Anwendungsfeldern sowie die Bewertung und Diskussion von Anwendungsbeispielen erfordern die Kenntnis der grundlegenden Blockchain-Konzepte. Die nachfolgende Darstellung bezieht sich primär auf die derzeit am häufigsten genutzten „Blockchain 1.0“- und „Blockchain 2.0“ -Plattformen wie Bitcoin bzw. Ethereum etc. Nachstehend werden grundlegende Konzepte und daraus resultierende wichtige Charakteristiken der DLT vereinfacht vorgestellt.

4.1.1 Blockchain-Netzwerk

Eine Blockchain-Infrastruktur basiert auf einem Netzwerk von Computern, die nach dem Peer-to-peer-Modell verbunden sind, d. h., alle Computer sind gleichberechtigt. Die Gestalt der Vernetzung der Computer (Topologie) ist nicht vorgegeben. Insbesondere ist nicht nötig, dass jeder Computer mit jedem anderen Computer im Netzwerk verbunden ist. Die einzelnen Computer werden auch als Knoten im Netzwerk bezeichnet. Der linke Teil der Abbildung 2 zeigt ein Blockchain-Netzwerk.

Dieses einfache Peer-to-peer-Modell unterstützt die leichte Änderbarkeit des Netzwerks und bietet den Vorteil, dass zusätzliche Computer mit geringem Aufwand als Knoten in das Netzwerk aufgenommen werden können. Ebenso einfach können Knoten aus dem Netzwerk ausscheiden. So ist es bspw. jederzeit möglich, einen Computer in das öffentliche Bitcoin-Netzwerk einzufügen, um Finanztransaktionen durchzuführen oder sich sogar am Mining von Bitcoins zu beteiligen. Letzteres dürfte jedoch mit einem marktüblichen Computer nicht besonders erfolgreich sein, da die Wahrscheinlichkeit, Bitcoins zu erzeugen, mit der Leistungsfähigkeit des Computers steigt.

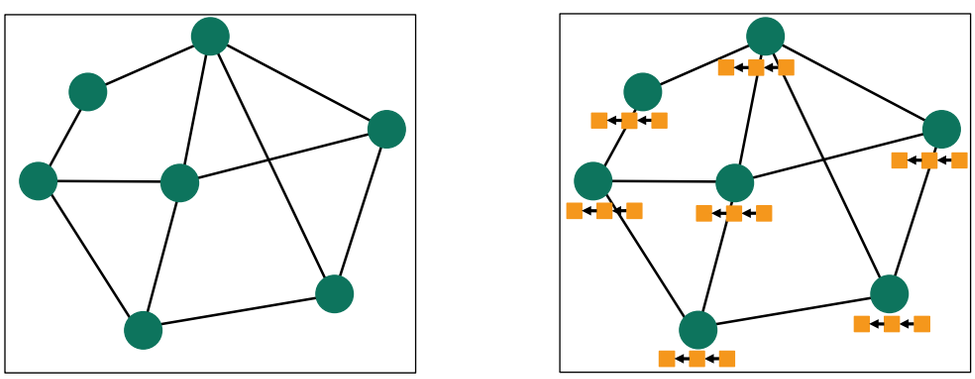


Abbildung 2: Blockchain-Netzwerk und DLT verfügbar an jedem Blockchain-Knoten

4.1.2 Transaktion, Distributed Ledger, digitale Signatur

Das zweite grundlegende Konzept betrifft die Speicherung und das Management von Daten in Form von Transaktionen. Eine bestimmte Anzahl von Transaktionen wird in einem Block zusammengefasst. Die Blöcke werden kryptografisch verkettet und bilden das dezentral geführte Kontenbuch (DL), das von jedem Blockchain-Knoten gespeichert wird (vgl. rechter Teil der Abbildung 2). Das Konzept Transaktion ist im Kontext von Blockchain weiter gefasst als die Überweisung von Geld oder die Übertragung von Gütern. So können insbesondere Zustandsinformationen als Transaktionen in einer Blockchain gespeichert werden. Beispiele für Transaktionen sind: „Alice überweist Bob 10 EURO“, „PKW 1518 hat an der Ladestation L 37 kWh Strom getankt“ oder „LKW 2324 ist von A nach B im Platoon an dritter Stelle mitgefahren“. Die Transaktionen werden digital

unterschrieben, damit sie in die Blockchain eingetragen werden können. Die digitale Signatur kann von Personen, aber auch von anderen Teilnehmern im Blockchain-Netzwerk wie Fahrzeugen, Maschinen etc. erstellt werden.

Die digitale Signatur basiert auf dem Public-Key-Infrastruktur-Verfahren (PKI), welches die Ausstellung und Prüfung von digitalen Zertifikaten unterstützt. Jeder Knoten im Blockchain-Netzwerk verfügt über Paare von öffentlichen und privaten Schlüsseln. Transaktionen werden mit dem privaten Schlüssel unterschrieben und enthalten überdies den entsprechenden öffentlichen Schlüssel. Auf diese Weise wird sichergestellt, dass sämtliche Knoten des Blockchain-Netzwerks die Identität desjenigen Knotens feststellen können, der die Transaktion erstellt hat.

4.1.3 Fluss der Transaktionen durch das Blockchain-Netzwerk

Die Art und Weise, wie Transaktionen sich durch das Blockchain-Netzwerk bewegen, ist ein weiteres grundlegendes Konzept. Angenommen, Alice sitzt vor ihrem Computer, der ein Knoten in einem Blockchain-Netzwerk ist; sie möchte 10 EURO an Bob überweisen. Alice erstellt die Überweisung, signiert sie und schickt sie ab. Dadurch wird eine entsprechende Transaktion publiziert und an die Knoten im Blockchain-Netzwerk weitergeleitet, mit denen der Computer von Alice direkt verbunden ist. Diese prüfen z. B., ob Alice über genügend Geld für die Überweisung verfügt. Ist diese Validierung erfolgreich, dann leiten diese Knoten die Transaktion an ihre Nachbarknoten weiter, sodass die Transaktion durch das gesamte Blockchain-Netzwerk propagiert wird. Der linke Teil der Abbildung 3 zeigt den Fluss von Alices Transaktion durch das Blockchain-Netzwerk.

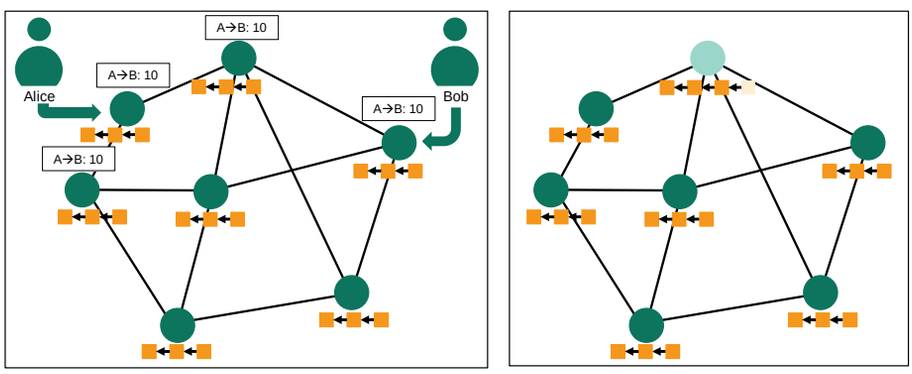


Abbildung 3: Transaktionen im Blockchain-Netzwerk (links); der oberste Knoten hat das kryptografische Rätsel gelöst (rechts)

4.1.4 Hashwert

Neben digitalen Signaturen haben kryptografische Hashfunktionen eine entscheidende Bedeutung in der Blockhain-Technologie. Sie sorgen dafür, dass Daten in der Blockchain manipulationssicher gespeichert sind. Ein Hashwert ist eine eindeutige Bit-Kette einer bestimmten Länge, z. B. 256 Bits, die von jeder digitalen Information wie Textdokumenten, Bildern, Videos oder anderen Datensätzen mit sogenannten Hashfunktionen effizient berechnet werden kann. Im Kontext von Blockchain werden spezielle kryptografische Hashfunktionen eingesetzt, die zusätzliche Eigenschaften aufweisen.

Die Einweg-Eigenschaft fordert, dass es praktisch unmöglich ist, aus einem vorgegebenen Hashwert die digitale Information zu ermitteln, die bei Anwendung der Hashfunktion den Hashwert ergibt. Die zweite Eigenschaft (collision resistance) fordert, dass es praktisch unmöglich ist, zwei unterschiedliche digitale Informationen zu finden, die denselben Hashwert ergeben.

In der Bitcoin-Blockchain wird als kryptografische Hashfunktion SHA-256 (secure hashing algorithm 256) verwendet. Benutzt man SHA-256, dann ergibt sich bspw. für den ersten Satz in diesem Abschnitt ein Hashwert von B268412D9ED0FAE71B480988CC15EA9B62092DAC79467A18C951502D5E871AD7 in hexadezimaler Darstellung.

4.1.5 Block

Ein Block enthält eine bestimmte Anzahl von signierten Transaktionen und eine Kopfzeile, die zur kryptografischen Verkettung mittels der Hashwerte der Blöcke benötigt wird. Die Kette der Blöcke bildet die sogenannte Blockchain. Diese Struktur wird in Abbildung 4 verdeutlicht.

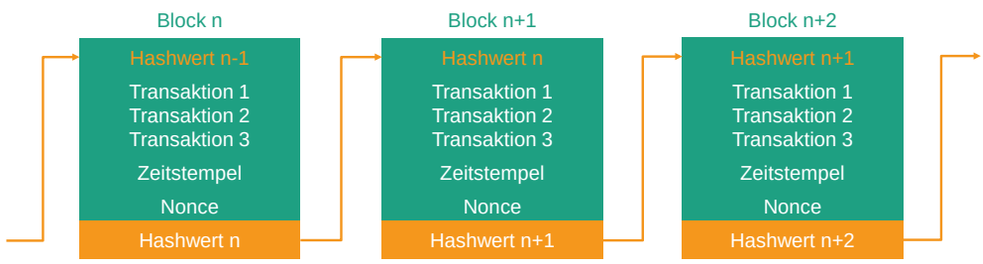


Abbildung 4: Struktur einer Blockchain – verkettet über Hashwerte

Wenn eine bestimme Anzahl von Transaktionen erreicht ist, wird ein neuer Block erzeugt und an die Blockchain angefügt. Die Entscheidung darüber, welcher Knoten des Blockchain-Netzwerks den Block erzeugt und an die Blockchain anfügt, ist Teil des sogenannten Konsensfindungsverfahrens und wird im nächsten Abschnitt diskutiert.

4.1.6 Konsensfindung

Die Konsensfindung trägt entscheidend zur Vertrauenswürdigkeit der Blockchain bei. An dieser Stelle wird das derzeit gebräuchlichste Konsensfindungsverfahren „Proof of Work“ beschrieben, das aktuell in der Bitcoin- und Ethereum-Blockchain verwendet wird.

Um einen neuen Block zu erzeugen und an die Blockchain anzuhängen, haben die Knoten des Blockchain-Netzwerks ein kryptografisches Rätsel zu lösen, das mehrere Eingabeparameter aufweist. Darunter sind die Liste der Transaktionen, die in dem neuen Block gespeichert sein sollen, der Hashwert des vorherigen Blocks und eine unbekannte Zahl, eine sogenannte Nonce. Das Rätsel ist gelöst, wenn eine Nonce gefunden wurde, die zusammen mit den anderen Eingabeparametern einen Hashwert erzeugt, der kleiner als ein vorgegebener Hashwert ist. Die Lösung des Rätsels kann aufgrund der zuvor erläuterten Eigenschaften der Hashfunktion nur durch rein zufälliges Ausprobieren gefunden werden: Es werden nacheinander verschiedene Werte für die Nonce eingesetzt und geprüft, ob das Ergebnis gültig ist. Der Schwierigkeitsgrad des Rätsels wird in der Regel von Zeit zu Zeit angepasst und ist bei der Bitcoin-Blockchain dergestalt gewählt, dass im Durchschnitt alle 10 Minuten ein Block an die Blockchain angefügt wird.

Der erste Knoten im Blockchain-Netzwerk, welcher das Rätsel gelöst hat, fügt den neuen Block an sein Kontenbuch an; dies ist im rechten Teil der Abbildung 3 dargestellt. Dazu wird in die Kopfzeile des neuen Blocks neben der Nonce auch der Hashwert des Vorgängerblocks eingetragen. Dessen Vorgängerblock enthält wiederum seine Nonce und den Hashwert seines Vorgängerblocks etc. Durch diese Konstruktion der Blockchain ist die Kette der Blöcke manipulationssicher verbunden. Die Integrität eines Blocks kann direkt geprüft werden, indem dessen Hashwert berechnet und mit dem im Vorgängerblock gespeicherten Hashwert verglichen wird.

Der neue Block wird an die Nachbarknoten weitergeleitet, welche die Richtigkeit der Lösung überprüfen. Im Gegensatz zur Lösung des Rätsels ist die Überprüfung der Richtigkeit der Lösung sehr einfach und nicht zeitaufwendig.[3] Falls die Lösung korrekt ist, wird der neue Block an die bisherige Kette des Knotens angefügt sowie an die Nachbarknoten weitergeleitet. Somit propagiert der neu erzeugte Block durch das Blockchain-Netzwerk und die Kette wird bei allen Knoten um den neuen Block erweitert.

4.1.7 Charakteristiken der Blockchain

Aus den voranstehend vorgestellten grundlegenden Konzepten ergeben sich direkt wichtige Charakteristiken der Blockchain. Die erste ist die Unveränderbarkeit der verteilten Datenbank (DL). Nach heutigem Stand der Technik ist es nicht möglich, nachträglich Transaktionen zu manipulieren. Eine Manipulation einer Transaktion hätte zur Folge, dass der Hashwert des entsprechenden Blocks sich ändert. Folglich wären ab dem Block, der die manipulierte Transaktion enthalten soll, alle kryptografischen Rätsel neu zu lösen, damit die Manipulation nicht auffällt.

Neben der Unveränderbarkeit des Distributed Ledgers ist die Dezentralisierung von Prozessen eine weitere Charakteristik der Blockchain. Die Dezentralisierung wird dadurch erreicht, dass keine zentrale Instanz, sondern die Knoten des Blockchain-Netzwerks darüber entscheiden, welche Transaktionen in das Kontenbuch aufgenommen werden. Zusätzlich ermitteln diese durch die Konsensfindung, welcher Knoten den neuen Block erstellt. Die DLT kann dadurch zentrale Instanzen ersetzen.

Eine dritte Charakteristik der DLT ist die Automatisierung von Prozessen. Diese wird durch sogenannte Smart Contracts erreicht, die im folgenden Abschnitt eingeführt und diskutiert werden.

4.2 Weitere Konzepte

Die Technologie der Bitcoin-Blockchain wurde weiterentwickelt und führte zu Systemen, die als Blockchain 2.0 bezeichnet werden. Es entstanden weitere Konzepte, welche die Anwendungsmöglichkeiten der DLT vergrößerten und die ebenfalls für die Anwendungsfallbeispiele im speziellen Teil dieses Gutachtens von Relevanz sind. Nachfolgend werden diese in kompakter Form vorgestellt.

4.2.1 Smart Contracts

Smart Contracts sind Skripte (Programmcode, Computeranweisungen), welche die Teilnehmer eines Blockchain-Netzwerks ausführen. Sie bieten in der Theorie die Ausführung beliebiger Berechnungen, solange diese deterministisch sind, d. h. bei gleichem Input kommt der gleiche Output heraus. Meistens beinhalten Smart Contracts IFTTT (if this then that)-Anweisungen und setzen damit Steuerungs- bzw. Geschäftslogiken um. Viele IFTTTs verschachteln Smart Contracts und machen sie „komplex". Aus rein juristischer Perspektive stellen Smart Contracts jedoch weder einen Vertrag dar noch sind sie sonderlich intelligent, sondern regeln und koordinieren in den allermeisten Fällen nur Abläufe bzw. Datenflüsse. Smart Contracts sind weder im Bitcoin-Netzwerk vorgesehen noch auf azyklisch gerichteten Graphen basierten DLT-Systemen. Auch wenn daran bereits gearbeitet wird, so liegen dessen ungeachtet bereits heute Anwendungen für diese Systeme vor, sodass offensichtlich DLT-Systeme auch ohne Smart Contracts Mehrwert bieten können. Dies ist zudem am Anwendungsfallbeispiel Platooning nachvollziehbar.

[3] Dieser Sachverhalt ist vergleichbar mit der sehr zeitaufwendigen Suche nach Primfaktoren von sehr großen Zahlen und der schnellen Ermittlung des Produkts von Primfaktoren.

Smart Contracts wirken sich auch auf die Speicherproblematik von DLT aus: Da alle Daten in einer Blockchain dauerhaft gespeichert sind, steigt der Speicherbedarf mit der Zeit kontinuierlich an. Zu diesen Daten zählt ebenfalls der Programmcode von Smart Contracts. Ein weiterer wichtiger Punkt besteht darin, dass mit Smart Contracts lediglich korrekte Rechenoperationen sichergestellt werden können. Dies umfasst nicht die Prüfung von Daten außerhalb der (Blockchain-)Systemgrenzen. Insbesondere Fehler beim Nutzer im Sinne von Fehleintragungen sowie defekte, korrupte, manipulierte Sensoren können problematisch sein. Diese Thematik wird in Abschnitt 4.2.5 adressiert.

Die Bitcoin-Blockchain ist hauptsächlich für finanzwirtschaftliche Anwendungen geeignet. Sie bietet eine Skriptsprache, mit der bspw. ein Treuhandkonto oder sogenannte Micro Payments realisiert werden können. Jedoch bietet die Skriptsprache von Bitcoin nicht die Möglichkeiten einer allgemeinen Programmiersprache wie C++ oder Java; folglich sind die Anwendungsbereiche von Bitcoin eingeschränkt. Die Ethereum-Blockchain bietet mit Solidity hingegen eine Programmiersprache an, mit der Smart Contracts realisiert werden können. Ein Smart Contract ist ausführbarer Programmcode, der in Transaktionen in der Blockchain unveränderbar gespeichert ist und der bei einem definierten Ereignis ausgeführt wird.

Im Mobilitätskontext kann z. B. mithilfe eines Smart Contracts automatisch die Bezahlung von Straßennutzungsgebühren ausgelöst werden, wenn ein Fahrzeug die entsprechenden Mautstationen durchfahren hat. Ebenso ist es möglich, Auktionsmechanismen als Smart Contract zu realisieren, die bspw. im lokalen Energiehandel angewendet werden könnten. So könnten Ladesäulen den Preis mit Stromerzeugern in der Nähe verhandeln und von diesen beziehen. Smart Contracts könnten ebenfalls das Ausleihen oder die Nutzung von Fahrzeugen oder Geräten einfacher gestalten, um (Sensor-)Daten zu aggregieren oder Identitäten zu verwalten.

Ein weiteres Anwendungsbeispiel von Smart Contracts ist die treuhänderische Hinterlegung von Daten (im englischen Sprachgebrauch auch bekannt als Escrow Smart Contract). Beim Onlinekauf stellt sich etwa häufig das Problem, dass der Kunde erst bezahlen möchte, wenn er das Produkt erhalten hat. Auf der anderen Seite möchte der Verkäufer erst dann liefern, wenn er das Geld bekommen hat. Dieses Problem kann durch einen Smart Contract gelöst werden, indem der Kunde das Geld an den Smart Contract überweist und somit den Zugriff auf das Geld verliert, gleichzeitig aber gewisse Bedingungen festgeschrieben werden, die eintreten müssen, damit das Geld vom Smart Contract freigegeben und an den Verkäufer überwiesen wird. Derartige Bedingungen können etwa in einer digitalen Bestätigung der Lieferung durch den Kunden oder einer vorher festgelegten dritten Partei, etwa den Spediteur, bestehen.

4.2.2 Alternative Konsensfindungsverfahren

In Abschnitt 4.1.6 wurde das Konsensfindungsverfahren Proof of Work vorgestellt, das in der aktuellen Bitcoin- und Ethereum-Blockchain verwendet wird. Bei beiden Beispielen handelt es sich um sogenannte öffentliche Blockchain-Netzwerke, bei denen im Prinzip jeder mitmachen kann; insbesondere kennt man die Vertrauenswürdigkeit der einzelnen Blockchain-Knoten nicht. Proof of Work gewährleistet den Wettbewerb unter den Blockchain-Knoten dahingehend, wer einen neuen Block erzeugen darf. Wechselnde Blockchain-Knoten erzeugen die neuen Blöcke und eine Manipulation von Blöcken sowie der darin enthaltenen Transaktionen wird auf diese Weise praktisch ausgeschlossen.

Im Gegensatz zu öffentlichen Blockchain-Netzwerken können an privaten oder konsortialen Blockchain-Netzwerken lediglich Partner teilnehmen, die dafür ausgewählt worden und vertrauenswürdig sind. Aufgrund des bereits bestehenden Vertrauens können die Verfahren zur Konsensfindung in solchen Blockchain-Netzwerken deutlich einfacher gestaltet werden. Dies reicht vom Proof of Work mit reduziertem Schwierigkeitsgrad über

Proof of Stake und Lottery Protocol bis hin zu ausgewählten Validierungsknoten. Der Zusammenhang zwischen dem Durchsatz an Transaktionen und dem Grad der Offenheit von Blockchain-Netzwerken abhängig vom eingesetzten Verfahren zur Konsensfindung ist in Abbildung 5 schematisch dargestellt.

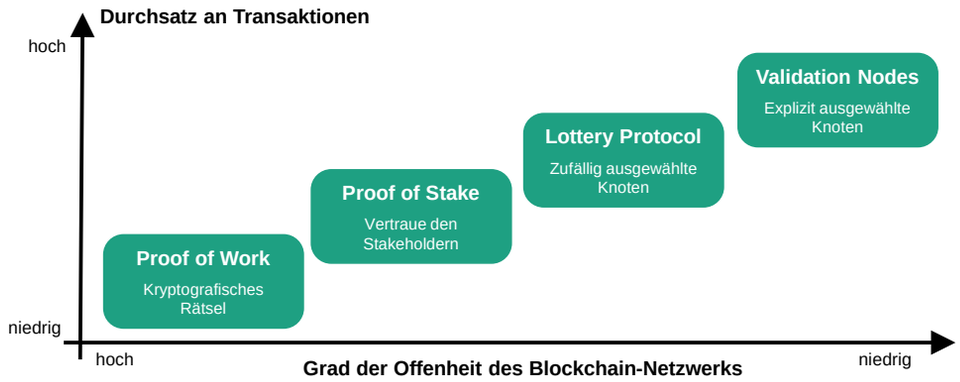


Abbildung 5: Leistungsstärke der Blockchain abhängig vom Konsensfindungsverfahren

Proof of Stake

Mit Proof of Stake wird eine Klasse von Verfahren zur Konsensfindung bezeichnet, die den Anteil der Blockchain-Knoten (Teilnehmer) am Blockchain-Netzwerk berücksichtigt. Anteile können z. B. die Menge an Vermögen (coins), die Anzahl der hinzugefügten Blöcke oder die Dauer der Beteiligung am Blockchain-Netzwerk sein. Der entsprechende Anteil lässt sich zügig berechnen und die Auswahl, wer den nächsten Block der Blockchain hinzufügt, erfolgt über eine Gewichtung des Anteils kombiniert mit einem Zufallsverfahren. Die Sicherheit besteht hier heuristisch darin, dass man mit einem gewissen Anteil dafür bürgt, dass man sich an die Regeln des Netzwerks hält (das Analogon zum Proof of Work wäre hier, dass man Energie verbraucht und so Kapital einsetzt) – versucht man, Blöcke hinzuzufügen, die eine Regel verletzen, so verliert man den eingesetzten Anteil.

Proof of Authority

Dieses Verfahren zur Konsensfindung setzt auf explizit ausgewählte Blockchain-Knoten, sogenannte Prüfknoten (validators). Nur die Prüfknoten dürfen Transaktionen zu Blöcken zusammen- und diese zur Blockchain hinzufügen. Über einen Reputationsmechanismus können Blockchain-Knoten mit positiver Reputation zu Prüfknoten werden. Ist die Reputation eines Knotens negativ, verliert der Prüfknoten seine Prüfeigenschaft.

4.2.3 Sharding

Sharding ist ein derzeit in Erprobung befindlicher Ansatz, den Durchsatz an Transaktionen in Blockchains zu erhöhen und damit die Skalierbarkeit einer Blockchain-Infrastruktur insgesamt zu verbessern. Diesem Verfahren liegt die Partitionierung (Sharding) der Blockchain zugrunde, d. h., die Knoten im Blockchain-Netzwerk verwalten jeweils verschiedene Teile des Kontenbuchs (Distributed Ledger). Bestimmte Blockchain-Knoten verarbeiten nur die Transaktionen der entsprechenden Partition, was eine parallele Verarbeitung von Transaktionen ermöglicht und so den Durchsatz an Transaktionen erhöht. Das Sharding ist so gestaltet, dass die Integrität des gesamten Kontenbuchs garantiert ist. OmniLedger ist ein Beispiel für eine prototypische DLT-Infrastruktur, die Sharding nutzt.

4.2.4 Integration externer Daten

In Blockchain-Plattformen werden Daten als Transaktionen gespeichert, die ihrerseits in Blöcken zusammengefasst sind und das dezentral geführte Kontenbuch (Distributed Ledger) bilden, vgl. Abschnitt 4.1.2. Diese Transaktionen sollten jedoch nicht zu viele Daten enthalten, da die Größe der DLT mit der Speichergröße der Transaktionen und deren Anzahl wächst. Ein Standardverfahren zur Integration externer Daten wie Textdokumenten, Bildern, Videos oder Auszügen von multimedialen Datenbanken ist die Verwendung eines sogenannten „digitalen Fingerabdrucks" in Form eines entsprechenden Hashwerts in den Transaktionen. Dabei wird ein „Link" zu den Daten zusammen mit einem Hashwert der Daten auf der Blockchain gespeichert. Über den Link kann dann jederzeit auf die Daten zugegriffen werden. Gleichzeitig kann dergestalt die Integrität der externen und damit veränderbaren Daten geprüft werden, indem der Hashwert der aktuellen externen Daten mit dem in der Blockchain gespeicherten Hashwert verglichen wird. Jede Manipulation der externen Daten würde somit direkt sichtbar werden, da dann der Hashwert des externen Datums nicht mit dem in der Blockchain gespeicherten übereinstimmen würde. Eine zweite Klasse von externen Daten sind Sensorwerte. Sensoren erfassen Zustände der realen Welt und werden insbesondere für Anwendungen im Internet der Dinge oder in Supply-Chain-Prozessen benötigt. In einer Lebensmittellieferkette unterstützen Sensoren etwa die Nachverfolgbarkeit von Lebensmitteln: Sie können Alarme auslösen, wenn bspw. der Kühlkreislauf unterbrochen wurde, oder Maßnahmen veranlassen, wenn die Lebensmittel an einem bestimmten Ort angekommen sind. Die Automatisierung von Prozessen kann insbesondere durch die Kombination von Sensorwerten und Smart Contracts unterstützt werden. Sensoren liefern jedoch zunächst Werte, die außerhalb der Blockchain liegen. Deshalb ist es wichtig, die Identität der Sensoren und die Korrektheit der Sensorwerte zu überprüfen, bevor diese in der Blockchain gespeichert werden. Vergleichbare Korrektheitsfragen treten auch bei anderen Informationen auf, die in die Blockchain eingetragen werden sollen (siehe auch Kapitel 4.2.5)

4.2.5 Orakel

Die in Kapitel 4.2.4 angeführten Fragestellungen haben zur Entwicklung von sogenannten Orakeln geführt. Damit werden Services von Dienstleistungsanbietern bezeichnet, die vertrauenswürdige Sensorwerte und Onlineinformationen wie etwa Wetterdaten, Spielergebnisse usw. zur Verfügung stellen. Besonders im Mobilitätssektor besteht Bedarf an Blockchain-Infrastrukturen, die entsprechende Blockchain-Clients direkt auf Geräten im Internet der Dinge (IoT) implementieren, um Sensorwerte und Kommunikationswege entsprechend abzusichern. Dazu müssen IoT-Geräte um die notwendige Rechenleistung und Speicherkapazität für die sichere Schlüsselverwaltung erweitert werden. Auf den Bezug von IoT zu DLT wird in Kapitel 5.1.1 noch ausführlich eingegangen.

4.3 Blockchain- und DLT-Infrastrukturen

Die DLT hat sich seit der Einführung von Bitcoin stetig weiterentwickelt. Insbesondere sind neben der Blockchain-Datenstruktur aus verketteten Blöcken, die Bitcoin und Ethereum zugrunde liegt, weitere Datenstrukturen entstanden, die bspw. eine erhöhte Performanz oder eine verbesserte Skalierbarkeit versprechen. Als umfassender Begriff für all diese Technologien hat sich der Begriff Distributed-Ledger-Technologien (DLT) etabliert.

4.3.1 Klassifikationen

Die Evolution der DLT lässt sich in mehrere Phasen unterteilen. Blockchain 1.0, welche den Grundstein für die Entwicklung aller DLT-Infrastrukturen legte, wurde 2008 zum ersten Mal genannt, als Satoshi Nakamoto (bzw. die Person, die hinter diesem Pseudonym steht) das Paper „Bitcoin: A Peer to Peer Electronic Cash System" veröffentlichte.

Im Anschluss wurde mit der ersten funktionsfähigen Implementierung von Bitcoin im Jahr 2009 die erste Blockchain eingesetzt.[4] Die Bitcoin-Blockchain ist transaktionsorientiert, d. h., dort können Transaktionen gespeichert werden, mit denen die Kryptowährung Bitcoin zwischen den Nutzern der Infrastruktur transferiert werden kann. Nach der Veröffentlichung von Bitcoin wurden zahlreiche weitere transaktionsorientierte DLT entwickelt, die alle auf ihrer eigenen Kryptowährung basieren. Diese alternativen Kryptowährungen werden Altcoins (Alternative Coins) genannt.

Während die Technologien von Blockchain 1.0 fast ausschließlich genutzt werden, Kryptowährungen zwischen Akteuren zu transferieren, gibt es – wie bereits in Abschnitt 4.2.1 erläutert – bei Blockchain 2.0 Smart Contracts.[5] Derartige Blockchains nennt man auch logikorientiert, da dort Smart Contracts, also Auszüge von Programmiercode, eingefügt und automatisch ausgeführt werden. Hieraus ergeben sich zahlreiche weitere Anwendungsfälle für Blockchain-Infrastrukturen, in denen ein gewisser Grad von Geschäftslogik notwendig ist. Abbildung 6 zeigt die Einordnung von einigen Blockchain-Infrastrukturen in die Klassifikation von Blockchain 1.0 und Blockchain 2.0.

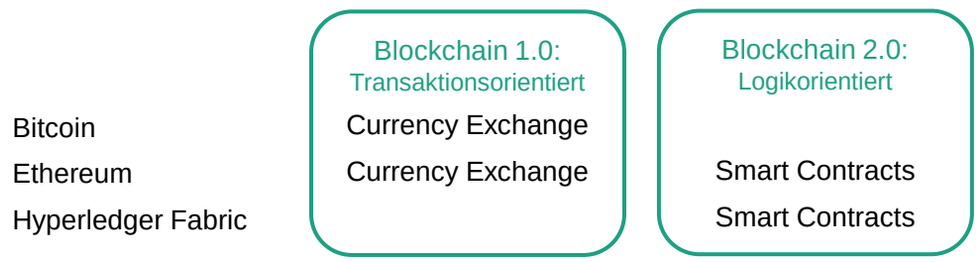


Abbildung 6: Einordnung einiger DLT in 1. und 2. Blockchain-Generation

Neben der Klassifikation der DLT in erste und zweite Generation kann man diese auch nach dem Grad der Öffentlichkeit in öffentliche und private sowie nach dem Grad der Zugriffsbeschränkung in permissioned (zugriffsbeschränkte) und permissionless Plattformen unterteilen.[6] Öffentliche Plattformen, wie bspw. Bitcoin, bieten unbeschränkten Zugriff für Nutzer, d. h., jeder kann am Netzwerk teilnehmen und sehen, welche Transaktionen der Blockchain hinzugefügt werden. In privaten Plattformen hingegen existieren Zugangsbeschränkungen, es kann also nicht jede beliebige Person Teil des Netzwerks werden, sondern für eine Aufnahme in das Netzwerk ist eine Registrierung, etwa in Form der Zustimmung aller bisherigen Teilnehmer, erforderlich. Der wichtigste Vertreter für private DLT sind sogenannte konsortiale DLT-Systeme. Dies bezeichnet in der Regel einen Zusammenschluss mehrerer Akteure, bspw. verschiedener Unternehmen.

Ist eine Plattform permissionless, können Netzwerkteilnehmer ohne Beschränkungen alle Aktionen ausführen; ist die Plattform hingegen permissioned, kann es verschiedene Rollenprofile geben, sodass einer Person nur bestimmte Aktionen möglich sind. In einer permissioned Plattform könnte bspw. ein Teilnehmer die Autorisierung haben, Transaktionen zu lesen, nicht aber selbst neue Transaktionen hinzuzufügen. Der Zusammenhang zwischen öffentlichen, privaten, permissioned und permissionless Blockchains ist im linken Teil der Abbildung 7 aufgeführt.

[4] *Lamberti/Gatteschi/Demartini/Pranteda* et al., IT Professional (Early Access) 2017, 1.
[5] *Lamberti/Gatteschi/Demartini/Pranteda* et al., IT Professional (Early Access) 2017, 1.
[6] *Vukolic,* Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts 2017, 3.

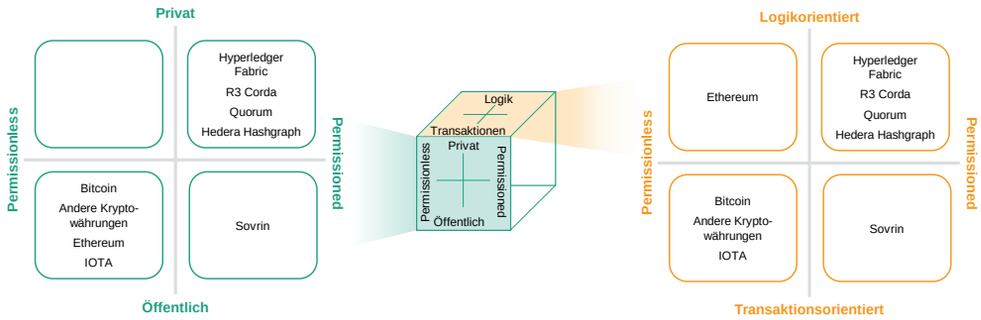


Abbildung 7: Klassifizierung von Blockchain-Plattformen nach Grad der Öffentlichkeit, Grad der Zugriffsbeschränkung und Programmierbarkeit

Eine weitere Dimension zur Klassifikation von Blockchain-Plattformen ist die Programmierbarkeit. Diese Dimension unterscheidet zwischen transaktions- und logikorientierten Plattformen. Die Bitcoin-Blockchain ist transaktionsorientiert und bietet eine Skriptsprache, mit der lediglich einfache Zusammenhänge dargestellt werden können. Logikorientierte Blockchain-Infrastrukturen bieten eine höhere Programmiersprache an, mit der Smart Contracts realisiert werden können. Im rechten Teil der Abbildung 7 sind Blockchain-Plattformen nach Grad der Zugriffsbeschränkung und Programmierbarkeit klassifiziert dargestellt.

Blockchain-Plattformen können gleichfalls nach der Nutzung oder Nichtnutzung von Kryptowährungen unterschieden werden. So nutzen die Bitcoin- und die Ethereum-Blockchain Kryptowährungen, mit denen die Speicherung von Transaktionen und das Ausführen von Smart Contracts bezahlt werden. Ferner erhalten die Miner als Vergütung für ihre Arbeit einen bestimmten Betrag in der entsprechenden Kryptowährung. Ist die Kryptowährung dringend für den Betrieb des DLT-Systems erforderlich, so wird diese auch als „nativ" bezeichnet.
Hyperledger Fabric ist ein Beispiel für eine Blockchain-Plattform, die für ihre Grundfunktionalität keine Kryptowährung benötigt – es gibt keine Belohnungen für das Minen neuer Blöcke und es fallen auch keine Transaktionskosten an – und entsprechend keine native Kryptowährung besitzt. Durch geeignete Smart Contracts (Chaincode) können allerdings durchaus Token erstellt werden, die sämtliche Eigenschaften einer Kryptowährung erfüllen.

4.3.2 Bitcoin

Wie in Abschnitt 4.3.1 dargestellt, hat die DLT ihren Ursprung in der Bitcoin-Blockchain. Diese ist öffentlich und permissionless, sodass jeder teilnehmen kann und keine Nutzungsbeschränkungen bestehen[7]. Als Teil der ersten Blockchain-Generation hat die Bitcoin-Blockchain eine native Kryptowährung, Bitcoin, und wird dazu verwendet, diese Währung zu erzeugen und zwischen Netzwerkteilnehmern zu transferieren. Als Konsensusmechanismus wird der Proof-of-Work-Algorithmus verwendet.

4.3.3 Ethereum

Die Ethereum-Blockchain wurde 2015 u. a. von Vitalik Buterin, Gavin Wood and Jeffrey Wilcke entwickelt. Ethereum stellt das erste Beispiel einer Blockchain 2.0 dar und bietet

[7] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System.; *Narayanan/Bonneau/Felten/Miller* et al., Bitcoin and cryptocurrency technologies: A comprehensive introduction.

somit die Möglichkeit, nicht nur digitalen Zahlungsverkehr über die Blockchain abzuwickeln, sondern ganze Prozesse mithilfe von Smart Contracts zu automatisieren.[8] Die Kryptowährung, auf der Ethereum basiert, heißt Ether. Ether können zudem zu sogenanntem Gas umgewandelt werden, welches benötigt wird, um Transaktionen und Smart Contracts ausführen zu können; Transaktionsgebühren bzw. Gebühren für die Ausführung von Smart Contracts werden demzufolge mit Gas bezahlt. Die Ethereum-Blockchain ist wie die Bitcoin-Blockchain öffentlich und permissionless, es kann also auch hier jede Person Zugriff auf die Blockchain erhalten und hat dieselben Berechtigungen wie alle anderen Teilnehmer am Netzwerk. Ethereum war damit auch der Ausgangspunkt für die Entwicklung zahlreicher verteilter Applikationen – sogenannter verteilter Apps („Dapps") – in einer Vielzahl von Anwendungsgebieten und Industrien, da der Nutzen von Blockchain nicht mehr nur für den Finanzsektor besteht. Ethereum verwendet wie Bitcoin einen Proof-of-Work-Konsensalgorithmus. Da dieser jedoch wie bereits erläutert äußerst ressourcenaufwendig ist, plant die Ethereum-Stiftung, in Zukunft mit Proof of Stake (siehe Abschnitt 4.2.2) auf ein anderes, ressourcenschonenderes Verfahren, zu wechseln.

4.3.4 Quorum

Quorum ist eine Blockchain, die auf der Ethereum-Blockchain basiert und ihren Ursprung in einer „Fork" – also einer Abzweigung des Ethereum-Codes – hat.[9] Im Gegensatz zu der Ethereum-Blockchain ist die Quorum-Blockchain allerdings eine konsortiale, permissioned Blockchain, zudem gibt es private Transaktionen, die nur von bestimmten Nutzern eingesehen werden können. Transaktionen, die getätigt werden, sind zudem kostenlos, es wird also kein Gas für Transaktionsgebühren benötigt. Durch diese Veränderungen sowie die Wahl eines alternativen Konsensmechanismus soll Quorum in Zukunft sowohl effizienter werden als auch den Nutzern einen höheren Grad an Privatsphäre für ihre Transaktionen bieten, was diese Blockchain insbesondere für Unternehmen interessant macht.

4.3.5 Hyperledger Fabric

Hyperledger Fabric ist eine weitere Blockchain-Plattform und eines von mehreren Hyperledger-Projekten, die unter der Linux Foundation entstanden sind.[10] Hyperledger Fabric wird seit 2017 von IBM entwickelt. Im Gegensatz zur Bitcoin- und der Ethereum-Blockchain benötigt Fabric keine native Kryptowährung. Stattdessen stellt Hyperledger Fabric Smart Contracts, die dort aufgrund einer im Vergleich zu anderen Blockchains leicht modifizierten Architektur „Chaincode" genannt werden. Falls es notwendig ist, können aber mithilfe dieser Funktionalitäten für einzelne Applikationen ebenfalls Kryptowährungen erzeugt werden. Auch in den Zugriffsrechten unterscheidet sich Hyperledger Fabric von Bitcoin und Ethereum, denn Fabric ist eine private und permissioned Blockchain. Wie in Quorum gibt es zusätzlich die Möglichkeit, verschiedene Rechte für die Teilnehmer zu implementieren, sodass bspw. ein Teil der Transaktionen bzw. die Ausführung von Smart Contracts nicht für alle sichtbar ist. Somit ist auch Hyperledger Fabric besonders für organisationsübergreifende Anwendungen interessant und dementsprechend unternehmensorientiert. Abhängig von der jeweils zu implementierenden Applikation können bestimmte Charakteristiken der Blockchain modular angepasst werden, wie etwa der Konsensfindungsmechanismus und die Verwaltung der Zugriffsrechte.

[8] *Buterin*, Ethereum White Paper.
[9] *Baliga/Subhod/Kamat/Chatterjee*, Performance evaluation of the quorum blockchain platform.
[10] *The Linux Foundation*, Hyperledger Architecture, Volume 1.

4.3.6 Corda

Corda ist im Gegensatz zu Ethereum und Hyperledger Fabric nicht dafür entwickelt, Applikationen in allen Industrien und Anwendungsbereichen zu unterstützen, sondern wurde durch das Industriekonsortium R3 speziell für die Finanzindustrie entworfen.[11] Genau wie Hyperledger Fabric besitzt Corda keine native Kryptowährung, bietet jedoch die Möglichkeit zur Implementierung von Smart Contracts. Die Smart Contracts in Corda können jedoch nicht nur Programmiercode, sondern auch juristische Prosa enthalten, was für die hochregulierte Finanzindustrie sehr sinnvoll ist. Ebenfalls ähnlich wie Hyperledger Fabric ist Corda privat und permissioned, also zugangs- und zugriffsbeschränkt. Auch bei Corda ist der Konsensmechanismus modular anpassbar.

4.3.7 Sovrin

Sovrin ist eine Blockchain-Initiative, die durch ihre Arbeit an Hyperledger Indy im weiteren Sinne ebenfalls dem Linux-Hyperledger-Projekt zugerechnet werden kann und die es sich zum Ziel gesetzt hat, umfassende selbstsouveräne digitale Identitäten zu ermöglichen.[12] Sovrin ist öffentlich und permissioned, es kann also jeder an dem Blockchain-System teilnehmen und von einer digitalen Identität profitieren, allerdings liegen innerhalb des Systems Rollenprofile mit bestimmten Rechten vor. Da eine selbstsouveräne digitale Identität unabhängig von einer zentralen Autorität verwaltet sein soll, hat jede Person selbst die komplette Kontrolle über die Informationen, aus denen sich die Identität zusammensetzt. Identitätsbezogene Informationen können als „Claim" einer Identität zugewiesen werden. Beispielsweise kann ein Führerschein von einer autorisierten Behörde als Claim erstellt und einer bestimmten Person zugeordnet werden und wird damit Teil der digitalen Identität dieser Person. Möchte die Person Informationen aus ihrer digitalen Identität teilen, kann dies selektiv geschehen. Somit können je nach Bedarf lediglich bestimmte Informationen zusammengestellt und geteilt werden, ohne sämtliche Aspekte der digitalen Identität offenzulegen. Diese Identitätsverwaltung auf der Blockchain soll die Notwendigkeit vieler einzelner Accounts, Benutzernamen und Passwörter obsolet machen und die Idee einer einzigen digitalen und manipulationssicheren Identität für jeden Menschen verwirklichen. Auch Sovrin verwendet nicht den Proof-of-Work-Konsensusalgorithmus, sondern einen sogenannten RBFT (Redundant Byzantine Fault Tolerance)-Algorithmus. An dieser Stelle ist besonders hervorzuheben, dass bei Sovrin keine personenbezogenen Daten auf der Blockchain gespeichert werden. Vielmehr dient die Blockchain an dieser Stelle der Verwaltung von öffentlichen Schlüsseln („Adressen") sowohl von vertrauenswürdigen, öffentlichen Behörden als auch von den Nutzern, die über Sovrin eine selbstsouveräne digitale Identität nutzen können. Persönliche Daten verbleiben zu jeder Zeit beim Nutzer und die Blockchain dient letztlich dazu, das Monopol von sogenannten Certificate Authorities, die traditionell dazu dienen, im Internet auf vertrauensvolle Weise Unternehmen öffentliche Schlüssel aus einer PKI zuzuordnen, aufzubrechen und dementsprechend auch privaten Nutzern schnell und kostengünstig öffentliche Adressen zu ermöglichen. Da die öffentlichen Schlüssel auf der Blockchain frei zugänglich und für jeden lesbar sind, könnten aber durch Betrachtung von mehreren Interaktionen dennoch potenziell Rückschlüsse auf personenbezogene Daten stattfinden. Zu diesem Zweck werden infolgedessen bei Sovrin außerdem Zero Knowledge Proofs eingesetzt, die in Kapitel 5.1.3 genauer beschrieben werden.

[11] *Valenta/Sandner*, Comparison of Ethereum, Hyperledger Fabric and Corda.
[12] *Sovrin Foundation*, A Protocol and Token for Self-Sovereign Identity and Decentralized Trust.

Pseudonymisierung vs. Anonymisierung

Regulär findet bei der Nutzung von DLT eine Pseudonymisierung des Benutzers statt, da nur die öffentlichen Schlüssel der PKI angegeben werden. Dadurch kann der Bezug zur wahren Identität eines Nutzers deutlich erschwert werden. Jedoch kann durch Betrachtung wiederholter Aktionen eines Pseudonyms in Verbindung mit zusätzlichen Informationen möglicherweise doch ein Bezug zum Nutzer hergestellt werden. Es gibt jedoch Möglichkeiten, auch die Pseudonyme zu verschleiern oder zu wechseln, was dann sogar Anonymisierung ermöglicht. Insbesondere mit selbstsouveränen, digitalen Identitäten ist eine vollständige Anonymisierung möglich, wobei dennoch Eigenschaften unter den eigenen Pseudonymen übertragen werden können.

4.3.8 IOTA

IOTA ist ein Beispiel für eine DLT, die keine Blockchain als zugrunde liegende Datenstruktur verwendet. Stattdessen werden hier Transaktionen auf dem sogenannten „Tangle" gespeichert, einer Datenstruktur, die auch als gerichteter, azyklischer Graph bezeichnet wird.[13] Im Tangle muss jede neue Transaktion zwei vorhergehende Transaktionen validieren, bevor sie selber in die Datenstruktur aufgenommen werden kann; auf diese Weise entsteht Konsens im Netzwerk. Ausgewählt werden die Knoten nach einem komplizierten Zufallsalgorithmus. Bei der Validierung wird darauf geachtet, dass die Signaturen von Transaktionen korrekt sind und ob die beiden validierten Transaktionen widersprüchliche Informationen zum Tangle hinzufügen. Je mehr neue Transaktionen direkt oder indirekt, d. h. über eine weitere Transaktion, die dazwischenliegt, eine Transaktion validiert haben, desto sicherer kann die Person, welche die Transaktion in das Netzwerk hinzugefügt hat, sein, dass die Transaktion gültig ist und tatsächlich im finalen Tangle verbleibt. Sobald eine Transaktion direkt oder indirekt von allen noch nicht validierten Enden des Tangles, sogenannten Tips, validiert wurde, gilt sie als vollständig akzeptiert. Abbildung 8 zeigt beispielhaft den Aufbau des Tangles, mit einer Gründungs (Genesis)-Transaktion, vollständig und teilweise validierten Transaktionen, sowie neuen, noch nicht validierten Transaktionen (Tips).

IOTA soll im Vergleich zu Blockchains eine besonders hohe Skalierbarkeit aufweisen und wäre demnach besonders für Anwendungen des Internet der Dinge geeignet, da aufgrund der nicht vorhandenen Transaktionskosten ebenfalls Mikrozahlungen sinnvoll umgesetzt werden können. Dies ist insbesondere für Maschine-zu-Maschine-Transaktionen relevant. Zudem ist ein Vorteil des Tangles, dass die Geschwindigkeit, mit der neue Transaktionen validiert werden, mit der Anzahl hinzugefügter Transaktionen steigt. Dies ist ein Kontrast z. B. zu der Bitcoin-Blockchain, bei der das Transaktionsvolumen, also die Anzahl an Transaktionen, gewichtet mit deren Datenvolumen, konstant ist und entsprechend subjektiv die Performanz mit steigender Teilnehmerzahl sinkt, gleichzeitig aber der kumulierte Rechenaufwand des Netzes steigt. Aktuell befindet sich das Netzwerk allerdings noch in einer Übergangsphase, in der laut IOTA-Foundation noch eine zentrale Instanz, der sogenannte Moderator, die Validierung von Transaktionen übernimmt.

[13] *Popov*, The tangle.

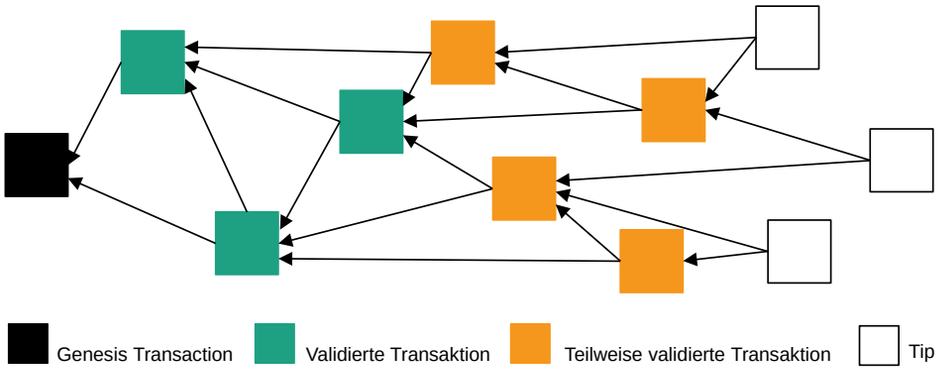


Abbildung 8: Darstellung des IOTA Tangles

4.3.9 Hedera Hashgraph

Hedera Hashgraph ist eine weitere DLT-Infrastruktur, die sich in ihrer Datenstruktur von einer Blockchain unterscheidet. Das durch den Hashgraph adressierte Ziele besteht darin, die Bandbreite der übertragenen Informationen so gering wie möglich zu halten und somit eine schnelle Verteilung der Informationen zu ermöglichen.[14] Das Prinzip des Hashgraphs basiert auf dem Prinzip des Gossips: Jeder Teilnehmer im Netzwerk wählt zufällig einen anderen Teilnehmer aus und erzählt diesem alles, was er über das Netzwerk weiß. Dabei werden nicht nur die Informationen über die getätigten Transaktionen verteilt, sondern der gesamte Hashgraph, also der Verlauf aller Gossip-Aktionen. Somit wird die Verteilung der Informationen im Hashgraph als „Gossip über Gossip" bezeichnet, der gesamte bisherige Verlauf des Gossips wird demzufolge im Rahmen von Gossip-Aktionen weitergegeben. Auf diese Art und Weise wird der Hashgraph immer weiter im Netzwerk verbreitet. Die Funktionsweise des Hashgraphs ist in Abbildung 9 dargestellt.

Ein weiteres wichtiges Prinzip in Bezug auf den Hashgraph ist das virtual voting, welches die Konsensfindung im Hashgraph darstellt: Dadurch, dass jeder Teilnehmer eine Kopie des Hashgraphs hat, kennt er das Wissen der anderen Teilnehmer und weiß demnach, wie diese bei einem Abstimmungsprozess abstimmen würden. Somit müssen keine tatsächlichen Stimmen abgegeben werden, wovon die Performanz des Hashgraph-Netzwerks erheblich profitiert.

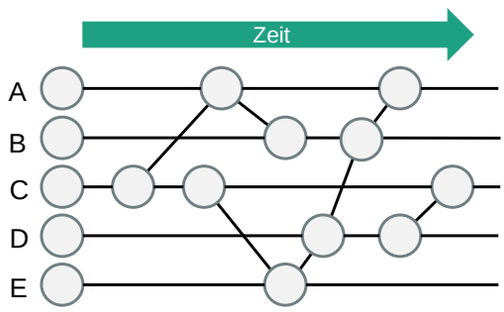


Abbildung 9: Darstellung des Hedera Hashgraphs. A, B, C, D und E sind Teilnehmer des Netzwerks. Jede Verbindung zwischen zwei Teilnehmern repräsentiert ein Gossip-Ereignis, in dem ein Teilnehmer einem anderen alle ihm vorliegenden Informationen weitergibt.

[14] *Baird/Mance/Madsen*, Hedera: A Governing Council & Public Hashgraph Network.

4.3.10 Übersicht über DLT-Infrastrukturen

Eine Übersicht über die in diesem Abschnitt vorgestellten DLT-Infrastrukturen befindet sich in Tabelle 1. Die verschiedenen Infrastrukturen werden aufgeteilt in allgemeine DLT und in Blockchain-Technologien, den Spezialfall der DLT. Zudem werden die Infrastrukturen hinsichtlich ihrer Zugriffsbeschränkungen verglichen und Besonderheiten aufgelistet.

	Zugriffsbeschränkungen	Besonderheiten
Bitcoin	Öffentlich, permissionless	Erste Blockchain
Ethereum	Öffentlich, permissionless	Geeignet für die Entwicklung von „massentauglichen“ DApps
Hyperledger Fabric	Privat, permissioned	Modularer Aufbau
R3 Corda	Privat, permissioned	Smart Contracts unterstützen juristische Prosa
Sovrin	Öffentlich, permissioned	Speziell für digitale Identitäten entwickelt
IOTA	Öffentlich, permissionless	Unterstützt Mikrozahlungen
Hedera Hashgraph	Privat, permissioned	Virtual Voting beschleunigt den Validierungsprozess

Tabelle 1: Übersicht über verschiedene DLT-Infrastrukturen

Neben den bereits genannten DLT-Infrastrukturen existieren noch zahlreiche weitere Beispiele. Hierbei handelt es sich sowohl um Blockchains, die alternative Kryptowährungen zur Verfügung stellen (sogenannte Altcoin-Blockchains wie Litecoin und Ripple) als auch solche, welche zusätzlich zu einer Kryptowährung auch die Implementierung von Smart Contracts unterstützen. Zudem sind Blockchains existent, die durch eine Abspaltung (Fork) von einer anderen Blockchain entstanden sind, wie bspw. Quorum, welche sich von Ethereum abgespaltet hat. Überdies wird daran gearbeitet, mit alternativen DLT-Infrastrukturen abseits der Blockchain-Technologie die Skalierbarkeit von verteilten Systemen zu verbessern.

4.4 Governance eines DLT-Netzwerks

DLT-Anwendungen erfordern entsprechende DLT-Netzwerke. Es gibt Anwendungen, die auf bestehenden öffentlich zugänglichen Blockchain-Netzwerken wie Bitcoin oder Ethereum implementiert werden können. Diese Anwendungen unterliegen dann den entsprechenden Regelungen des jeweiligen Systems, wie dem vorgegebenen Verfahren zur Konsensfindung oder den Transaktionskosten.

Besonders in industrienahen Anwendungen werden oftmals nichtöffentliche DLT-Netzwerke eingesetzt. In diesen Netzwerken ist es häufig eine entscheidende Frage, wer Partner im Netzwerk wird und welche Partner einen Knoten betreiben. Nachfolgend werden Gestaltungsprinzipen zur Bestimmung von Regeln zur Zusammenarbeit, der sogenannten Governance, diskutiert, die auch für die Anwendungsbeispiele im Mobilitätssektor relevant sind.

4.4.1 Blockchain-Netzwerk

Das Netzwerk einer öffentlichen Blockchain organisiert sich selbst: Die Blockchain ersetzt dabei eine zentrale Instanz, die normalerweise für die Steuerung und Kontrolle eines Netzwerks verantwortlich ist. Die Mitglieder des Netzwerks treffen mithilfe des Konsens-

mechanismus Entscheidungen, ohne eine solche zusätzliche Instanz zu benötigen.[15] Hierbei ist es wichtig, dass es für die Mitglieder des Netzwerks genügend Anreize gibt, sich an der Konsensfindung zu beteiligen. Erfolgt dies nicht, kann es leicht zu einer Dominanz von einigen wenigen Mitgliedern kommen, was dem Grundgedanken von Blockchain widerspricht und Manipulationen ermöglichen kann. Bei einer privaten, permissioned Blockchain ist das Netzwerk nicht komplett selbst organisiert. Daher gibt es dort in der Regel ein Gremium, das dafür verantwortlich ist, neue Mitglieder in das Netzwerk aufzunehmen, wieder zu entfernen und Zugriffsberechtigungen zu vergeben. Neben der Mitgliederverwaltung ist eine wichtige Aufgabe dieses Gremiums, das sowohl eine einzelne, vertrauenswürdige Drittpartei als auch ein Teil oder die Gesamtheit der Mitglieder bilden können, die Entscheidung über das Verfahren zur Konsensfindung. Da bei einer privaten oder konsortialen Blockchain häufig ein höherer Grad an Vertrauen zwischen den Netzwerkmitgliedern vorhanden ist als bei öffentlichen Blockchains, können hier effizientere Konsensmechanismen verwendet werden. Beispielsweise nimmt dann etwa nur eine geringe Anzahl von Akteuren aktiv an der Konsensfindung teil.

4.4.2 Technologische Governance

Neben der Organisation des Netzwerks muss auch auf die Weiterentwicklung der zugrunde liegenden Technologie geachtet werden.[16] Von besonderer Relevanz sind regelmäßige Sicherheitsupdates, welche die Sicherheit der Technologie aufrechterhalten. Besonders bei privaten oder konsortialen Blockchains gibt es dafür häufig ein Gremium, welches die Verantwortung für die technologische Weiterentwicklung übernimmt. Eine Alternative hierfür sind Open-Source-Blockchains wie Bitcoin, bei denen sich eine Gemeinschaft aus unabhängigen Programmierern bildet, die sich um die Weiterentwicklung der Infrastruktur kümmert.

4.4.3 Forks

In einer Blockchain hat normalerweise jeder Block genau einen Nachfolger. In manchen Situationen kann es jedoch zu einer „Fork", also einer Gabelung, kommen, sodass sich die Blockchain spaltet und ein Block mehrere Nachfolger hat. Ein Grund für eine solche Spaltung kann ein Software-Update sein.[17] In diesem Fall wird zwischen einer „Hard Fork" und einer „Soft Fork" unterschieden. Bei einer Hard Fork ist die neue Version der Blockchain nicht kompatibel mit der alten Version, sodass es ab diesem Zeitpunkt zwei Blockchains gibt: eine bestehend aus den Netzwerkknoten, die das Update übernommen haben, und eine weitere aus den Knoten, die das Update nicht übernommen haben. Dies ist in Abbildung 10 dargestellt. Bei einer Soft Fork ist die neue Software mit der alten kompatibel und auch Knoten, die das Update nicht übernehmen, bleiben weiterhin Teil der originalen Blockchain. Falls allerdings Knoten, die auf der alten Software laufen, Transaktionen hinzufügen, die nicht mit der neuen Software kompatibel sind, kann es auch hier zu einer Hard Fork kommen.

[15] *Osterland/Rose,* Proceedings of 1st ERCIM Blockchain 2018, 1.
[16] *Osterland/Rose,* Proceedings of 1st ERCIM Blockchain 2018, 1.
[17] *Lin/Liao,* International Journal of Network Securtiy 2017, 653.

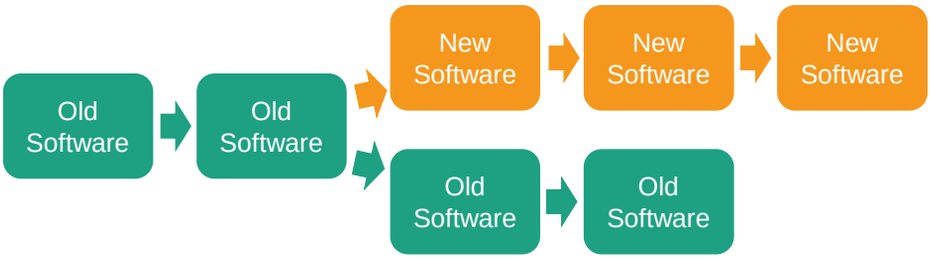


Abbildung 10: Eine „Hard Fork", die in einer Blockchain durch ein Software-Update hervorgerufen wurde

Ein weiterer Grund für eine Fork kann dann entstehen, wenn durch den Konsensmechanismus gleichzeitig mehrere Blöcke fertiggestellt werden, sodass auch hier verschiedene Versionen der Blockchain im Netzwerk vorliegen.[18] In diesem Falle reguliert sich die Blockchain jedoch selbst, da auf Dauer stets die jeweils längste Version der Blockchain übernommen wird und die Alternativen verworfen werden. Solche vorübergehenden Soft-Forks können durchaus häufiger vorkommen und sind der Hauptgrund, warum man in der Regel eine Transaktion in der Blockchain erst als unveränderbar betrachten sollte, wenn bereits eine genügend große Anzahl an Folgeblöcken ebenfalls in der Blockchain eingetragen sind. Bei der Bitcoin-Blockchain spricht man hier von etwa sechs Folgeblöcken, bis eine Transaktion als sicher gelten kann, da dann mit einer sehr hohen Wahrscheinlichkeit ausgeschlossen werden kann, dass die betrachtete Kette und damit der entsprechende Block durch eine alternative Kette mit einem anderen Block ersetzt wird.

4.5 Interoperabilität und Standardisierung

Wie bereits in Abschnitt 4.3 vorgestellt, gibt es viele verschiedene DLT- und Blockchain-Infrastrukturen. Mit der Zeit entwickelt sich auf diese Weise eine Ansammlung unterschiedlicher Systeme, die zwar grundsätzlich auf derselben Technologie basieren, allerdings nicht per se miteinander kommunizieren können. Zudem gibt es für die Entwicklung von DLT-Infrastrukturen momentan noch keine standardisierten Richtlinien. Um dem entgegenzuwirken, beschäftigen sich verschiedene Organisationen damit, Transaktionen zwischen verschiedenen Blockchains zu ermöglichen. Zudem befindet sich aktuell eine neuer ISO-Standard für Blockchains und DLT-Infrastrukturen in der Entwicklung, welcher die Standardisierung vorantreiben soll.

4.5.1 Blockchain-zu-Blockchain-Kommunikation

Unterschiedliche Blockchain- bzw. DLT-Anwendungen wie die Sicherung von Herkunftsnachweisen, Unterstützung von Platooning (siehe auch Kapitel 10) oder die Implementierung von Anwendungen im Supply-Chain-Bereich (siehe auch Kapitel 7) weisen verschiedene Anforderungen sowohl hinsichtlich der genutzten Technologie (Skalierbarkeit) als auch an die Governance des entsprechenden Netzwerks auf. Dahingehend ist zunächst eine Vielzahl von Blockchain-Netzwerken zu erwarten. Dennoch wird es Anwendungen geben, die auf Informationen in verschiedenen Blockchains zugreifen oder Transaktionen in verschiedenen Blockchains auslösen. Ebenso ist zu erwarten, dass Smart Contracts aus einer Blockchain Smart Contracts in anderen Blockchains z. B. als Orakel aufrufen oder diesen Anweisungen schicken. Beispiele für interoperable Blockchain-Netzwerke könnten sich in Machine-to-machine-Anwendungen ergeben.

Entsprechend müssen Standards auf der Daten- und Schnittstellen-Ebene definiert werden, damit Inhalte nicht spezifisch für eine Blockchain kodiert werden und anwendungsübergreifend genutzt werden können. Im Anwendungsfeld Herkunftsnachweise liegt mit

[18] *Natoli/Gramoli,* 2016 IEEE 15th International Symposium 2016, 310.

dem OpenBadges-Standard für digitale personenbezogene Zertifikate bereits eine entsprechende Lösung vor. Anwendungsschnittstellen, die Blockchain-Funktionen abstrakt umsetzen, ermöglichen eine Inter-Blockchain-Kommunikation. Derartige Standards für Daten und Schnittstellen sowie entsprechende Identitätsmanagement-Systeme bilden die Basis für ein Internet der Blockchains.

Da es für die momentan verfügbaren Blockchains keine einfache Möglichkeit gibt, vertrauensvoll untereinander zu kommunizieren, sind verschiedene Ansätze vorhanden, um eine Interoperabilität von Blockchain-Infrastrukturen zu ermöglichen.[19] Das Ziel ist hierbei ein „Internet der Blockchains", also eine Vernetzung aller Blockchains, so wie sich momentan Computer über das Internet miteinander vernetzen können. Durch eine so entstehende Blockchain-zu-Blockchain-Kommunikation könnte z. B. die Kombination von öffentlichen und privaten Blockchains ermöglicht werden, um Anwendungen mit besonderen Anforderungen umzusetzen. Die Blockchain Interoperability Alliance (BIA) ist ein Zusammenschluss von mehreren Initiativen, die ein solches Internet der Blockchains entwickeln möchten. Die BIA betreibt Forschung über Transaktionen und Kommunikation zwischen verschiedenen Blockchains und arbeitet an der Entwicklung eines globalen Industriestandards und einer Protokoll-Architektur für Blockchain-zu-Blockchain Netzwerke.

Eine konkrete Technologie zur Kommunikation zwischen Blockchains ist Blocknet. Blocknet ermöglicht Verbindungen, sogenannte XBridges, zwischen einzelnen Knoten unterschiedlicher Blockchains. Dies soll u. a. den Austausch verschiedener Kryptowährungen ohne die Notwendigkeit einer Tauschbörse sowie den Austausch von beliebigen anderen Daten oder Smart Contracts ermöglichen.

Eine weitere Technologie, die auf einer alternativen Herangehensweise basiert, ist Cosmos. Die von Cosmos entwickelte Idee basiert auf sogenannten „Zones" und „Hubs". Zones repräsentieren dabei einzelne, unabhängige Blockchains, während Hubs spezielle Blockchains sind, die mehrere Zones miteinander verbinden (vgl. dazu auch Abbildung 11). Über den Hub können die Blockchains dann Informationen austauschen, ohne dass jede Blockchain eine direkte Verbindung zu jeder anderen Blockchain benötigt, mit der sie kommunizieren will.

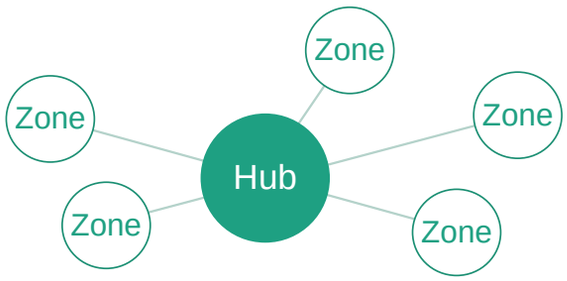


Abbildung 11: Darstellung der auf Cosmos basierten Blockchain-zu-Blockchain-Kommunikation basierend auf Hubs und Zones

Die Herausforderungen der Interoperabilität von Blockchains erstrecken sich auf mehrere Ebenen: Neben der rein technischen Ebene, die den Austausch von Token, also bspw. Kryptowährungen, und die Übertragbarkeit von Smart-Contract-Sprachen beinhaltet, muss auch auf die syntaktische , die organisatorische und die rechtliche Ebene geachtet werden. Während die syntaktische Ebene ein Blockchain-übergreifendes Identitätsmanagement und eine Interoperabilität von Smart Contracts inkludiert, geht es bei der organisatorischen Ebene um Governance-Aspekte und die Abbildung von Prozessen. Die

[19] *Underwood,* Communications of the ACM 2016, 15.

rechtliche Ebene dreht sich hingegen um die Wirksamkeit der zugrunde liegenden Vereinbarungen sowie gegebenenfalls die Frage, ob diese Vereinbarungen auf technischer Ebene jeweils korrekt umgesetzt wurden.

4.5.2 ISO-Normen zur Standardisierung

Um einen standardisierten Umgang mit Blockchain- und weiteren DLT-Infrastrukturen zu ermöglichen, werden von der Internationalen Organisation für Standardisierung (ISO) momentan 11 Normen entwickelt. Beispielsweise wird die ISO/TC307-Norm u. a. Anwendungsfälle von DLT behandeln, technologische Grundlagen beleuchten, Standards für Sicherheit, Privatsphäre und Identität setzen sowie sich mit Smart Contracts und deren Anwendungen befassen. Zudem werden in der Norm auch die Interoperabilität von Blockchain-Technologien und DLT- sowie Governance-Aspekte behandelt.

4.5.3 Sidechains

Eine etwas vereinfachte Möglichkeit, zwischen Blockchains zu kommunizieren, sind Sidechains. Eine Sidechain ist eine Blockchain, die mit einer anderen Blockchain, der „Hauptchain" verbunden ist, wobei eine Hauptchain über mehrere Sidechains verfügen kann. Token einer Kryptowährung können von der Hauptchain auf eine Sidechain übertragen und dort genutzt werden, später aber auch wieder zurück auf die Hauptchain übertragen werden. Ein großer Vorteil von Sidechains besteht darin, dass mit ihnen eine höhere Skalierbarkeit ermöglicht werden kann: Indem Transaktionen der Hauptchain auf den Sidechains abgewickelt werden können, erhöht sich der Transaktionsdurchsatz der Hauptchain.

4.6 Trends

Als Grundlagentechnologie ist Blockchain relativ jung und hat sich seit der Implementierung von Bitcoin dynamisch weiterentwickelt. Insbesondere sind neue Blockchain-Plattformen entstanden, die universell einsetzbar sind, besonders auf betriebliche Anwendungen zugeschnitten sind oder alternative, nicht auf linear verketteten Blöcken basierende Datenstrukturen nutzen, um Transaktionen effizient und sicher zu verwalten. Nachfolgend werden weitere Trends vorgestellt.

4.6.1 Zertifizierung

Smart Contracts sind transparent und unveränderbar in der Blockchain gespeichert und tragen wesentlich zum Vertrauen in die Blockchain bei. Sie unterstützen die Automatisierung von Prozessen und sind zentral für die Implementierung von Kooperationslogiken zwischen Geschäftspartnern.

Die Erstellung und Prüfung von Smart Contracts auf Korrektheit wird durch Geschäftspartner nicht immer geleistet werden können, die jedoch von der Einbindung in Blockchain-Netzwerke wesentlich profitieren. Infolgedessen ist es wünschenswert, dass Bibliotheken mit geprüften korrekten Smart Contracts entstehen. Diese Bibliotheken werden neben generischen allgemein verwendbaren Smart Contracts auch anwendungsspezifische Smart Contracts enthalten. Ein diskutierter Ansatz sind Zertifizierungsstellen für Smart Contracts. Diese führen jedoch in gewisser Weise zu „Kompromisslösungen", da sie selbst zentrale Instanzen darstellen.

Gegenwärtige Smart Contracts sind nur von IT-Spezialisten lesbar. Es ist wünschenswert, dass Laien ebenso Smart Contracts lesen und verstehen könnten. Demzufolge werden derzeit in der Forschung Modelle entwickelt, die Smart Contracts einerseits für Laien

lesbar machen[20] oder die die halbautomatische Übersetzung von Vertragstexten in entsprechende Smart Contracts unterstützen.[21]

Technisch scheint die Rechtssicherheit über Frameworks und eine damit einhergehende Eingrenzung der Gestaltungsmöglichkeiten umsetzbar, wobei sogenannte Ricardian Contracts seitens des Rechtsgebers Rechtssicherheit erlauben würden. Bei der Rechtsformulierung müsste bereits darauf geachtet werden, dass die Regeln in Software übersetz- und durch Software ausführbar sind. Realistischer erscheint, dass lediglich agile (und damit temporäre) Gesetzgebung, Vertragswerke oder von zentralen Prüfstellen verlangte Regelwerke das Konzept der Ricardian Contracts berücksichtigen.

4.6.2 Quantencomputing und Blockchain

Die Sicherheit von Blockchain- und DLT-Infrastrukturen beruht auf Algorithmen zur Verschlüsselung von Daten und auf kryptografischen Verfahren wie Einweg-Hashfunktionen. Bislang kann lediglich mit sehr hohen Rechenleistungen die Sicherheit von Blockchain- oder DLT-Infrastrukturen angegriffen werden. Allerdings muss man neben der stetigen Zunahme konventioneller Rechenleistung ebenfalls die Möglichkeit bzw. Realität neuartiger technologischer Entwicklungen, z. B. von Quantencomputern, in Betracht ziehen. Mit dem Durchbruch des Quantencomputings stünde möglicherweise eine Rechenleistung zur Verfügung, die ausreicht, um gängige kryptografische Verfahren wie Hashfunktionen, asymmetrische Verschlüsselung (PKI) und symmetrische Verschlüsselung, auf denen Blockchain bzw. DLT beruhen, stellenweise unsicher werden zu lassen. Dies wirkt sich indes auf nahezu alle digitalen Services gleichermaßen aus, da bspw. auch digitale Signaturen sowohl auf asymmetrischer Verschlüsselung als auch auf Hashfunktionen beruhen. Nach aktueller Prognose werden Quantencomputer mit einer entsprechenden Rechenleistung allerdings frühestens in den nächsten 5-10 Jahren zur Verfügung stehen. Weiter ist anzunehmen, dass sichere Alternativen für die aktuellen kryptografischen Verfahren gefunden werden. Beispielsweise ist im Falle kontinuierlich wachsender konventioneller Rechenleistung ein ebenfalls kontinuierliches Anpassen des Schwierigkeitsgrads des kryptografischen Rätsels oder eine entsprechende Skalierung der Länge von öffentlichen bzw. privaten Schlüsseln oder der Länge von Hashwerten denkbar. Gleichzeitig wird daran gearbeitet, entsprechende kryptografische Methoden zu entwickeln, die ebenfalls gegenüber Quantencomputern sicher sind. Das entsprechende Forschungsfeld in der Kryptografie wird als post-quanten-Kryptografie bezeichnet.[22] Im Übrigen sind für den Fall, dass die gegenwärtig verwendete Kryptografie unsicher wird und keine entsprechenden neuen Verfahren gefunden werden, nicht nur die DLT, sondern jeglicher Wertetransfer über das Internet hinfällig, sodass die DLT nicht in besonderer Weise durch Quantencomputer gefährdet ist. Der Unterschied zwischen herkömmlichen Systemen und der Blockchain, die ja durch Software-Updates stets an den aktuellen Stand der Technik angepasst werden kann, besteht lediglich darin, dass bei unveränderlichen, sprich bereits gespeicherten Daten, eine nachträgliche Änderung nicht möglich ist. Auf diesen wichtigen Unterschied und dessen Implikationen vor allem im Bereich des Datenschutzes wird in Kapitel 5.3.2.3 vertiefend eingegangen.

4.6.3 Identifikation von DLT-geeigneten Geschäftsprozessen

Die Grundlagentechnologie DLT eröffnet eine Vielzahl von Anwendungsmöglichkeiten (siehe dazu auch Kapitel 5.2.5). Indes bleibt für Praktiker häufig unklar, welche ihrer

[20] *Hazard/Haapio,* Proceedings of the 20th International Legal Informatics Symposium IRIS 2017, 425.
[21] *Frantz/Nowostawski,* IEEE 1st International Workshops on Foundations and Applications on Self* Systems 2016, 210.
[22] *Bernstein/Buchmann, J. (Hrsg.), Dahmen E. (*Hrsg.), Post-Quantum Cryptography 2009, 1.

Geschäftsprozesse von der Blockchain- bzw. DLT-Technologie profitieren könnten. Erste Rahmenwerke sind diesbezüglich bereits entwickelt worden. In dem wissenschaftlichen Artikel[23] sind Rahmenwerke vergleichend dargestellt. Dabei wird ein zweistufiges Rahmenwerk vorgestellt. Dieses hilft Praktikern, Geschäftsprozesse auszuwählen, die Charakteristiken der DLT-Implementierung festzulegen und die Vorteile abzuschätzen. Ein technisches Rahmenwerk, das die Kooperation verschiedener Partner berücksichtigt, Leistungsanreize aufzeigt und die Plattformauswahl unterstützt, ist in (Osterland, 2018) dargestellt.

[23] *Klein/Prinz/Gräther,* Reports of the European Society for Socially Embedded Technologies 2018, 1.

5 Gesellschaftlich-ökonomische Grundlagen

Digitale Produkte und Dienstleistungen verändern den Alltag von Einzelpersonen, Unternehmen und die Gesellschaft im Allgemeinen. Die Auswirkungen der Digitalisierung werden immer deutlicher und zwingen Organisationen auf der ganzen Welt, auf sich ändernde Geschäftsregeln und -modelle zu reagieren. Heute haben mehr Menschen Zugang zu Mobiltelefonen als zu Toiletten[24] und mindestens jeder fünfte Mensch auf der Welt besitzt ein aktiv genutztes Facebook-Konto[25]. Die Digitalisierung verändert etablierte Geschäftsregeln sowohl in der digitalen als auch in der physischen Welt und wirkt sich auf alle Lebensbereiche aus. Zu den jüngsten Beispielen gehören bspw. Uber, das größte Taxiunternehmen der Welt, das gleichzeitig keine eigenen Fahrzeuge besitzt; YouTube, der vermeintlich weltweit beliebteste Medienbereitsteller, der jedoch selbst keine Inhalte erstellt; Alibaba, der wertvollste Einzelhändler der Welt, der dabei über keine eigenen Lager verfügt; Airbnb, der weltweit größte Anbieter von Unterkünften, der keine Immobilien besitzt. DLT sind eine weitere Art digitaler Technologien, welche den Wandel, die Chancen und auch die Risiken, die mit der Digitalisierung für Gesellschaft und Wirtschaft einhergehen, nicht bremsen, sondern vielmehr beschleunigen und verstärken. Aus diesem Grund sollen diese Technologien zunächst in den Kontext der Digitalisierung eingeordnet werden, bevor ihr Potenzial und ihre Perspektiven der Umsetzung bzw. der Innovationsdiffusion untersucht werden.

5.1 Einordnung der DLT in die Digitalisierung

DLT wird von vielen als Basisinnovation eingestuft[26]. Die (Weiter-)Entwicklung ihrer Bestandteile (z. B. Konsensmechanismen) macht die DLT für viele grundlegende Anwendungsfälle einsetzbar. Um viele anvisierte und perspektivische Anwendungsfälle jedoch tatsächlich umsetzen zu können, ist die Kombination verschiedener emergenter, digitaler Technologien notwendig. Im Folgenden werden drei Schlüsseltechnologien, die starke Synergien mit DLT aufweisen, vorgestellt: Das Internet der Dinge (IoT), Künstliche Intelligenz (KI) und Methoden des Privacy-Preserving Computings.

Integrierte Betrachtung der Blockchain-Technologie

Das Internet ist ein globales (digitales Informations- und Kommunikations-) Netzwerk bestehend aus Netzwerken, während das Web, formal auch als World Wide Web (www) bezeichnet, eine Sammlung von Informationen ist. Auf diese Informationen kann mithilfe technischer Artefakte wie Browsern zugegriffen werden. Das Internet ist also eine grundlegende Infrastruktur, während das Web eine Anwendung auf dieser Infrastruktur darstellt. Analog ist die DLT (die selbst wiederum auf dem Internet beruht) eine Infrastrukturtechnologie, auf der verschiedene Anwendungen umgesetzt werden können. Für diese Anwendungen wird die DLT oftmals mit anderen Technologien kombiniert verwendet, weshalb eine integrierte Betrachtung der Technologie im Rahmen einer größeren Technologielandschaft notwendig ist.

[24] *UN News*, World Book Day: new UN report spotlights potential of mobile technology to advance literacy.
[25] *Thomas Halleck*, Facebook: One Out Of Every Five People On Earth Have An Active Account.
[26] *Klein/Kottbauer*, Strategien erfolgreich entwickeln und umsetzen.

5.1.1 DLT und das Internet der Dinge

5.1.1.1 Das Internet der Dinge verändert Wirtschaft und Gesellschaft

Die Digitalisierung fordert von Unternehmen, ihre bestehenden Geschäfts- und Betriebsmodelle vor dem Hintergrund digitaler Technologien fundamental zu überdenken[27]. Digitale Technologien sind dabei zunehmend schneller und immer günstiger auf dem Markt verfügbar. Eine digitale Technologie, der über verschiedene Anwendungsbereiche hinweg sehr großes Potenzial zugesprochen wird, ist das Internet der Dinge (IoT). Im IoT werden physische Objekte mit Sensoren, Aktuatoren[28] und Rechenleistung ausgestattet sowie mit dem Internet verknüpft. Die dadurch entstehenden Smart Things[29] werden zunehmend selbstständig und tragen zu einer Verschmelzung der digitalen und physischen Welt bei. Gleichzeitig ermöglichen derartige Smart Things völlig neuartige Interaktionen zwischen Unternehmen, Dingen und Individuen sowie innovative Geschäftsmodelle auf Basis neu verfügbarer Daten und zunehmender Vernetzung.[30] Schätzungen zufolge sollen im Jahr 2020 über 50 Milliarden Smart Things mit dem Internet und damit untereinander verbunden sein, was mit einem Wertschöpfungspotenzial von 8 Billionen US-Dollar einhergeht.[31] Bereits heute finden sich vielseitige Beispiele für das Internet der Dinge in unterschiedlichen Anwendungsbereichen wie Smart Home, Smart Mobility oder Smart Factory.[32] So ermöglicht ein smartes Thermostat, von unterwegs die Raumtemperatur zu Hause zu steuern. Zudem kann sich ein entsprechendes Thermostat selbstlernend an den Tagesrhythmus der Hausbewohner anpassen, um Energie zu sparen. Sämtliche Aktivitäten dieser intelligenten Geräte sowie alle Informationen über die erfasste Umwelt liegen in Form maschinenlesbarer Daten vor. Diese Daten werden wiederum zunehmend Einzug in private und wirtschaftliche Abläufe finden. Smart Things und die von ihnen generierten bzw. gesammelten Daten werden unterschiedlichen Akteuren gehören. Das Vorhandensein dieser Daten bzw. das Interesse, diese Daten als Ressource in Prozessen einzusetzen, wird also zunehmend bedingen, dass Daten und damit Eigentum unterschiedlicher Akteure zusammengeführt werden sollen. Nicht in allen Fällen ist davon auszugehen, dass diese Akteure sich untereinander Vertrauen schenken – umso weniger, je größer die vermuteten Werte hinter den Informationen sind, die durch die Daten repräsentiert werden.

Smart Things bilden die Grundlage des Internets der Dinge. Um dies zu veranschaulichen, fokussieren wir das Beispiel einer Landmaschine.[33] Dessen traditionelle Funktion, wie z. B. das Pflügen eines Felds, hat sich längst weiterentwickelt. So kann die Landmaschine lokale Wetter- oder Boden- sowie Maschinendaten an Hersteller oder Landwirte senden, welche diese anschließend (teil-)automatisiert analysieren, auswerten und daraus Handlungen ableiten. Daraus ergeben sich neue Möglichkeiten, wie im Bereich der vorausschauenden Instandhaltung (Predictive Maintenance).[34] So lässt sich bspw. der Verschleiß stark beanspruchter Maschinenkomponenten besser antizipieren und Ausfallzeit reduzieren sowie der Nutzungsgrad bzw. die Produktivität steigern. Auch Leistungskennzah-

[27] *Porter/Heppelmann,* Harvard business review 2014, 1.

[28] Aktuatoren (auch: Aktoren) sind Bauteile, die (i. d. R. vom Steuerungseinheiten ausgegebene) elektrische Signale in Veränderungen physikalischer Größen, wie etwa mechanischer Bewegung oder Temperatur, umsetzen und damit die aktive Steuerung von Prozessen ermöglichen.

[29] Dt. intelligente Geräte.

[30] *Oberländer/Röglinger/Rosemann/Kees,* European Journal of Information Systems 2018, 486.

[31] *Macaulay/Buckalew/Chung*, Internet of Things in Logistics..

[32] *Borgia,* Computer Communications 2014, 1.

[33] *Porter/Heppelmann,* Harvard business review 2014, 1.

[34] Dt. „vorausschauende Instandhaltung".

len wie die Tagesproduktivität lassen sich auf dieser Basis ermitteln. Im vorliegenden Beispiel werden Daten nicht nur durch die Maschine versendet. Vielmehr kann die Landmaschine ebenfalls über das Internet gesteuert werden, bis hin zur synchronen Koordinierung und Steuerung mehrerer Landmaschinen. Zudem kann die Landmaschine Daten anderer Maschinen, Landwirtschaftsbetriebe und Unternehmen nutzen. Durch die Vernetzung mit Landwirtschafts- und Wettersystemen kann die Landmaschine auf neue, sich extern potenziell weiterentwickelnde Funktionen zurückgreifen (z. B. Wetterprognose) und ihren Einsatz selbstständig optimieren. Wo bisher die Grenzen einer Branche galten, werden sich in Zukunft vernetzte smarte Systeme zu sogenannten „Systems of Systems" verknüpfen.[35]

5.1.1.2 Das Internet der Dinge erfordert eine integrierte Technologiearchitektur

Auch wenn sich der Mehrwert des IoT erst an der Kundenschnittstelle oder durch den Einsatz von Smart Things in betrieblichen Prozessen manifestiert, müssen Unternehmen zunächst intern die technologischen Voraussetzungen dafür schaffen. In diesem Zusammenhang werden diverse Technologiearchitekturen diskutiert, die allesamt ähnliche Ebenen aufweisen.

Alle Architekturen betrachten dabei das physische Objekt, das mit Sensoren, Aktuatoren und Rechenleistung ausgerüstet ist, als Fundament auf einer sogenannten „Thing-Ebene". Auf Basis ihrer Anbindung an das Internet können Smart Things auf einer weiteren Ebene mit verschiedenen Akteuren aus ihrer Umwelt interagieren – bspw. mit Individuen, Unternehmen oder anderen Smart Things. Eine wesentliche Eigenschaft von Smart Things ist die potenzielle Integrationsfähigkeit von Daten aus unterschiedlichen Quellen sowie deren Verarbeitung auf Basis Web-basierter und damit interoperabler Standards. Die gewonnenen Daten werden etwa genutzt, um innovative Services zu kreieren. Da sich der Innovationscharakter von Smart Things insbesondere durch kombinierbare (Informations-)Services ausdrückt, findet man so als oberste Ebene von Technologiearchitekturen üblicherweise eine Service-Ebene.

5.1.1.3 Das Internet der Dinge ist Grundlage für den Einsatz der DLT in der physischen Welt

DLT sind prädestiniert, um die Schnittstellen zwischen der Thing-, Interaktions-, Daten- und Service-Ebene der Endgeräte im Internet der Dinge sicherer zu gestalten. Dies lässt sich am zuvor aufgezeigten Beispiel des Smart Homes sehr gut darstellen und auf den Einsatz im industriellen Internet der Dinge übertragen. Neben diversen Vorteilen birgt das IoT allerdings u. a. auch diverse Risiken, die es zu lösen gilt. Unter den zehn größten Sicherheitsrisiken im Kontext des IoT finden sich bspw. der Identitätsdiebstahl, die Installation von Schadsoftware auf den entsprechenden Geräten, die Änderung von (System-)Informationen, der Diebstahl oder die Manipulation von Log-Daten, sowie der Diebstahl privater Informationen.[36] DLT können diese Sicherheitsrisiken durch ihre inhärente Manipulationssicherheit, Redundanz und Ausfallsicherheit oftmals deutlich reduzieren.

Das Risiko eines erfolgreichen Identitätsdiebstahls kann bspw. durch den Einsatz von Zero-Knowledge-Proofs (siehe Kapitel 5.1.3) reduziert werden. Des Weiteren kann die Installation von Schadsoftware erschwert werden, indem man unter Einsatz der DLT sicherstellt, dass lediglich autorisierte Endgeräte Kontakt mit dem System aufnehmen können. Insbesondere die Änderung von Systeminformationen fällt ungleich schwerer, wenn diese auf unterschiedlichen physischen und virtuellen Systemen mittels einer DLT-Schicht verteilt sind. Hinzu kommt, dass auch die Manipulation angemessen dezentralisierter

[35] *Porter/Heppelmann,* Harvard business review 2014, 1.
[36] *Ali/Awad,* Sensors (Basel, Switzerland) 2018, 1.

Log-Daten nach aktuellem Stand der Technik und Forschung in diesem Szenario nur unter außerordentlich hohen Kosten möglich ist. Diese Punkte sind auch im industriellen Rahmen gegeben und können, ebenso wie die Sicherheitsrisiken im privaten Kontext (z. B. Smart Home), auch unter Zuhilfenahme der DLT adressiert werden.

Sofern die zuvor beschriebenen Risiken soweit gesenkt werden, dass das Internet der Dinge sowohl im privaten als auch im geschäftlichen Kontext sicher genug für einen produktiven Einsatz ist, kann das IoT wiederum die Grundlage für den Einsatz der DLT in der physischen Welt bieten. Im Zuge dessen kann die DLT den Übergang zwischen Maschine/Mensch und einer allgegenwärtigen Service-Ebene abbilden. Dabei steht insbesondere die Möglichkeit, durch einen Einsatz der DLT die Vertrauenswürdigkeit der im IoT generierten Daten zu erhöhen, im Vordergrund.

Während DLT derzeit insbesondere für die Umsetzung von Kryptowährungen und Kapitalmarktgeschäften eingesetzt werden, ist bereits jetzt absehbar, dass die Technologie gleichfalls als Befähiger für das Internet der Dinge agieren kann und wird. Dies ist der Fall, da die DLT die im vorangegangenen Abschnitt dargelegten Sicherheitsrisiken der Machine-to-Machine-Kommunikation im IoT deutlich reduzieren kann. Daher ist ein breitgestreuter Einsatz der DLT in dieser Umgebung äußerst wahrscheinlich. In Kombination mit den derzeit drastisch sinkenden Kosten für IoT-Endgeräte könnten diese zudem der erste „echte" Kontakt des Großteils der Bevölkerung mit DLT sein. Sollte der Technologie infolgedessen ein erfolgreicher Einstieg in den Markt gelingen, so stellt sie in Zukunft einen zentralen Aspekt des täglichen Lebens vieler Menschen dar. Mit der hohen Reichweite, die durch die Kombination der DLT mit dem Internet der Dinge erreicht werden kann, steigt also auch die Relevanz der DLT. Die Kernaufgabe bzw. -funktion von DLT ist in diesem Kontext, Vertrauen bei der Interaktion von Smart Things mit Individuen, Akteuren und anderen Smart Things, die sich vor Interaktionsbeginn in der Regel nicht kennen, zu schaffen. Theoretisch können das IoT ohne DLT und DLT ohne das IoT eingesetzt werden. Dennoch scheinen beide Technologiebündel insgesamt sehr synergetisch.

5.1.2 DLT und Künstliche Intelligenz

5.1.2.1 Die Zukunftstechnologien DLT und KI nähern sich zukünftig an

Künstliche Intelligenz (KI) entwickelt sich zunehmend zu einem wichtigen Treiber der Digitalisierung. KI ist dabei ein Überbegriff für die Simulation menschlicher Intelligenz durch Maschinen und umfasst u. a. Fähigkeiten wie Denken, Lernen und Selbstkorrektur.[37] Dabei wird zwischen zwei Arten von KI unterschieden: Eine „starke" KI bezeichnet ein System, das die intellektuellen Fähigkeiten eines Menschen besitzt oder diese sogar übertrifft. Für die Lösung von Anwendungsproblemen ist dagegen die „schwache" KI (zunächst) wichtiger. Zur Konstruktion dieser Systeme werden nicht nur Methoden der Mathematik und Informatik genutzt, es werden gezielt Aspekte menschlicher Intelligenz nachgebildet. Derartige Systeme können vielfältige Aufgaben erfüllen und finden schon heute in einer Vielzahl von Bereichen Anwendung. Beispiele sind in der Umsetzung autonomer Fahrzeuge oder der Persönlichkeitserkennung zu finden.

Sowohl Deutschland als auch die EU haben die Bedeutung der Künstlichen Intelligenz für Industrie und Gesellschaft erkannt und entsprechend jeweils eine KI-Strategie erarbeitet. Im Rahmen der KI-Strategie der EU wurden durch eine entsprechende Expertengruppe im April 2019 sieben Voraussetzungen für eine „vertrauenswürdige KI" formuliert.[38] Zu diesen zählen u. a. die Punkte „Privatsphäre und Datenqualitätsmanagement",

[37] *Bitkom*, Künstliche Intelligenz.

[38] *Europäische Kommission*, Künstliche Intelligenz: Kommission treibt Arbeit an Ethikleitlinien weiter voran.

„Transparenz“ und „Rechenschaftspflicht“. Damit werden klar Bezüge zu Zielen und Potenzialen der DLT in Verbindung mit KI hergestellt und eine Steigerung des hohen Potenzials der KI in Verbindung mit DLT suggeriert. Allgemein kann DLT durch die Schaffung von Vertrauen zwischen zuvor unbekannten Teilnehmern die Einsatzmöglichkeiten von KI steigern. Aber auch KI wird in vielen Bereichen einen direkten Einfluss auf die Entwicklung der DLT haben. Durch die komplementären Eigenschaften von DLT und KI ist zu erwarten, dass die Schnittmenge dieser beiden revolutionären Technologien in Zukunft stetig wachsen wird. Diese soll im Folgenden an Beispielen skizziert werden. Dabei werden auch die Bezüge zu den Voraussetzungen für eine „vertrauenswürdige KI“ deutlich.

5.1.2.2 DLT als Datenbasis für KI

In der Anwendung von KI haben Daten eine zentrale Bedeutung. Die Verfügbarkeit von Daten ist in allen KI-bezogenen Anwendungsfällen ein wesentlicher Faktor (bspw. zur Erkennung von Mustern in den Daten, aus denen sich kontextuelle Schlüsse ziehen lassen). Bei der Nutzung von Daten durch KI entsteht oftmals ein wirtschaftlicher Mehrwert. Für Privatpersonen und Unternehmen besteht allerdings gleichzeitig der Wunsch nach Datensouveränität, d. h. der Kontrolle über die Datennutzung oder zumindest einer entsprechenden finanziellen oder anderweitigen Vergütung. Mithilfe der DLT existiert nun eine technische Möglichkeit, Daten in der Hoheit der Privatpersonen oder Unternehmen zu belassen und den Zugriff nur selektiv durch vorherige Einwilligung zu gewähren, ohne dabei einem Akteur die Berechtigung einzuräumen, diese Rechte zu setzen, zu verändern und aufzuheben.

Ein Beispiel zur Veranschaulichung lässt sich wiederum aus dem Bereich des Smart Homes ziehen. Eine Privatperson erzeugt in ihrem Haushalt (Smart Home bzw. Smart City) Daten. Diese Daten sind offensichtlich personenbezogen[39] (Stromverbrauch, Onlineshopping-Verhalten, Fernsehgewohnheiten), daher soll ein ungefilterter Zugriff von Dritten, etwa Unternehmen, nicht ohne Einwilligung möglich sein. Andererseits könnte die Privatperson beim nächsten Onlineeinkauf entscheiden, gegen einen Rabatt den temporären Zugriff auf die in den letzten drei Monaten erzeugten Nutzungsdaten des Fernsehers zu erlauben, bspw. damit ein Unternehmen diese für Zwecke der KI-basierten Datenanalyse verwenden darf. Die DLT kann dabei unterstützen, diesen Zugriff verschiedenen Unternehmen selektiv zu gewähren und zu protokollieren, sodass die Wirtschaft weiter von den Daten profitieren und ihre Produkte verbessern kann. Außerdem kann die DLT genutzt werden, um die Herkunft von Datensätzen und unter verschiedenen Bedingungen ihre Integrität zu beweisen[40].

5.1.2.3 DLT als Protokollierungsplattform für KI

Wenn Maschinen mit Menschen oder anderen Maschinen interagieren, werden auch zukünftig Fehler in Protokollen vorkommen. Im integrativen Zusammenspiel zwischen Akteuren besteht, wie bereits dargestellt, die Notwendigkeit einer Infrastruktur des Vertrauens. Dies resultiert daraus, dass in Schadensfällen[41] geklärt werden sollte bzw. muss, wer welche Verantwortung trägt. Sollte das Risiko (zu) hoch eingeschätzt werden, dass entsprechende Fälle eintreten und nicht aufgeklärt werden können, werden Akteure wenig Interesse an einer Kollaboration zeigen. Dazu sollte es insbesondere intelligenten, zunehmend autonom(er) agierenden Akteuren (Künstlichen Intelligenzen) nur schwer möglich bzw. im besten Fall unmöglich sein, Daten für berechtigte Stakeholder unbe-

[39] Für die rechtliche Definition personenbezogener Daten siehe auch Kapitel 6.2.2.

[40] Eine beispielhafte Anwendung bietet das Unternehmen Ocean Protocol (https://oceanprotocol.com/).

[41] Ein Schadensfall kann zunächst auch ein Verdachtsfall sein, indem ein Akteur die Frage aufwirft, ob ein Ablauf im Einklang mit geltenden Regeln und Recht ablief.

merkt zu re-interpretieren oder gar rückwirkend anzupassen. Gleichzeitig sind KI-Verfahren häufig dadurch gekennzeichnet, dass ihre Entscheidungen durch Menschen nicht mehr nachzuvollziehen sind. Durch DLT wird es möglich, Aktivitäten und Entscheidungen von KI zu protokollieren. Die Eigenschaften von DLT machen diese Einträge dabei im Nachhinein manipulationssicher und transparent, sodass im Falle von Unfällen, Betrug oder anderen Fehlern die Aufklärung auf Basis unabhängiger Informationsquellen geschehen kann. So können anhand des Protokolls im Nachhinein auffällige Handlungen oder Vorkommnisse untersucht werden.

Ein Beispiel zur Veranschaulichung ist dem Bereich des autonomen Fahrens zu entnehmen. Zwei autonome Fahrzeuge verursachen einen Unfall mit erheblichem Schaden. Um den Unfallhergang und damit die Schuldfrage zu klären, ist die Untersuchung der protokollierten Daten und daraus abgeleiteter Aktionen beider Fahrzeuge notwendig. Über die DLT wird sichergestellt, dass diese Daten im Nachhinein nicht mehr verändert werden können. So kann beweissicher protokolliert werden, dass ein Fahrzeug zwar bspw. eine Warnung verschickt, das andere Fahrzeug diese aber nie empfangen hat und sie demnach auch nicht verarbeiten konnte. Die Untersuchung zum Unfallhergang kann sich somit auf die Unterbrechung der Kommunikation – bspw. durch externe Störquellen – konzentrieren und die KI ist vom Verdacht befreit. Eine Grundvoraussetzung ist in diesem Fall jedoch, dass die Daten oder Referenzen dazu regelmäßig in eine geeignete DLT-Infrastruktur geschrieben werden.

5.1.3 DLT und Methoden des Privacy-Preserving Computing

Die bislang erfolgreichsten DLT-Systeme wie Ethereum und IOTA sind öffentliche DLT-Lösungen. Um ihr volles Potenzial zu entfalten, dürfte die Privatheit von Informationen nicht nur für personenbezogene, sondern allgemein schützenwerte Daten entsprechend bedeutsam sein. Es bliebe sonst fraglich, ob Unternehmen mit einer öffentlichen DLT-Lösung arbeiten würden, wenn aus ihrer Sicht schützenwerte Daten öffentlich und transparent sind. Andernfalls besteht die sehr reale Gefahr, dass Wettbewerber vertrauliche Informationen in Erfahrung bringen und für eigene Zwecke einsetzen. Aufgrund der Transparenz von Daten in DLT-Systemen ist also eine Art komplementäre Technologie, welche bei Bedarf auch Privatheit von Daten in DLT-basierten Systemen technisch ermöglicht und unterstützt, erstrebenswert. Oft wird etwa gefordert, dass lediglich „Beweise" auf der Blockchain abgespeichert werden, alle anderen Daten jedoch auf anderen, privaten Datenbanken („off-Chain"). Dies gilt umso mehr für öffentliche Blockchains. In diesem Kontext werden die Methoden des sogenannten Privacy-Preserving Computings diskutiert. In der Tat liegen Ansätze für solche auf Kryptografie basierenden Technologien bereits seit den späten 1970er-Jahren vor. Sie existieren zwar auch unabhängig von der DLT, werden jedoch im Rahmen der Basisinnovation besonders interessant und können selbst Entwicklungssprünge erfahren und diese in andere Anwendungsfelder transferieren. Entsprechend hat sich die Forschung in diesem Bereich in den letzten Jahren stark beschleunigt und fokussiert. So befruchten sich die Technologien DLT und Privacy-Preserving Computing gegenseitig.

Diese Methoden des Privacy-Preserving Computing sind insofern aufbauend, als dass sie zu praktisch jeder DLT-Lösung im Sinne einer weiteren Schicht hinzugefügt werden können; analog wie DLT eine Schicht oberhalb des Internets darstellt. Relevante Verfahren bzw. Klassen an Verfahren sind sogenannte Zero-Knowledge-Proofs, die wiederum ein Spezialfall der Methoden der Secure-Multiparty-Computation sind. Diese sollen im Folgenden skizziert werden, um die Relevanz der (Ko-)Entwicklung mit DLT-Lösungen zu demonstrieren.

Secure Multiparty Computation (SMC)-Protokolle sind eine Klasse von Algorithmen, die einer Gruppe von sich gegenseitig nicht trauenden Akteuren erlauben, Funktionen (Be-

rechnungsvorschriften) auszuwerten, ohne dabei ihre privaten Inputs offenbaren zu müssen. Das bekannteste Beispiel ist das sogenannte „Millionaire's Problem": Zwei Akteure wollen ermitteln, wer von ihnen der Reichere ist (Auswertung der „Größer-Funktion"), ohne dabei ihr Vermögen (Input) zu verraten. Dieses Problem wurde zuerst durch Yao's Algorithmus gelöst. Dieser Algorithmus wurde bereits in 1970er-Jahren und damit zeitlich erheblich vor der Konzeptionierung der ersten DLT-Anwendung vorgestellt. Yao's Algorithmus und darauf aufbauende Algorithmen stellen eine bedeutende Grundlage für sowohl öffentliche als auch private DLT-Lösungen dar, um Berechnungen zweier oder mehrerer Parteien zu verifizieren, ohne dass diese ihre privaten Daten auf die DLT-Schicht legen zu müssen. Ein anschauliches Beispiel, wie man sich ein SMC-Protokoll vorstellen kann, bietet die sichere, verteilte Addition[42]. Wenn drei Personen A, B und C die jeweils privaten Zahlen a, b und c besitzen und diese addieren wollen, ohne dass irgendein Beteiligter die private Zahl einer weiteren Person erfährt, kann man das wie folgt erreichen: A wählt eine weitere, geheime Zufallszahl r und addiert diese zu a. Danach leitet A das Ergebnis zu B weiter. Da r für B unbekannt ist, kann B aus der Summe $r + a$ nicht die Zahl a rekonstruieren. Nun addiert B seine private Zahl b und leitet dieses Ergebnis $r + a + b$ an C weiter. C addiert schließlich noch c und gibt das Ergebnis weiter an Person A, die als einzige die Zahl r kennt, diese subtrahiert und so das Endergebnis $a + b + c$ erfährt, welches dann an die anderen beiden Teilnehmer kommuniziert wird. Um die Sicherheit zusätzlich zu erhöhen, etwa falls B und C nicht vertrauen, dass A ihnen das korrekte Ergebnis mitteilt, sind weitere Methoden möglich. Diese können kryptografischer Natur sein, oder auch nur in einer Permutation der Rollen von A, B und C bestehen, wobei dann durch Wiederholung des Protokolls getestet werden kann, ob in jeder Konstellation dasselbe Ergebnis erzielt wird. Im Allgemeinen sind SCM-Protokolle natürlich deutlich komplexer. Bemerkenswert an SMC ist, dass DLT diese aufgrund ihrer Transparenzeigenschaften und somit zuvor skizzierter Problematik bezüglich privater Daten interessant macht. Gleichzeitig liefert DLT auch die zur Umsetzung nötige IT-Infrastruktur und macht SMC damit erst praktikabel. Im Rahmen von DLT-Lösungen werden bestimmte Spezialfälle von SMC – sogenannte Zero-Knowledge-Proofs – besonders häufig betrachtet.

Zero-Knowledge-Proofs (ZKP) sind Verfahren, mit denen man Eigenschaften von Daten beweisen kann, ohne die Daten selbst vorzeigen zu müssen. Mittels dieser ist es möglich, ausschließlich Beweise und keine Inputdaten in DLT-Systemen ablegen zu müssen. Als intuitives Negativbeispiel hierfür kann ein Passwort dienen, das ohne ZKP im Klartext vorgezeigt werden müsste, um eine Zugangsberechtigung nachzuweisen. Möchte man verifizieren, dass ein Anwender Zugangsberechtigung hat, so kann man etwa leicht vergleichen, ob das eingegebene Passwort dasjenige ist, welches im Klartext vorliegt. Ein solches Passwort ist jedoch nicht auf ein (öffentliches) DLT-System zu legen, da es sonst von jedem Beteiligten Node gelesen werden könnte und demzufolge kein Geheimnis mehr repräsentieren würde. Mit ZKP ist es nun möglich, zu überprüfen, ob der Anwender ein bestimmtes Passwort kennt, ohne dass das Passwort selbst auf das DLT-System geschrieben werden muss. Einen Zero-Knowledge-Proof kann man sich bspw. als die wiederholte Beantwortung von speziellen Ja-/Nein-Fragen, deren Beantwortung keine Rückschlüsse auf das Passwort erlauben und die man aufgrund des Passworts sicher beantworten kann, vorstellen. Zwar ist dann auch die Wahrscheinlichkeit, durch Raten die richtige Antwort zu finden, bei 50 Prozent, durch wiederholtes Stellen modifizierter Fragen kann aber bei geeigneter Anzahl mit einer sehr hohen Wahrscheinlichkeit ausgeschlossen werden, dass nur durch Zufall stets die richtigen Antworten gegeben wurden. Durch die dazu nötige wiederholte Kommunikation zwischen demjenigen, der behauptet, das Passwort zu kennen, und der Instanz, die den entsprechenden Beweis einfordert, nennt man solche ZKP auch interaktiv. Für DLT-Systeme sind jedoch solche Formen von ZKP nicht besonders gut geeignet. Sogenannte zk-SNARKs (zero knowledge succinct

[42] *Schneier*, Applied Cryptography.

non-interactive argument of knowledge) können dagegen auf Interaktion vollständig verzichten und bieten sich somit für Verwendungen im Kontext von DLT deutlich besser an. Sie sind in der Regel mathematisch komplexer als interaktive ZKP.

Das Interessante an ZKP ist, dass diese Technologie verspricht, solche Beweise allgemein zu erbringen – nicht nur im Kontext von korrekten Passwörtern, sondern etwa auch dem Erfüllen bestimmter Eigenschaften der Daten oder einer korrekt erfolgten Berechnung. Mit ZKP und insbesondere zk-SNARKs kann demnach die Richtigkeit von Berechnungen überprüft werden, ohne sie ausführen zu müssen. Zudem wird nicht in Erfahrung gebracht, was ausgeführt wurde, sondern ausschließlich, dass es richtig ausgeführt wurde. Während diese Technologie sehr vielversprechend und bedeutsam für die Basisinnovation DLT ist, gilt die Erstellung von solchen Beweisen für komplexere Berechnungen und Funktionen heute noch als zu rechenintensiv, um für viele Anwendungen praktikabel zu sein. Während in die DLT selbst sehr viele Entwicklungskapazitäten eingeflossen sind und nach wie vor einfließen, scheint dieser Bereich – angesichts des Potenzials hinter der Technologie und dem Nutzen für die Basisinnovation DLT selbst – von zentraler Bedeutung. ZKPs können also ein weiter zu erforschender Baustein sein, um die nötige Privatheit von Informationen in öffentlichen DLT-Lösungen zu unterstützen.

5.2 Potenziale von DLT

5.2.1 Status quo

Der DLT werden weltweit große Potenziale zugeschrieben. In den letzten Jahren wurden bereits einige quantitative Einschätzungen des ökonomischen Potenzials der Technologie veröffentlicht. Die tatsächliche Validität der darin enthaltenen Schätzungen lässt sich allerdings aufgrund der Neuartigkeit der Technologie, der fehlenden Vergleichbarkeit mit bisherigen Entwicklungen sowie der schnellen technischen und ökonomischen Weiterentwicklung lediglich schwer überprüfen. Eine prominente Studie des Weltwirtschaftsforums bspw. postuliert, dass schätzungsweise 10 Prozent des globalen Bruttoinlandsprodukts im Jahr 2027 auf IT-Systemen, die auf DLT basieren, abgespeichert wird. Potenziell können dieser Einschätzung nach weltweit Güter und Werte an eine DLT-Applikation geknüpft und über diese ausgetauscht werden und somit von ihren Eigenschaften profitieren.[43] Das Marktforschungsunternehmen Gartner Inc. wiederum schätzt den Mehrwert, der durch die flächendeckende Einführung und Nutzung der DLT entsteht, bis zum Jahr 2030 auf ca. 3,1 Billionen US-Dollar alleine im Bereich Informationstechnik.[44] Insgesamt ist auch die Aussagekraft dieser Schätzung kritisch zu betrachten, da aufgrund des aktuellen Entwicklungsstands der Technologie viele Annahmen zur zukünftigen Entwicklung getroffen werden müssen.

Um die enormen in Aussicht gestellten Potenziale zu heben und gleichzeitig Konkurrenten keinen Innovationsvorsprung zu erlauben, investieren Unternehmen hohe Summen in die Entwicklung von DLT-Lösungen. Gemäß Zahlen des Marktforschungsunternehmens IDC wurden im Jahr 2017 weltweit etwa 950 Millionen US-Dollar und im Jahr 2018 etwa 1,5 Milliarden US-Dollar für DLT-Lösungen ausgegeben. Wie in Abbildung 12 dargestellt, werden entsprechend die jährlichen Ausgaben im Jahr 2022 auf etwa 11,7 Milliarden US-Dollar ansteigen. In den USA wird laut der Studie mit ca. 4,2 Milliarden US-Dollar der Großteil dieser Ausgaben getätigt.[45]

[43] *Global Agenda Council on the Future of Software & Society*, Deep Shift..
[44] *Panetta*, Gartner Top 10 Strategic Technology Trends for 2019.
[45] *Statista*, Blockchain.

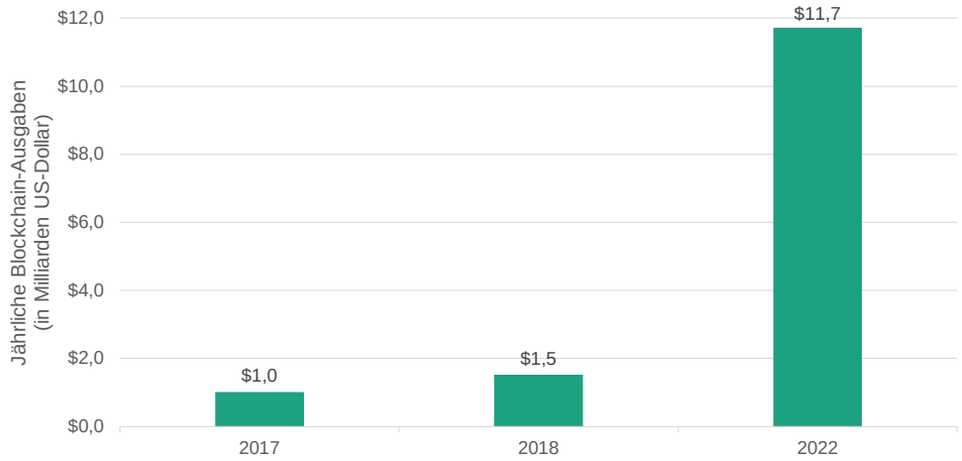


Abbildung 12: Erwartete jährliche Blockchain-Ausgaben (in Milliarden US-Dollar)

Auch diesbezüglich ist anzumerken, dass bei vergleichbaren Schätzungen der Marktforschungsinstitute die erwarteten Zahlen zum Teil stark divergieren. Während etwa das Marktforschungsinstitut Tractica das weltweite Marktvolumen von DLT im Jahr 2025 auf 20,3 Milliarden US-Dollar schätzt[46], trifft WinterGreen Research die Annahme, dass das Marktvolumen im Jahr 2024 schon bei 60 Milliarden US-Dollar liegen könnte[47]. Analysen von MarketsandMarkets hingegen erwarten im Jahr 2023 einen weltweiten Blockchain-Markt von 23,3 Milliarden US-Dollar.[48]

Die Menge an Blockchain-verwandten Patentanmeldungen zeigt ebenso, dass seitens Unternehmen ein hohes Interesse an der Technologie sowie eine hohe Innovationskraft bestehen. Seit 1999 wurden insgesamt 3 021 Patentfamilien angemeldet, die entweder direkten Bezug zur DLT oder indirekten Bezug zu den technischen Grundlagen der Technologie aufweisen. Solche mit indirektem Bezug zu den technischen Grundlagen, die inhaltlich etwa Hashbäume (Merkle Trees) oder verteilte und dezentrale Ledger-Systeme thematisieren, existierten somit bereits lange vor der Erfindung der Bitcoin-Blockchain im Jahr 2008. Auffällig ist, dass in den Jahren 2014 bis 2016 ein explosiver Anstieg an Neuanmeldungen von Blockchain-Patentfamilien zu verzeichnen war. Die Wachstumsrate an Neuanmeldungen betrug in diesen Jahren zwischen 143 bis 231 Prozent. Von den 3 021 genannten Patentfamilien wurden insgesamt 1 581 in China und 951 in den USA eingereicht. Europa belegt mit 131 Anmeldungen Platz 5.[49]

Auch der Bereich der Kryptowährungen (vgl. Kapitel 5.2.5.6) zieht zunehmend Interesse auf sich. Ende 2013 lag bspw. die Marktkapitalisierung aller Kryptowährungen bei etwa 10,3 Milliarden US-Dollar. Aus den insgesamt 63 der Schätzung zugrunde liegenden Kryptowährungen hatte allein Bitcoin eine Marktkapitalisierung von etwa 9 Milliarden US-Dollar. Im Jahr 2017 erreichte das Aufsehen um Kryptowährungen vorerst einen Höhepunkt und trieb die Marktkapitalisierung aller zu dem Zeitpunkt existierenden Kryptowährungen zwischenzeitlich auf ungefähr 614 Milliarden US-Dollar. Seit diesem Zeitpunkt verzeichnen die Kurse jedoch starke Rückgänge und befinden sich aktuell auf einem stetigen Abwärtstrend. Zum Stichtag 24. Februar 2019 liegt die Marktkapitalisierung aller Kryptowährungen bei etwa 127 Milliarden US-Dollar.

[46] *Tractica*, Enterprise Blockchain Revenue to Surpass $20 Billion by 2025.
[47] *Shah*, Global Blockchain Market Could Reach $60 Billion by 2024, Shows Report.
[48] *MarketsandMarkets*, Blockchain Market by Provider, Application (Payments, Exchanges, Smart Contracts, Documentation, Digital Identity, Supply Chain Management, and GRC Management), Organization Size, Industry Vertical, and Region - Global Forecast to 2023.
[49] *Acs*, Blockchain Innovation.

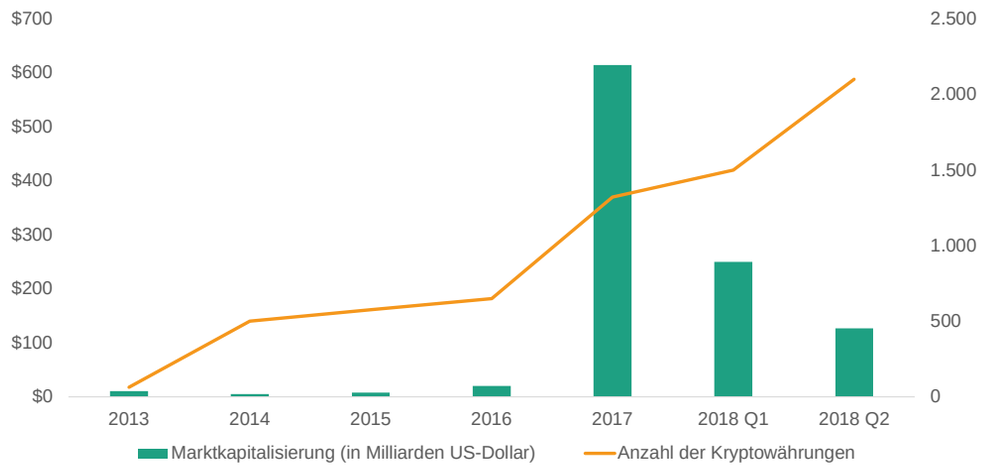


Abbildung 13: Marktkapitalisierung und Anzahl aller Kryptowährungen[50]

Im Bereich der Kryptowährungen können darüber hinaus Trends beobachtet werden, die vermehrt Auswirkungen auf die Finanzwirtschaft nach sich ziehen. Einer dieser Trends, der vorrangig in den USA vorzufinden ist, ist die Bemühung von Finanzdienstleistungsunternehmen wie etwa SolidX und VanEck, Bitcoin-Indexfonds aufzusetzen. Ein Indexfonds stellt dabei ein Investitionsobjekt dar, das den Kurs eines bestimmten Vermögenswerts, in diesem Fall Bitcoin, oder einer Gruppe von Vermögenswerten abbildet. Ein Bitcoin-Indexfonds ermöglicht entsprechend Investitionen in die Kryptowährung, ohne dabei tatsächlich Bitcoins zu halten.[51] Sollte ein solcher Bitcoin-Indexfond zugelassen werden, hätten nicht nur private Investoren, sondern auch internationale Fonds eine vereinfachte Investitionsmöglichkeit in Bitcoin. Bisher müssen Investoren die Währung entweder direkt kaufen und mittels spezieller Software verwalten oder über Wechselbörsen erwerben. Aktuell wird die Möglichkeit einer Zulassung von Bitcoin-Indexfonds durch die amerikanische Börsenaufsichtsbehörde SEC untersucht. Gemäß dieser sind wesentliche Probleme bei einer Zulassung, dass die Kryptowährung Bitcoin überwiegend unreguliert ist und die beantragten Bitcoin-Fonds nicht ausreichend die Anforderungen der SEC erfüllen, um betrügerisches und manipulatives Verhalten zu verhindern.[52] Generell sind Kryptowährungen ein kontrovers diskutiertes Thema. Gemäß der Datenbank Dead Coins sind zum heutigen Stand insgesamt 934 Kryptowährungen gescheitert. Davon wurden mindestens 680 Vorhaben aufgegeben, während es sich bei 182 nachweislich um Betrug und bei 60 um Spaßprojekte handelte. 12 Währungssysteme wurden durch Hacker sabotiert.[53]

Auch das Interesse an sogenannten Initial Coin Offerings (ICOs), die ein Mittel zur Unternehmensfinanzierung anhand von Kryptowährungen darstellen, steigt. Kumuliert wurde bis 2019 durch ICOs Kapital in Höhe von etwa 14,2 Milliarden US-Dollar beschafft. Abbildung 14 verdeutlicht, dass das jährlich beschaffte Kapital durch ICOs stark ansteigt. Dies liegt insbesondere daran, dass durch das gestiegene Interesse an ICOs einzelne Akteure in der Lage sind, signifikante Summen an Wagniskapital einzusammeln. So hat bspw. das Start-up Block.One mit seiner Kryptowährung EOS im Jahr 2018 insgesamt

[50] Eigene Darstellung in Anlehnung an und beruhend auf Daten von *CoinMarketCap*, Historical Snapshots.
[51] *Reiff*, Bitcoin ETFs Explained.
[52] *Marquette*, Crypto-based funds crawl toward mom and pop.
[53] *Dead Coins*, Curated List of cryptocurrencies forgotten by this world…and more.

200 Millionen US-Dollar eingenommen.[54] Interessant ist hierbei, dass mit ca. 6,2 Milliarden US-Dollar etwa 79 Prozent der im Jahr 2018 durch ICOs eingenommenen Geldmenge im ersten Halbjahr beschafft wurde. Dies lässt deutlich werden, dass sich hier nicht unbedingt ein stabiler, steigender Trend abzeichnet, sondern die durch ICOs eingesammelte Geldmenge wie bei den Kryptowährungen starken Schwankungen unterliegt. Gleichzeitig divergieren auch hier die Zahlen der verschiedenen Studien. So identifiziert eine Studie von Ernst & Young 15,5 Milliarden US-Dollar, die in ICOs im ersten Halbjahr 2018 eingesammelt worden sind.[55] Weitere Informationen zum Thema ICOs sind dem Kapitel 5.2.5.6.3 zu entnehmen.

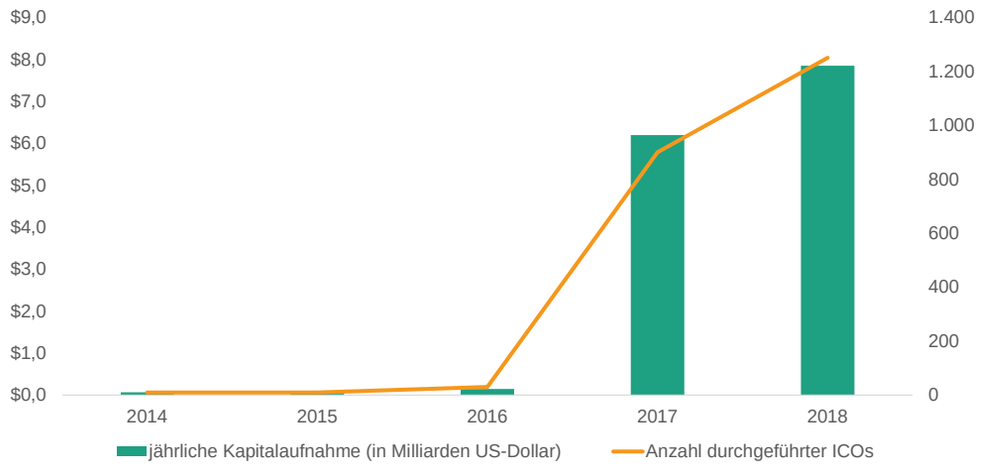


Abbildung 14: Anzahl sowie jährliche Kapitalaufnahme durch ICOs in Milliarden US-Dollar[56]

In Deutschland hat sich mittlerweile sowohl in der Forschung als auch in der Wirtschaft ein umfangreiches Ökosystem im Bereich der DLT entwickelt. Dabei sind die meisten Initiativen allerdings noch mit der Entwicklung von Prototypen oder der Erstellung von Proof-of-Concepts beschäftigt. Nur wenige Lösungen befinden sich im produktiven Einsatz. Entsprechend dieser Entwicklungen herrscht auf dem Arbeitsmarkt ein hoher Bedarf an Blockchain-Fachkräften. So sind in Deutschland im Zeitraum von August 2016 bis August 2018 alleine 737 neue Stellen bei Start-ups und weitere 790 Stellen bei anderen Unternehmen im Bereich DLT entstanden. Insbesondere bei Großkonzernen hat sich in diesem Zeitraum das Interesse an Fachkräften vervierfacht.[57] Auch im internationalen Vergleich ist Deutschland für Fachkräfte ein attraktiver Standort, da bei jeder offenen Stelle im Bereich DLT die Konkurrenz um die Stelle mit 18 potenziellen Fachkräften als Mitbewerber niedrig ist. In den USA kommen bspw. auf jede offene DLT-Stelle etwa 57 Fachkräfte.[58] Entsprechende Stellen benötigen in der Regel eine hohe fachliche Qualifizierung. Um den steigenden Bedarf an Fachkräften zu decken, wird aktuell auf verschiedenen Ebenen (Ausbildung, Forschung und Wirtschaft) Wissensaufbau betrieben. Während erste dezidierte Studiengänge, wie bspw. der Master in Blockchain und DLT an der Hochschule Mittweida, Studierende für die Thematik ausbilden sollen, fördern Einrichtungen wie das Blockchain-Labor des Fraunhofer Instituts für Angewandte Informationstechnik FIT den Übergang von Forschungsergebnissen in die Wirtschaft.

[54] *ICOdata.io*, ICO Status.
[55] *Ernst & Young*, Initial Coin Offerings (ICOs): The Class of 2017 – one year later.
[56] Eigene Darstellung in Anlehnung an *ICOdata.io*, ICO Status.
[57] *Joblift*, Nach Start-ups entdecken auch Konzerne die Blockchain: über 1.500 Stellen rund um die innovative Technologie in Deutschland.
[58] *Müller*, Studie über internationalen Arbeitsmarkt.

Darüber hinaus entstehen weltweit aktuell sowohl auf Unternehmensebene als auch auf Regierungsebene zahlreiche Initiativen zur Förderung und Erforschung der DLT. Start-ups ergründen innovative Geschäftsideen, etablierte Unternehmen evaluieren – sowohl intern als auch in Konsortien – mögliche Anwendungen der Technologie sowohl innerhalb bestimmter Branchen als auch branchenübergreifend. Öffentliche Initiativen unterstützen diese Initiativen über Förderprogramme oder untersuchen selbst die Potenziale der Technologie in der Verwaltung.

5.2.1.1 Start-ups

Zahlreiche Unternehmensgründungen sorgen für ein reges Ökosystem junger Start-ups im Umfeld der DLT, wie eine Studie aus dem Jahr 2018 belegt: Ca. 179 Jungunternehmen aus verschiedenen Wirtschaftsbereichen wurden mittlerweile in Deutschland gegründet. Dabei wird deutlich, dass Innovationshubs wie Berlin mit 89 der vertretenen Start-ups äußerst attraktiv für Unternehmensgründungen sind.[59] Mit den in Berlin ansässigen Start-ups besitzt Deutschland eine der größten und wichtigsten DLT-Szenen weltweit. Gemäß der Konzentration von Start-ups ist in Berlin ebenfalls ein hoher Anteil der deutschen Fachkräfte in dem Bereich zu finden.[60] Mit 23 Start-ups ist München auf Platz zwei der deutschen Blockchain-Hubs.

5.2.1.2 Konsortien

DLT haben im Unternehmenskontext das Potenzial, als Werkzeug eingesetzt zu werden, um die Kollaboration zwischen verschiedenen Unternehmen zu fördern (vgl. Kapitel 5.2.5.4). Aus diesem Grund erfordert auch die Entwicklung und Nutzbarmachung derartiger DLT-Lösungen Kollaborationen von Unternehmen und damit Initiativen, um u. a. Standards und Infrastrukturen für eine solche Lösungen zu erarbeiten.[61] Es ist daher zu beobachten, dass sich im DLT-Ökosystem immer häufiger Konsortien herausbilden, an denen sowohl etablierte Unternehmen als auch Start-ups beteiligt sind. Dabei entstehen zum einen Konsortien, die primär technologieorientierte Ziele verfolgen, und zum anderen wirtschaftsorientierte Konsortien, die das Anwendungspotenzial von DLT in einer spezifischen Branche untersuchen.[62] Gleichzeitig bilden sich Konsortien wie R3, die beiden Kategorien zuzuordnen sind.

Technologieorientierte Konsortien verfolgen das Ziel, DLT für unterschiedliche Unternehmen und Anwendungsgebiete nutzbar zu machen. Dafür setzen sie technische Standards etwa bei Architektur und Spezifikationen hinsichtlich Performanz und Skalierung. Beispiele für solche Konsortien sind Hyperledger, Ethereum sowie IOTA. Letztlich ist auch die internationale Organisation für Normung (ISO) an dieser Stelle anzuführen. Diese ist zwar kein Unternehmenskonsortium, sondern eine unabhängige, internationale Vereinigung, jedoch mit technologieorientierten Zielen am ehesten dort einzuordnen. Aktuell sind elf verschiedene Standards im Bereich Blockchain und DLT in Entwicklung, bspw. zur Standardisierung der Terminologie, Architektur und Rechtswirksamkeit von Smart Contracts.[63]

Wirtschaftsorientierte Konsortien bilden sich aktuell vorwiegend im Finanzsektor sowie in den Bereichen Mobilität und Energie. Als Beispiel für ein Konsortium im Bereich Finan-

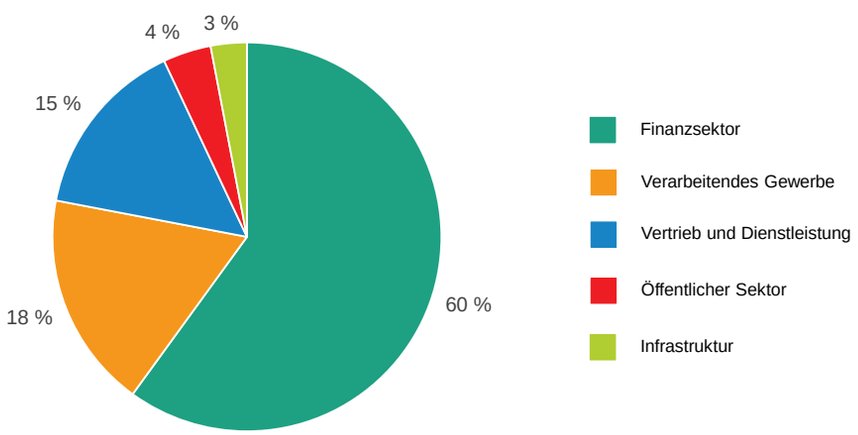
[59] *BTC-Echo*, Der deutsche Blockchain Index.
[60] *Müller*, Studie über internationalen Arbeitsmarkt.
[61] *Gratzke/Schatsky/Piscini*, Banding together for blockchain.
[62] *Virmani*, 18 blockchain consortia you should know about.
[63] *International Organization for Standardization*, Standards catalogue ISO/TC 307.

zen kann das in Indien gestartete Banken-Konsortium Bankchain angeführt werden. Dieses ermöglicht etwa die Erkundung von DLT-Anwendungsfällen in einer speziellen Softwareumgebung und verfolgt die Ziele, Betrug in der Finanzbranche zu minimieren und gleichzeitig Effizienz, Sicherheit sowie Transparenz von Finanzdienstleistungen zu steigern.[64] Neben Konsortien, die sich auf eine bestimmte Branche konzentrieren, existieren ebenso branchenübergreifende Konsortien – wie etwa die Climate Chain Coalition. Dieses orientiert sich an den langfristigen Zielen des Klimaschutzübereinkommens von Paris und fördert gezielt die Entwicklung von DLT-Lösungen, welche die Bekämpfung des Klimawandels unterstützen.[65]

5.2.1.3 Etablierte Unternehmen

Etablierte Player entdecken zunehmend die Potenziale von DLT für sich. Die prototypische Umsetzung von DLT-Lösungen und die Entwicklung von Proof-of-Concepts, denen spezifische Anwendungsfälle zugrunde liegen, nimmt daher stetig zu. Da das unternehmensinterne Know-how bezüglich DLT in der Regel allerdings gering ist, nutzen Unternehmen die Möglichkeit, Anwendungsfälle durch die Inanspruchnahme von Beratungsdienstleistungen oder in Kooperation mit anderen Initiativen innerhalb eines Konsortiums zu erkunden. Allein der amerikanische Technologiekonzern IBM hat im Jahr 2018 mit 45 Kunden aus unterschiedlichen Branchen an der Entwicklung von DLT-Lösungen gearbeitet. Aus einer Zusammenarbeit mit dem Logistikkonzern Maersk ging etwa im August 2018 die DLT-Plattform TradeLens live, welche der effizienteren Abwicklung von Güterprozessen dient.[66] Darüber hinaus zeichnet sich ein Trend ab, dass Unternehmen zunehmend Blockchain-as-a-Service (BaaS) von großen Cloudanbietern wie etwa Microsoft, Amazon, IBM und SAP beziehen. Dies ermöglicht es Unternehmen ohne eigene DLT-Infrastruktur, die Technologie zur Automatisierung, Absicherung sowie Verbesserung von Arbeitsabläufen nutzbar zu machen.[67]

Eine Betrachtung des Blockchain-Markts in Abbildung 15 zeigt, dass im Jahr 2018 der Finanzsektor mit 60,5 Prozent den größten Anteil des gesamten Marktwerts an Blockchain-Lösungen besitzt.



[64] Für weitere Informationen siehe http://www.bankchaintech.com/index.php.
[65] Für weitere Informationen siehe https://www.climatechaincoalition.io/.
[66] *Bajpai*, IBM and Blockchain: What It Did In 2018, And Where It's Going In 2019.
[67] *Joos/Karlstetter*, Blockchain-as-a-Service im Unternehmen nutzen.

Abbildung 15: Blockchain-Marktwert nach Wirtschaftssektoren im Jahr 2018[68]

Gemäß dem Marktforschungsunternehmen Tractica werden zukünftig der Finanzsektor, das verarbeitende Gewerbe, der öffentliche Sektor, das Gesundheitswesen und die Versicherungsbranche die fünf größten Wirtschaftssektoren für DLT-Anwendungen sein.[69] Auch diesbezüglich ist anzumerken, dass Vorhersagen bezüglich zukünftiger Potenziale noch schwer zu treffen sind und gegebenenfalls abweichen können.

Da bisher die Potenziale von DLT primär von Start-ups und größeren Konzernen wahrgenommen werden, bleibt die Frage offen, inwiefern kleine und mittelständische Unternehmen von der Technologie profitieren. Entsprechend gaben in einer Umfrage von YouGov 43 Prozent der befragten Entscheider aus mittelständischen Unternehmen an, keine der gängigen Einsatzmöglichkeiten der DLT zu kennen.[70]

5.2.1.4 Öffentliche Initiativen

Im DLT-Bereich bilden sich vermehrt öffentliche Initiativen heraus. Dies könnte u. a. auf die folgenden zwei Gründe zurückzuführen sein: Zum einen haben Staaten ein originäres Interesse daran, die Potenziale von DLT innerhalb staatlicher Strukturen zu erkunden. Bisherige Untersuchungen zeigen u. a., dass Regierungen kritische Informationen wie etwa Identitätsnachweise von Bürgern auf einer DLT-Lösung abspeichern können. Diese können Bürger nutzen, um sich bei digitalen Diensten eindeutig, sicher und nachprüfbar zu authentifizieren.[71] Zum anderen entstehen öffentliche Initiativen, da Staaten ein Interesse daran aufweisen, dass sich die Technologieentwicklung inklusive des Aufbaus an Know-how und der damit verbundenen Arbeitsplätze im eigenen Land stattfindet.

Auch auf EU-Ebene bilden sich öffentliche Initiativen heraus, welche die Förderung der DLT adressieren. So wird bspw. mit der „European Blockchain Partnership" ein Rahmen geschaffen, der es 27 Mitgliedstaaten erlaubt, sich über internationale Einsatzmöglichkeiten der Technologie auf Regierungsebene auszutauschen.[72] In einem noch breiter gefassten Rahmen beobachtet das EU Blockchain Observatory and Forum die aktuellen Aktivitäten im europäischen DLT-Ökosystem.[73]

5.2.1.5 Resümee

Förderung und Regulierung der DLT in Deutschland stehen bisweilen noch in ihren Anfängen. Insbesondere die Regulierung von Kryptowährungen rückt (auch international) zunehmend in den Fokus. Hier ist positiv hervorzuheben, dass diese Regulierungsmaßnahmen in den meisten Fällen aktuell nicht so weit gehen, dass sie die Innovationskraft der zugrunde liegenden DLT einschränken. Derzeitig bietet vor allem der Standort Berlin ein attraktives Umfeld zur Ansiedlung von Start-ups im Kontext von DLT. Dies gilt es durch eine enge Vernetzung zu Wirtschaft, Wissenschaft und Politik zu fördern. Der Standort Deutschland steht jedoch in großer Konkurrenz zu aufstrebenden Standorten, wie z. B. Malta, die sich zum Ziel gesetzt haben mit einem regulatorischen Rahmen und einer DLT-Strategie junge Start-ups anzuwerben. So wird dort aktuell an einem regulatorischen Rahmenwerk für DLT und Kryptowährungen gearbeitet. Dieses soll für Transparenz und Rechtssicherheit sorgen. Mit der Februar 2018 geschaffenen Malta Digital

[68] *Statista*, Blockchain.
[69] *Tractica*, Enterprise Blockchain Revenue to Surpass $20 Billion by 2025.
[70] *YouGov*, Umfrage zur Bekanntheit von Einsatzmöglichkeiten einer Blockchain im Mittelstand 2017.
[71] *Lyons/Courcelas/Timsit*, Blockchain for Government and Public Services.
[72] *European Commission*, European countries join Blockchain Partnership.
[73] *EU Blockchain Observatory and Forum*, About the European Union Blockchain Observatory and Forum.

Innovation Authority, die sich u. a. mit DLT und KI beschäftigt, stehen digitale Innovationen weit oben auf der Agenda. Themen, die durch diese Institution im Kontext der DLT bearbeitet werden, umfassen beispielsweise die Schaffung von Rahmenbedingungen zur Zertifizierung von DLT-Plattformen und die rechtliche Anwendbarkeit von Smart Contracts.

Hier gilt es nicht den Anschluss und Standortvorteil zu verlieren. In Bezug auf die strukturellen und finanziellen Rahmenbedingungen ist bedauerlicherweise zu verzeichnen, dass in Deutschland derzeit zu wenige Absolventen mit entsprechender DLT-Expertise aus den Universitäten auf den Arbeitsmarkt kommen. Nötig wäre hier aufgrund des Charakters der Technologie insbesondere eine Förderung von Programmen, welche die Schnittstelle mindestens zweier der Disziplinen Wirtschaft, Recht, Informatik und gegebenenfalls Ingenieurwissenschaften bedienen. Zudem bedarf es projektbezogener Förderprogramme durch die Ministerien, die sich explizit auf den Aufbau von DLT-Infrastrukturlösungen beziehen, welche ohne diese Technologien gar nicht denkbar wären. Derartige Förderprogramme müssten in der Zusammensetzung der Konsortien ebenfalls den interdisziplinären Charakter von DLT betonen.

Die Kooperation im Rahmen der Europäischen Blockchain-Partnerschaft, die Einrichtung des EU Blockchain Observatory and Forum, die European Blockchain Services Infrastructure (EBSI)-Initiative sind wichtige Schritte in die richtige Richtung. Im Rahmen dieser Zusammenarbeit und Initiativen können gemeinsame Grundlagen und Rahmenbedingungen geschaffen werden, die auch in Zukunft die Entwicklungen im Bereich der DLT innerhalb der EU nicht nur fördern, sondern ebenfalls gestalten. Wichtig ist, dieser Partnerschaft auch in juristischer, wirtschaftlicher und politischer Hinsicht Handlungen folgen zu lassen und die Zusammenarbeit in die Tat umzusetzen. So muss die Zusammenarbeit auf den verschiedenen Ebenen weiter intensiviert werden, damit letztlich der notwendige Beitrag geleistet werden kann.

In diesem Sinne ist von zentraler Bedeutung und werden die Entwicklungen im DLT-Bereich davon profitieren, wenn die Zusammenarbeit auf allen Ebenen weiter intensiviert wird. Die bereits über Ländergrenzen hinweg existierenden Start-ups, Konsortien, Initiativen und Organisationen sind darauf angewiesen, einen einheitlichen Rechts- und Handelsraum zu haben und sich an klaren Rahmenbedingungen zu orientieren.

5.2.2 DLT-Wertversprechen: Vertrauen

Nach dem sogenannten Internet der Informationen, dem Internet der Dienstleistungen und dem Internet der Dinge wird die DLT als Enabler für die vierte Generation des Internets gesehen: Das Internet des Vertrauens.[74] Die DLT kommt also mit dem Werteversprechen, Vertrauen zu stiften.

Vertrauen stellt einen wünschenswerten Zustand dar, der als kostbares Gut bezeichnet werden kann[75], denn Vertrauen muss erworben und erhalten werden. Schließlich bleibt Vertrauen nicht für immer bestehen, sondern kann auch wieder verloren gehen. Vertrauen entsteht bei einer Interaktion zwischen mindestens zwei Akteuren, wie z. B. Personen, Institutionen oder Organisationen und ist generell in Situationen notwendig, in denen sich eine Person darauf verlässt, „dass der Handlungspartner […] eine Vorleistung nicht zu seinem Vorteil ausnutzt“[76] . Mit anderen Worten ausgedrückt, vertraut der Vertrauensgeber einem Vertrauensnehmer. Je mehr gegenseitiges Vertrauen vorhanden ist, desto stärker verringert sich die gesamte Unsicherheit. Auf diese Weise hilft Vertrauen Komplexität zu reduzieren. Schließlich ist es dem Menschen nicht möglich, alle potenziell zur Verfügung stehenden Informationen aufzunehmen und zu verarbeiten, sodass letztlich asymmetrische Informationen reduziert und Informationsdefizite überwunden werden können.[77] Somit eröffnet Vertrauen Spielräume für Kooperationen und kann dadurch für ein effizienteres Wirtschaften sorgen.[78]

Insbesondere durch die zunehmende Digitalisierung und die wachsende Bedeutung von Plattformökonomien für unsere Gesellschaft wächst der Bedarf an Sicherheit, Identifizierbarkeit und Nachverfolgbarkeit zur Schaffung eines digitalen Vertrauens (digital Trust). Schließlich kann bspw. gekaufte Software schädlich sein, eine involvierte Partei sich als jemand anderes ausgeben, als sie eigentlich ist oder vertragliche Vereinbarungen schwer nachvollziehbar und durchsetzbar sein. Besonders die durch die Plattformen, wie bspw. Uber oder Airbnb entstehenden Möglichkeiten zur Selbstständigkeit schaffen zunehmend einen steigenden Bedarf an Vertrauen, da als Vertragspartner vermehrt Privatpersonen und keine Unternehmen auftreten.[79] Plattformen treten meist nur noch als Vermittler und Mediatoren auf. An dieser Stelle kann die DLT die geforderte Identifizierbarkeit und Nachverfolgbarkeit zur Schaffung von digitalem Vertrauen bieten und somit den bisherigen effizienten Rand des Vertrauens erweitern bzw. ergänzen.

In der heutigen Zeit können nämlich differierende Arten des Vertrauens auf unterschiedliche Weisen erzeugt werden. Systemvertrauen wird bspw. häufig über Institutionen[80] hergestellt und „[…] beschreibt das Phänomen des Vertrauens eines Individuums in gesellschaftliche Systeme bzw. Organisationen und Institutionen“[81]. Diese Institutionen sind üblicherweise in einem bestimmten Wirtschaftsbereich, bspw. wie die Europäische Zentralbank im Finanzdienstleistungsbereich, oder branchenübergreifend, wie TÜV-Zertifizierungseinrichtungen, tätig. Ist ein Produkt entsprechend zertifiziert, vertraut der Käufer auf dieses Zertifikat und damit auf die Qualität des Produkts. Die Zertifizierung begründet

[74] *Prinz*, Blockchain and CSCW – Shall we care?
[75] *Beck*, Die Finanzkrise ist auch eine Vertrauenskrise.
[76] *Beck*, Die Finanzkrise ist auch eine Vertrauenskrise.
[77] *Römer/Tscheulin,* Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 2008, 434.
[78] *Beck*, Die Finanzkrise ist auch eine Vertrauenskrise.
[79] *Mattila/Seppälä*, Digital trust, platforms, and policy.
[80] Eine für bestimmte Aufgabenbereiche zuständige öffentliche Einrichtung, die dem Wohl oder Nutzen des Einzelnen oder der Allgemeinheit dient.
[81] *Bruckner*, Organisationales Vertrauen initiieren.

also Vertrauen. Eine andere Form der Vertrauensbildung erfolgt z. B. über Reputation.[82] Je vertrauenswürdiger ein Akteur in früheren Interaktionen gehandelt hat, umso vertrauenswürdiger wird er für zukünftige Interaktionen eingestuft. Auf diesem Grundprinzip aufbauende Reputationssysteme sind mittlerweile in vielen Onlinesituationen[83] anzutreffen: Beim Einkauf bestimmter Waren in Onlineshops, bei der Auswahl des Hotels im Urlaubsort oder bei der Auswahl des Arztes in der Nähe.

Wichtige vertrauensbildende Institutionen in unserer Gesellschaft sind Banken. Schließlich vertrauen Kunden ihrer Bank eine Vielzahl von Informationen und die Verwaltung (eines Teils) ihres Vermögens an. Möchte eine Person bspw. eine bestimmte Menge Geld an eine andere transferieren, so vertrauen nahezu alle Bankkunden zunächst darauf, dass ihre Bank die ihr übertragenen Aufgaben wahrnimmt und dass das Kundenkapital bei der Bank – wenn überhaupt – nur einem sehr geringen Risiko ausgesetzt ist.

Die Finanzkrise der Jahre 2007/2008 erschütterte dieses Vertrauen in das weltweite Banksystem. Auch in Deutschland mussten einige Finanzinstitute Insolvenz anmelden, Bundeskanzlerin Angela Merkel und Finanzminister a.D. Peer Steinbrück sahen sich gezwungen, öffentlich die Einlagensicherheit der Sparer zu betonen.[84]

Zum Teil als Reaktion auf die Entwicklungen vor und während der Finanzkrise wurde das auf DLT-basierte Zahlungsmittel Bitcoin entwickelt, da insbesondere in dieser Zeit das Vertrauen in die weltweiten Finanzmärkte mit ihren Banken verloren ging.[85,86] In DLT-Systemen wird das Vertrauen nicht mehr über Institutionen geschaffen, sondern durch das DLT-System selbst, das durch seine Architektur einen transparenten Zugang zu Informationen ermöglicht, sodass asymmetrische Informationen abgebaut und direkte Peer-to-peer-Interaktionen ohne Mittelsmänner durchgeführt werden können. Das Vertrauen basiert somit auf einer anderen Form der Vertrauensbildung und zwar auf dem Vertrauen in das Protokoll, den Algorithmus bzw. den Code.

Peer-to-peer-Interaktionen sind in anderer Form auch bereits auf verschiedenen, nicht DLT-basierten Plattformen möglich. Beispielsweise besteht die Möglichkeit, von privat zu privat Unterkünfte zu mieten und zu vermieten oder gebrauchte Dinge zu handeln. Allerdings handelt es sich hier um eine Interaktion, die technisch über einen Mittelsmann, nämlich den Plattformbetreiber abgewickelt wird. Entsprechend besteht das Vertrauen zum einen darin, dass der Plattformbetreiber die Abwicklung wie gewünscht vornimmt und z. B. auch mögliche Konfliktfälle lösen kann, zum anderen wird Vertrauen z. B. durch zusätzliche Reputationssysteme geschaffen, indem alle Teilnehmer der Plattform bewertet werden können. Er kann Regeln ändern, Transparenz einschränken und auch den Wettbewerb auf der Plattform gemäß seinen Interessen steuern.

Direkte Peer-to-peer-Interaktionen, die nicht das Vertrauen in eine Institution (einen Mittelsmann) erfordern, werden durch die DLT möglich. Hier bildet das Vertrauen in das DLT-System selbst die Basis. Das Vertrauen wird maßgeblich durch die Aspekte Verteiltheit, Unveränderbarkeit, Transparenz erzeugt. Durch die Unveränderbarkeit von Einträgen, die verteilt auf den Knoten des Netzwerks gespeichert werden, wird für jeden (oder gegebenenfalls nur für beteiligte oder berechtigte) Teilnehmer sichergestellt, dass einmal gespeicherte Informationen nicht nachträglich änderbar sind. Je nachdem wie groß die Transparenz im spezifischen System (gewünscht) ist, kann diese Transparenz über die

[82] *Beck*, Die Finanzkrise ist auch eine Vertrauenskrise.

[83] Hier sei anzumerken, dass besonders diese Art des Vertrauens missbraucht wird, indem vermehrt von sogenannten Fake-Bewertungen die Rede ist. Fake-Bewertungen stellen Bewertungen dar, die nicht von realen Kunden, sondern bspw. von gekauften Dienstleistern geschrieben wurden.

[84] *Spiegel Online*, Merkel und Steinbrück im Wortlaut.

[85] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System.

[86] *Otte*, Die Finanzmärkte und die ökonomische Selbstbehauptung Europas.

gespeicherten Informationen das Vertrauen zusätzlich erhöhen. Zudem sind für sämtliche Teilnehmer am System die „Regeln" vordefiniert, d. h., alle Abläufe folgen den Regeln des DLT-Protokolls und unterliegen nicht den Interessen eines Plattformanbieters. Entsprechend basiert das Vertrauen in einem solchen Netzwerk auf dem Vertrauen in das (technische) System, seine Regeln und seine Implementierung. Hinzu kommt, dass mit Smart Contracts die Möglichkeit gegeben ist, vielseitige Interaktionen und Zusammenarbeitsmodi über Implementierungen abzubilden und dadurch auch in zuvor unbekannten Situationen vergleichsweise dynamisch Vertrauen herzustellen. Dieses Prinzip, auf den Programmcode zu vertrauen, wird auch durch die Begrifflichkeit „Code is law" verdeutlicht: Der Programmcode definiert die Regeln der Zusammenarbeit, eine nachträgliche Änderung ist nicht möglich und die Ausführung wird automatisiert.[87]

Am Beispiel eines Geldtransfers soll der Unterschied kompakt erläutert werden. Möchte eine Person heute Geld zu einer anderen Person transferieren, so wickelt diese Transaktion eine oder mehrere Institutionen ab, in der Regel Banken. Die beiden Transaktionspartner vertrauen also auf die korrekte Abwicklung durch die Institutionen (Person 1 – Bank – Bank – Person 2). In einem DLT-System gibt es keinen Mittelsmann, keine Institution, welche die Abwicklung vornimmt. Die Transaktion wird direkt „Peer-to-peer" durchgeführt (Person 1 – Person 2). Die beiden Transaktionspartner vertrauen auf das System, dass die Transaktion korrekt abgewickelt wird. Die Regeln für die Abwicklung sind zuvor klar definiert und können nicht durch Einzelne geändert werden.

Diesem Prinzip sind zugleich jedoch auch Risiken immanent. Zum einen ist Programmcode häufig sehr kontextspezifisch und hat daher eine geringere Flexibilität als es rechtliche Verträge (oder Gesetze) haben können. Es liegt kein oder nur sehr eingeschränkter Interpretationsspielraum vor. Insbesondere besteht zudem die Gefahr, dass Implementierungen fehlerhaft sind. Das wohl bekannteste Beispiel für eine fehlerhafte bzw. unsichere Implementierung stellt der sogenannte „DAO-Hack" dar. Dabei wurde die Kryptowährung Ether in einer Größenordnung von ca. 50 Mio. Dollar aus einer sogenannten „Dezentralen Autonomen Organisation" (DAO) entwendet, weil die Implementierung dieser DAO Schwachstellen aufwies.

Vorfälle dieser Art erschüttern entsprechend auch das Vertrauen in ein System. Für den Anwender wird es häufig kaum möglich sein zu beurteilen, ob ein solches System Schwachstellen aufweist oder nicht. Ähnlich verhält es sich jedoch mit anderen Systemen: Für Anwender ist es ebenso kaum möglich nachzuvollziehen, ob Institutionen heute das Vertrauen rechtfertigen oder den Wettbewerb oder die Reputationsmechanismen auf ihren Plattformen beeinflussen.

Die DLT bietet eine neuartige Möglichkeit der Vertrauensbildung, die auf dem Vertrauen in die Technologie, ihr zugrunde liegendes Konzept und in die Implementierung basiert. An dieser Stelle sei angemerkt, dass ungeachtet DLT auch weiterhin eine gewisse Art von Vertrauen notwendig ist. Dieses verschiebt sich jedoch von den involvierten Personen, Institutionen und Organisationen hin zum DLT-Protokoll und dessen Konsensmechanismus.

Die DLT kann somit andere Vertrauensbildungsmechanismen ablösen oder auch ergänzen. Denkbar ist bspw. der Einsatz von DLT zur Schaffung von Transparenz und Nachvollziehbarkeit bei Drittparteien, wie z. B. einer Bank oder TÜV-Zertifizierungsstelle.

Es ist denkbar, dass dadurch zukünftig völlig neue Ökosysteme entstehen oder bestehende abgelöst werden. Es ist überdies vorstellbar, dass sich verschiedene vertrauensbil-

[87] *Filippi/Hassan,* First Monday 2016, 1.

dende Maßnahmen in gemeinsamen Ökosystemen zukünftig sinnvoll ergänzen. Beispielsweise scheint eine Ergänzung von DLT-Systemen durch Reputationssysteme sinnvoll, um ein möglichst hohes Maß an Vertrauen zu schaffen.

Wertversprechen von DLT

Es bedarf weiterer Untersuchungen, wie das Zusammenspiel von bereits existenten, vertrauensstiftenden Mechanismen mit DLT wirkt. Fragen, die sich dabei stellen, sind zum Beispiel ob DLT komplementär zu existierenden, vertrauensstiftenden Mechanismen steht, oder ob DLT diese potenziell ersetzen kann. Wenn ja, unter welchen Bedingungen würde dies geschehen? Und inwiefern verändert DLT die Vertrauensbildung? Welche Vertrauensrisiken sind DLT inhärent? Ein Beispiel zur Verdeutlichung ist Sovrin, das eine selbstsouveräne digitale Identität ermöglicht. Ebenso stiftet die DLT „Vertrauen" zwischen Institutionen wie bspw. Ministerien, Bildungseinrichtungen etc. – zu diesen wiederum besteht ein klassisches Vertrauensverhältnis seitens des Bürgers. Smart Contracts können gleichzeitig Vertrauen heben und gefährden: Einerseits dokumentieren sie Abläufe, d.h., es wird sichergestellt, dass Inputs durch diese deterministisch und verifizierbar in Outputs umgewandelt werden („Whitebox"). Andererseits können Programmierfehler auftreten, bspw. wird die Nebenläufigkeit dieser Skripte nicht selten unterschätzt. Bereits in der jüngeren Vergangenheit kam es zu Hacks, die dadurch entstehende Schwachstellen ausnutzten und auch in Zukunft dürften Hacks vorkommen. Es sollte überlegt werden, ob Zertifizierungsstellen für Smart Contracts zusätzliches Vertrauen stiften oder in der Community auf Argwohn stoßen, da die Zertifizierungsmechanismen und -stellen zentralistische Instanzen sind.

5.2.3 Generische Rollen von DLT

Im Gegensatz zu Software für spezifische Aufgaben, wie bspw. ein Lohnbuchhaltungssystem, ist die DLT als Software mit grundlegendem infrastrukturellem Charakter zu verstehen. Die entsprechenden Systeme bringen kein eigenes Geschäftsmodell mit sich, sondern dienen vielmehr als Basis für die Implementierung beliebiger Anwendungen und gegebenenfalls Geschäftsmodelle.

In den meisten Fällen ist die Nutzung einer DLT-basierten IT-Lösung nicht aus technischer Perspektive, sondern vielmehr wirtschaftlich bzw. organisatorisch motiviert. Wegen der redundanten Datenhaltung und Programmausführung (Smart Contracts) ist die Performanz und die Skalierbarkeit von DLT zumindest bislang einem zentral organisierten System technisch unterlegen. Vielmehr bietet die DLT die Möglichkeit, Prozesse, die bislang lediglich durch Einbindung einer vertrauenswürdigen zentralen Instanz umsetzbar waren, digital umzusetzen. Dennoch lässt sich ein Einsatz nicht in allen Szenarien als grundsätzlich sinnvoll erachten. Auf sogenannten Plattformen steigt der Nutzen aufgrund sogenannter Netzwerkeffekte für alle Beteiligten typischerweise, je mehr Teilnehmer es sowohl auf der Anbieter- als auch auf der Nachfragerseite gibt. Dadurch konzentriert sich die gesamte Marktkoordination auf wenige Plattformanbieter. Als Konsequenz können die monopolistischen Plattformen dann erfahrungsgemäß ihre Vormachtstellung nutzen, um Markteintrittsbarrieren für neue Mitbewerber zu schaffen („Datensilos") oder Nutzungsentgelte unangemessen hoch anzusetzen. Insbesondere im B2B-Bereich besteht eine grundlegende Skepsis oder Abneigung gegenüber Plattformbetreibern, die den Markt potenziell dominieren könnten. Insgesamt bestehen bei zentralen Lösungen langfristig entsprechend Gefahren für den freien Wettbewerb und daraus resultierende Nachteile für Endkunden. Demzufolge ist der Grund für den Einsatz von DLT in der Regel

ökonomischer Art, nämlich die Vermeidung von Monopolen. Nicht immer ist es jedoch notwendig oder sinnvoll, gänzlich auf zentrale Strukturen zu verzichten. Diesbezüglich ist es wichtig zu untersuchen, wie das Zusammenspiel von bereits existenten, Vertrauen stiftenden Mechanismen mit DLT wirkt. Allgemein gesprochen kann die DLT direktes Vertrauen zwischen Parteien schaffen und somit Intermediäre effektiv ersetzen sowie Integrität bezüglich Daten und Prozessabläufen erhöhen. In Bezug auf die zu implementierenden Prozesse kann die DLT dabei verschiedene Rollen einnehmen. In einer möglichen generischen Klassifizierung kann sie zum Beispiel entweder als Verbesserer, Transformator oder Befähiger gesehen werden.[88]

5.2.3.1 Verbesserer

Zum Ersten kann die DLT bestehende Prozesse, die bereits ohne Intermediäre über bilaterale (Peer-to-peer) Schnittstellen (digital oder nicht-digital) abgewickelt werden, verbessern. Hierbei stehen insbesondere Eigenschaften, die zuvor nicht auf demselben Niveau umsetzbar waren oder traditionell mittels papierbasierter Abläufe umgesetzt wurden, im Vordergrund. Dies umfasst z. B. die rückwirkende Manipulationssicherheit abgespeicherter Daten in dezentralen Systemen oder die digitale Abbildung papierbasierter Prozesse mittels Smart Contracts.

5.2.3.2 Transformator

Zum Zweiten kann die DLT bestehende Prozesse, die zuvor unter Einbindung klassischer Intermediäre durchgeführt worden sind, transformieren und somit Prozessabläufe verschlanken. In diesem Fall steht insbesondere die Vertrauen schaffende Eigenschaft als System zur dezentralen Koordination und integren Abbildung direkter Interaktionen im Vordergrund. Ein hypothetisches Anwendungsbeispiel, in dem die Technologie als Transformator auftritt, ist die Implementierung von Treuhandverträgen mittels Smart Contracts.[89] Während bisher dritte Parteien als Treuhänder aufgetreten sind und Garantien übernommen haben, können die Modalitäten bestimmter Vereinbarungen nun im Programmcode eines Smart Contracts implementiert und Funktionen wie die Ausschüttung bestimmter Geldbeträge garantiert, autonom und dezentral ausgeführt werden.[90]

5.2.3.3 Befähiger

Zum Dritten kann die DLT als Wegbereiter für die Umsetzung innovativer Systeme dienen, die zuvor nicht technisch realisierbar waren. Häufig ermöglichen bzw. verbessern diese Systeme direkte Interaktionen zwischen unterschiedlichen Parteien. Diese oftmals generischen Dienste lassen sich in einer Vielzahl von verschiedenen Anwendungen einsetzen. Ein Beispiel für die DLT in der Rolle als Befähiger ist die Implementierung neuartiger (digitaler) Identifikationssysteme (digitale Identität), mittels derer anwendungsübergreifend selektiv Informationen unter Wahrung der Privatsphäre (informationelle Selbstbestimmung) freigegeben werden können.

Auf einer interorganisationalen Ebene kann die DLT ermöglichen, Transaktionen zwischen sich nicht vertrauenden Teilnehmern eines Netzwerks manipulationssicher durchzuführen. Dadurch kann die DLT die Grundlage bilden, um kontrollierte Kooperation zwischen Konkurrenten zum Vorteil der Kunden zu etablieren. Bislang konnte dies nur durch vertrauenswürdige Intermediäre oder strenge Regulierung erreicht werden. Die

[88] *Shen/Pena-Mora,* IEEE Access 2018, 76787.

[89] Siehe auch: allg. technischer Teil, spezieller Teil zu Frachtpapieren.

[90] Hierbei ist jedoch zu beachten, dass nach wie vor die Logik des Treuhandvertrags in einer Software abgebildet werden muss.

DLT kann auf technischer Ebene ungeachtet fehlenden Vertrauens zwischen unterschiedlichen Beteiligten ein faires und transparentes Verhalten technisch sicherstellen und macht somit Intermediäre oder strenge Regulierung potenziell obsolet.

Eine weitere, allgemeine Klassifizierung unterschiedlicher Anwendungsfälle der DLT basiert auf den jeweils genutzten Eigenschaften der Technologie.[91] Dabei haben die manipulationssichere Aufzeichnung von Daten sowie die Koordination anwendungsübergreifender Prozesse Priorität. Zudem werden die Potenziale der DLT im Zusammenhang mit Zugriffsverwaltung hinsichtlich Informationen oder Befehlen (Access Management), der Abbildung direkter Interaktionen zwischen verschiedenen Parteien sowie der Implementierung kollektiver Entscheidungsfindungsmechanismen hervorgehoben.

5.2.4 Entwicklungsstufen des Internets

Die DLT bietet eine digitale Infrastruktur zur Umsetzung verschiedener Dienstleistungen und Anwendungen. Dabei lässt sie sich als nächster Schritt in einer evolutionären Entwicklung technologischer Infrastrukturen einordnen. Generell impliziert die Natur digitaler Inhalte (Software, Medien, Daten jeder Art), dass eine beliebige Vervielfältigung nahezu ohne Grenzkosten möglich ist. Somit war es bisher im Allgemeinen ausgeschlossen, digitale Werttransaktionen ohne Einbindung einer zentralen Instanz abzuwickeln. Der Austausch von Informationen ist hingegen nicht betroffen, entsprechend kann das Internet in seiner herkömmlichen Architektur auch als „Internet der Informationen" bezeichnet werde. Aufbauend auf der Ermöglichung von informationsgetriebenen Dienstleistungen wurden dann in einem nächsten Schritt cyber-physische Systeme umgesetzt, die physische Objekte in die digitale Welt einbeziehen und somit ihre Fähigkeiten erweitern. Auf diese Weise wurde das Internet um cyber-physische Systeme um eine Vielzahl von Anwendungen erweitert; das Resultat ist das sogenannte „Internet der Dinge" (siehe dazu auch Abschnitt 5.1.1). Mit der Lösung des Double-Spending-Problems wurde im Rahmen der Erfindung von Bitcoin die Grundlage für ein weitergreifendes Ökosystem als bisher möglich geschaffen: Die DLT ermöglicht nun aufbauend auf dem Internet der Informationen auch entsprechende direkte Transaktionen ohne Abhängigkeit von bzw. Vertrauen in eine andere Partei. So wird in diesem Rahmen häufig von „Internet des Vertrauens" oder „Internet der Werte" gesprochen. Dabei ist zu beachten, dass die DLT auch Interaktionen zwischen nicht-menschlichen Parteien ermöglichen kann und somit auch das Internet der Dinge erweitert.

[91] *Shen/Pena-Mora,* IEEE Access 2018, 76787.

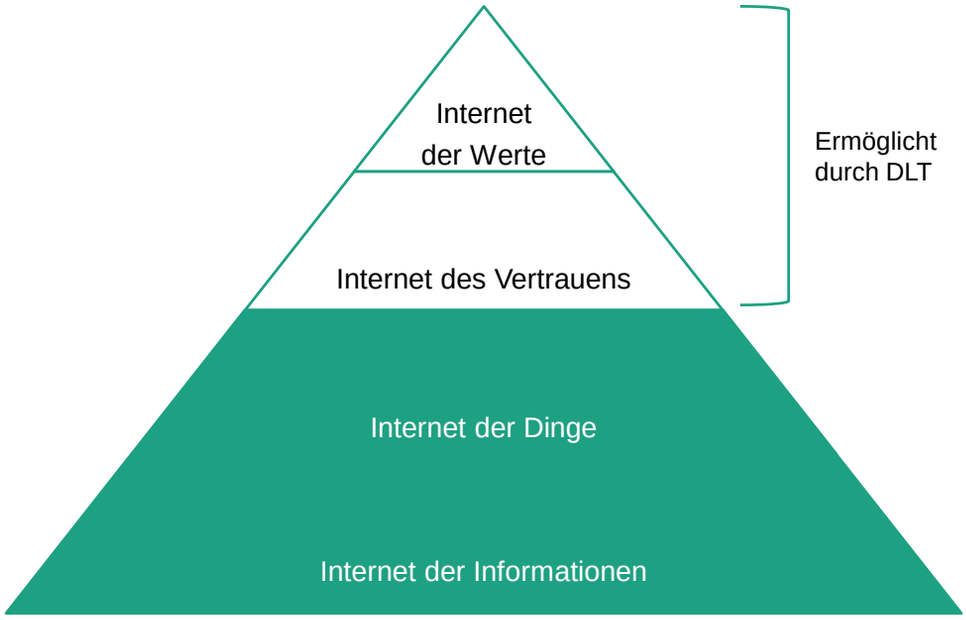


Abbildung 16: Entwicklungsstufen des Internets (eigene Darstellung)

5.2.5 Anwendungsmuster

Aus rein technischen Gründen ist die Nutzung von DLT nicht sinnvoll, da sowohl für die genutzten kryptografischen Verfahren (insbesondere für das Mining bei DLT-Systemen mit Proof-of-Work-Konsensmechanismus) als auch für die redundante Ausführung von Smart Contracts und die redundante Datenhaltung eine geringere Effizienz als bei zentralen Systemen gegeben ist[92,93]. Vielmehr ist der Einsatz einer verteilten Lösung in den meisten Fällen wirtschaftlich bzw. organisatorisch motiviert. So können bspw. Prozesse effizienter gestaltet werden, indem direktes Vertrauen ohne die Einbindung zentraler Betreiber hergestellt werden kann.[94]

Die potenziellen Anwendungsfälle für den Einsatz der DLT sind vielfältig. Entsprechend wird die Technologie über nahezu alle Branchen und Gesellschaftsbereiche hinweg diskutiert und getestet. Zwar sind die Anwendungsfälle jeweils spezifisch, gleichwohl lassen sich bestimmte Muster erkennen, die wir im Folgenden als *Anwendungsmuster* bezeichnen. Diese Anwendungsmuster verallgemeinern die spezifischen Anwendungsfälle, indem sie wiederkehrende Eigenschaften, die branchen- oder industrieübergreifend anzutreffen sind, auf sich vereinen. Die Anwendungsmuster sind dabei nicht durchschnittsfremd, d. h., ein Anwendungsfall kann sich prinzipiell in mehrere Anwendungsmuster einordnen lassen. Die Anwendungsmuster stellen eine Ebene zwischen konkreten Anwendungsfällen einerseits und andererseits abstrakten Konzepten, wie dem „Herstellen von Vertrauen", dar. Dies soll das Verständnis der breiten Anwendungsmöglichkeiten der Technologie fördern. Wie bereits erwähnt, muss in diesem Zusammenhang allerdings beachtet werden, dass grundsätzlich auch mittels zentraler Systeme jedes einzelne Anwendungsmuster umgesetzt werden könnte. Die Frage, ob DLT für ein konkretes durch

[92] Dies könnte man sogar als Theorem formulieren: Angenommen, es gäbe ein dezentrales System, das „besser" ist als ein zentrales System, so könnte man dieses dezentrale System in ein zentrales System integrieren („einbauen") und besäße dementsprechend ein zentrales System, welches ähnlich effizient / leistungsfähig ist.

[93] Siehe dazu auch Kapitel 5.3.2.1.

[94] Siehe dazu auch Kapitel 5.3.

ein Anwendungsmuster beschriebenes Problem eine geeignete Lösung ist, muss im Einzelfall geklärt werden und ist – wie voranstehend erörtert – eher eine organisationale und keine technische Frage.

5.2.5.1 Neutrale Plattform

Neben entstehenden Informationsasymmetrien und Datensilos weisen monopolistische Plattformen auf zentralen Infrastrukturen diverse weitere Herausforderungen auf. Die damit einhergehenden Fragestellungen hinsichtlich der Governance und der Nutzung der Daten verkomplizieren sich, je mehr Unternehmen an der Plattform beteiligt sind. Auch führt Misstrauen gegenüber und die Angst vor Abhängigkeit von einem zentralen Betreiber oft dazu, dass Unternehmen sich nicht an prozessual sinnvollen Plattformen beteiligen. Die aktuell insbesondere im B2C-Markt existierenden, quasi-monopolistischen Plattformen (z. B. Facebook) zeigen dieses „Winner-takes-all"-Prinzip eindrucksvoll. Unternehmen versuchen in der Regel zu vermeiden, in eine solche Abhängigkeit zu geraten und sind daher bestrebt, die Entstehung monopolistischer Plattformen in ihrer Industrie zu verhindern.

Neutrale Plattformen, die DLT als Infrastruktur nutzen, ermöglichen die Abwicklung von Geschäftsprozessen zwischen verschiedenen Organisationen auf einer neutralen technologischen Basis, die Fehlverhalten einzelner Teilnehmer technisch verhindert. Die DLT schafft durch ihre Dezentralität und (in bestimmten Ausprägungen) Transparenz die Möglichkeit, dass die Plattform durch deren Teilnehmer gemeinschaftlich koordiniert und verwaltet wird. Dabei steht insbesondere das Paradigma im Vordergrund, dass eben nicht ein einzelnes Unternehmen die Plattform zur Verfügung stellt, sondern die Plattform auf einem dezentralen Ansatz beruht. Natürlich muss es auch für eine solche Plattform bspw. Verantwortlichkeiten für Entwicklung und Wartung geben. Es gibt allerdings keinen zentralen Plattformbetreiber, der vom Betrieb der Plattform profitiert und diese hin zu einem Monopol entwickeln will. Eine derartige Plattform kann bspw. genutzt werden, um (interorganisationale) Prozesse durch den Einsatz von Smart Contracts zu automatisieren. Somit können die Vorteile einer Platform Economy erschlossen werden, ohne die Nachteile eines potenziellen Monopolisten in Kauf nehmen zu müssen. Auf diesen neutralen Plattformen können außerdem digitale Anwendungen bspw. in Form von Marktplätzen, Spielen oder anderen Anwendungen umgesetzt werden und digitale Ökosysteme entstehen.

5.2.5.2 Fälschungssichere Dokumentation

Eine der grundlegenden Eigenschaften von DLT-Systemen ist deren Unveränderbarkeit, durch welche die nachträgliche Manipulation dort abgelegter Daten oder Informationen (z. B. Dokumente, Verträge, Maschinenprotokolle) verhindert oder mindestens dokumentiert werden kann. Die Nutzung eines DLT-Systems erlaubt es insofern, eine glaubwürdige und für alle beteiligten Akteure einsehbare Historie für verschiedene Arten von Informationen zu etablieren. Auf diese Weise kann auch die Möglichkeit geschaffen werden, die abgelegten Daten u. a. für eine Auditierung zu nutzen. Beispielsweise ist es denkbar, den Zugriff einzelner Personen auf sensible Daten in einer DLT-Anwendung nachzuverfolgen und vor fremdem Zugriff zu schützen. Dazu werden in der Regel aber nicht die Daten selbst in DLT-Systemen gespeichert, sondern nur deren Hashwerte[95], mit denen bestätigt werden kann, dass ein außerhalb des DLT-Systems verfügbares Dokument bereits zu einem früheren Zeitpunkt in genau dieser Form vorlag.

[95] Eine Art „digitaler Fingerabdruck" der Daten, siehe 4.1.4.

5.2.5.3 Zahlungsverkehr

Das Anwendungsmuster Zahlungsverkehr stellt den in der Öffentlichkeit wohl bekanntesten Einsatzzweck der DLT dar. Die in diesem Kontext wohl prominentesten Beispiele sind Kryptowährungen wie Bitcoin. Der Einsatz von DLT schafft die Möglichkeit zur Umsetzung digitaler Zahlungsmittel, ohne dabei auf Intermediäre wie etwa das Bankensystem zurückzugreifen. Somit können zwei Parteien direkt miteinander Zahlungen abwickeln, ohne dass dazu der Weg über ihre Bank oder einen anderen Intermediär wie z. B. PayPal notwendig ist. Die gesamte Abwicklung findet über die DLT als Infrastruktur direkt „Peer-to-peer" statt, wobei auch der Transfer von Kleinstbeträgen möglich ist.[96] Die Nutzung eines derartigen direkten Wertetransfers kann in vielen Szenarien sinnvoll sein, oft auch als Ergänzung zu anderen Funktionen, die ein DLT-System bietet.

5.2.5.4 Management organisationsübergreifender Prozesse

Prozesse zwischen Unternehmen oder Business-to-Business (B2B)-Prozesse, die sich über mehrere Unternehmen oder Organisationen innerhalb eines Wertschöpfungsnetzwerks erstrecken, sind – oft zur Wahrung von Geschäftsgeheimnissen, aber auch wegen fehlender Standardisierung – üblicherweise geprägt von System- und Medienbrüchen. Somit weisen sie letztlich eine hohe Intransparenz und Fragmentierung auf. Teilweise entsteht in solchen organisationsübergreifenden Situationen eine zentrale Lösung (bspw. betrieben durch einen Prozessbeteiligten mit hoher Marktmacht), die Daten und Prozessschritte aller Beteiligten integriert. Allerdings gelingt dies in der Praxis lediglich in Ausnahmefällen und verlagert weitere Einflussmöglichkeiten auf ohnehin schon starke Marktteilnehmer. Hintergrund sind in vielen Fällen nicht notwendigerweise technische Herausforderungen, sondern vielmehr politische und wirtschaftliche Fragestellungen. Im Falle einer zentralen Lösung müsste sich ein Unternehmen bzw. eine Organisation um den Aufbau und den Betrieb des Systems kümmern und dem Unternehmen dergestalt einen Informationsvorsprung gegenüber den Wettbewerbern innerhalb des Wertschöpfungsnetzwerks einräumen. Im Übrigen entstehen oftmals Datensilos. Eine Alternative zu solchen monopolistischen Plattformen können neutrale Plattformen bieten, die mittels DLT umgesetzt und im nächsten Anwendungsmuster detailliert beschrieben werden.
Die zeitnahe Verteilung von Informationen an alle Teilnehmer eines DLT-Netzwerks ermöglicht eine organisationsübergreifende Koordination von Prozessen. Einmal in das DLT-System geschriebene Prozessinformationen können somit als Auslöser für den Beginn von Folgeprozessen genutzt werden. Prozesszwischenzeiten können somit potenziell deutlich reduziert werden. Durch den überlegten Einsatz von Smart Contracts auf DLT-Systemen kann zudem eine automatisierte Prozesskontrolle und perspektivisch auch eine (Teil-)Automatisierung ausgewählter Prozessschritte erfolgen.

Beispielsweise wird die Logistikbranche in der Regel durch eine hohe Anzahl an unterschiedlichen Prozessbeteiligten charakterisiert, die von Beginn bis zum Ende eines Güterflusses an unterschiedlichen Stellen involviert sind. Häufig werden die dabei anfallenden Daten und Informationen zur Produktion, Verpackung, Inventarisierung, Transport, Verzollung, Lagerabwicklung und Sicherheitsmanagement erst mit zeitlicher Verzögerung

[96] Bei Bitcoin und Ethereum sind die Transaktionskosten wegen der (aktuell) hohen Kurse der zugehörigen Kryptowährungen sehr hoch (im Bereich von einigen Euro je Transaktion), sodass Mikrotransaktionen hier zu teuer sind. Öffentliche Systeme, die praktisch transaktionskostenfrei sein sollen, werden jedoch aktuell bereits erforscht. Ein prominentes Beispiel ist IOTA. Für nicht-öffentliche Systeme (Ripple) liegen bereits Lösungen ohne großen Energieverbrauch und entsprechend aber ohne nennenswerte Transaktionsgebühren vor. A priori sind die Kosten, die bei Abwicklungen mittels traditioneller Banken für eine digitale Transaktion entstehen, gegenüber dem Overhead, der durch die Verwaltungskosten etc. entsteht, vernachlässigbar.

transparent gemacht oder gar überhaupt nicht kommuniziert.[97] Diese Informationsdefizite und -asymmetrien resultieren in Ineffizienzen und Wartezeiten. Um den Informationsfluss zwischen den Prozessbeteiligten zu verbessern, bieten sich bspw. private DLT-Systeme an. Darin können bspw. Informationen zu Prozessfortschritten manipulationsresistent in einem chronologischen Register abgebildet werden. So können Auftragspapiere, Rechnungen, Herkunftsnachweise und Zollpapiere einfacher und unter Wahrung von Integrität und Sicherheit dokumentiert werden. Gleichzeitig ermöglicht dies die Zusammenarbeit aller am Güterfluss beteiligten Unternehmen durch organisationsübergreifende Prozesse.[98] Somit kann eine DLT-basierte IT als dezentrale, transparente und manipulationssichere Infrastruktur eine valide Alternative darstellen, um die unternehmensübergreifende Zusammenarbeit in gemeinsamen Prozessen zu verbessern, dadurch die Informationstransparenz zu erhöhen und Ineffizienzen in der Zusammenarbeit zwischen den beteiligten Unternehmen verringern.

5.2.5.5 Digitale Identität

In vielen Anwendungsfällen werden digitale Entsprechungen von physischen Dingen benötigt (sogenannte digitale Identitäten oder digitale Zwillinge[99]) mithilfe derer Personen oder Objekte in der digitalen Welt repräsentiert werden können. Diese bilden Eigenschaften und Verhalten einer Person oder eines Objekts digital ab, sodass mit dieser Person oder diesem Objekt im Nachgang digital interagiert werden kann.[100] Die DLT bietet eine Möglichkeit, derartige Identitäten zu etablieren. Durch eineindeutige, validierte und souveräne Identitäten können so auch Identitätsdiebstahl oder Manipulationen deutlich erschwert werden.

Das Bundesamt für Migration und Flüchtlinge ist in dieser Thematik bereits aktiv und untersucht die Möglichkeit, eine eindeutige und für Verwaltungszwecke geeignete digitale Identität von Geflüchteten zu schaffen.[101] Hier zeigt sich auch der Zusammenhang mit unternehmensübergreifenden Prozessen: Über die verschiedenen staatlichen Institutionen hinweg ist es von Relevanz, für die Prozesse eine über die Organisationsgrenzen hinweg eindeutige, digitale Identität nutzen zu können. Eine solche Eindeutigkeit ist mit heutigen zentralen Systemen zwar technisch möglich, allerdings in der Praxis bei mehreren tausend beteiligten Einrichtungen schwer umzusetzen. Die Nutzung einer DLT-Anwendung bietet hier das Potenzial, digitale Identitäten auf einer übergreifenden Infrastruktur zu etablieren.

5.2.5.6 Digitale Urkunden

Analog zum Konzept digitaler Identitäten können auch andere Objekte oder Vermögenswerte aus der Realwelt in Form eines Tokens repräsentiert werden und spiegeln so – wie heute eine Urkunde – z. B. den Besitz eines Guts wider. Im Rahmen dieser digitalen Urkunde (Tokenisierung) werden dabei Eigenschaften eines Objekts digital abgebildet. Aus der digitalen Urkunde resultiert dabei auch die Möglichkeit, Objekte wie bspw. Vermögenswerte, (nahezu) beliebig zu stückeln und zu handeln. Die digitale Urkunde bildet damit eine Alternative zu papierbasierten Beurkundungen, die hinsichtlich Fälschungssicherheit bzw. Validierbarkeit (zu jedem Zeitpunkt und an jedem Ort) und Dokumentenlogistik meist schwer zu handhaben sind. Damit können sowohl neue Anwendungsfelder

[97] *Christopher/Lee*, Mitigating supply chain risk through improved confidence.

[98] *Gilbert Fridgen/Sven Radszuwill et al.*, 51st Annual Hawaii International Conference on System Sciences (HICSS) 2018, 1.

[99] Für das Grundgutachten wird der Begriff „Digitaler Zwilling" verwendet. Theoretisch wäre jedoch der Begriff „Digitaler Schatten" genauer, da das digitale Abbild eines Objekts keine vollständige Simulation darstellt, sondern nur Metadaten des realen Objekts in der digitalen Welt.

[100] Siehe auch Abschnitt 5.2.4.

[101] *Florian Guggenmos/Jannik Lockl et al.*, Informatik-Spektrum 2019, 1.

erschlossen werden, die heute zu viel Aufwand generieren würden, als auch bisherige Anwendungsfelder effizienter oder betrugssicherer gestaltet werden (z. B. gegebenenfalls auch im Kontext der seit spätestens November 2018 wegen Steuerbetrugs in die Kritik geratenen American Depositary Receipts).

Mit der DLT und darauf implementierten Token können also erstmals digitale Werte und digitales Eigentum ohne Mittelsmann manipulationssicher geteilt werden. Eine exakte Definition für einen DLT-Token existiert derzeit noch nicht. Der ursprüngliche Begriff des digitalen Tokens stammt aus der Informatik, in der Token als Mittel zur Identifizierung und Authentisierung genutzt werden. Grundsätzlich sind aber mit einem DLT-Token Werte oder Berechtigungen verknüpft. Zu diesen zählen u. a. Stimmrechte, Vermögenswerte oder Dienstleistungen. Der Einsatz von DLT-Token als allgemeine Kryptowährung bildet einen prominenten Anwendungsfall, z. B. für die Währung Bitcoin. Neben der funktionalen Unterscheidbarkeit kann zusätzlich bezüglich der Handelbarkeit von Token unterschieden werden. Handelbare Token werden danach auch als fungibel und nicht handelbare Token als nicht-fungibel bezeichnet. Ebendiese nicht-fungiblen Token können nicht übertragen werden. Dies ist u. a. bei der digitalen Urkunde von Identitäten bedeutend, da diese meist an eine bestimmte Person oder ein Objekt gebunden sind. In den letzten Jahren ist eine Vielzahl an neuen digitalen Token-Systemen entstanden, da derartige Token neue Formen der Unternehmens-, Start-up- und Projektfinanzierung ermöglichen können. Dies wird realisiert, indem sie nach ihrer Erzeugung über verschiedene Wege an Investoren ausgegeben werden können. Der am weitesten verbreitete Ansatz ist dabei das sogenannte ICO (oft auch als „Token Generating Event" bezeichnet). Dabei werden Token durch Smart Contracts und gegen Bezahlung mit einer Fiat-Währung (bspw. EUR, USD) oder Kryptowährung ausgegeben. Die primär im Rahmen solcher ICOs entstandenen Token eröffnen aufgrund ihrer individuellen Ausgestaltungsmöglichkeiten eine Vielzahl an technologischen und ökonomischen Möglichkeiten. So können diese bspw. als Utility-, Security- oder Equity-Token, die nachfolgend ausführlicher diskutiert werden, ausgegeben werden.

5.2.5.6.1 Klassifikationen von Token

Im Verlauf der letzten Jahre hat sich eine Vielzahl an unterschiedlichen Arten von Token herausgebildet, sodass das Phänomen mittlerweile in den Fokus wissenschaftlicher Forschung gerückt ist.[102] Insgesamt existieren inzwischen mehrere unterschiedliche Klassifikationen von Token. Welche Ziele mit Token erreicht werden können und welche Einsatzmöglichkeiten sich daraus ergeben, ist allerdings noch nicht abschließend geklärt. Grundsätzlich kann zwischen drei Token-Klassen unterschieden werden: Kryptowährungen, Utility-Token und Security-Token. Die älteste Form von Token bilden Kryptowährungen, die als digitales Geld, u. a. für den Bezug von Gütern oder Services, genutzt werden können. Ein Utility-Token kann hingegen unterschiedliche Funktionen besitzen. So kann dieser bspw. seinem Besitzer eine Zugangsberechtigung erteilen (ähnlich einer Zutrittskarte) oder als „Wert-Behälter" dienen, um bestimmte Verhaltensweisen eines Nutzers zu be- und entlohnen. Security-Token schließlich bilden Unternehmensanteile ab, mit dem einhergehenden Recht zum Bezug von Dividenden oder einer Beteiligung am Gewinn. Insbesondere die letzte Art von Token rückt zunehmend in den Fokus von Regulierungsinstitutionen, da Token als Securities dem Wertpapierhandelsgesetz und somit der Finanzdienstleistungsaufsicht unterliegen.[103] Bis heute existiert jedoch noch kein einheitlicher Rechtsrahmen für Token auf EU- oder Bundesebene. Hier besteht insgesamt noch ein großer wissenschaftlicher und politischer Handlungsbedarf.

[102] *Oliveira/Zavolokina/Bauer/Schwabe*, To Token or not to Token: Tools for Understanding Blockchain Tokens.

[103] *Blockchain Bundesverband Finance Working Group*, Statement on Token Regulation with a Focus on Token Sales.

5.2.5.6.2 Kryptowährungen

Kryptowährungen sind eine beispielhafte Anwendung digitaler Token. Generell haben (als übergeordnete Kategorie zu betrachtende) digitale Währungen gemeinsam, dass sie als Austauschmedium, Wertspeicher oder Rechnungseinheit genutzt werden.[104] So können sie u. a. für den Bezug von physischen Gütern oder Dienstleistungen genutzt werden. Weiterhin ist es möglich, dass deren Nutzung lediglich auf einen Onlinebereich, wie z. B. ein Online-Casino oder eine Airline, begrenzt ist. In diesem Zusammenhang werden sie ebenfalls als virtuelle Währung bezeichnet. Erst mit dem Bitcoin verbreitete sich eine neue Form der digitalen Währungen – genannt Kryptowährungen. Der Ursprung von Bitcoin geht auf die Finanzkrise aus dem Jahre 2007 zurück. Damals fluteten die Zentralbanken die Märkte mit frischem Geld, sodass der Wert physischer Währungen signifikant gesunken war. In diesem Kontext entwickelte ein Individuum oder eine Gruppe unter dem Pseudonym Satoshi Nakamoto Bitcoin als neue, von Banken und damit Staaten unabhängige Währung, die nicht zentral gesteuert werden kann. Somit unterscheiden sich entsprechende Kryptowährungen von anderen digitalen Währungen durch die Nutzung eines dezentralen Netzwerks als Basis. Im März 2019 existierten mehr als 2 000 verschiedene Kryptowährungen[105], welche die DLT im weiteren Sinne nutzen. Ein Vorteil von Kryptowährungen gegenüber herkömmlichen Zahlungsmitteln zeigt sich in der schnellen und länderübergreifenden Abwicklung von Transaktionen. Während das Bankensystem teilweise mehrere Tage zur Abwicklung von Auslandstransaktionen benötigt, bieten Kryptowährungen ein einheitliches System, in welchem Transaktionen weltweit innerhalb weniger Sekunden oder Minuten abgewickelt werden können. Schweden und China gehen an dieser Stelle sehr innovative Wege und lassen durch ihre Zentralbanken eigene Kryptowährungen entwickeln. Auch die Direktorin des Internationalen Währungsfonds Christine Lagarde hat im Oktober 2017 durch ihren Vorschlag für eine Digitalwährung deren Potenziale und zukünftige Bedeutung unterstrichen.[106] Eine oft als Nachteil eingestufte Eigenschaft von aktuellen Kryptowährungen sind dagegen ihre oft hohen Kursschwankungen. Auf diese Thematik wird in Kapitel 5.2.5.6.4 noch näher eingegangen.

Token-Einordnung

Eine Klärung der rechtlichen Einordnung von Token sollte kurzfristig realisiert werden, um Rechtssicherheit zu schaffen. Damit werden auch die Pflichten für Tokenbesitzer und emittierende Unternehmen deutlich. Eine rechtliche Einordnung ist zunächst voraussichtlich hauptsächlich im Bereich des Wertpapier- und Steuerrechts sinnvoll. Klassifikationen von Token sollten fortgeschrieben und weiterentwickelt werden, um die Basis für eine rechtliche Einordnung zu schaffen. Sollte keine Rechtssicherheit geschaffen werden, besteht die Gefahr, dass sich Talente/Fachkräfte und unternehmerisches Potenzial aus Deutschland abwenden, da andere Staaten ggf. entsprechende Rechtssicherheit bieten können.

[104] Monetary Authority of Singapore. 2018. Crowd Genie Financial Services pte. ltd.: Incorporated in Singapore. https://eservices.mas.gov.sg/fid/institution/detail/201066-CROWD-GENIE-FINANCIAL-SERVICES-PTE-LTD.

[105] https://coinmarketcap.com.

[106] *Schulze*, 'We are about to see massive disruptions': IMF's Lagarde says it's time to get serious about digital currency.

5.2.5.6.3 Initial Coin Offerings

Ein ICO ist eine Form der Finanzmittelbeschaffung und kann aus Finanzmarktsicht am ehesten mit einem traditionellen Initial Public Offerering oder Crowdfunding verglichen werden. ICOs werden auch als Fundraising bezeichnet, bei welchem die Blockchain genutzt wird, um die Grundidee des Crowdfundings[107] ohne Intermediäre wie Banken umzusetzen. Im Gegensatz zum klassischen Crowdfunding kommt hierbei keine Drittpartei zur Vermittlung für Vertragsabschlüsse oder zur Abwicklung des Geldtransfers zum Einsatz. Deshalb spricht man bei ICOs auch davon, dass sie „truly peer-to-peer" sind – also wirklich ohne Intermediär umgesetzt werden. Bei einem ICO erhält ein Investor Token als Gegenwert für die eingelagerte Investition. Die Investition findet als Tausch von Kryptowährungen statt. Ein Investor schickt somit bspw. eine Anzahl Bitcoin an die Netzwerkadresse des jeweiligen Projekts und erhält in einem entsprechenden Verhältnis die mit dem Projekt assoziierten Token. Neue Token werden oftmals mithilfe eines Smart Contracts auf einem DLT-System erzeugt. Der Gegenwert und die Funktionalität, die hinter einem investierten Token stehen, können hierbei, je nach Ausgestaltung des ICOs, variieren. Dabei kann es sogar auftreten, dass Projekte nach dem ICO die Art ihres Tokens ändern, um auf diese Weise Regulierungskonflikte zu vermeiden. Generische Funktionalitäten der Token wurden bereits zuvor näher beschrieben. Die durch den ICO erzielten Erlöse stehen vollumfänglich zur Finanzierung des Entwicklungsvorhabens zur Verfügung. Somit versuchen ICOs letztlich, Anreize für private Investitionen in die Technologie zu schaffen. Aufgrund der selbstständigen Organisation der „Blockchain-Community" und einer fehlenden Regulierung nutzen „schwarze Schafe" diese Situation oftmals aus. Diese versuchen durch Scheininitiativen, die Blockchain oft nur im Namen beinhalten, Geld einzusammeln und Investoren zu betrügen. So hat im Jahr 2018 ein vietnamesisches Unternehmen namens Modern Tech rund 32 000 Investoren um 660 Millionen Dollar betrogen, als es nach ihrem Pincoin-ICO die eingeworbenen Mittel veruntreute.[108] Aufgrund des offenen und globalen Charakters der Blockchain und der ICOs lassen sich derartige Schemata national kaum regulieren und insbesondere nur schwer „verbieten". Insgesamt gilt es, genauer zu untersuchen, unter welchen Rahmenbedingungen ICOs eine sinnvolle Finanzierungsmethode für Start-ups und Unternehmen begründen können und wie Investoren besser vor „schwarzen Schafen" geschützt werden können.

5.2.5.6.4 Kursschwankungen

Der Wert handelbarer Token ist in der Regel abhängig von Angebot und Nachfrage im Markt. Somit fluktuiert der Wert (insbesondere von Kryptowährungen) häufig – nicht zuletzt aufgrund der Vielzahl spekulativer Anleger in dem Bereich. Da Token oftmals als Anreizmittel zur aktiven Teilnahme am Betrieb von DLT-Systemen genutzt werden, sind diese Kursschwankungen als problematisch einzustufen. Wie in Kapitel 4.3.1 beschrieben, kosten bspw. Rechenoperationen in Smart Contracts oftmals einen Betrag in der jeweiligen Währung. Durch die hohen Kursschwankungen sind die Kosten für die Ausführung der darauf implementierten Anwendungen dementsprechend schwer zu prognostizieren, was ökonomisch als problematisch anzusehen ist. Insbesondere bei Utility-Token, die einen Nützlichkeitsgedanken inhärent haben, also z. B. für die Bezahlung von Dienstleistungen innerhalb eines Netzwerks dienen, entstehen Fehlanreize. Oftmals steht dieser Nützlichkeitsgedanke konträr zum Anteilsgedanken an dem Ökosystem, den dieselben Token oftmals gleichzeitig innehaben. Beispielsweise kann innerhalb bestimmter Ökosysteme ein Token zum Erwerb von Leistungen eingesetzt werden, besitzt allerdings auch einen fluktuierenden Anteilswert. Durch Verwendung der Token steigert man so den Anteilswert, den man aber selbst gleichzeitig damit einhergehend verliert. Abgese-

[107] Crowdfunding bezeichnet eine Finanzierungsart, bei der eine Gruppe von Individuen oder Organisationen durch Zusammenlegen ihrer Mittel Projekte finanziert.

[108] *Bambrough*, A Gold Standard Of ICOs Is Needed -- But It Won't Be Easy.

hen von handelbaren Token, deren Wert direkt durch den Markt bestimmt wird, bestehen auch Modelle, in denen Token an den Wert anderer Objekte, wie bspw. Fiat-Währungen, gekoppelt sind.

5.2.5.7 Dienstleistungen ohne Dienstleister

Im Zusammenhang mit der DLT werden regelmäßig zukunftsgerichtete Konzepte diskutiert, die an dieser Stelle zumindest erwähnt werden sollen. Ein häufig zu findendes Konzept ist das der dezentralen autonomen Organisation (DAO). Darunter versteht man eine Organisationsform, die rein auf Basis der DLT aufbaut und deren Regeln (und Geschäftsprozesse) vollständig in Smart Contracts implementiert sind. Eine DAO besitzt bspw. keine Geschäftsführung im klassischen Sinne, sondern die Entscheidungen werden sämtlich von Anteilseignern getroffen.

Dezentrale Autonome Organisationen (DAOs)

Dezentrale Autonome Organisationen koordinieren eine Gruppe von Individuen mit denselben Interessen und Zielen mittels Smart Contracts. Sie funktionieren gemäß festgelegter Governance-Regeln und mittels Token und bedürfen nach ihrer Umsetzung nicht mehr notwendigerweise menschlicher Beteiligung.[109]

In diesem Zusammenhang sind ebenso „Dienstleistungen ohne Dienstleister" denkbar. In Form von Smart Contracts verankerte digitale Dienstleistungen können – einmal veröffentlicht – ohne weitere Wartung durch den ursprünglichen Entwickler verfügbar bleiben, solange das zugrunde liegende DLT-System durch die Allgemeinheit (oder z. B. eine DAO) weiter betrieben, d. h. genutzt, wird. Damit entstehen gewissermaßen Dienstleistungen ohne Dienstleister – ein Zustand, der sich in der bisherigen ökonomischen Theorie nicht wiederfindet.

5.2.5.8 Ökonomisch autonome Maschinen

Autonom handelnde Maschinen (bspw. autonome Fahrzeuge) werden derzeit in erheblichem Ausmaß weiterentwickelt. So ist es nur eine Frage der Zeit, bis Maschinen auch miteinander wirtschaftlich autonom interagieren. Ohne zentrale Überwachung benötigt diese Interaktion eine Vertrauen stiftende Technologie wie die DLT. Durch parallele Entwicklungen in den Bereichen Künstliche Intelligenz und Internet der Dinge sind autonom agierende Maschinen in den kommenden Jahren in vielfältigen Anwendungsfeldern zu erwarten, so z. B. im Bereich der Mobilität (autonome Fahrzeuge), im Bereich Transport/Logistik (Drohnen) oder auch in der Industrie (Industrieroboter). Damit diese Maschinen ebenfalls wirtschaftlich interagieren können (bspw. Leistungen auf „Pay-per-Use"-Basis untereinander abzurechnen) könnte eine Blockchain als Infrastruktur dienen. Im Übrigen könnten dabei gleich die im Rahmen einer denkbaren Besteuerung von Roboterarbeit fälligen Abgaben automatisiert und auditierbar an den Fiskus getätigt werden.

5.2.6 Entscheidungskriterien für den Einsatz von Blockchain

Die Entscheidung über einen Einsatz der DLT muss differenziert betrachtet werden. Per Design steht ein verteiltes System herkömmlichen Technologien zur Datenspeicherung (z. B. zentralen Datenbanken) in vielem nach. Deshalb ist es wichtig, für jeden Anwendungsfall einzeln zu prüfen, ob der Einsatz der DLT einen deutlichen Mehrwert liefert. Zur Erleichterung dieser Entscheidung entwickelten Forschung und Praxis verschiedene

[109] *Shermin,* Strategic Change 2017, 499.

Vorgehensweisen mit zum Teil unterschiedlichem Fokus bzw. unterschiedlicher Schwerpunktsetzung. Das Weltwirtschaftsforum hat bspw. einen Entscheidungsbaum auf Basis relevanter Kriterien vorgestellt[110]. Unter diesen werden drei übergeordnete Ausschlusskriterien hinsichtlich der Verwendung der DLT angeführt. Das erste ist, ob ein Intermediär entfernt bzw. vermieden werden soll. Aufgrund des dezentralen Charakters der DLT entsteht in den meisten Fällen wenig zusätzlicher Nutzen, wenn eine zentrale Einheit das System ohnehin adäquat verwaltet und bestimmt. Das nächste Kriterium ist, ob das zu implementierende System mit digitalen oder digital abbildbaren Gütern arbeitet. Ist dies nicht der Fall, so können diese Güter auch nicht von der Blockchain verarbeitet werden. Diese Voraussetzung kann als ein grundlegendes Designprinzip in DLT-Systemen angesehen werden. Da eine der Kerneigenschaften der DLT die dauerhafte und veränderungssichere Speicherung darstellt, muss es außerdem möglich sein, eine permanente digitale Repräsentation des betreffenden Guts zu erstellen. Demgemäß wäre also von der Implementierung einer DLT abzusehen, wenn nicht sämtliche drei Kriterien erfüllt sind. Zu beachten ist, dass betriebswirtschaftliche Faktoren und die Kombination technischer Eigenschaften verschiedener DLT sowie unterschiedliche Generationen in der Studie des Weltwirtschaftsforums nicht berücksichtigt werden.

Konsolidiert man die bisherige Entwicklung von DLT, lassen sich regelmäßig vier technologische Eigenschaften identifizieren, aus welchen die Entscheidungskriterien der verschiedenen Tests abgeleitet werden. Mit dem Bitcoin-Protokoll wurde etwa ermöglicht einen Intermediär (im konkreten Fall: Banken) zu ersetzen. Als wesentliche technologische Eigenschaften bilden hierfür ein hoher Grad an Fälschungssicherheit und ein einziger gemeinsamer Informationsstand die Basis. Der hohe Grad an Fälschungssicherheit, der oftmals unkorrekterweise als unveränderlich beschrieben wird, wird durch den Proof of Work erreicht. Das Vorliegen eines einzigen gemeinsamen Informationsstands wird – unter Ausklammerung vorübergehender paralleler Führung zweier Ketten durch sogenannte „Forks" – dadurch erreicht, dass sich alle Parteien auf einen Zeitstempel einigen. Ethereum war die erste evolutionär bedeutende Weiterentwicklung des Konzepts „Blockchain", indem auf Protokollebene ermöglicht wurde sogenannte Smart Contracts (spätere Bezeichnung u. a. „Chaincode") und damit für alle Teilnehmer ausführbaren Code auf der Blockchain zu speichern. Hierdurch gewann der durch Blockchain für Organisationen generierbare Mehrwert eine neue Dimension: Abbildung und Ausführung von Logik über eine beliebige Menge an Teilnehmern. Somit wurde es ermöglicht bspw. organisationsübergreifendes Prozessmanagement zu betreiben. In diesem Fall geht es weniger um den Ersatz eines zentralen Prozessmanagers und damit eines Intermediärs, sondern ebenso um eine bestandssystemunabhängige Verbindung der Teilnehmer und Abbildung geteilter Logik. Seither sind zahlreiche weitere Bestrebungen zu konstatieren, bestimmte technologische Einschränkungen (z. B. die Nachhaltigkeit des Proof of Work, Interoperabilität verschiedener DLT-Technologien) zu adressieren, wobei die prägnanteste das Schaffen theoretisch unbegrenzter Skalierbarkeit ist. IOTA, als eine Distributed-Ledger-Technologie, versucht diese Eigenschaft etwa durch das Loslösen vom Grundkonzept der Blockchain und Umsetzen der Datenbankstruktur durch einen gerichteten azyklischen Graphen zu erreichen. Die Eigenschaft des gleichzeitigen gemeinsamen Informationsstands allerdings wird durch diese Technologie nicht erreicht.

Insbesondere das letzte Beispiel zeigt auf, dass die Entscheidungskriterien umfassend und flexibel sein müssen. Blockchain kann nicht ausschließlich auf einen Anwendungsfall eingegrenzt werden, was allerdings bspw. beim Entscheidungsbaum des Wirtschaftsforums durch den Fokus auf die Eigenschaft der Disintermediation erfolgt. Vielmehr muss eine Abwägung der aktuellen und sich stetig weiterentwickelnden Fähigkeiten der Distributed-Ledger-Technologie hinsichtlich eines konkreten Anwendungsfalls getroffen

[110] *Mulligan/Scott/Warren/Rangaswami*, Blockchain Beyond the Hype.

werden. Kombinationen aus Fälschungsresistenz, gleichzeitiger Information, geteilter Logik und hoher Skalierbarkeit werden durch die differenten Technologiederivate angestrebt und sind nur in der jeweiligen Form mit herkömmlichen Technologien in Vergleich zu setzen.

5.2.7 Blockchain als digitale Infrastruktur

Obwohl die DLT ursprünglich zur technischen Umsetzung einer digitalen Währung konzipiert wurde[111], sind insbesondere modernere Ausprägungen als generisch nutzbare digitale Infrastruktur anzusehen[112]. Diese Infrastruktur erlaubt es, ihre Eigenschaften wie bspw. Manipulationssicherheit über Schnittstellen für verschiedenartige Anwendungen nutzbar zu machen und diese zu verbreiten. Auf technischer Ebene interagiert die DLT dabei in der Regel mit herkömmlichen IT-Systemen und wird nicht als alleinstehende Infrastruktur genutzt.
Zur Verdeutlichung des Infrastrukturcharakters der DLT-Technologie eignet sich – vor dem Hintergrund der noch neuen und kaum erforschten Effekte auf Wirtschaft und Gesellschaft – eine Analogie aus einem sehr klassischen Bereich: Eine Stadt ist zweifelsohne verantwortlich für städtische Infrastrukturen wie bspw. deren Straßennetz oder auch zentrale Plätze. Um die Lebensqualität zu erhöhen, Gewerbe zu locken und dadurch Einnahmen zu generieren, nutzen Städte die grundlegende Infrastruktur „Straße", um höherwertige Infrastruktur wie „Wochenmarkt" bieten zu können. Auf dieser höherwertigen Infrastruktur werden dann wiederum Angebote privatwirtschaftlicher Anbieter gebündelt und zugänglich gemacht. In der Analogie wären die Straßen die im Rahmen des Breitbandausbaus vorangetriebenen Datenleitungen, das „Internet der Informationen" (siehe auch Abschnitt 5.2.4). Die Analogie zum Wochenmarkt wären DLT-basierte Infrastrukturen des „Internet der Werte und des Vertrauens". Auch auf Basis einer DLT-basierten Infrastruktur würde der Handel durch privatwirtschaftliche Anbieter getrieben. Eine zentrale Frage ist, wie in Deutschland solche Infrastrukturen aufgebaut werden können und wie insbesondere dahingehend sichergestellt werden kann, dass diese einem deutschen Rechts- und Wertesystem entsprechen und der deutschen Wirtschaft und Gesellschaft Mehrwert stiften. Ohne eine frühzeitige Klärung dieser Fragen und die Entwicklung darauf aufbauender Strategien für die Bundespolitik könnten sich langfristig andernfalls DLT-Infrastrukturlösungen aus dem Ausland durchsetzen.

Insbesondere durch die Verwendung von Smart Contracts und Token lassen sich Beziehungen und Interaktionen verschiedener Entitäten sehr gut abbilden. Diese Interaktionen finden auf unterschiedlichen Ebenen statt, wobei zumeist jeweils einschlägige Ausprägungen von DLT-Systemen verwendet werden. Beziehungen zwischen gleichgestellten Privatpersonen, die in der Regel keine bestehende Vertrauensbeziehung haben, lassen sich im ökonomischen Kontext unter dem Begriff Consumer-to-Consumer (C2C) zusammenfassen. Beziehungen zwischen Wirtschaftsunternehmen werden als Business-to-Business (B2B) bezeichnet. Auch Beziehungen, die Regierungsorganisationen involvieren, werden z. B. unter dem Begriff Government-to-Business (G2B) zusammengefasst.

In diesem Zusammenhang wird häufig postuliert, dass C2C-Beziehungen sich geeigneterweise mittels öffentlicher DLT-Systeme (vgl. technischer Teil) abgebildet werden, da sich die in die Beziehung involvierten Parteien nicht notwendigerweise vertrauen und somit eine allgemein zugängliche Infrastruktur mit objektiv verifizierbarer Manipulationssicherheit benötigen. Besonders solche DLT-Systeme sind als öffentliche digitale Infrastruktur anzusehen. Jedes Individuum oder jede Organisation kann an den entsprechenden Netzwerken teilnehmen, indem sie einen Netzknoten mit dem jeweiligen Protokoll

[111] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System.
[112] *Olnes* in Scholl/Glasseyet al., Electronic Government, 253; *Schlatt/Schweizer* et al., White paper / Fraunhofer Institute for Applied Information Technology FIT 2016.

betreibt. Genauso kann jede dieser Entitäten Anwendungen basierend auf der Infrastruktur entwickeln und somit z. B. Geschäftsmodelle umsetzen oder komplett eigennützige Anwendungen implementieren. Die öffentlichen Systeme zeigen folglich das Potenzial, neuartige Ökosysteme zu generieren, die auf den generischen Eigenschaften der DLT aufbauen. Technisch gesehen basiert die DLT wiederum selbst auf dem Internet als digitaler Infrastruktur. Ein klares und allgemein anerkanntes, vergleichbares Schichtenmodell fehlt der DLT allerdings aktuell noch. Zudem stellt die Vielzahl von öffentlichen DLT-Systemen, der Mangel an Standards und die oftmals fehlende Interoperabilität einzelner Systeme die Anwender bisweilen vor Herausforderungen. Dies ist in Anbetracht der notwendigen Skaleneffekte in öffentlichen DLT-Systemen problematisch. Neben generischen DLT-Systemen, die sich für allgemeine Anwendungen eignen, existieren auch domänenspezifische Systeme, die z. B. optimierte Protokolle für Finanzanwendungen bieten.

DLT als höherwertige digitale Infrastruktur

Die DLT als digitale Infrastrukturtechnologie für generische Dienstleistungen in verschiedenen Bereichen sollte weiter untersucht werden. Die DLT kann zur Umsetzung verschiedener Anwendungen dienen, die unabhängig vom Anwendungsbereich Nutzen für Privatpersonen und Unternehmen stiften können, wie zum Beispiel im Identitätsmanagement. Dafür ist Forschung zu Grundlagentechnologien und anwendungsübergreifenden Wertschöpfungsmodellen der DLT nötig. Insgesamt muss die DLT als digitale Infrastrukturtechnologie verstanden und gemanaged werden.

5.2.8 Informationelle Selbstbestimmung und digitale Souveränität

In den letzten Jahren sind die großen Digitalunternehmen, die u. a. auch unter dem Begriff FAANG (Facebook, Amazon, Apple, Netflix und Google) gebündelt werden, vermehrt im Zusammenhang mit exzessiver Datenspeicherung, Datengebrauch oder auch Datenmissbrauch in die Schlagzeilen geraten. Die wohl öffentlichkeitswirksamste Debatte fand im Anschluss an die US-Präsidentschaftswahlen 2016 statt, als bekannt wurde, dass die britische Firma Cambridge Analytica mit Millionen von Facebook-Profilen Wahlbeeinflussung betrieben haben soll. Die Daten der Nutzer wurden dabei ohne die Zustimmung und ohne das Wissen der Nutzer verwendet.

Solche und ähnliche Vorfälle zeigen deutlich, dass der Nutzer selbst zum einen oft wenig Wissen über, zum anderen häufig wenig Einfluss auf die Verbreitung seiner persönlichen (Nutzungs-)Daten hat, wenn er gängige Onlineservices nutzen möchte. Viele Smartphone-Apps geben Nutzungsdaten z. B. automatisiert an Facebook oder Google weiter, auch wenn die App selbst gar keinen direkten Bezug zu den Diensten hat. Forscher der Universität Oxford fanden bspw. heraus, dass über 90 Prozent aller Apps Trackingfunktionen beinhalten, die einem US-amerikanischen Unternehmen gehören[113]. Bei dem Umfang des Trackings liegt Alphabet, Googles Mutterkonzern, noch vor Facebook (44 Prozent) mit Abstand auf Platz 1 (88 Prozent)[114]. Eine Einschränkung dieses umfassenden Trackings ist für den Fall, dass die App eine Einschränkung zulässt, selbst für digitalaffine Nutzer oft nur sehr schwer möglich.

Dabei besagt das Recht der informationellen Selbstbestimmung, dass es das Recht des Einzelnen ist, über die Verwendung seiner personenbezogenen Daten selbst zu bestimmen. In diesem Zusammenhang wird häufig ebenfalls der Begriff „digitale Souveränität" eingestreut.[115] Zwar gibt es für den Begriff noch keine einheitliche Definition, mit digitaler Souveränität ist jedoch im Allgemeinen gemeint, dass der Einzelne befähigt wird, „sich selbstbestimmt in der digitalen Welt zu bewegen […] und [sein] Rechte auf informationelle Selbstbestimmung aktiv auszuüben"[116]. Dabei stellt der Begriff digitale Souveränität implizit einen stärkeren Bezug zu unserer heutigen, digitalisierten Welt und ihren Gegebenheiten und Herausforderungen her.

Die Datenschutzgrundverordnung adressiert bereits einige der Herausforderungen, die sich in diesem Zusammenhang ergeben. Beispielsweise werden darin Datenschutz und Datensicherheit von personenbezogenen Daten geregelt. So dürfen lediglich Daten vom Nutzer gesammelt werden, die auch für den Betrieb des jeweiligen Systems bzw. der jeweiligen Anwendung notwendig sind[117]. Überdies muss für den Nutzer Transparenz geschaffen werden, wie diese Daten gespeichert und verwendet werden. Dass diese und ähnliche Regelungen wohl häufig nicht eingehalten werden, zeigt die jüngst von der französischen Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) verhängte Rekordstrafe gegen Google. Google soll 50 Mio. Euro Strafe für die Verletzung von „Transparenz- und Informationspflichten" zahlen[118]. Für die Nutzer sei es nicht nachvollziehbar, wie Google ihre Nutzungsdaten verarbeite, heißt es. Zudem fehle Google eine spezifische Zustimmung der Nutzer, ihre Daten über verschiedene Dienste wie bspw. die Google-Suche, Google Maps oder YouTube hinweg zu verarbeiten[119].

[113] *Binns/Lyngs/Kleek/Zhao* et al., Proceedings of the 10th ACM Conference on Web Science 2018, 23.
[114] *Binns/Lyngs/Kleek/Zhao* et al., Proceedings of the 10th ACM Conference on Web Science 2018, 23.
[115] *Beyerer/Müller-Quade/Reussner,* DuD 2018, 277.
[116] *Beyerer/Müller-Quade/Reussner,* DuD 2018, 277.
[117] *Beyerer/Müller-Quade/Reussner,* DuD 2018, 277.
[118] *Böhm,* Spiegel Online 21.01.2019.
[119] *Böhm,* Spiegel Online 21.01.2019.

Hier zeigen sich exemplarisch einige fundamentale Probleme. Zum einen ist die Nutzung bestimmter Software ohne die implementierten Trackingfunktionen kaum möglich, da die Software ohne diese Funktionen schlicht nicht angeboten wird bzw. es Software ohne diese Funktionen am Markt kaum gibt. Zum anderen ist das Deaktivieren dieser Funktionen mit hohen Hürden für den Nutzer verbunden. Hinzu kommt der bereits mehrfach angesprochene Plattform- oder Netzwerkeffekt: Die Nutzung von weit verbreiteten Services, wie bspw. bestimmte Chatdienste, ist für viele Nutzer alternativlos, da nur diese Services eine entsprechend große Nutzerbasis aufweisen, um einen echten Mehrwert zu stiften. Um diese Services nutzen zu können, werden also eventuelle Datenschutzprobleme oder mangelnde Privatsphäre oft wissentlich oder unwissentlich in Kauf genommen.

Ein Übergang von diesem Status quo hin zu mehr digitaler Souveränität der Individuen, aber auch der Regierungen und der Unternehmen erfordert vermehrt Ansätze, welche die Entscheidungsgewalt aktiv in die Hände der Nutzer legen und nicht allein in die Hände von Softwareanbietern und Plattformbetreibern. Derartige Ansätze müssen in der digitalen Welt entsprechend softwarebasiert sein bzw. bei bestehenden Lösungen integrierbar sein. Damit die Anforderungen, bspw. der DS-GVO, erfüllt werden können, sind die verschiedenen rechtlichen Anforderungen technisch umzusetzen, wozu beispielhaft interoperable Datenformate und die Möglichkeit der Löschung von Daten notwendig sind[120]. Außerdem sind ebenfalls die ökonomischen und sozialen Aspekte – wie eben Plattform- oder Lock-in-Effekte – bei der Umsetzung zu beachten.

In der Realwelt ist die Souveränität über die persönliche Identität vergleichsweise einfach handhabbar. Ein häufig verwendetes Beispiel ist die Verifikation des Alters von Personen: Soll z. B. das Alter einer Person für den Kauf von Alkoholika oder bestimmten Computerspielen überprüft werden, so zeigt diese Person ihren Identitätsnachweis in Form eines Personalausweises oder Reisepasses beim Kauf vor. Über das Alter der Person hinaus sind in diesem einfachen Beispiel keine weiteren Daten relevant, werden also nicht benötigt und im Allgemeinen auch nicht erfasst. Wie bereits geschildert ist die Situation „Online" aktuell eine andere, denn ständig werden diverse Informationen über Personen gesammelt, verbreitet und ausgewertet.

Die DLT kann einen Beitrag dazu leisten, die exzessive Datennutzung zu adressieren, d. h., bspw. die Verwendung bestimmter Daten für andere als den konkreten Anwendungszweck auszuschließen und somit zu mehr digitaler Souveränität beizutragen. Sie kann zukünftig als Enabler-Technologie für eine digitale, selbst-souveräne Identität fungieren. Beispielsweise werden bezüglich digitaler Identitäten DLT-basierte Plattformen diskutiert und bereits entwickelt (vgl. Kapitel 5.2.5.5). Eine derartige Plattform stellt die Infrastruktur zur Verfügung, auf der jeder der Teilnehmenden seine digitale Identität aktiv verwalten kann. Dabei ist es von Relevanz, dass keine der Daten direkt auf der DLT-basierten Infrastruktur gespeichert werden, sondern die Blockchain nur als Verifikationslayer dient. In diesem Kontext ist die Sicherheit, die Kontrollierbarkeit sowie die Portabilität der Identität zentrale Bausteine[121]. Wie der Begriff bereits suggeriert, soll die Handhabe der persönlichen Identität vollständig dem Nutzer überlassen sein und damit die tatsächliche digitale Souveränität ermöglicht werden. Lediglich der Nutzer entscheidet, mit wem er welche Attribute seiner Identität teilt, z. B. können unabhängig voneinander Alter, Größe, Geschlecht, Kontakt- oder Zahlungsinformationen in verschiedenen Anwendungsfällen relevant sein. Diese Attribute können unabhängig voneinander genutzt werden.

[120] *Diepenbrock/Sachweh,* DuD 2018, 281.

[121] *Mühle/Grüner/Gayvoronskaya/Meinel,* Computer Science Review 2018, 80; *Tobin/Reed*, The Inevitable Rise of Self-Sovereign Identity.

Die Nutzung einer selbst-souveränen Identität soll am Beispiel der digitalen Altersverifikation kurz und vereinfacht dargestellt werden: Ein Nutzer meldet sich auf der Identitäts-Plattform an. Natürlich muss sein Alter zunächst verifiziert werden, bevor er bspw. altersabhängige Produkte wie Alkoholika kaufen kann. Es benötigt also bestätigende Instanzen, z. B. könnte der neue Personalausweis als Grundlage dienen, um das tatsächliche Alter des Nutzers zu verifizieren. Sind die Daten über das Alter des Nutzers verifiziert, ist nun der Nutzer allein dazu in der Lage zu bestimmen, mit wem er diese Informationen teilt. Wichtig ist dabei, dass die Informationen – bspw. das exakte Geburtsdatum – nicht öffentlich zugänglich auf der Plattform gespeichert sind. Vielmehr liegen nur Verweise auf die Daten in verschlüsselter Form vor und die Plattform dient zur Bestätigung von Attributen (wie dem Alter) gegenüber anderen Nutzern (wie einem Onlineshop). Somit kann der Nutzer nun beim Onlineeinkauf die Frage „Sind Sie über 18 Jahre alt?" mit „Ja" bestätigen, indem er das verifizierte Attribut „Alter" direkt mit dem Onlineshop teilt. Dabei muss nicht einmal die Information über das tatsächliche Alter geteilt werden, sondern lediglich die Information darüber, ob Max Mustermann bereits 18 Jahre alt ist (ja/nein). Ein solcher Prozess steht in engem Zusammenhang mit anderen digitalen Technologien bzw. Konzepten wie z. B. Secure-Multiparty-Computation[122,123].

In diesem Prozess ist die initiale Verifikation bestimmter Attribute ein häufiger Diskussionspunkt darüber, ob die DLT die beste technische Grundlage für ein solches System bildet. Da in diesem Prozess wiederum auf eine bestimmte verifizierende Instanz zurückgegriffen werden muss, steht die Frage im Raum, ob andere technologische Lösungen nicht ebenso geeignet sind. Es existieren mittlerweile verschiedene Start-ups, die sich zum Ziel gesetzt haben, DLT-basierte, digitale Identitäten zu entwickeln und entsprechende Plattformen zur Verfügung zu stellen, die dem Nutzer vollständige Privatsphäre und Kontrolle ermöglichen.

Konzepte auf DLT-Basis sind ein erster Schritt, der es technisch in der Zukunft ermöglichen kann, zu mehr digitaler Souveränität zu gelangen. Die reine technische Möglichkeit wird jedoch kaum ausreichen, vielmehr werden ökonomische und rechtliche Rahmenbedingungen notwendig sein, um tatsächlich eine Änderung im Umgang mit dem Thema informationeller Selbstbestimmung bzw. digitaler Souveränität herbeizuführen. In der Praxis wird sich wohl insbesondere die Frage stellen, wie der Weg vom Status quo „vollständiger Abhängigkeit von Plattform- oder Softwareanbietern" hin zu „vollständiger digitaler Souveränität des Einzelnen" gelingen kann. Verschiedene Aspekte werden diesbezüglich bereits diskutiert. Zum einen muss ein entsprechender Rechtsrahmen gegeben sein, um bspw. Verstöße gegen geltendes Recht auch gegen große Digitalunternehmen durchzusetzen[124]. Zudem ist es bereits aus rein marktwirtschaftlichen Perspektiven schwierig, die Speicherung und Verarbeitung von Daten, die von US-amerikanischen Unternehmen dominiert wird, auf europäische oder deutsche Rechtsräume einzuschränken. Die marktbeherrschenden Services werden in der Regel nicht von europäischen Unternehmen angeboten[125], denn europäische oder deutsche Alternativen zu vorrangig US-basierter Software sind rar. Auch in einer DLT-basierten IT-Infrastruktur sind diese Fragen zu klären, da zumindest in öffentlichen Blockchains keine räumliche Einschränkung gewährleistet werden kann. Zudem wird es für die Zukunft notwendig sein, dass die Nutzung neuer digitaler Services (wie bspw. intelligenter Assistenzsysteme für den Haushalt) auch unter Wahrung von Privatsphäre und Sicherheit möglich ist[126]. Technologische Weiterentwicklung darf nicht im Widerspruch zu digitaler Souveränität stehen. Dazu kann die DLT einen Beitrag liefern.

[122] *Zare-Garizy/Fridgen/Wederhake,* Security and Communication Networks 2018, 1.
[123] Siehe auch Abschnitt 5.1.3.
[124] *Beyerer/Müller-Quade/Reussner,* DuD 2018, 277.
[125] *Markl,* Informatik Spektrum 2018, 433.
[126] *Beyerer/Müller-Quade/Reussner,* DuD 2018, 277.

5.3 Aspekte der Realisierung/Umsetzung

5.3.1 Diffusion von DLT-basierten Innovationen

5.3.1.1 Volkswirtschaftliche Perspektive

DLT kann eine höherwertige, digitale Infrastruktur für effizientes Wirtschaften bieten. Dabei stellt sie jedoch für sich alleine genommen kein Geschäftsmodell dar. Trotz der starken Medienpräsenz innovativer Technologien und insbesondere der Blockchain herrscht mitunter in Politik, Wirtschaft und Gesellschaft noch eine Ungewissheit hinsichtlich der Potenziale von Blockchain und der Frage, ob und wie diese Potenziale zielführend genutzt werden können. Im Zuge der Digitalisierung und einer stetigen Verkürzung von Innovationszyklen suchen Unternehmen immer wieder nach Ideen und Ansätzen, um neue Geschäftsfelder zu erschließen oder bestehende Prozesse zu optimieren (vgl. Kapitel 5.2.7).

Prinzipiell ist jedoch nicht davon auszugehen, dass durch DLT bereits erfolgreich etablierte Intermediäre ersetzt werden. Ferner ist anzunehmen, dass zukünftig sowohl zentralisierte Plattformen als auch dezentrale, demokratisch organisierte DLT-Plattformen präsent sein werden und in verschiedenen Anwendungsbereichen koexistieren. Bei den heute weit verbreiteten Geschäftsmodellen auf Plattformbasis (bspw. Amazon, Uber) liegt der Wert für den Kunden meist in der Vielzahl an Interaktionen und Geschäftspartnern, die dort zur Verfügung stehen. Dies hat jedoch auch zur Folge, dass meist die gesamte Marktmacht bei (quasi-)monopolistischen Anbietern zentralisiert ist („Winner-takes-all-Prinzip"). Ein herkömmlicher, zentraler Plattformanbieter kann daher dabei unternehmerisch und souverän handeln, insbesondere kann er schneller und dynamischer auf positive und negative Externalitäten reagieren. Zudem verfolgt er mit der Plattform und ihrer Bereitstellung ein Eigeninteresse, sodass er Investoren leichter von der Rentabilität seines Geschäftsmodells überzeugen kann. Damit erlangen zentrale Plattformanbieter einen initialen Effizienzvorteil im Vergleich zu dezentralen Plattformen, welche eigenständig kein Geschäftsmodell darstellen und bei denen Entscheidungen von allen Teilnehmern (bzw. von einem Großteil der Teilnehmer) abgestimmt und mitgetragen werden müssen. Langfristig besteht allerdings für den Fall, dass die zentralen Plattformbetreiber ihre marktbeherrschende Stellung ausnutzen oder die Bedürfnisse der Kunden nicht hinreichend beachten (bspw. Datenschutz) durchaus die Möglichkeit, dass es zur Etablierung einer koordinierten, nachhaltigen Abwanderung zu einer DLT-basierten, neutralen und dezentral organisierten Alternative kommt. Da schließlich die Nutzer über den Erfolg einer Plattform entscheiden und auch unterschiedliche Präferenzen hinsichtlich der genannten Vor- und Nachteile besitzen, ist es wahrscheinlich, dass zukünftig zentralisierte und dezentrale DLT-basierte Plattformen nebeneinander koexistieren. Es ist davon auszugehen, dass in Bereichen, in denen sich eine zentrale Plattform durchgesetzt hat, bereits die Möglichkeit einer DLT-basierten, dezentralen Alternative ausreicht, um den Plattformbetreiber von den voranstehend beschriebenen monopolistischen Tendenzen abzubringen. Dies bedeutet, dass die Existenz einer potenziell realisierbaren DLT bereits als Marktkorrektiv fungieren kann.

Zudem kann der Einsatz von DLT in Anwendungsfeldern vielversprechend sein, in denen ein Intermediär nutzenstiftend wäre, der Markt oder das politische Umfeld diesen aber nicht hervorgebracht haben. So wäre es zwar auf absehbare Zeit zwar nicht sinnvoll, das Grundbuchamt in Deutschland durch eine DLT zu ersetzen. In Ländern, in denen solche Register jedoch nicht existieren oder nicht zuverlässig funktionieren (bspw. aufgrund von Korruption) kann es gleichwohl durchaus sinnvoll sein, ein entsprechendes System auf DLT-Basis einzuführen.

Eine allgemeine Voraussetzung für den erfolgreichen Einsatz von DLT ist die Digitalisierung der bestehenden, zu unterstützenden Prozesse.[127] Sodann können in der Folge verschiedene E-Government-Lösungen mit den Eigenschaften der DLT angereichert werden.

E-Government

E-Government bezeichnet die Verwendung von zumeist web-basierter Technologie, um verschiedenen Stakeholdern Dienstleistungen und Informationen der Regierung zugänglich zu machen.[128]

Die DLT bietet eine infrastrukturelle IT-Lösung für föderale Geschäfts- und Verwaltungsprozesse, in denen die Wahrung der Datensouveränität der jeweiligen Stakeholder und das Once-only-Prinzip eine wichtige Rolle spielen.

Once-Only-Prinzip

Das Once-Only-Prinzip beschreibt den Umstand, dass Bürger nur einmalig Informationen mit Regierungsbehörden teilen müssen, und stellt eines der zentralen Ziele der Digitalisierungsstrategie der Europäischen Union dar.[129]

Das Potenzial besteht im Allgemeinen vor allem dort, wo Prozesse organisationsübergreifende Kommunikation und Zusammenarbeit erfordern. Die aktuelle dezentrale Datenhaltung bei einer Vielzahl an Organisationen erschwert bei all ihren Vorteilen allerdings auch die Zusammenarbeit, da oft die wechselseitige Daten- und technische Integration fehlt. Im Bereich der Verwaltungsprozesse und Behörden wäre dies aus wirtschaftlicher Perspektive ein Grund für eine Integration der Daten, in welcher sämtliche Informationen aller Behörden vorgehalten werden würden („Bundesdatenbank“).

Da in Deutschland als föderalistischem Staat die zentrale Datenhaltung („der gläserne Bürger“) gerade vermieden werden soll, könnte die DLT dabei unterstützen, behördenübergreifende Prozesse abzuwickeln, ohne dass dafür eine zentrale Datenhaltung nötig wäre. Dies würde die Kommunikation erleichtern, die Zusammenarbeit unterstützen und gleichzeitig die Datensouveränität des einzelnen Bürgers stärken.

Die öffentliche Verwaltung benötigt für einen effizienten Einsatz von DLT das organisationale Wissen bezüglich behördeninterner und -übergreifender Prozesse, Know-how im Bereich Prozessreorganisation vor dem Hintergrund der Möglichkeiten der DLT, rechtlichen Sachverstand (bspw. in Bezug auf die Speicherung von Daten) sowie das technische Verständnis in der Umsetzung. Die Begleitung solcher Projekte kann dabei von Einrichtungen mit entsprechender Expertise geleistet werden.

In einer globalen Umfrage des Weltwirtschaftsforums wird von 73 Prozent der 816 befragten Experten aus dem Bereich der Informations- und Kommunikationstechnik erwartet, dass bereits im Jahr 2023 Steuern offiziell durch eine Regierung mittels DLT eingesammelt werden[130]. Im Folgenden sind drei weitere vielversprechende Anwendungen der

[127] *Nærland/Müller-Bloch/Beck/Palmund*, 38th International Conference on Information Systems (ICIS), 1.
[128] *Layne/Lee,* Government information quarterly 2001, 122.
[129] *TOOP Project*, Once-Only.
[130] *Global Agenda Council on the Future of Software & Society*, Deep Shift.

DLT im Bereich des E-Government aufgeführt: Zum einen kann ein digitaler Identitätsnachweis ohne Kommunikation irrelevanter identitätsbezogener Daten konzeptioniert werden. Dessen Kernelement ist die Schaffung einer sicheren DLT-ID, die einmalig durch eine vertrauenswürdige Instanz (z. B. Kommunen) verifiziert und danach durch Bürger genutzt werden kann. Des Weiteren bieten sich interessante Anwendungen für einmalig auf einer DLT-Anwendung dokumentierte Sachstände. Die zeitnahe und gesicherte Verteilung neuer Informationen an alle Teilnehmer eines Blockchain-Netzwerks ermöglicht zudem eine organisationsübergreifende Koordination von Geschäftsprozessen und Verwaltungsvorgängen. Die Sachstände können bspw. als Auslöser für den Beginn von Folgeprozessen bei anderen Behörden genutzt werden. Neben bisher dargestellten Anwendungsfällen verfügt die DLT auch über das Potenzial im demokratischen Prozess eingesetzt zu werden. Konkret kann die Technologie dabei helfen die Demokratisierung von Wahlen und Verwaltung voranzutreiben und gleichzeitig die Souveränität der Bürger zu stärken.

Die Digitalisierung von Wahlen geht generell mit hohen Sicherheitsanforderungen einher. Nicht nur Geheimhaltung und Anonymität sind hier problematisch, Wahlen sind ebenso attraktives Ziel für Manipulationsversuche. Mit ihrer Eigenschaft der Fälschungssicherheit, Unveränderbarkeit und Transparenz hat die DLT die Möglichkeit, bisherigen Problemen bei der Digitalisierung von Wahlen entgegenzuwirken und sogar einen sichereren Standard als papierbasierte Wahlen zu schaffen. Dies liegt darin begründet, dass auch auf Papier abgegebene Stimmen bei der Auszählung digitalisiert werden müssen, wodurch wiederum Fehler und Angriffspunkte entstehen. Die Nachvollziehbarkeit des Ergebnisses ist dann nur noch mit hohem Aufwand möglich. Bei mithilfe der DLT ausgeführten Wahlen ist der komplette Prozess von vornherein digital, gleichzeitig fälschungssicher und transparent. Die Identifizierung könnte dabei außerhalb dieses Systems erfolgen, etwa durch biometrische Merkmale wie Retina-, Handvenen- oder Fingerabdruck. Die Sicherstellung der Identifizierung ist nicht der Kern der DLT, sondern die Schnittstelle zum Nutzer. Hierbei ist jedoch besonders sorgfältig darauf zu achten, dass durch den Einsatz von DLT keine (ungewollten) Überwachungsmöglichkeiten entstehen. Zwar gibt es Ansätze und Pilotprojekte, wie ein solches System aussehen kann, jedoch bedarf es vor einem tatsächlichen Einsatz noch intensiver Forschung und Tests.[131] Auch bei behördenübergreifenden Prozessen und zwischenbehördlicher Kommunikation kann DLT helfen, einen gemeinsamen Informationsstand zu schaffen, ohne dass ein zentraler Datensatz für jeden Bürger nötig wäre. Am Beispiel des Bundesamts für Migration und Flüchtlinge wird nach erfolgreichen Tests bereits eine DLT-Lösung zur besseren behördenübergreifenden Zusammenarbeit pilotiert.[132]

Damit sich DLT in einem Anwendungsfall durchsetzen kann, muss eine relevante/kritische Masse vom Vorteil des Anwendungsfalls überzeugt sein. Die Herausforderung einer Anwendung von DLT besteht meist nicht in technischen oder rechtlichen Fragestellungen, sondern in politischen und organisatorischen Hürden. Auch wenn der Initialaufwand für den Einstieg niedrig ist, so ist die produktive Nutzung höchst aufwendig. Es bedarf einer kritischen Anzahl an Unternehmen, die sich an einer DLT-Anwendung beteiligen, um Vorteile der Netzwerkökonomie realisieren zu können. Selbst wenn DLT die Effizienz im Konsortium heben würde, müssen zunächst alle Stakeholder von der Sinnhaftigkeit einer solchen Lösung überzeugt werden. Dies führt in großen und dynamischen Konsortien zu Ineffizienz. Gleichzeitig gibt es Alternativen für Konsortien ohne die Anwendung einer DLT. Eine Möglichkeit sind Joint Ventures mit einem zentralen System, das nicht durch technische, sondern durch rechtliche Regeln gesteuert wird. Doch auch diese Kooperationsform ist oftmals mit Schwierigkeiten behaftet, die wiederum Chancen für DLT eröffnen. Oft scheitern Joint Ventures an einem Mangel an Vertrauen gegenüber

[131] *Kshetri/Voas*, Blockchain-Enabled E-Voting.
[132] *Fridgen/Guggenmos/Lockl/Rieger* et al., Bundesamt für Migration und Flüchtlinge 2018, 1

den anderen Partnern oder parteiischen Mitgliedern und daraus resultierender Korruption. Diese Problematik wird anhand der Frachtpapier-Thematik in Kapitel 7 dargestellt. Eine gezielte Förderpolitik kann den Zusammenschluss von Konkurrenten fördern, auch ohne den Einsatz von DLT. Damit förderungspolitische Akzente gesetzt werden können, scheint die Schaffung von Rechtssicherheit durch eine kartellrechtliche Einstufung notwendig

Eine weitere Herausforderung der Anwendung von DLT ist das geringe Verständnis der Marktakteure von dieser Technologie, sodass DLT oftmals nicht im Entscheidungsprozess der Unternehmen berücksichtigt werden. Dabei führt insbesondere die Rolle des Koordinators eines Konsortiums zu Verständnisschwierigkeiten und zwei möglichen Problemen. Erstens kann durch das fehlende technische Verständnis das Vertrauen in eine dezentrale Lösung fehlen. So ist es bspw. fraglich, inwiefern ein kleiner ÖPNV-Verbund die nötige Expertise zur Umsetzung und aktiven Beteiligung an Konzepten für dezentrale Mobilitätsplattformen wie OMOS hat. Zweitens kann es vorkommen, dass die Dezentralität eines Konsortiums durch den Koordinator lediglich vorgegeben wird. Eine Förderung des technischen Verständnisses von DLT und damit das Vertrauen in DLT ist deshalb insbesondere im deutschen Mittelstand von hoher Bedeutung, auch wenn das allein noch keinen produktiven Einsatz der Technologie ermöglicht. In großen DAX-Konzernen werden Investitionsentscheidungen oftmals von Entscheidungsträgern ohne technisches Hintergrundwissen über DLT getroffen. Dennoch können sich diese Unternehmen eine R&D-Abteilung zur Erforschung dieser Technologie leisten. Ein anderes Bild zeigt sich im deutschen Mittelstand. Diese Unternehmen sind meistens zu klein, um selbst aktiv Forschung zu einer solchen Technologie zu betreiben. Aus diesem Grund könnte eine Förderung des Wissensaufbaus insbesondere in einem Mittelstand-orientierten Land wie Deutschland förderpolitisch sinnvoll sein. Ein Konsortium aus Mittelständlern würde zur kritischen Masse beitragen und damit die Diffusion der Technologie beschleunigen. Auch wenn noch keine passenden Lösungen für diese Unternehmen auf dem Markt sind, so ist die Technologie dennoch reif genug, um dadurch frühzeitig Chancen zu nutzen und Wettbewerbsvorteile zu sichern. Durch die geringere Bedeutung des Mittelstands in anderen Ländern geht damit auch keine Gefahr eines Technologieabflusses einher.

5.3.1.2 Betriebswirtschaftliche Perspektive

Die DLT zählt als disruptive Technologie. Digitale Disruption beschreibt diejenigen Innovationen, die etablierte Technologien, Produkte oder Dienstleistungen weitgehend oder vollständig verdrängen. Für Unternehmen stellen sich diesbezüglich Fragen, die es zwar in der Vergangenheit in ähnlicher Form auch gab, die aber schlicht weniger selten und die vor allem nicht in dieser Breite relevant gewesen sind: Wie gehe ich mit den neuen Möglichkeiten und Herausforderungen um, welche die Digitalisierung mir als Unternehmen bietet?

5.3.1.2.1 DLT als disruptive Technologie

Wurde die Nutzung der DLT zunächst primär in der Finanzdienstleistungsbranche diskutiert, so sind in den vergangenen Monaten (Stand April 2019) diverse Unternehmen im Bereich DLT aktiv geworden und erarbeiten – oftmals in branchenspezifischen Konsortien – entsprechende Anwendungsfälle und Problemlösungen. Diese Entwicklung zeigt einen grundlegenden Unterschied zwischen disruptiven und traditionellen Technologien auf. So werden existierende oder sich entwickelnde Anwendungsfälle gesucht, in denen disruptive Technologien sinnvoll eingesetzt werden können (vgl. Abbildung 17). Dabei versuchen Unternehmen immer wieder, disruptiven Innovationen mit herkömmlichen Praktiken und Vorgehensweisen zu begegnen – und drohen dabei zu scheitern. Die Fehlinterpretationen namhafter Unternehmen (bspw. Nokia, Kodak) hinsichtlich disruptiver Technologien sind ebenso bekannt wie die negativen Auswirkungen und Schicksale.

Werden Trends falsch interpretiert, können aktuelle Technologieführer bereits in wenigen Jahren vom Markt verdrängt sein.

Abbildung 17: Disruptive Technologien bringen andere Voraussetzungen mit als normale Technologien

Bei „normalen“ Innovationen liegen bereits Anwendungsfälle vor, für deren Umsetzung eine passende Technologie gesucht wird. Im Falle von disruptiven Innovationen ist es demgegenüber meist so, dass zwar die Technologie bereits bekannt ist, deren sinnvoller Einsatz allerdings erst erörtert werden muss.

5.3.1.2.2 DLT erfordert ein anderes Innovationsmanagement

Vergangene Entwicklungen rund um die DLT weisen deutliche Analogien zu früheren Disruptionen auf. Folglich ist denkbar, dass es etablierten Marktteilnehmern ähnlich ergehen kann, wenn diese das Potenzial und die Auswirkungen der DLT falsch einschätzen. Bei der Evaluation disruptiver Technologien ist es wichtig, die Entwicklungen von Technologie, Markt und Wettbewerb umfassend im Blick zu behalten (bspw. im Branchenumfeld, in der generellen Technologieentwicklung). Der Fokus auf eine bestimmte Informationsquelle ist hier nicht empfehlenswert. Fokussiert man sich als Unternehmen zu stark auf die Wünsche und Erwartungen der Kunden – ein häufig propagierter Ansatz in Zeiten der Digitalisierung – kann dies dazu führen, dass der Blick „über den technologischen Tellerrand“ hinaus verloren geht und der Beobachtungshorizont zu stark eingeschränkt wird. Eine einfache Analogie verdeutlicht dies: Wären im frühen 20. Jahrhundert Kaufleute oder Unternehmer gefragt worden, wie in Zukunft der Atlantik schneller überquert werden könnte, so wäre vermutlich die bevorstehende nächste Generation schnellerer Schiffe die Antwort gewesen. Im Jahr 1919 folgte dann die Disruption: Der erste Transatlantikflug durch die Briten Alcock und Brown. Erst im Jahr 1927 gelang Charles Lindbergh mit seinem Flug von New York nach Paris der erste öffentlichkeitswirksame Transatlantikflug. Auch von der Schöpfung der ersten Bitcoins im Jahr 2009 bis zur breiten Öffentlichkeitswirksamkeit vergingen einige Jahre. Vermutlich wird es bis zur weit verbreiteten produktiven Nutzung der zugrunde liegenden DLT, noch einige Zeit dauern. Dennoch wäre es heute ein Fehler, die Technologie nicht in strategische Überlegungen einzubeziehen. Derzeit steht außer Frage, wie groß der Einfluss der DLT in den verschiedenen Branchen letztlich sein wird. Der aktuelle Hype Cycle von Gartner sieht Blockchain bzw. DLT kurz nach dem sogenannten Gipfel der überzogenen Erwartungen.[133] Während dies für DLT-Anwendungen nach den seit Mitte 2018 negativen Berichterstattungen insbesondere am Beispiel von Kryptobörsen erkennbar geworden ist, bleibt unklar, ob diese Einschätzung auch für DLT im Allgemeinen so getroffen werden kann.

Geht man davon aus, dass das Bündel an Technologien, welches wir in diesem Grundgutachten als DLT bezeichnen, an der Spitze der überzogenen Erwartungen steht , sind

[133] *Panetta*, Gartner Top 10 Strategic Technology Trends for 2019.

von dort aus grundsätzlich drei Szenarien denkbar (vgl. Abbildung 18). Erstens, die DLT wird ohne große Verzögerungen zu einer Standard-Technologie, die diverse Märkte und Branchen grundlegend verändert. Zweitens, nach dem derzeit zu beobachtenden Hype sehen wir zunächst eine Phase der Konsolidierung. Es zeigt sich im Laufe der Zeit, in welchen Anwendungsgebieten wirklich Vorteile der Anwendung von DLT liegen. In diesen Bereichen findet die Technologie produktive Anwendung. Drittens, das disruptive Potenzial der Technologie wird nach heutigem Stand in erheblichem Maß überschätzt, die bestehenden Herausforderungen können nicht überwunden werden, und die DLT wird zu einer Nischentechnologie. Es ist zu erwarten, dass DLT wie viele andere Technologien Szenario 2 durchlaufen wird. Innovative Unternehmen sollten daher Vorbereitungen für das „Plateau der Produktivität" treffen und sich nicht vom „Tal der Enttäuschung" abschrecken lassen.

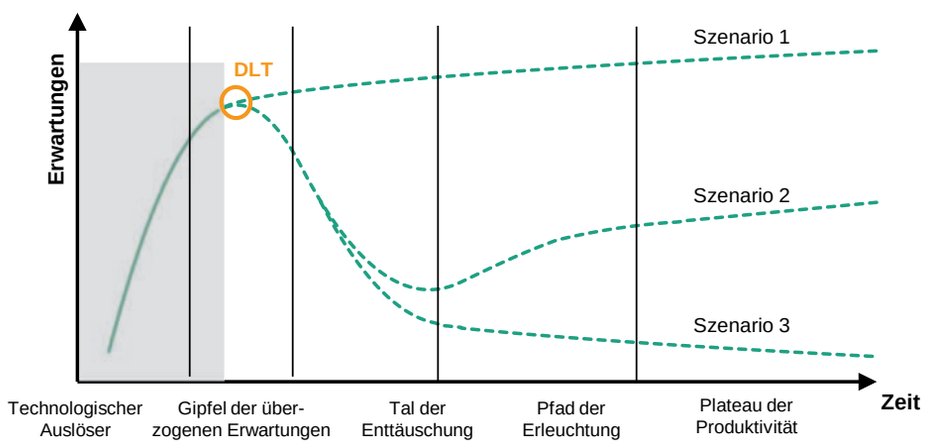


Abbildung 18: DLT auf dem Gipfel der überzogenen Erwartungen: Von hier sind drei grundsätzliche Szenarien denkbar.

Dazu gehen Unternehmen im Idealfall mehrstufig vor (vgl. Abbildung 18). Wichtig ist hierbei in allen Branchen gleichermaßen, dass sowohl Mitarbeiter mit fachlichem als auch mit technischem Hintergrund in den Innovationsprozess involviert werden. Nur auf diese Weise kann gewährleistet werden, den disruptiven Charakter der Technologie auch über die verschiedenen Ebenen eines Unternehmens hinweg zu betrachten. Mitarbeiter mit Expertenwissen auf Infrastruktur- oder Anwendungsebene haben häufig einen anderen Blickwinkel als Verantwortliche für das Geschäftsmodell eines Unternehmens. Diese verschiedenen Perspektiven sind jedoch wichtig, um die gesamte Breite möglicher Anwendungen sowie deren Implikationen zu erfassen. Ein Beispiel für die erfolgreiche Anwendung des Vorgehensmodells ist in Fridgen et al. (2017) dargestellt.

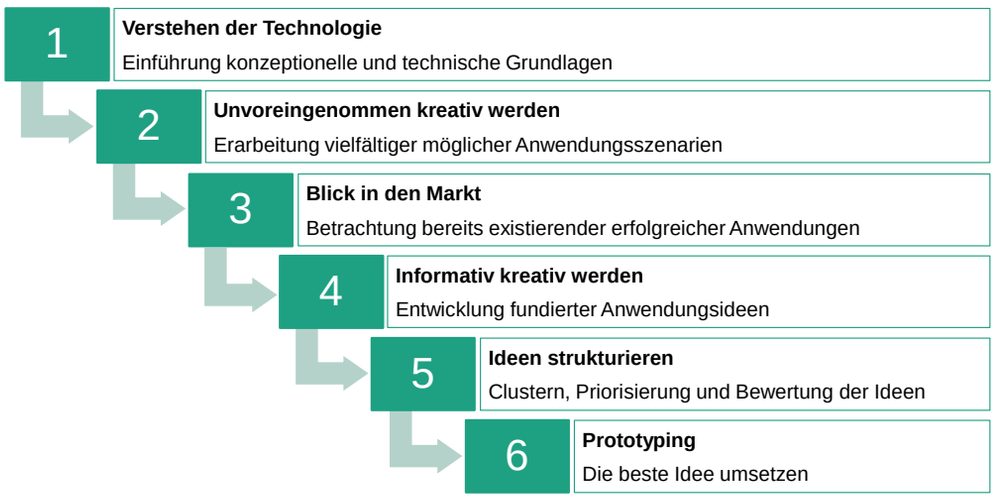


Abbildung 19: Vorgehensmodell im Umgang mit disruptiven (digitalen) Technologien

1. Verstehen der Technologie: Einführung in konzeptionelle und technische Grundlagen
In den meisten Fällen haben sich Unternehmen und deren Mitarbeiter bislang nur sehr rudimentär mit der DLT beschäftigt, wodurch das Know-how entweder fehlt oder sich auf einzelne Anwendungen wie Kryptowährungen beschränkt. Damit jedoch alle beteiligten Mitarbeiter das Potenzial der DLT erkennen, überzogene Erwartungen vermeiden und möglichst genau die Auswirkungen auf das eigene Unternehmen sowie auf die eigene Branche beurteilen können, bedarf es einer umfassenden Aufarbeitung der konzeptionellen und technischen Grundlagen. Für diese Stufe des Vorgehensmodells sollte ausreichend Zeit eingeräumt werden, da diese das Fundament jeglicher weiterer Bestrebungen bildet und für die Entwicklung und Diskussion möglicher DLT-Anwendungen unumgänglich ist.

2. Unvoreingenommen kreativ werden: Erarbeitung möglicher Anwendungsszenarien
Im Anschluss an die Aufarbeitung der Grundlagen und Eigenschaften der DLT bietet es sich an, sich potenziellen Anwendungen unvoreingenommen und mit Kreativität zu nähern. Dabei kann es in dieser Stufe sinnvoll sein, Mitarbeiter einzubeziehen, die bisher noch keine Berührungspunkte mit der Technologie hatten, um eine solche unvoreingenommene Kreativität zu ermöglichen. Im Rahmen eines Kreativ-Workshops sollten die folgenden Fragen im Fokus stehen: Wie könnte Ihr Unternehmen die Technologie nutzen? Welcher Intermediär stört Ihr Unternehmen aktuell am meisten? Sind die Daten Ihres Unternehmens in bestimmten Prozessen stark manipulationsgefährdet? Welche Prozesse dauern zu lange? Welche Prozesse haben (zu) viele Beteiligte? Für welchen Prozess und welche Dienstleistung zahlt Ihr Unternehmen zu viel?

3. Blick in den Markt: Betrachtung bereits existierender erfolgreicher Anwendungen
In einem weiteren Schritt werden bereits vorhandene Projekte der gleichen Branche betrachtet und analysiert. Auch ein Blick „über den Tellerrand" hinaus, der andere Perspektiven und Anwendungsbereiche für die Technologie aufzeigt, ist empfehlenswert. Dieser Schritt vermittelt ein sehr gutes Verständnis darüber, was mögliche Rahmenbedingungen sein könnten und wie es um den Reifegrad der Technologie bestellt ist.

4. Informiert kreativ werden: Erarbeitung weiterer Anwendungsideen
Hat man sich auf diese Art und Weise mit den existierenden Anwendungsmöglichkeiten vertraut gemacht, empfiehlt es sich, mit einem weiteren Workshop auf die gesammelten Eindrücke aufzubauen und sich wiederum die Frage zu stellen: Wie könnte Ihr Unternehmen diese Technologie nutzen? Die erneuten Überlegungen hinsichtlich möglicher An-

wendungsfälle können erfahrungsgemäß in diesem Schritt bereits zu detaillierten Zwischenergebnissen führen, da die Erkenntnisse und Erfahrungen aus der Marktbetrachtung einfließen.

5. Ideen strukturieren: Clustering, Priorisierung und Bewertung der Ideen
Durch die vorherigen Stufen wurde bereits eine gewisse Anzahl an möglichen DLT-Anwendungsfällen identifiziert. Daraus sollten nun die vielversprechendsten Anwendungsfälle ausgewählt werden, welche für eine weitere nähere Betrachtung geeignet sind. Dabei kann mittels ausgewählter Kriterien und Fragestellungen relativ rasch ein guter, detaillierter Überblick über die Eignung möglicher Anwendungsfälle entstehen. Eine exemplarische Fragestellung für die Konsolidierung ist bspw.: Wie sähe der Prozess mit DLT im Vergleich zum Status quo aus und welche Vorteile bzw. Nachteile treten dadurch auf? Bleiben auf diese Weise noch immer viele Erfolg versprechende DLT-Anwendungsfälle, sollte eine weitere Konsolidierung in Betracht gezogen werden. Beispielsweise kann ein zielführendes Vorgehen darin bestehen, die Anwendungsfälle auszuwählen, die möglichst wenig Komplexität aufweisen und die Eigenschaften der Technologie gut zum Ausdruck bringen. Überdies sollten die Entwicklungsprozesse und die Erkenntnisse daraus gut auf weitere Anwendungsfälle übertragbar sein.

6. Prototyping: Umsetzung der besten Ideen
Bei der prototypischen Umsetzung ist das Ziel nicht notwendigerweise, sofort eine marktreife Lösung zu entwickeln. Vielmehr geht es darum, im Unternehmen umfängliches Know-how aufzubauen, um auf zukünftige Entwicklungen schnell reagieren zu können. Zur Realisierung der ausgewählten Anwendungsfälle empfiehlt sich ein agiles Vorgehen, um iterativ vom initialen Beispiel bis zur produktiven Anwendung zu gelangen. Durch das iterative Vorgehen können schnell erste Ergebnisse erzielt werden, die zur Kommunikation und Aufklärung über die Technologie im Unternehmen eingesetzt werden können. Des Weiteren ermöglicht diese Umsetzungsweise rasch auf Änderungen bspw. durch neue Erkenntnisse aus der DLT-Entwicklung eingehen zu können.

Die Digitalisierung und insbesondere disruptive Technologien üben einen weitreichenden Einfluss in fast allen Gesellschaftsbereichen, Branchen und Unternehmen aus. Dabei betreffen die damit verbundenen Veränderungen oftmals alle Bereiche eines Unternehmens, von der Infrastruktur bis zum Geschäftsmodell. Von der Entwicklung neuer Produkte und Dienstleistungen bis hin zur Verdrängung von „Big Playern" und der Generierung neuer Märkte sind dabei viele Entwicklungsszenarien denkbar. Unternehmen stellen sich die Frage, wie sie in diesem komplexen Umfeld mit den Entwicklungen Schritt halten können. Häufig fehlt ein Konzept, das auf diese Umstände und das Management disruptiver Innovationen zugeschnitten ist. Am Beispiel Blockchain wird deutlich, dass sich die Technologien rapide entwickeln. Auch wenn ihr volles Potenzial von niemandem völlig absehbar ist, sollten sich Unternehmen mit ihnen beschäftigen. Es ist empfehlenswert, sich als vorausschauendes Unternehmen mit kontinuierlichem Know-how-Aufbau aktiv mit Blockchain zu beschäftigen.

Doppelstrategie zur Innovationsdiffusion

Für die Innovationsdiffusion scheint eine Doppelstrategie ratsam. Dabei ist zum einen eine „Push"-Strategie empfehlenswert: KMUs sollten gezielt mit verschiedenen Mitteln angesprochen werden. Dies kann die Ansprache über Branchenverbände mit einer Multiplikatorwirkung beinhalten, oder auch eine Verbreitung mittels Dialogveranstaltungen umfassen. Zum anderen sollte eine „Pull"-Strategie angewendet werden: Dies umfasst die Nutzung bestehender niederschwelliger Instrumente wie des mFUND-Förderprogramms und die Förderung von strategischen Leuchtturmprojekten. Im Idealfall sind die entsprechenden Projekte synergetisch mit anderen nationalen bzw. internationalen Zielen, wie der Verbreitung der Elektromobilität und erzeugen weitgehendes Interesse.

Um die Möglichkeiten von DLT hinreichend zu verstehen und Anwendungsfälle zu identifizieren, bedarf es eines Vorgehens, das analytische Ansätze und kreative Methoden kombiniert. Unternehmen sollten den Markt beobachten und sich mit anderen und durchaus in Teilbereichen konkurrierenden Unternehmen austauschen: Sowohl in ihrer Branche als auch darüber hinaus lohnt es sich oftmals, die aktuellen technologischen Entwicklungen im Blick zu behalten.

5.3.2 Hemmnisse

5.3.2.1 Energieverbrauch und Transaktionsgeschwindigkeit

Ein häufig genannter Kritikpunkt an der DLT ist die niedrige Transaktionsgeschwindigkeit bei einem gleichzeitig hohen Energieverbrauch. Im Folgenden soll in kompakter Form auf diese beiden Sachverhalte eingegangen und ihr Bezug zur DLT hergestellt werden.

5.3.2.1.1 Transaktionsgeschwindigkeit

Die Transaktionsgeschwindigkeit und der Stromverbrauch eines DLT-Systems hängen im Wesentlichen mit dem jeweils eingesetzten Konsensmechanismus zusammen. Insgesamt existieren mittlerweile über 30 verschiedene Konsensmechanismen, von denen der Proof of Work nach wie vor der bekannteste ist. Dies ist auf seine lange Historie und die enge Verknüpfung mit dem Bitcoin-System zurückzuführen. Dementsprechend wird dieser häufig für Vergleiche herangezogen und als Standard bzw. Repräsentant für alle anderen DLT-Systeme gesehen. Dabei ist jedoch zu beachten, dass der Vergleich eines auf dem Proof of Work aufbauenden DLT-Systems mit zentralen Datenbanken oftmals nicht mehr dem aktuellen technischen Stand entspricht. Alternative Konsensmechanismen implizieren verschiedene Effizienzvorteile; ein Überblick ist dem Abschnitt 4.2.2 zu entnehmen.

Generell ist die Transaktionsgeschwindigkeit eines DLT-basierten Systems aus zwei wesentlichen Gründen niedriger als bei einer zentralen Datenbank. Zum einen erfordert der Konsensmechanismus typischerweise Verifikationen und iterative Kommunikation mit anderen Teilnehmern im Netzwerk, was sich bei einer weltweiten Kommunikation schnell aufsummiert. Zum anderen müssen durch die Dezentralisierung alle Transaktionen redundant in allen, bzw. in einer Teilmenge aller Netzwerkknoten gespeichert werden. Insbesondere bedeutet dies, dass jede Transaktion jedem Netzwerkknoten mitgeteilt und von diesem verarbeitet werden muss.

Die Transaktionsgeschwindigkeit eines DLT-Systems hängt in erheblichem Maß mit der Frage zusammen, wie dieses ausgestaltet ist. Öffentliche und zulassungsfreie DLT-Systeme weisen in der Regel eine niedrigere Transaktionsgeschwindigkeit als private und

zulassungsbeschränkte auf. Dies ist auf die unterschiedlichen Sicherheitsanforderungen an die DLT-Systeme zurückzuführen. Während sich bei öffentlichen zulassungsfreien DLT-Systemen (bspw. Bitcoin-Blockchain) jeder an der Erzeugung neuer Blöcke beteiligen kann, ist dieses Recht bei einem privaten zulassungsbeschränkten DLT-System wie bspw. Hyperledger Fabric nur bestimmten Nodes vorbehalten. In der Regel gilt: Je offener ein DLT-Netzwerk ist, desto höher sind die Sicherheitsanforderungen und desto langsamer dessen Konsensmechanismus. Dies ist darauf zurückzuführen, dass in öffentlichen, zulassungsfreien DLT-Systemen grundsätzlich Misstrauen gegenüber anderen Netzwerkteilnehmern herrscht. Weiterhin tritt jeder Teilnehmer unter einem Pseudonym auf und ist somit quasi unbekannt. Im Gegensatz dazu besteht in einem privaten, zulassungsbeschränkten DLT-System immer ein Mindestmaß an Vertrauen. Dieses Mindestmaß an Vertrauen beruht auf der allgemeinen Bekanntheit der Netzwerkteilnehmer, die neue Blöcke erzeugen dürfen. Sollte sich dort ein Netzwerkknoten schädlich verhalten, trägt dies dazu bei, dass einzelne Nutzer leicht identifiziert und gegebenenfalls juristisch belangt werden können. Letztlich führt das Basisvertrauen zu geringeren Sicherheitsanforderungen an den Konsensmechanismus, wodurch dieser schneller und effizienter ausgestaltet werden kann.

Für öffentliche DLT-Systeme stellt die Transaktionsgeschwindigkeit aktuell noch einen Flaschenhals dar – es ist jedoch zu erwarten, dass mit Weiterentwicklung von Konsensalgorithmen, wie etwa Proof of Stake[134], auch die Performanz von öffentlichen DLT-Systemen wächst. Auch die Entwicklung neuer Datenstrukturen, wie etwa gerichteten azyklischen Graphen (DAGs)[135], könnte deutlich höhere Transaktionsgeschwindigkeiten ermöglichen. Auch wenn DLT-Systeme in der Regel nicht die Leistungsfähigkeit und Effizienz eines zentralen Systems erreichen, so ist dennoch anzumerken, dass durchaus eine Reihe von Anwendungen existiert, in denen eine niedrige Transaktionsgeschwindigkeit ausreichend ist. In Bezug auf ökonomische Aspekte ist die Transaktionsgeschwindigkeit insofern relevant, als dass die resultierenden Effizienzverluste für jede Anwendung gesondert berücksichtigt werden müssen. Dadurch können sich bei Einführung DLT-basierter-Lösungen in ein System erhebliche Veränderungen gegenüber aktuellen Prozessabläufen ergeben, weswegen eine spezifische Betrachtung der Implikationen für jeden Anwendungsfall anzuraten ist.

5.3.2.1.2 Energieverbrauch

Neben der niedrigeren Transaktionsgeschwindigkeit wird in der Öffentlichkeit oftmals der Energieverbrauch von Bitcoin thematisiert. Dabei ist zu beachten, dass der Konsensalgorithmus Proof of Work, der bei Bitcoin eingesetzt wird, gezielt so konzipiert ist, dass er rechen- und damit energieintensiv ist. Die damit verbundenen Kosten des Minings sind für das Anreizsystem essenziell. Der Anspruch des rechenintensiven Rätsels und damit auch die Energieintensität des Minings werden regelmäßig angepasst. Der Energieverbrauch von Bitcoin skaliert dabei nicht mit der Anzahl von Transaktionen pro Sekunde – diese wird nur künstlich beschränkt, um die Menge an Daten, die jeder Netzwerkknoten verarbeiten und speichern muss, zu beschränken. Vielmehr wächst der Energieverbrauch mit dem Aufwand, den die Miner auf sich nehmen, um neue Blöcke zu generieren und damit die Belohnung in Form einer bestimmten Menge an Bitcoin zu erhalten. Andere Konsensmechanismen, wie etwa Proof of Stake[136], könnten dazu führen, dass der Energieverbrauch derartiger DLT-Systeme im Vergleich zu Bitcoin vernachlässigbar wird.

[134] Siehe hierzu auch Abschnitt 4.2.2.
[135] Wie bei IOTA eingesetzt, siehe auch Abschnitt 4.3.8.
[136] Siehe hierzu auch Abschnitt 4.2.2.

Die Datenhaltung selbst ist im Vergleich zur Berechnung deutlich weniger energieintensiv, und neuere Entwicklungen (etwa Memristoren) könnten die Speicherproblematik noch weiter entschärfen. Darüber hinaus gibt es technische Ansätze, um besonders bei öffentlichen DLT-Systemen die Menge an zu verarbeitenden und zu speichernden Datenmengen zu reduzieren, wie etwa Sharding[137]. Die nachfolgende Tabelle 2: Dauer von 100 000 Transaktionen bei maximaler Kapazität gibt einen abschließenden Überblick über den Energieverbrauch und die durchschnittlichen Transaktionsgeschwindigkeiten verschiedener DLT-Systeme im Vergleich zu herkömmlichen Werttransfersystemen.

Tabelle 2: Dauer von 100 000 Transaktionen bei maximaler Kapazität

VISA	ripple	NANO	Ethereum	Bitcoin
1,8 Sek	2 Sek	10 Sek	2 Std	4 Std
Betriebsdauer einer Glühbirne (60 Watt) äquivalent zum Stromverbrauch für eine Transaktion[138]				
1 Std 48 Min	11 Sek	3 Tage 11 Std	1 Jahr 118 Tage	9 Jahre 187 Tage

5.3.2.2 Sicherheit, Missbrauch und Kriminalität

DLT ist keine Technologie, die Kriminalität ausschließlich erschwert oder ausschließlich erleichtert. Vielmehr kommt es auf die Ausgestaltung der DLT-Anwendung an. Durch die Möglichkeiten, Transaktionen pseudonym oder anonym zu gestalten, können die angesprochenen Problematiken natürlich verschärft werden. Entsprechend wichtig ist, dass diese Herausforderungen bereits in der Entwicklungsphase von DLT-Anwendungen im Zahlungsverkehr diskutiert und technische sowie organisatorische Lösungsmöglichkeiten erarbeitet werden.

Ein Ansatz könnte die Einführung einer offiziellen Europäischen Digitalwährung (bspw. e Euro, Krypto-Euro) als rechtskonforme Basiseinheit für DLT-Anwendungen sein. Dieser Vorschlag wurde im November 2018 ebenfalls von der Direktorin des Internationalen Währungsfonds Christine Lagarde im Rahmen des Singapore Fintech Festivals in einer Rede eingebracht.[139] Durch die eindeutige Identifikation von (juristischen) Personen und die mögliche Nachvollziehbarkeit von Transaktionen könnten Kryptowährungen auch solche Anwendungen ermöglichen, die Kriminalität sogar leichter bekämpfbar machen und dennoch in ihrer Ausgestaltung unseren Ansprüchen an Sicherheit, Verbraucherschutz und Datenschutz gerecht werden.

5.3.2.2.1 Verlust oder Diebstahl von Passwörtern bzw. privaten Schlüsseln

Die derzeit wohl größte grundsätzliche Sicherheitsproblematik für DLT-Implementierungen besteht im Zusammenhang mit privaten Schlüsseln, die in asymmetrischen Kryptosystemen benötigt werden. Der Verlust des privaten Schlüssels durch technische Defekte, Diebstahl oder schlicht Unachtsamkeit und Vergessen führt bspw. dazu, dass bei Kryptowährungen kein Zugriff mehr auf selbige besteht. Anders als bei Systemen, die durch einen Intermediär wie eine Bank betrieben werden, ist es in DLT-Systemen in der Regel

[137] Siehe auch Abschnitt 4.2.3.
[138] *Brandt*, Neue Kryptoprojekte bald so effizient wie Visa.
[139] *Christine Lagarde* 14.11.2018.

nicht möglich, den Schlüssel wiederherzustellen. Für Kryptowährungen bedeutet das: Das Geld ist verloren.

Das zeigt auch das aktuelle Beispiel der kanadischen Krypto-Börse QuadrigaCX. Deren Gründer kannte als einziger bestimmte Schlüssel, die Zugriff auf die Einlagen der Börse erlauben und ist im Dezember 2018 unerwartet verstorben. Dies hat zur Folge, dass die Börse nach eigenen Angaben auf Einlagen in Höhe von ca. 190 Mio. Euro nicht mehr zugreifen kann.[140] Aufgrund der gleichen Problematik gelten nach Angaben der Firma Chainalysis bspw. bis zu 23 Prozent aller Bitcoin als verloren.[141]

Ein weitläufig bekannt gewordenes Angriffsmuster ist der Diebstahl von Kryptowährungen im großen Stil. Die großen Diebstähle oder Angriffe waren stets darauf zurückzuführen, dass Anbieter von Kryptobörsen angegriffen und die verwahrten Coins entwendet wurden (ein prominentes Beispiel ist hier der mittlerweile insolvente japanische Anbieter MtGox[142]). Diese Angriffe betreffen jedoch nicht die eigentliche DLT, sondern eher die IT-Sicherheit dieser Börsen – sie sind eher vergleichbar mit einem klassischen Bankraub.

Um das Problem des Schlüsseldiebstahls- bzw. -verlusts zu umgehen, können diese Schlüssel bspw. wiederum von Intermediären oder Softwareanbietern aufbewahrt werden, z. B. in sogenannten Wallets. Die Anbieter dieser Wallets verwahren diese, was die Wahrscheinlichkeit des Totalverlusts mindert. Im Gegenzug ist diese Lösung jedoch problematisch, da die Walletanbieter ein sehr attraktives Ziel für Kriminelle darstellen und daher in der Vergangenheit häufig Opfer von Hackerangriffen wurden. Befinden sich die Schlüssel einmal in den Händen von Kriminellen, können diese frei über die Gelder verfügen. Auf diese Weise wurden in den vergangenen Jahren Gelder (Kryptowährungen) in Milliardenhöhe entwendet.[143]

Das gleiche grundsätzliche Problem, das sich am Beispiel von Kryptowährungen gut nachvollziehen lässt, besteht auch für viele weitere Anwendungsfälle. Gelangen Kriminelle in den Besitz privater Schlüssel, können sie damit Transaktionen ausführen oder bspw. Prozessschritte fälschlich signieren. Es hängt vom Anwendungsfall ab, was die konkreten Konsequenzen sind, wobei dies häufig einem Identitätsdiebstahl gleichkommen könnte.

Es sollte hervorgehoben werden, dass DLT-Systeme selbst als vergleichsweise sicher gelten. Die geschilderte Problematik ist in ähnlicher Form bei anderen IT-Systemen ebenfalls vorhanden. Wie bei allen anderen IT-Systemen auch ist jedoch die Gesamtheit aller Sicherheitsvorkehrungen entscheidend. Gerade durch die rasante Entwicklung von Kryptowährungen wurden oder konnten diese jedoch zum Teil nicht mit gebührender Sorgfalt umgesetzt werden, was zu den geschilderten Situationen führte.

5.3.2.2.2 DAO-Hack

Im Jahr 2015 begann das DLT-Start-up „Slock.it" mit der Entwicklung eines Frameworks für Dezentrale Autonome Organisationen (DAOs) auf Basis der Smart-Contract-Programmiersprache „Solidity" von Ethereum.[144] Die Idee war es, einen Open-Source-Standard für zukünftige dezentrale Organisationen zu schaffen. Im März 2016 veröffentlichte

[140] *Martin-Jung,* Süddeutsche Zeitung 04.02.2019.
[141] *Dittmer,* n-tv 29.11.2017.
[142] Siehe https://www.mtgox.com/.
[143] *Martin-Jung,* Süddeutsche Zeitung 04.02.2019.
[144] *DuPont,* Bitcoin and Beyond 2017, 157.

Christoph Jentzsch, ein Mitarbeiter von Slock.it, das entsprechende Whitepaper, in dem der DAO-Code zur Automatisierung von organisatorischer Steuerung und Entscheidungsfindung beschrieben wird.[145] Um das Projekt herum entstand eine bedeutende Community und startete das DAOhub-Forum, um das Projekt unabhängig von Slock.it zu machen. Die DAOhub-Gemeinschaft wählte eine Gruppe von 12 Kuratoren, die für die Unterstützung des Projekts verantwortlich waren. Das entsprechende Projekt hieß „The DAO" und sollte die „Mutter aller DAOs" sein.[146] Am 30. April 2016 wurde The DAO gegründet und konnte innerhalb der 4-wöchigen Gründungsphase über ein DLT-basiertes Crowdfunding Mittel in Höhe von 250 Millionen US-Dollar sammeln.[147] Etwa sechs Wochen später nutzte eine unbekannte Person eine Schwachstelle im Smart-Contract-Code von The DAO aus, räumte die zugehörigen Adressen und erlangte über 3,6 Millionen Ether, die zu diesem Zeitpunkt einem Wert von 70 Millionen US-Dollar entsprachen.[148] Sofort traten Slock.it, zahlreiche Kryptowährungsbörsen und andere informelle technische Meinungsführer ein, um die daraus resultierenden Schäden einzudämmen, den Verkauf auf Börsen zu verhindern und Gegenangriffe zu starten. Letztlich wurde das gesamte Projekt allerdings terminiert und ein Hard Fork der Ethereum-Blockchain durchgeführt, um einen früheren Zustand des eigentlich „unveränderlichen" Ledgers herbeizuführen.[149]

In dem genannten Szenario wurden fehlerhafte Smart Contracts gezielt durch Angreifer ausgenutzt. Somit war hierbei nicht das Protokoll der DLT, in diesem konkreten Fall die Ethereum-Blockchain, selbst betroffen. Vielmehr wurde der fehlerhafte Quellcode eines durch einen Nutzenden hochgeladenen Programms zum Ziel. Um derartigen Vorfällen zukünftig vorbeugen bzw. diese komplett vermeiden zu können, ist zu erwarten, dass für häufig genutzte Anwendungsfälle Muster und Vorlagen für Smart Contracts entstehen werden. Um hierfür verlässliche Standardbausteine zu entwickeln, bedarf es der Etablierung von Zertifizierungsstellen und technischen Prüfinstanzen, die Smart Contracts auf ihre Prozess- und Anwendungsintegrität testen, sowie Bibliotheken und Marktplätzen, über die Smart Contracts zur Verfügung gestellt werden. Außerdem sollten Warnsysteme für die frühzeitige Erkennung und Behandlung von Schwachstellen entwickelt werden.[150]

Insbesondere die Nutzung der Blockchain und DLT könnte von solchen Entwicklungen positiv beeinflusst werden, da diese im Vergleich zu großen Unternehmen nicht in der Lage sind, eigene Abteilungen zur Entwicklung von Blockchain-/DLT-Anwendungen und Smart Contracts zu etablieren, und somit darauf angewiesen sind, entsprechendes Know-how und Dienstleistungen einzukaufen.[151]

5.3.2.2.3 Weitere Angriffsmöglichkeiten

Ein DLT-Netzwerk, welches den Proof-of-Work-Konsensmechanismus verwendet, wird u. a. durch eine sogenannte 51-Prozent-Attacke bedroht. Dabei muss ein Angreifer über mehr als 50 Prozent der Rechenleistung des Netzwerks verfügen und kann dergestalt bspw. eigene Transaktionen vortäuschen. Verhindert wird ein derartiger Angriff durch

[145] *Jentzsch*, Decentralized autonomous organization to automate governance. White paper, November.
[146] *Tual*, Vitalik Buterin, Gavin Wood, Alex van De Sande, Vlad Zamfir announced amongst exceptional DAO Curators.
[147] *DuPont,* Bitcoin and Beyond 2017, 157, *Etherscan*, www.etherscan.io.
[148] *Falkon*, The Story of the DAO—Its History and Consequences.
[149] *Securities Exchange Comission*, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO.
[150] *Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau*, Blockchain und Smart Contracts.
[151] *Schütte/Fridgen/Prinz/Rose* et al., Blockchain und Smart Contracts.

die Größe des Netzwerks und den dadurch notwendigen Einsatz von Rechenleistung, sodass ein Angriff auf die großen Kryptowährungen heute unrealistisch erscheint.

Beim „Double Spending" nutzt ein Angreifer die Latenzzeit bis zur endgültigen Bestätigung einer Transaktion, um Geschäfte mit zwei verschiedenen Nutzern abzuschließen. Dieses Szenario wird durch die schnellere Transaktionsabwicklung neuerer DLT erschwert und kann durch vorsichtige Nutzer insbesondere bei großen Transaktionen verhindert werden.
Schließlich bleibt die Schnittstelle zur Realwelt ein Schwachpunkt in der Sicherheit von DLT. Sollen bspw. Sensordaten fälschungssicher dokumentiert werden, so bleibt die Möglichkeit, den Sensor selbst zu manipulieren. Dies ist jedoch ein Angriffsszenario, das nur zum Tragen kommt, wenn Nutzer sich dieser Möglichkeit nicht bewusst sind und folglich den in der DLT abgelegten Informationen vollständig vertrauen. Grundsätzlich mindert DLT also die Möglichkeiten betrügerischer Angriffe, kann diese aber auch nicht völlig ausschließen.

5.3.2.2.4 Anonymität, Steuerhinterziehung und Geldwäsche

Anonymitätsbewahrende DLT-Implementierungen können kriminelles Verhalten, wie bspw. Steuerhinterziehung und Geldwäsche ermöglichen. Insbesondere die Kryptowährung Bitcoin hatte lange Zeit den Ruf, hauptsächlich für Schwarzmarkt-Transaktionen und Geldwäsche genutzt zu werden. Da im Bitcoin-System Pseudonymität herrscht, lassen sich Geschäfte, die mit Bitcoin durchgeführt werden, zumindest nicht direkt natürlichen oder juristischen Personen zuordnen. Diese Eigenschaft haben Kriminelle in der Vergangenheit für Geldwäschezwecke genutzt.

Für andere Anwendungsfälle der DLT ist die Frage nach der Nutzung anonymitätsbewahrender oder nicht anonymitätsbewahrender Implementierungen im Einzelfall zu beantworten. Insbesondere im B2B-Bereich wird es in den meisten Fällen nicht möglich oder sinnvoll sein, ein anonymitätsbewahrendes System zu nutzen, da sich die jeweiligen Vertragsparteien in aller Regel bekannt sind. Es ist daher zu vermuten, dass die bei Kryptowährungen vorherrschenden Probleme für andere Anwendungsfälle, wenn überhaupt nur in deutlich geringerem Maße zum Tragen kommen.

5.3.2.3 Datenschutz/DS-GVO

Bei jeder Anwendung von DLT muss berücksichtigt werden, dass im Klartext in einem DLT-System gespeicherte Daten von jedem berechtigten Teilnehmer gelesen werden können. Um dennoch Daten zu schützen, könnte man auf die Idee kommen, etwa persönliche Daten oder Geschäftsgeheimnisse verschlüsselt auf einem DLT-System abzuspeichern. In diesem Zusammenhang muss man aber berücksichtigen, dass die auf einem DLT-System liegenden Daten dort möglicherweise für immer unveränderbar gespeichert sein werden.

Aus den in Kapitel 4.6.2 beschriebenen Gründen muss man damit rechnen, dass Daten, die nach heutiger Technik sicher verschlüsselt auf einem DLT-System abgespeichert sind, in Zukunft mit verhältnismäßig geringem Aufwand entschlüsselt und von jedem gelesen werden können. Dabei muss man jedoch zwischen klassischer Verschlüsselung und dem Bilden von Hashwerten unterscheiden: Bei der klassischen Verschlüsselung (mit symmetrischen Schlüsseln) gibt es eine 1:1-Beziehung zwischen Klartext und verschlüsseltem Text – kennt man den Schlüssel, so kennt man auch den Klartext. Bei Hashfunktionen, sogenannten „One-Way-Funktionen", findet typischerweise eine Komprimierung statt, d. h., jedes Datenpaket wird auf ein Datenpaket kleiner (fester) Länge abgebildet. Insbesondere führen sehr viele Datenpakete zum gleichen Hashwert, es gibt keinen eindeutigen „Schlüssel". Das Erzielen höherer Rechenleistung würde lediglich bedeuten, dass man viele Kandidaten für die ursprünglichen Datenpakete findet.

Daraus ergeben sich bestimmte „Verwendungshinweise“[152]: In Klartext sollten nur Daten, die für die jeweilige Anwendung unbedingt nötig und datenschutzrechtlich unbedenklich sind („sofort wertlos werden“) auf einem DLT-System abgelegt werden, in verschlüsselter Form nur Daten, die auf absehbare Zeit „wertlos“ werden. In gehashter Form können Daten nach aktuellem Forschungsstand sicher abgelegt werden, sofern die Ursprungsdaten genügend lang und „unstrukturiert“ sind (dies kann bspw. durch zusätzliche Verschlüsselung vor dem Verhashen oder das Einfügen von langen Zufallszahlen erreicht werden). Allerdings entspricht dies genau genommen nicht mehr dem Abspeichern der tatsächlichen Informationen, da diese bei dem Verhashen verloren gehen. Vielmehr kann man damit beweisen, dass Informationen seit dem Ablegen ihres Hashwerts in der Blockchain nicht geändert wurden: Stimmt der alte Hashwert auf einem DLT-System mit dem Hashwert von Daten, deren Integrität man beweisen will, überein, so kann man davon ausgehen, dass die ursprünglichen Daten dieselben sind. Dieses Konzept nennt man auch „Kombination von On-Chain- und Off-Chain-Speicherung“, da die tatsächlichen Daten nicht auf dem DLT-System liegen (insbesondere gelöscht werden können) und das DLT-System mittels Abspeicherns von Hashwerten nur Beweise der Integrität ermöglicht.

Im öffentlichen Diskurs wird zudem oft eine Inkompatibilität von DLT mit der Datenschutzgrundverordnung (DS-GVO) diskutiert. Dieses Thema wird im Detail in Kapitel 6.2 aufgegriffen, hier werden jedoch bereits kurz die zentralen nicht-juristischen Gedanken dargestellt.

Da DLT a priori zwar Pseudonymisierung, nicht aber Anonymisierung ermöglicht, kann jeder Node-Betreiber aus den (unverschlüsselten oder verschlüsselten) Daten auf DLT-Systemen alleine oder durch Kombination von Informationen jetzt oder in Zukunft Informationen über Individuen oder Firmenprozesse erlangen. Ein kluger Einsatz von Hashwerten (s. o., On-Chain-, Off-Chain-Kombinationen) kann die Gefahr, dass daraus personenbezogene oder vertrauliche Informationen gewonnen werden können, drastisch reduzieren und somit den Personenbezug umgehen. Dadurch, dass Daten nicht nachträglich gelöscht werden können, ist Datensouveränität bei falscher Konzipierung / Verwendung / willentlichem Missbrauch dennoch zunächst einmal nicht gegeben. Zudem können durch Analyse der Metadaten in einem DLT-System (Aktivitäten von Adressen (Public Keys)) möglicherweise Daten mit Personenbezug gewonnen werden. Insbesondere für öffentliche DLT-Systeme, in denen dann praktisch die einzelnen Teilnehmer die Verantwortlichkeit für den Datenschutz innehaben, ergeben sich somit Probleme hinsichtlich der Löschungspflichten aus der DS-GVO. DLT ist indes durchaus im Geiste der DS-GVO: Sie fördert den vernünftigen Umgang mit und trifft vor allem große Datenverarbeiter, da gerade diese dadurch bedroht bzw. obsolet gemacht werden könnten. Man kann DLT-Lösungen durchaus so konzipieren, dass sie mit der DS-GVO vereinbar sind, jedoch ist dies häufig nur über Umwege möglich und erzeugt möglicherweise unnötige Komplexität im Design der Anwendungen. Beispielhaft sind hier drei Punkte zu nennen:

(1) Bei Blockchains, die über eine Dokumentationsanwendung hinausgehen (Transaktionen), gibt es Ansätze (z. B. Zerocoin), mittels kryptografischer Verfahren (Zero Knowledge Proofs) besessene Assets und Adressen voneinander zu entkoppeln.
(2) Eine vollständige Anonymisierung, etwa durch das Verwenden neuer Adressen (Public Keys) für jede Interaktion auf der Blockchain, ist prinzipiell möglich. Dies

[152] Zu den technischen Restriktionen siehe Abschnitt (In-)Effizienz.

könnte etwa durch Initiativen im Bereich selbstsouveräne Identität (z. B. Sovrin[153]) erreicht werden.

(3) Auf der anderen Seite ist vollkommene Anonymität aus Sicht von Regulierungsbehörden insbesondere im Finanzbereich auch nicht erwünscht. Es gibt aber Versuche, „Hintertüren" in derartige Anonymisierungslösungen zu integrieren, die notfalls einen Zugriff definierter Instanzen erlauben, diesen aber transparent machen.

Insofern könnte man prüfen, ob die DS-GVO in einer Richtung angepasst werden kann, die zwar keinen Missbrauch eröffnet, aber auch der DLT-Technik den Weg ebnet, Ziele der DS-GVO umzusetzen.

5.3.3 DLT und Governance

5.3.3.1 Governance-Mechanismen zum Betrieb von DLT-Systemen

Im Zusammenhang mit der Governance der DLT-Systeme stellt sich die Frage, wer für die Entwicklung, Implementierung, den Betrieb und die Wartung des Systems verantwortlich ist. Auch die Frage der kontinuierlichen Weiterentwicklung des DLT-Systems bildet einen zentralen Aspekt. Schließlich gilt es die Systeme in Einklang mit künftigen technischen und gesellschaftlichen Anforderungen zu bringen.

Bedingt durch den grundlegenden dezentralen Charakter der DLT sind für die neu entstehenden DLT-Systeme neue Governance-Ansätze notwendig, welche sich von bestehenden Lösungen unterscheiden. Anders als bei einem zentral geführten System ist bei einer DLT-basierten Lösung eine Vielzahl an Stakeholdern direkt an der Entwicklung und Unterhaltung beteiligt. Fragestellungen, die bis dato eher der internen Governance zugeordnet gewesen sind, werden durch ein Netzwerk aus verschiedenen Interessensvertretern vergleichsweise komplex. Hierbei ist es entsprechend notwendig, ein passendes Regelwerk zu definieren, welches die Verantwortlichkeiten, Entscheidungsgewalten und Anreize so implementiert, dass ein möglichst hoher Nutzen für alle Beteiligten erreicht wird. Auch entstehen durch die neuartigen Akteure in DLT-Systemen, die bis dato nicht Teil regulärer techno-ökonomischer Systeme waren, neuartige Fragestellungen.[154] Das damit verbundene Forschungsfeld ist noch vergleichsweise jung und viele Fragestellungen sind Teil des aktiven, wissenschaftlichen Diskurses.[155]

Governance

Um in der digitalen Wirtschaft konkurrenzfähig zu sein, sind nicht nur Investitionen in Informationstechnologie (IT), sondern auch Wissen im Bereich IT-Governance nötig. IT-Governance spiegelt die Mechanismen wider, die IT richtig organisieren und effektiv nutzbar machen.[155]

Mit der zunehmenden Etablierung der DLT haben sich unterschiedliche Ausprägungsformen der DLT-Governance herausgebildet. Aufgrund der grundsätzlich dezentralen Struktur einer DLT-Lösung sollte deren Betrieb und die entsprechende Wartung möglichst auch von keiner zentralen Partei durchgeführt werden. Die Entwicklung eines DLT-Systems und die dafür notwendige Forschung setzt jedoch, meist aus Effizienzgründen, eine

[153] Siehe allgemeiner technischer Teil.

[154] *Mattila/Seppälä,* Collaborative Value Co-Creation in the Platform Economy 2018, 183.

[155] *Beck/Müller-Bloch* et al., Journal of the Associacion for Information Systems, 2018, S. 1020-1034.

[156] *Grembergen/Haes* in Bui, Proceedings of the 51st Hawaii International Conference on System Sciences, 4877.

zentrale Struktur voraus. Um dieser organisatorischen Zentralisierung einen technisch-dezentralen Charakter zu verleihen, sind DLT-Systeme zumeist Open-Source-Projekte. Dies bedeutet, dass ihr Quellcode öffentlich eingesehen, und oftmals auch genutzt bzw. verändert werden kann. Für die Entwicklung, Implementierung, Weiterentwicklung und Vermarktung von DLT-Systemen haben sich im Wesentlichen drei unterschiedliche Governance-Modelle herausgebildet. Dazu zählen von der Community, Stiftungen oder Gesellschaften getriebene Projekte.

Viele DLT-Systeme, bspw. das Bitcoin-Netzwerk, besitzen im weitesten Sinne keine verwaltende zentrale Entität. Dabei werden sowohl der organisatorische als auch der produktive Bereich größtenteils von der Community übernommen. An dieser Stelle sei jedoch erneut anzumerken, dass auch hinter Bitcoin ein Kernteam aus Entwicklern steht, welches das Repository der Bitcoin-Blockchain verwaltet. Signifikante Änderungen des Programmcodes benötigen die Zustimmung der Community und können nicht unkontrolliert vom Entwicklerteam umgesetzt werden. Bei derartigen Systemen entsteht die Governance primär durch das Entwicklerteam und die Akzeptanz des Protokolls durch die Community.[157] Entwicklung, Implementierung, Weiterentwicklung, Vermarktung, Betrieb und die Wartung der Infrastruktur werden größtenteils von der Community übernommen. Dies bedeutet, dass sich jeder an der Weiterentwicklung und der Ausführung des Protokolls beteiligen kann. Ob letztlich eine Änderung auch für das gesamte System übernommen wird, hängt dann insbesondere von den Netzwerk-Teilnehmern, welche das DLT-Protokoll nutzen, ab. Je größer die Unterstützung unter den Teilnehmern ist, desto wahrscheinlicher ist eine Übernahme der Änderung. Eine besondere Problematik entsteht, wenn sich verschiedene Ansichten über die Zukunft des Systems in der Community entwickeln. Dieses Phänomen konnte vor wenigen Jahren sowohl bei der Bitcoin- als auch bei der Ethereum-Blockchain beobachtet werden, als sich beide jeweils in zwei unterschiedliche Netzwerke aufgeteilt haben. Hintergrund der Aufspaltungen waren unterschiedliche Ansichten der Community: bei Bitcoin in Bezug auf die Lösung der Skalierungsproblematik und bei Ethereum in Bezug auf eine rückwirkende Schließung einer Sicherheitslücke. Während ein Teil der Communities das klassische Protokoll unterstützen wollte, spaltete sich der andere Teil mit den vorgenommenen Protokolländerungen ab.

Neben dieser vollständig durch die Community getriebenen Governance-Form wurden in den vergangenen Jahren besonders Stiftungen und Gesellschaften als bevorzugte Entitäten zur Übernahme von Governance-Funktionen eingesetzt. Mit diesen Formen können eigene Projekte finanziert und der gesamte Entwicklungsprozess eines Systems effizienter gestaltet werden. Die Effizienz entsteht besonders dadurch, dass Änderungen am Protokoll auch ohne einen Konsens der Community durchgeführt werden können.

Beide Formen haben sich besonders im Zusammenhang mit ICOs und den sich daraus ergebenden Besonderheiten gebildet. Mithilfe eines Verkaufs von Token soll die Finanzierung der Entwicklung und Vermarktung des DLT-Systems sichergestellt werden.

Diese Art der Beschaffung von Finanzmitteln unterliegt jedoch oftmals den Regulierungen des jeweiligen Finanzmarkts, in denen der ICO durchgeführt wird. Dabei gibt es Regionen auf der Welt, die eine derartige Investitionsform erlauben und wiederum andere, die sie verbieten. In Deutschland ist für eine Regulierung bspw. die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zuständig.[158] Eine andere Governance-Form, die auch aus dem Umfeld von ICOs hervorgegangen ist, stellen Gesellschaften, bspw. in Form einer GmbH oder AG, dar. Bei diesen ähnelt die Governance der von Stiftungen, jedoch steht bei ihnen häufig die unternehmerische operative Tätigkeit deutlich stärker im Fokus. Die Protokollentwicklung ist im Gegensatz zur Stiftung meist eher zentralisiert.

[157] *Beck/Müller-Bloch/King,* Journal of the Association for Information Systems 2018, 1020.
[158] *Hahn/Wons*, Initial Coin Offering (ICO).

Neben diesen aus ICOs hervorgegangenen Stiftungen und Gesellschaften können auch etablierte Unternehmen ein Konsortium für die Entwicklung und den Betrieb eines DLT-Systems gründen. Ein bekanntes Beispiel ist das R3-Konsortium[159], welches mehr als 200 Unternehmen umfasst. Auch hier ist das Protokoll Open Source, sodass es frei eingesehen und genutzt werden kann. Das von R3 entwickelte Corda-Netzwerk wird nicht von der Community, sondern von der Corda Network Foundation (= Stiftung)[160] verwaltet. Das Direktorium der Foundation wird von den Mitgliedern des Corda-Netzwerks gewählt und soll unabhängig vom R3-Unternehmen agieren. Auf diese Weise soll das Netzwerk transparenter und vertrauenswürdiger gesteuert werden. Ein weiteres Beispiel für ein DLT-System, das aus einer Kooperation von Industrieunternehmen hervorgegangen ist, ist Hyperledger.[161] Auch die Hyperledger-Protokolle sind eine Open-Source-Software. Hyperledger ist mittlerweile ein Projekt der Linux Foundation[162], welche die technische Steuerung des Projekts verantwortet. Dies bedeutet, dass alle technischen Entscheidungen, bspw. welche neuen Funktionen implementiert werden sollen, von Entwicklern, die von der Community gewählt worden sind, getroffen werden. Der Betrieb und die Wartung des Netzwerks unterscheiden sich dahingehend von Bitcoin, Ethereum und IOTA, da es kein öffentliches und zulassungsfreies, sondern privates und zulassungsbeschränktes ist. Hier betreibt also jedes Unternehmen, oder ein Konsortium aus Unternehmen, das DLT-System. Änderungen können auch individuell nach gemeinsamer Absprache vorgenommen werden, sodass sich nicht erst eine breite Community auf diese einigen muss.

5.3.3.2 DLT als Governance-Mechanismus

DLT-Systeme und deren Entwicklung bedürfen nicht nur selbst angemessener implementierter Governance-Regeln, sondern können potenziell auch ihrerseits mittels ihrer Eigenschaften und Möglichkeiten zur Implementierung verbesserter Governance-Mechanismen beitragen. Governance bezeichnet wie bereits erwähnt ein Regelwerk zur Organisation eines Systems. Die diesbezüglichen Diskussionen finden bislang zumeist auf einer theoretischen Ebene statt und involvieren oftmals Konstrukte, die in der Praxis noch nicht umgesetzt worden sind. Die bisherigen Überlegungen beruhen hauptsächlich auf zwei zentralen Konzepten. Zum einen betrifft dies das Transparenzprinzip in DLT-Systemen, durch das viele Vorteile erhofft werden, und zum anderen sogenannte Dezentrale Autonome Organisationen (DAO).[163]

Ein möglicher Ansatz zur Verbesserung der Governance von Unternehmen bezieht sich auf die Abbildung der Besitzverhältnisse an Unternehmen mittels Anteilsscheinen auf einem DLT-System.[164] Darauf basierend sind verschiedene Vorteile wünschenswert. Zum einen soll eine größere Transparenz über die Besitzverhältnisse geschaffen werden, wodurch unterschiedliche Auswirkungen auf die verschiedenen Interessengruppen erwartet werden. Während Anteilseigner mit geringen Anteilen oder Fondsmanager ein Interesse an einer größeren Transparenz haben dürften, gestaltet sich die Situation bei Anteilseignern oder Mitarbeitern des Unternehmens divergent. So könnten bspw. Anteilseigner laut den Autoren vermehrt Unternehmensanteile von Unternehmen kaufen, die nicht auf einer DLT-Lösung abgebildet sind und daher weniger Transparenz bieten. Zudem ließe sich potenziell Insiderhandel leichter aufdecken. Dennoch scheint es frag-

[159] https://www.r3.com.
[160] https://corda.network.
[161] https://www.hyperledger.org.
[162] https://www.linuxfoundation.org.
[163] *Shermin,* Strategic Change 2017, 499.
[164] *Yermack*, Corporate Governance and Blockchains.

würdig, inwiefern eine De-Anonymisierung der Anteilseigner von Unternehmen gewünscht bzw. umsetzbar ist. Auch für Wahlvorgänge und die damit einhergehende Stimmrechtsvergabe könnten sich DLT-Systeme in diesem Kontext anwenden lassen, indem wahlberechtigende Token an die gelisteten Anteilseigner verteilt werden. Dadurch wird erhofft, die Präzision und Nachprüfbarkeit von Wahlergebnissen zu verbessern und unentdeckte Wahlbeeinflussung durch geheim gehaltene Anteilsleihen einzudämmen. Zudem könnte die Wirtschaftsprüfung unter der Annahme, dass Unternehmen ihre Finanztransaktionen auf einem DLT-System durchführen, durch die Nachvollziehbarkeit und rückwirkende Manipulationssicherheit vereinfacht werden.[165]

Aus ökonomischer Perspektive können Smart Contracts potenziell Auswirkungen auf Prinzipal-Agenten-Beziehungen haben.

Prinzipal-Agent-Theorie

Im Rahmen der Prinzipal-Agent-Theorie werden Probleme behandelt, die durch eine Leistungsbeziehung zwischen Auftraggeber (Prinzipal) und Auftragnehmer (Agent) entstehen. Diese Beziehung ist immer dann problematisch, wenn Interessenkonflikte bestehen und eine Partei besser als die andere informiert ist. Die im Zusammenhang der Prinzipal-Agent-Theorie entstehende Differenz der realen Kosten zu den Kosten einer idealen Lösung wird als Agenturkosten bezeichnet. Ziel der Theorie ist es, diese beispielweise durch Anreizverträge zu minimieren.[166]

Beispielsweise kann das moralische Risiko verringert werden, indem Unternehmen durch das Eingehen eines nach der Aktivierung auf einem DLT-System unveränderbaren Smart Contracts signalisieren, opportunistisches Verhalten in der Zukunft zu unterlassen. Dadurch werden die Agenturkosten potenziell gesenkt.[167] In diesem Kontext können Smart Contracts die Interessen verschiedener Gruppen z. B. durch Anreizsysteme, die mittels der Verteilung von Token (vgl. 5.2.5.6) an Interessengruppen über ein DLT-System implementiert werden, angleichen.[168] Die Grundidee hierbei ist, dass Teilnehmer eines Netzwerks und gegebenenfalls darauf implementierter Geschäftsmodelle als direkte Teilhaber ein Interesse am Erfolg der jeweiligen Anwendung haben. Durch die Standardisierung von Transaktionsregeln im Rahmen der Transaktionsabwicklung mittels Smart Contracts können zudem die Transaktionskosten gesenkt werden. Die Begründung hierbei ist, dass die Interaktionsregeln in Smart Contracts formalisiert und nach der Einwilligung (bspw. im Rahmen digitaler Signaturen) der verschiedenen Parteien in den Smart Contract unter definierten Bedingungen automatisch in dem DLT-System ausgeführt werden.[169,170,171]

Eine Fallstudie[172] einer dezentralen (autonomen) Organisation deutet die Potenziale von DLT für Governance an. Dabei zeigt sich, dass Kriterien insbesondere in der Entwicklung von DLT-basierten Anwendungen diametral zum Gedanken der Dezentralität häufig noch zentralisiert sind. Bei der Anwendung seitens der Endnutzer allerdings zeigt sich

[165] *Yermack*, Corporate Governance and Blockchains.
[166] *Hochhold/Rudolph,* Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende 2011, 131.
[167] *Yermack*, Corporate Governance and Blockchains.
[168] *Shermin,* Strategic Change 2017, 499.
[169] *Glatz*, What are Smart Contracts? In search of a consensus.
[170] *Shermin,* Strategic Change 2017, 499.
[171] *Pike/Capobianco/Gomes*, Blockchain Technology and Competition Policy - Issues paper by the Secretariat.
[172] *Beck/Müller-Bloch* et al., Journal of the Associacion for Information Systems, 2018, S. 1020-1034.

eine stärkere Dezentralisierung der Entscheidungsrechte verglichen mit zentralisierten Anwendungen, da z. B. die Preisgestaltung den Anbietern direkt überlassen wird, während sonst die Besitzer der technischen Infrastruktur oftmals die Preisgestaltung beeinflussen. Bezüglich der Verantwortungsübernahme bei DLT-Anwendungen ist laut den Autoren im Falle von Disputen nach wie vor ein zentraler Intermediär zur Schlichtung notwendig. Häufig werden deshalb Reputationssysteme in DLT-Systemen implementiert, um eine Verantwortungsübernahme zu fördern. Ein interessanter Aspekt hinsichtlich der Anreizsetzung ist zudem, dass Interessengruppen, die DLT-Systeme bspw. zum Angebot von Dienstleistungen als digitale Infrastruktur nutzen, ebenfalls einen Anreiz haben, diese Infrastruktur selbst zu warten.[173] Insbesondere könnte dies den Betrieb von Netzwerkteilnehmern, die aktive Teilnahme an der Open-Source-Entwicklung der Protokolle und die Veröffentlichung relevanter Tools beinhalten.

5.3.4 Wettbewerbspolitische Implikationen

Unter der Hypothese einer weitreichend verbreiteten Anwendung der DLT können zudem wettbewerbspolitische Implikationen abgeleitet werden. Dabei kann die Schaffung einer neutralen Informationsschicht mittels DLT potenziell Informationsasymmetrien abbauen. Des Weiteren kann die Möglichkeit zu der Teilnahme an einem offenen System den Markteintritt erleichtern, indem durch die generelle Möglichkeit zur Implementierung von Anwendungen auf (öffentlichen) DLT-Systemen und Smart Contracts Markteintrittsbarrieren verringert werden und damit einhergehend der Wettbewerb gefördert wird[174]. Eine weitere Idee betrifft die Nutzung von Smart Contracts. Hierbei können bspw. Patentierungsprozesse standardisiert und Patentinformationen allgemein einsehbar mittels DLT-Systemen umgesetzt werden[175].

In Bezug auf die erhöhte Transparenz in DLT-Systemen ist zu erwarten, dass Unregelmäßigkeiten bei Finanztransaktionen bzw. allgemein bei Interaktionen leichter aufzudecken sind. So könnte bspw. unerlaubte Kollusion aufgedeckt werden, wobei sich allgemein die Frage stellt, inwieweit dazu der Zugang zu DLT-Systemen gewährleistet werden muss[176]. Diese Frage drängt sich insbesondere im Bereich der permissioned DLT-Systeme auf (vgl. 4.3.1). Eine Gegenposition beschreibt hingegen, dass die DLT Kollusion eher fördern könnte, da durch sie Marktinformationen leichter zugänglich gemacht werden und somit auch die Basis für unerlaubte Absprachen geschaffen werden kann[177]. Einschätzungen zu dieser Position suggerieren jedoch, dass diese Bedenken zum Teil übertrieben sind und öffentliche Wettbewerbsbehörden ihre Überwachungsprozesse und -methoden an neue technologische Entwicklungen anpassen werden[178]. Insgesamt könnte die DLT durch ihre rückwirkende Manipulationssicherheit die Beweisführung bei etwaigen Kartellverfahren verbessern[179].

Die rechtliche Einschätzung und die subsequente Anwendung rechtlicher Maßnahmen in Bezug auf Wettbewerbspolitik, die sich durch die Verwendung von DLT für Unternehmen ergeben, können potenziell große Auswirkungen nach sich ziehen. Eine initiale Einschätzung ergibt, dass insbesondere domänenspezifische DLT-Systeme (bzw. deren Entwickler) Wettbewerbsregelungen, aufgrund ihrer Rolle als Betreiber einer dominierenden

[173] *Beck/Müller-Bloch* et al., Journal of the Associacion for Information Systems, 2018, S. 1020-1034.
[174] *Cong/He*, Blockchain disruption and Smart Contracts.
[175] *Tulpule,* CPI Antitrust Chronicle 2017, 45.
[176] *Pike/Capobianco/Gomes*, Blockchain Technology and Competition Policy - Issues paper by the Secretariat.
[177] *Cong/He*, Blockchain disruption and Smart Contracts.
[178] *Simpson/Cooke*, Blockchain: competition issues in nascent markets.
[179] *Tulpule,* CPI Antitrust Chronicle 2017, 45.

Infrastruktur, auferlegt bekommen könnten. Somit könnten diese bspw. davon abgehalten werden, willkürliche Preise in dem jeweiligen DLT-System zu setzen oder andere Maßnahmen zu ergreifen, die potenziell Konkurrenten ausschließen könnten[180]. Insgesamt spricht dieser Aspekt für die Implementierung adäquater Governance-Mechanismen und die Implementierung entsprechender Systeme durch geeignete neutrale Organisationen.

Auch technische Standards, die oftmals von Vertretern verschiedener Branchen für eine weite Verbreitung der DLT als notwendig erachtet und gefordert werden[181], haben Relevanz für die Wettbewerbspolitik. Beispielsweise werden technische Standards generell als wettbewerbsfördernd angesehen. Dennoch muss sichergestellt werden, dass Standards nicht durch bestimmte Interessengruppen gesetzt werden und gleichzeitig andere Interessengruppen ausschließen bzw. deren Markteintritt erschweren[182]. In diesem Kontext wird außerdem diskutiert, inwiefern ein Zugang zu permissioned DLT-Systemen verpflichtend gegeben werden muss, sofern dieser notwendig ist, um in einem Markt teilzunehmen bzw. bedeutenden Mehrwert für die Teilnehmer im Wettbewerb zu bringen. Dabei sind jedoch mehrere Argumente zu betrachten, bspw. unter welchen Kriterien ein Ausschluss gerechtfertigt werden kann.[183]

Förderung von Kooperation

Es ist zu eruieren, inwieweit förderungspolitisch Anreize gesetzt werden können, um insbesondere solche Marktakteure zur Partizipation zu motivieren, die in Konkurrenzverhältnissen stehen. DLT-Systeme sind aufgrund ihrer Natur und ihres Aufbaus insbesondere auf die Kooperationen verschiedener Organisationen angewiesen, da andernfalls die Dezentralität in den Netzwerken nicht hergestellt werden kann. Es ist bekannt, dass DLT-Lösungen dem Konzept der kritischen Masse nach Metcalf unterliegen.[184] Kooperation wird in Zeiten der Digitalisierung aufgrund kleinteiligerer Wertschöpfung immer wichtiger. Es scheinen für viele DLT-Netzwerke Anfangsinvestitionen im Sinne von Werbungskosten notwendig, um Kollaboration und Kooperation zu initiieren. Bei Erreichen der kritischen Masse können diese hingegen selbsttragend sein. Damit förderungspolitische Akzente gesetzt werden können, scheint die Schaffung von Rechtssicherheit durch eine kartellrechtliche Einordnung und Analyse notwendig.

[180] *Simpson/Cooke*, Blockchain: competition issues in nascent markets.
[181] *Hyland-Wood/Khatchadourian,* The JBBA 2018, 3724; *Michael Ortmeier* 13.02.2019.
[182] *Simpson/Cooke*, Blockchain: competition issues in nascent markets.
[183] *Simpson/Cooke*, Blockchain: competition issues in nascent markets.
[184] *Metcalfe,* Computer 2013, 26.

Sandboxes & Reallabore

Analog zu anderen technologischen Erprobungen kann auch DLT davon profitieren, in zeitlich oder räumlich (sowie ggf. weiteren Parametern) abgegrenzten Testräumen wertvolle Erfahrungen zu sammeln und zur Innovationssteigerung beizutragen (z. B. Ladeinfrastruktur in Wohneigentümergemeinschaften). Lokal und zeitlich abgegrenzte Testräume, in denen bestimmte juristische Klauseln ausgeschaltet sind, müssen dementsprechend eingerichtet und/oder gefördert werden. Diese sind nötig, weil die technische Entwicklung in der Regel schneller ist als die Regulierung. Das Konzept wird vielfach in anderen Staaten erfolgreich angewendet und z. T. auch in Deutschland insbesondere im Rahmen der Energiewende (z. B. SINTEG-Projekte) umgesetzt.

Gestaltung nach freiheitlich-demokratischen Prinzipien

DLT-Lösungen und -Systeme sollten aktiv nach freiheitlich-demokratischen Idealen durch den Staat mitgestaltet werden. Dies umfasst auch, dass der Staat die Technologie in Pilotprojekten selbst anwendet und somit eine Vorbildfunktion einnimmt. Ein Verbot der Nutzung der Technologie (vgl. zum Beispiel hinsichtlich Kryptowährungen in anderen Nationen) sollte abgewendet werden. Eine Nutzung ist aufgrund der Eigenschaften der Technologie (wie beispielsweise Dezentralität) ohnehin schwer auszuschließen. Da DLT-Systeme prinzipiell eine Disintermediation ermöglichen, könnte dies auch für staatliche Funktionen umgesetzt werden. Dies sollte der Staat rechtzeitig bedenken. Wenn DLT für staatliche Aufgaben und Funktionen angewendet wird, so kann der Staat für den Aufbau und/oder Betrieb der entsprechenden Systeme und Netzwerke mitverantwortlich sein. Eine entsprechende Kompetenzaufteilung (Ministerien, Organisationen, Bund, Länder) sollte frühzeitig diskutiert werden.

Technologiestrategie

Da sich das Technologiefeld der DLT nichtlinear entwickelt, ist es wichtig, regelmäßig Nutzen und Realisierung zu prüfen. Eine neutral-objektive Einschätzung ist notwendig, um Chancen und Risiken etc. sinnvoll einschätzen zu können. Vorurteilbehafte Einschätzungen können die sozioökonomischen Verwertungschancen potenziell nachteilig beeinflussen. Falsche Wahrnehmungen, Mythen und „Fake News“ (vgl. Energieverbrauch oder Kriminalität) verhindern die Potenzialnutzung. Ein Stakeholder-Dialog mit (interessierten) Bürgern, Großunternehmen, KMUs und Blockchain-Start-ups trägt dazu bei, dass ein realistisches Bild der Technologie und der damit verbundenen Chancen und Risiken präsentiert werden kann. Zudem hat der deutsche Staat das Thema DLT vergleichsweise früh als untersuchungswert erkannt und bereits gezeigt, dass er seiner Verantwortung diesbezüglich gerecht wird.

5.4 DLT im Mobilitätssektor

Im Mobilitätssektor, der zunehmend von Automatisierung und Digitalisierung geprägt ist, kommt verstärkt die DLT zum Einsatz. Die DLT adressiert durch ihre inhärenten Eigenschaften eine Vielzahl der Anforderungen aktueller Entwicklungen wie zunehmend vernetzte Fahrzeuge, intermodale Verkehrskonzepte und die zukünftig verstärkte Dezentralisierung des Sektors durch autonom agierende Verkehrsteilnehmer. Dieser Abschnitt vermittelt einen Überblick über bereits bestehende DLT-Initiativen im Mobilitätsbereich. Davon ausgehend werden die grundlegenden Anwendungsfelder der DLT im Mobilitätsektor abgeleitet und beschrieben. Schließlich folgt ein Ausblick auf die vier Anwendungsfälle, die im speziellen Teil des Grundgutachtens detailliert analysiert werden.

5.4.1 Anwendungsfelder

Im ersten Schritt wurden mittels Literatur- und Internetrecherche sowie umfassender Experteninterviews zahlreiche bestehende DLT-Initiativen identifiziert und deren Auswirkungen auf den Mobilitätsbereich abgeschätzt. Hieraus ergab sich die in Abbildung 20: Überblick über existierende Initiativen und Identifikation von Anwendungsfeldern dargestellte Grafik.

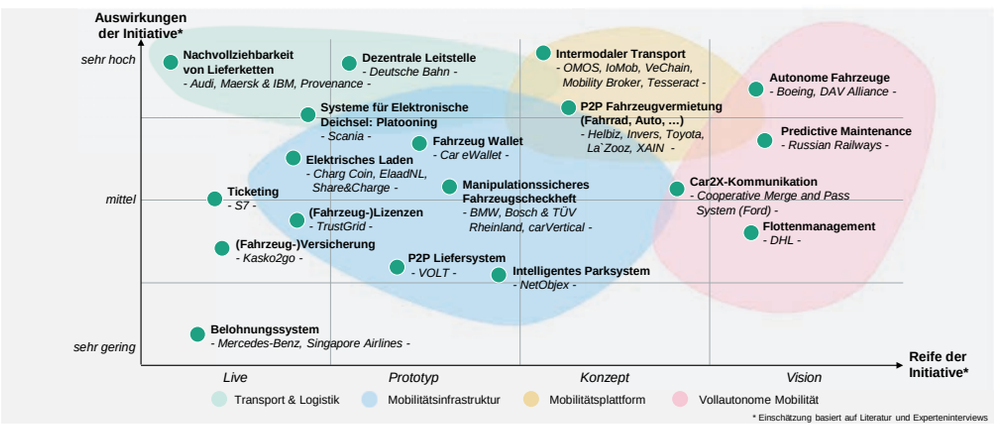


Abbildung 20: Überblick über existierende Initiativen und Identifikation von Anwendungsfeldern

In Abhängigkeit der jeweiligen Reife der Initiative erfolgt eine Einordnung in Live, Prototyp, Konzept und Vision. Seitens der Auswirkungen wird auf einer Skala von sehr gering bis sehr hoch qualitativ differenziert. Durch Einordnung der Initiativen gemäß den Dimensionen Reife der Initiative und (mögliche) Auswirkungen der Initiative auf den Mobilitätssektor zeigen sich Cluster von ähnlich gelagerten und ähnlich fortgeschrittenen Initiativen. Die vier identifizierten Cluster lassen sich mit *Transport & Logistik*, *Mobilitätsinfrastruktur*, *Mobilitätsplattform* und *Vollautonome Mobilität* überschreiben. Bei der Einordnung wird deutlich, dass auch an den Schnittstellen bzw. anwendungsfeldübergreifend zahlreiche Initiativen existieren.

Zur Schaffung eines einheitlichen Verständnisses und der Definition wichtiger Begrifflichkeiten erfolgt im Anschluss eine kurze Beschreibung der vier identifizierten Anwendungsfelder.

Das Anwendungsfeld Transport & Logistik beinhaltet Initiativen, deren Ziel es ist, durch DLT-Lösungen insbesondere Prozesse und die Zusammenarbeit verschiedener Transport- und Logistikanbieter transparenter und effizienter zu gestalten. Aufgrund des harten Wettbewerbs herrscht im Anwendungsfeld Transport & Logistik ein besonders hoher Innovationsdruck. Dementsprechend werden aktuell bereits viele Anwendungsfälle erprobt, wodurch das Anwendungsfeld bereits eine vergleichsweise hohe Reife aufweist.

Etwa wurde von Maersk und IBM unter dem Namen Trade Lens ein dezentrales DLT-Register entwickelt und eingeführt, auf dem global agierende Handelspartner die Lieferketten ihrer Güter abbilden und die Zusammenarbeit zwischen Behörden und Frachtspeditionsdiensten beschleunigen und verbessern[185]. In einem Projekt mit der Nord/LB wurde darüber hinaus ein DLT-basierter Prototyp zur Prozessoptimierung bei der Erstellung und Abwicklung von Dokumentenakkreditiven entwickelt. Speziell in der Logistikbranche sind Dokumentenakkreditive von erheblicher Relevanz, da mit deren Hilfe Importeure einem Exporteur gegenüber die Rechnungsbegleichung unter bestimmten Bedingungen zusichern. Da der aktuell papierbasierte Prozess durch die Vielzahl der Beteiligten nur langsam abläuft, besteht großes Potenzial, diesen durch einen digitalen, DLT-basierten Prozess zu ersetzen. Ferner arbeitet das we.trade-Konsortium an einer DLT-Plattform, die Vertragseinigungen zwischen Banken und ihren Klienten, u. a. Logistikdienstleistern, lanciert und deren Verwaltung vereinfacht. Durch den bereits jetzt wegweisenden Charakter der einzelnen Initiativen ist davon auszugehen, dass die Verwendung der DLT im Anwendungsfeld Transport & Logistik signifikante Auswirkungen auf die Mobilitätsbranche haben wird. Die Herausforderung bei den genannten Initiativen besteht jedoch weiterhin darin, Erfahrungen zu sammeln und die entwickelten DLT-Lösungen zu erproben.

Dem Anwendungsfeld Mobilitätsinfrastruktur werden Initiativen mit infrastrukturellem Charakter zugeordnet. Ein Beispiel hierfür sind Lösungen, die eine intelligente und preiswerte Inbetriebnahme sowie eine zuverlässige und für den Verbraucher unkomplizierte, transparente Abrechnung von Ladesäulen für Elektrofahrzeuge ermöglichen. Initiativen in diesem Anwendungsfeld sind oft schon auf dem Stand eines Prototyps und werden voraussichtlich mittlere bis hohe Auswirkungen auf die Mobilität der Zukunft besitzen sowie eine flächendeckende Verbreitung von Ladeinfrastruktur fördern. Somit könnten insbesondere die Herausforderungen hinsichtlich geringer Reichweite und langer Aufladedauer adressiert werden. Dies kann das im Energiekonzept 2010 beschlossene Ziel der Bundesregierung, die Anzahl an Elektrofahrzeugen in Deutschland bis zum Jahr 2030 auf sechs Millionen zu erhöhen, weiter vorantreiben.[186] Beispiele für Initiativen mit Fokus auf den Bereich der Ladeinfrastrukturen sind etwa Share&Charge, ElaadNL und Charg Coin, die allesamt bereits anhand von Prototypen erprobt werden. Der Fokus liegt dabei auf der Etablierung eines einheitlichen, DLT-basierten Ladeprotokolls, welches unterschiedliche Anbieter vereint und die Abrechnung zwischen Nutzer und Anbieter vereinfacht oder sogar automatisiert. Darüber hinaus sind allerdings ebenfalls Initiativen wie digitale (Fahrzeug-)Lizenzen und Führerscheine, Fahrzeug-Wallets, manipulationssichere Fahrzeugcheckhefte und intelligente Parksysteme zu nennen. Charakteristisch für das Anwendungsfeld Mobilitätsinfrastruktur ist auch, dass praktisch alle darin enthaltenen Initiativen ebenfalls im Bereich der Vollautonomen Mobilität eine Rolle spielen werden, jedoch bereits heute (ohne vollautonome Fahrzeuge) nutzbar sind. Somit können sie auch als Beschleuniger oder Enabler einer für das vollautonome Fahren benötigten Infrastruktur und Standardisierung angesehen werden. Darüber hinaus besteht die Herausforderung in der Schaffung weiterer Anreize, um Initiativen und Investitionen im Bereich der Mobilitätsinfrastruktur sowie die Etablierung von Standards zu stimulieren. Beispielsweise besteht die Chance, mithilfe von DLT und darauf aufbauenden Crowdfunding-Konzepten, privaten Firmen und Personen zu ermöglichen, Investitionen in öffentliche Infrastruktur in Teilen mitzutragen und später davon zu profitieren.

Das Anwendungsfeld Mobilitätsplattform umfasst die Vision, das Konzept der intermodalen Mobilität zu verwirklichen. Initiativen in diesem Cluster adressieren das Ziel, unterschiedliche Mobilitätsservices in einer einzigen Plattform zu integrieren, um diese den

[185] Diese Initiative wird im Anwendungsfall „Frachtpapiere" im speziellen Teil (Kapitel 7) aufgegriffen und vertieft behandelt.

[186] *BMWi*, Energiekonzept für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung.

Kunden mithilfe eines einheitlichen Portals oder einer einzigen App zugänglich zu machen (MaaS Alliance 2017).[187] Eine solche Mobilitätsplattform bietet die Möglichkeit, den intermodalen Transport fundamental zu verbessern und die Mobilität von Personen in hohem Maße zu steigern. Verkehrsteilnehmer könnten durch solch eine Lösung bspw. bei einer geplanten Reise ein Taxi zum Bahnhof, eine Fernzugverbindung zum Flughafen und einen Flug zum Urlaubsziel in einem einzigen Bestätigungsvorgang buchen, anstatt bei jedem einzelnen auf der Reise genutzten Anbieter separat ein Ticket erwerben zu müssen. Die hohe Benutzerfreundlichkeit und geringe Komplexität beim Buchungsvorgang könnten gleichzeitig dazu beitragen, Hürden für die Nutzung des öffentlichen Verkehrs zu senken und eine höhere Auslastung dessen zu erreichen. Dies würde zudem dazu führen, dass weniger Fahrzeuge am Straßenverkehr teilnehmen und ein Beitrag zur ökologischen Nachhaltigkeit der Mobilität geleistet wird. Prinzipiell ist die technische Realisierung einer solchen Mobilitätsplattform auch ohne die DLT als von einem zentralen Unternehmen errichtete und kontrollierte Infrastruktur denkbar. Allerdings scheiterten Versuche einer Realisierung in der Vergangenheit vor allem daran, dass etablierte Mobilitätsanbieter aus Angst vor Abhängigkeiten keine Kooperation eingehen wollen. Lediglich in kleinem Maße konnten durch Initiativen wie moovel Plattformen für intermodale Mobilität in einzelnen Städten wie Stuttgart geschaffen werden. Um eine flächendeckende, skalierbare Lösung zu finden, ist aufgrund der hohen Anzahl an beteiligten Mobilitätsanbietern und dem hohen Kooperationscharakter bei einer Mobilitätsplattform langfristig eine DLT-Lösung sinnvoll. Derartige Initiativen, wie bspw. IoMob, Mobility Broker, OMOS, Tesseract und VeChain, stehen aktuell allesamt noch in der Konzeptionsphase. Die Einigung auf gemeinsame Standards ist ein langwieriger Prozess und stellt Mobilitätsanbieter vor die Herausforderung, strategische Partnerschaften zu schließen. Daher ist von einer Implementierung nur mittel- bis langfristig auszugehen.

Das Anwendungsfeld Vollautonome Mobilität inkludiert Initiativen, welche die Vision der vollautomatisierten Mobilität verfolgen. Eine zentrale Bedeutung hat dabei der Anwendungsfall der autonomen Fahrzeuge. In der Automobilbranche arbeiten bereits mehrere Unternehmen an Konzepten zur Umsetzung des autonomen Fahrens bei Pkw und Lkw. Darüber hinaus werden voraussichtlich auch Fahrzeuge des öffentlichen Personenverkehrs, Wasserfahrzeuge und Luftfahrzeuge autonom betrieben werden können. Der Flugzeugbauer Boeing entwickelt und testet etwa bereits autonome Flugzeuge, die bis 2030 einsatzbereit sein sollen. Die Schlüsselfunktion für das autonome Fahrzeug stellt dabei die sichere Kommunikation mit seiner Umwelt dar. Ein vielversprechender Ansatz dafür findet sich in einem Kommunikationsprotokoll auf Basis der DLT. Im Falle von Pkw würde dadurch eine drahtlose Car-2-X-Kommunikation, also zwischen Pkw und Elementen der Straßeninfrastruktur, ermöglicht.[188] Insbesondere die Dezentralität von DLT soll dabei für Sicherheit vor bösartigen Angriffen und Systemausfällen schützen. Darüber hinaus wird die Entwicklung autonomer Fahrzeuge wesentlich von den Initiativen der Anwendungsfelder Infrastruktur sowie Mobilitätsplattform profitieren. Das autonome Fahrzeug birgt sehr hohe potenzielle Auswirkungen auf verschiedene Teilbereiche des Mobilitätssektors. Unter anderem kann durch intelligent gesteuertes Fahrverhalten der Kraftstoffverbrauch gesenkt und die Sicherheit für Passagiere gesteigert werden. Zudem kann durch die Verringerung benötigter Pkw in Ballungszentren die Anzahl notwendiger Stellplätze reduziert und durch individualisierte Services die Mobilität von Passagieren verbessert werden. Die Reife der vorgestellten Initiativen ist aktuell sehr gering, da das vollautonome Fahren vorerst noch als Zukunftsvision zu betrachten ist. Vor einer umfas-

[187] *MaaS Alliance*, Guidelines & recommendations to create the foundations for a thriving MaaS Ecosystem.

[188] *Rowan/Clear/Gerla/Huggard* et al., Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels.

senden Einführung vollautonomer Fahrzeuge muss besonders auch bei ethischen Fragestellungen Klarheit geschaffen werden. Ein erster Ansatz hierfür stellen die 20 Thesen der vom BMVI eingesetzten Ethik-Kommission dar (BMVI 2017).[189]

Eine zusammenfassende Übersicht der identifizierten Anwendungsfelder ist in Abbildung 21 zu finden.

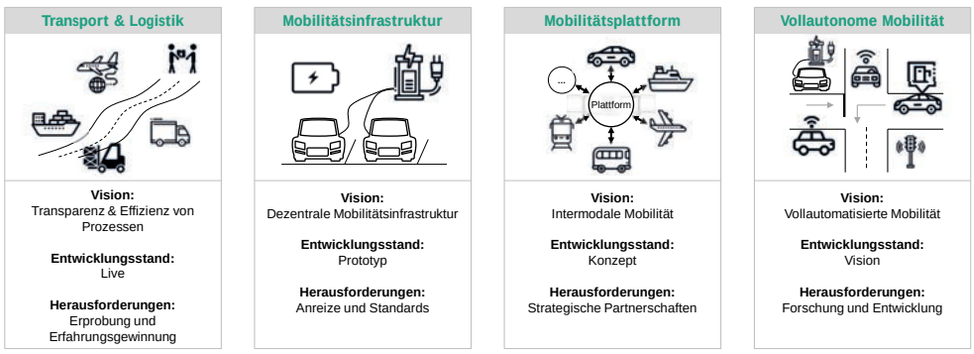


Abbildung 21: DLT-Anwendungsfelder im Mobilitätssektor

5.4.2 Ausblick auf den speziellen Teil

Im Speziellen Teil des Grundgutachtens sollen die eben beschriebenen vier Anwendungsfelder aus dem Mobilitätsbereich, die laut öffentlichem oder akademischem Diskurs prädestiniert für den Einsatz von DLT sind, genauer untersucht werden. Um den Umfang der Analyse in einem geeigneten Rahmen zu halten, wurde dabei explizit aus jedem der vier Anwendungsfelder je ein Vertreter ausgewählt, detailliert beschrieben und hinsichtlich seiner Potenziale analysiert. Alle vier Anwendungsfallbeschreibungen gliedern sich in einen ökonomisch-technischen und einen juristischen Teil. Im ökonomisch-technischen Teil werden jeweils zunächst das Ausgangsszenario, d. h. der Status quo, beschrieben sowie Nachteile, die die aktuelle Lage aufweist, aufgezeigt. Davon wird dann abgeleitet, an welchen Stellen sich die DLT möglicherweise als vorteilhaft herausstellen kann, um Effizienz in der jeweils betroffenen Branche zu heben. In konsequenter Fortsetzung der Analyse wird nach dem Aufzeigen des Einsatzpotenzials der DLT eine mögliche Architektur einer DLT-Lösung skizziert. Im Anschluss werden die im ökonomisch-technischen Teil gewonnenen Erkenntnisse zusammengefasst und – sofern indiziert – Handlungsempfehlungen gegeben. Im rechtlichen Teil eines jeden Anwendungsfalls wird aufbauend auf den ökonomisch-technischen Teil geprüft, inwieweit die vorgestellte DLT-Lösung mit geltendem Recht vereinbar ist. Sofern Problemstellungen ausgemacht werden, erfolgen – insbesondere auch in Hinblick auf die Herausforderungen durch den Datenschutz – Überlegungen zu möglichen Lösungen, die in Handlungsempfehlungen münden.

Der erste Anwendungsfall ist im Bereich Transport & Logistik angesiedelt und besteht in einer Digitalisierung des Bill of Lading (Konnossement) und damit zusammenhängender Bank- und Supply-Chain-Prozesse im internationalen Seehandel. Bei diesem kann die DLT als Enabler dienen und zuvor aus ökonomisch-gesellschaftlichen Gründen nicht digitalisierbare Prozesse auf einer IT-Plattform abbilden. Da diese Thematik bereits vor der Verbreitung von DLT wegen des enormen Potenzials häufig diskutiert wurde, können bei diesem Anwendungsfall einige Initiativen beschrieben sowie eine quantitative Potenzialanalyse durchgeführt werden. Zudem kann aufgezeigt werden, dass die bestehende Regulierung in diesem Bereich durch digitale Öffnungsklauseln bereits fortgeschritten ist.

[189] *BMVI*, Ethik-Kommission: Automatisiertes und Vernetztes Fahren.

Demgegenüber divergiert die Situation beim Anwendungsfall Elektrisches Laden, welcher dem Anwendungsfeld Mobilitätsinfrastruktur entstammt. In diesem wird analysiert, inwiefern die DLT die Prozesse zwischen Ladesäulenbetreibern und Roaming-Anbietern (B2B[190]) verbessern kann. Im Gegensatz zu den Dokumentenprozessen im internationalen Seehandel sind dort praktisch alle Abläufe bereits digitalisiert. Jedoch ist der Markt noch vergleichsweise klein und jung sowie stark fragmentiert. Somit kann dort nur qualitativ beschrieben werden, wie sich eine DLT-basierte Lösung möglicherweise von einem prospektiven monopolitischen Anbieter unterscheiden und positiv auf die Akzeptanz von Elektromobilität auswirken könnte.

Der dritte Anwendungsfall, das Ridesharing, also das organisierte Vermitteln von nichtkommerziellen Mitfahrgelegenheiten, ist von der Reife her vergleichbar mit dem elektrischen Laden, hat jedoch aufgrund seiner Ansiedlung im C2C[191]-Bereich eine andere Struktur und andere Anforderungen als der des elektrischen Ladens. Auch hier stellt sich eine quantitative Beschreibung der Potenziale einer DLT-Lösung als schwierig dar, da es in diesem Bereich bereits etablierte Plattformanbieter wie etwa Uber gibt und die Fragestellung, in welchem Maße eine neutrale Plattform volkswirtschaftlich besser ist als eine etablierte, kommerzielle Fahrvermittlungsplattform, erst noch erforscht werden muss. Zudem stellt sich in diesem Anwendungsfall heraus, dass die Potenziale der DLT nicht bei jedem Plattform-Anwendungsfall in gleicher Ausprägung vorzufinden sind: Im Falle von Ridesharing liegen diese aktuell eher in ergänzenden Funktionen, bspw. der Zahlungsabwicklung, als in der reinen Vermittlung von Fahrtdienstleistungen.

Schließlich wird der spezielle Teil mit dem Anwendungsfall Platooning – einem technoökonomischen System für den Straßenverkehr, bei dem zwei oder mehrere Fahrzeuge in sehr geringem Abstand hintereinanderfahren, um Kosteneinsparungen zu realisieren – abgeschlossen. Dieser ist sicher der visionärste Anwendungsfall, da im Gegensatz zu den anderen drei Anwendungsfällen umfassende Hardware-Nachrüstungen von Lkw nötig wären, um eine Verbreitung des Platoonings zu ermöglichen. Dennoch könnte die DLT in Form einer dezentral verwalteten Bezahlinfrastruktur zum Ausgleich von erzielten (Treibstoff-)Einsparungen dazu beitragen, das Platooning im Logistikbereich zu etablieren. Da eine DLT-basierte Zahlungsabwicklung beim Platooning bereits vorhandene Fahrten in der Logistikbranche effizienter gestalten würde, kann man hier wiederum eine quantitative Potenzialanalyse durchführen.

Die Chance für die Bundesrepublik zeigt sich darin, als große Volkswirtschaft mit hoch angesehenen regulatorischen Standards eine jetzt noch existierende Leerstelle in Europa zu besetzen.

[190] Business-to-business.
[191] Customer-to-customer.

6 Rechtliche Grundlagen

6.1 Zivilrechtliche Betrachtungen

6.1.1 Smart Contracts und automatisierte Vertragsabwicklung

Als Smart Contract wird Software verstanden, die digital prüfbare Ereignisse verarbeitet und auf deren Grundlage rechtlich relevante Handlungen ausführt, sodass es zu einer automatisierten Vertragsabwicklung kommt.[192] Bei entsprechender Programmierung kann ein Smart Contract ebenfalls Funktionen ähnlich denen eines Treuhänders übernehmen.[193] So kann bspw. die Zahlungsfähigkeit einer Vertragspartei dadurch sichergestellt werden, dass der geschuldete Betrag vorab an den Smart Contract gesendet wird. Der Empfänger erhält den Betrag allerdings nur, wenn der Eintritt des vereinbarten auslösenden Ereignisses an den Smart Contract gemeldet wird. Der Smart Contract übernimmt in diesem Fall die Funktionen einer vertrauenswürdigen dritten Instanz, welche den zu zahlenden Betrag verwahrt, den Eintritt des vereinbarten Ereignisses prüft und die Auszahlung vornimmt. Andersherum kann der Smart Contract so eingesetzt werden, dass eine andere Leistung erst freigegeben wird, wenn der geschuldete Betrag gezahlt worden ist. So könnte bspw. ein gemietetes Fahrzeug erst gestartet werden, nachdem der Smart Contract eine Information über den Zahlungseingang erhält. Es entsteht ein Anreiz, die eigene Leistung zu erbringen, indem dies zur faktischen Bedingung für den Erhalt der Gegenleistung gemacht wird. Insgesamt sollen durch den Einsatz von Smart Contracts Vorleistungsrisiken für beide Seiten verringert werden.

Da es sich bei Smart Contracts um nichts anderes als Software handelt, können sie auch unabhängig von der DLT eingesetzt werden. Die Implementierung in einem DLT-System erlaubt allerdings Direkttransaktionen und hat den Vorteil einer hohen Manipulationssicherheit, sodass die Integrität des Programmcodes gewährleistet ist. Die Ausführung der vereinbarten Handlung ist (eine korrekte Programmierung vorausgesetzt) garantiert. Insofern wird das Vertrauen in Vertragspartner und Intermediäre zumindest teilweise durch das Vertrauen in die zugrunde liegende Technologie, d. h. das Vertrauen in eine fehlerfreie Transaktionsdurchführung, ersetzt.

6.1.2 Grenzen der Einsatzmöglichkeiten

Der Einsatz von Smart Contracts zur Vertragsabwicklung unterliegt gewissen faktischen Grenzen. Nicht jede Form des Leistungsaustauschs kann nämlich durch Software vollständig abgebildet werden.[194] Vielmehr muss sich der Leistungsaustausch nach dem Wenn-dann-Prinzip darstellen lassen. Als Auslöser kommen nur digital erfassbare Ereignisse in Betracht, bspw. das Laden einer Batterie mit einer bestimmten Menge Strom oder das Zurücklegen einer bestimmten Strecke in Kilometern. Solche Informationen aus der realen Welt können über Schnittstellen, sogenannte Oracles, an den Smart Contract weitergegeben werden. Auch die dadurch ausgelöste Handlung muss softwaregestützt ausführbar sein oder zumindest in Gang gesetzt werden können, wie bspw. die Freigabe einer Zahlung.

Unbestimmte Rechtsbegriffe (z. B. der Ablauf einer angemessenen Frist) können dagegen von Smart Contracts nicht erfasst werden,[195] da Software nach vordefinierten Parametern arbeitet und (bisher) keine wertenden Entscheidungen treffen kann.

[192] Vgl. Definitionsansatz bei *Kaulartz/Heckmann,* CR 2016, 618; siehe auch 4.2.1.
[193] *Heckelmann,* NJW 2018, 504.
[194] *Kaulartz/Heckmann,* CR 2016, 618 (620).
[195] *Kaulartz/Heckmann,* CR 2016, 618 (620).

Diese Grenzen sind nicht starr, sondern stets an die aktuellen technischen Möglichkeiten gekoppelt. Mit einer Weiterentwicklung von KI-Technologien können daher auch erweiterte Einsatzbereiche für Smart Contracts einhergehen.

6.1.3 Vertragsschluss

Die Grundlage für einen Leistungsaustausch zwischen zwei oder mehr Akteuren bildet ein Vertragsverhältnis. Ein Vertragsschluss setzt mindestens zwei übereinstimmende, aufeinander bezogene Willenserklärungen (Angebot und Annahme) voraus.[196] Unter einer Willenserklärung ist jede Äußerung zu verstehen, die einen auf die Herbeiführung einer Rechtswirkung gerichteten Willen zum Ausdruck bringt.[197] Einem Smart Contract kann im Rahmen des Vertragsschlusses unterschiedliche rechtliche Relevanz zukommen.

6.1.3.1 Der Smart Contract als Gegenstand der Vereinbarung

Die größere Praxisrelevanz scheint aktuell den Fällen zuzukommen, in denen der Vertragsschluss rechtlich unabhängig vom Einsatz eines Smart Contracts ist.
Ob ein bestimmtes Verhalten eine Willenserklärung begründet, also den rechtsgeschäftlichen Willen einer Person zum Ausdruck bringt, ist durch Auslegung (§§ 133, 157 BGB) nach dem objektiven Empfängerhorizont unter Einbeziehung aller Umstände des Einzelfalls zu bestimmen.[198] An dieser allgemeinen Regel ändert sich auch im Kontext von DLT-Anwendungen nichts. Einerseits können in der Vornahme von DLT-Transaktionen also konkludente Willenserklärungen (sowohl im Rahmen schuldrechtlicher als auch dinglicher Rechtsgeschäfte) liegen.[199] Häufiger wird der Vertragsschluss aber unabhängig davon stattfinden, d. h., sich bereits aus den äußeren Umständen ergeben.[200] So wird bspw. das Bereitstellen einer betriebsbereiten Tanksäule als Angebot, das Betanken in Selbstbedienung als Annahme dieses Angebots angesehen.[201] Diese Überlegungen können auf das Aufstellen von Elektroladesäulen und die Ingangsetzung eines Ladevorgangs übertragen werden. Dass die Abrechnung unter Einsatz eines Smart Contracts stattfinden soll, wird lediglich als Zahlungsmodalität mitvereinbart.[202]
Diesbezüglich ist insbesondere folgende Überlegung zu beachten: Soll es in der Praxis zum Einsatz von Smart Contracts gegenüber einer breiten Öffentlichkeit kommen (wie es im Mobilitätssektor der Fall ist), ist nicht zu erwarten, dass die Beteiligten in der Lage sein werden, direkt mit der DLT-Ebene zu interagieren und die Wirkungen eines Smart Contracts aus dem Programmcode abzulesen.[203] In aller Regel wird also eine für jedermann lesbare und verständliche Nutzeroberfläche, bspw. eine App, konzipiert werden müssen.[204] Je nach Ausgestaltung im jeweiligen Anwendungsfall wird schon im Bedienen der entsprechenden Funktionen die Abgabe einer Willenserklärung zu erkennen sein.[205] Der Vertragsschluss ist dem Einsatz des Smart Contracts also regelmäßig vorgelagert.[206] Insofern ist der Smart Contract vergleichbar mit der Mechanik eines Warenautomaten,

[196] Jauernig/Ma*nsel*, Vorbemerkungen zu §§ 145 ff. Rn. 2.
[197] Staudinger/*Singer*, Vorbem. zu §§ 116-144 Rn. 1.
[198] Staudinger/*Singer*, § 133 Rn. 18.
[199] *Kaulartz/Heckmann,* CR 2016, 618 (621); *Paulus/Matzke,* ZfPW 2018, 431 (448).
[200] Vergleiche *Bertram,* MDR 2018, 1416 (1419); *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Froitzheim* in Taeger, Rechtsfragen digitaler Transformationen, 311 (314); vgl. *Heckelmann,* NJW 2018, 504 (507); *Kaulartz/Heckmann,* CR 2016, 618 (621); *Paulus/Matzke,* ZfPW 2018, 431 (447).
[201] Jauernig/*Mansel*, § 145 Rn. 7.
[202] Siehe auch *Paulus/Matzke,* ZfPW 2018, 431 (438).
[203] Vgl. *Kaulartz/Heckmann,* CR 2016, 618 (621).
[204] U. a. auch, um Informationspflichten nach §§ 312 ff. BGB nachzukommen, vgl. unten 6.1.4.2.
[205] Vgl. zum Mausklick auf eine Schaltfläche Hoeren/Sieber/Holznagel/*Kitz*, Teil 13.1 Rn. 11.
[206] Vgl. *Kaulartz,* Taeger (Hg.) 2016 – Smart world 2016, 1023 (1031).

die eine schuldrechtlich vereinbarte Leistung zu festgelegten Bedingungen lediglich ausführt.[207]

Im Ergebnis muss stets zwischen der rechtlichen (semantischen) und der technischen (syntaktischen) Ebene unterschieden werden,[208] wobei für die rechtliche Bewertung nur erstere maßgeblich ist. Entgegen seiner Bezeichnung ist ein Smart „Contract" selbst also nicht als Vertrag im Rechtssinne anzusehen.[209]

6.1.3.2 Vertragsschluss unter Einsatz eines Smart Contracts[210]

Es ist allerdings auch möglich, Willenserklärungen unter Verwendung von Programmcode inhaltlich auszudrücken,[211] sodass der Smart Contract einem schriftlichen Vertragsdokument ähnelt. Die Verwendung einer Programmiersprache als Vertragssprache ist, zumindest bei individualvertraglichen Vereinbarungen, als zulässig anzusehen. Wegen des Grundsatzes der freien Sprachenwahl[212] und der Gestaltungs- und Formfreiheit aus § 311 Abs. 1 BGB steht es den Parteien frei, jede lebende oder tote Sprache[213] für den Ausdruck ihrer Willenserklärungen zu wählen. In einer technikoffenen Rechtsordnung sollte kein Unterschied zwischen Formulierungen in einer natürlichen Sprache oder in Programmcode gemacht werden.[214] Die Abgabe einer Willenserklärung kann im Versenden der Transaktion, der Zugang in ihrer Abrufbarkeit in der Zielwallet gesehen werden.[215] Ein Smart Contract kann Willenserklärungen überdies nicht nur inhaltlich ausdrücken, sondern auch (automatisiert) erzeugen und übermitteln, sodass der Vertragsschluss hierdurch zustande gebracht wird.[216]

Zweifelhaft ist die Zulässigkeit der Verwendung von Programmcode als Vertragssprache gegenüber Verbrauchern, wenn dieser allgemeine Geschäftsbedingungen (AGB) enthält, d. h., wenn (auch) die AGB durch eine Programmiersprache ausgedrückt werden.

Zunächst lässt sich anführen, dass es an einer Möglichkeit der zumutbaren Kenntnisnahme i. S. v. § 305 Abs. 2 Nr. 2 BGB fehlt. In einem solchen Fall werden die Klauseln nicht in den Vertrag einbezogen. Eine ausreichende Kenntnisnahmemöglichkeit ist zu bejahen, wenn die AGB ohne zusätzlichen Aufwand zumindest verstanden werden können. Ungeachtet einer relativ großen Verbreitung entsprechender Sprachkenntnisse wird dies bereits bei AGB, die in Englisch abgefasst sind, abgelehnt.[217] Für den durchschnittli-

[207] *Kaulartz/Heckmann,* CR 2016, 618 (621).
[208] *Kaulartz/Heckmann,* CR 2016, 618 (624).
[209] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Kaulartz/Heckmann,* CR 2016, 618 (619); *Paulus/Matzke,* ZfPW 2018, 431 (433 f.).
[210] Dies kann insbesondere bei einer zukünftigen Zunahme der M2M-Kommunikation an Relevanz gewinnen, siehe *Kaulartz/Heckmann,* CR 2016, 618 (621); zu Fragen im Zusammenhang mit maschinellen Erklärungen *Heckelmann,* NJW 2018, 504 (506); *Kaulartz,* Taeger (Hg.) 2016 – Smart world 2016, 1023 (1032); *Paulus/Matzke,* ZfPW 2018, 431 (439 ff.) m. w. N.
[211] *Heckelmann,* NJW 2018, 504 (505); a.A. *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1.
[212] *Kling*, Sprachrisiken im Privatrechtsverkehr., S. 305.
[213] Staudinger/*Singer*, § 119 Rn. 18.
[214] Zum Ganzen *Kaulartz/Heckmann,* CR 2016, 618 (621 f.).
[215] *Paulus/Matzke,* ZfPW 2018, 431 (447); für Zugang beim Anhängen eines neuen Blocks an die Blockchain *Heckelmann,* NJW 2018, 504 (506).
[216] *Paulus/Matzke,* ZfPW 2018, 431 (439).
[217] Ulmer/Brandner/Hensen/*Ernst*, Teil 2 (44) Rn. 32.

chen Verbraucher wird es daher einen unzumutbaren Aufwand darstellen, einen Programmcode inhaltlich zu verstehen.[218] Verneint man die Anwendbarkeit von § 305 Abs. 2 Nr. 2 BGB mit Hinweis auf die Ähnlichkeit von Smart Contracts zu Formularverträgen,[219] könnte es sich bei Vertragsbestimmungen, die in Softwarecode abgefasst sind, um überraschende Klauseln i. S. v. § 305c Abs. 1 BGB handeln. Allein die Verwendung einer Fremdsprache genügt in der Regel allerdings nicht, um Klauseln *inhaltlich* ungewöhnlich oder überraschend zu machen.[220]

Die Verwendung von Softwarecode als Vertragssprache kann schließlich eine unangemessene Benachteiligung i. S. v. § 307 Abs. 1 S. 2 BGB darstellen, was zu einer Unwirksamkeit der entsprechenden Klauseln gem. § 307 Abs. 1 S. 1 BGB führt. Zur Erfüllung der Vorgaben des Transparenzgebots müssen die Rechte und Pflichten der Vertragsparteien vom Verwender möglichst klar und verständlich beschrieben werden, sodass der Leser bei Anwendung der von ihm zu erwartenden Sorgfalt den Inhalt der Klausel hinreichend verstehen kann.[221] Mangels Verständlichkeit genügt die Verwendung fremdsprachiger Klauseln dem Transparenzgebot regelmäßig nicht.[222] Dies muss erst recht für die Verwendung einer Programmiersprache gelten, da es dort ganz überwiegend selbst an rudimentären Sprachkenntnissen fehlen wird. Der Verbraucher wäre auf eine aufwendige Übersetzung angewiesen, um vom Vertragsinhalt Kenntnis nehmen zu können. Infolgedessen würde die Formulierung von AGB in einer Programmiersprache den Verbraucher gem. § 307 Abs. 1 S. 1, 2 BGB unangemessen benachteiligen. Dies kann sich in Zukunft ändern, falls es zu einer Entwicklung allgemein verständlicher Programmiersprachen kommt.

6.1.4 Vertragsinhalt und zwingendes Recht

Auch bei der Bestimmung des Vertragsinhalts kommt es auf die rechtliche und nicht die technische Ebene an.[223] Der Inhalt der Vereinbarung[224] ist nach den allgemeinen Regeln durch Auslegung der Willenserklärungen nach §§ 133, 157 BGB zu ermitteln. Diese Parteivereinbarung muss dann technisch umgesetzt werden. Entstehen Widersprüche oder Lücken zwischen dem Vereinbarten und dem Umgesetzten, ist der vereinbarte Zustand herzustellen.[225]
Selbstverständlich müssen die Wirkungen eines Smart Contracts mit geltendem Recht in Einklang stehen.[226] Dieses bildet stets den Maßstab für die Wirksamkeit und Rechtmäßigkeit des Vertrags.[227] Die im DLT-System erfassten Inhalte treffen dagegen keine Aussage

[218] *Paulus/Matzke,* ZfPW 2018, 431 (459 f.); vgl. zur Verständlichkeit BeckOGK/*Lehmann-Richter*, Stand: 01.06.2018, BGB § 305 Rn. 220, 256.3; zur Abfassung in deutscher Sprache Ulmer/Brandner/Hensen/*Ulmer/Habersack*, § 305 BGB Rn. 151, Teil 2 (44) Rn. 32; zu englischer Sprachfassung LG Berlin, Urteil vom 9.5.2013 – 15 O 44/13, CR 2014, 676; Jauernig/*Stadler*, § 305 Rn. 14.

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

[220] Vgl. zu deutschsprachigen AGB gegenüber sprachunkundigen Ausländern BAG, Urteil vom 19.3.2014 – 5 AZR 252/12 (B), JuS 2015, 65 (66); Ulmer/Brandner/Hensen/*Ulmer/Schäfer*, § 305c BGB Rn. 18.

[221] Schulze/*Schulte-Nölke*, § 307 Rn. 21.

[222] Ulmer/Brandner/Hensen/*Ernst*, Teil 2 (14) Rn. 15, (44) Rn. 23, (51) Rn. 5.

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

[224] Zum Einfluss des Einsatzes virtueller Währungen auf die Vertragstypologie siehe *Ammann,* CR 2018, 379 (380 f.); *Beck/König,* JZ 2015, 130; *Heckelmann,* NJW 2018, 504 (508); *Kaulartz,* CR 2016, 474 (477 f.); *Paulus/Matzke,* ZfPW 2018, 431 (450 f.); *Reiter/Methner* in Taeger, Rechtsfragen digitaler Transformationen, 359 (365 f.); *Shmatenko/Möllenkamp,* MMR 2018, 495 (498 ff.); *Spindler/Bille,* WM 2014, 1357 (1362).

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

[226] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; *Froitzheim* in Taeger, Rechtsfragen digitaler Transformationen, 311 (314); *Heckelmann, NJW 2018, 504* (509); *Kaulartz/Heckmann,* CR 2016, 618 (623).

[227] *Heckelmann,* NJW 2018, 504 (507); *Paulus/Matzke, ZfPW 2018, 431* (448).

über die materiell-rechtliche Richtigkeit der jeweiligen Einträge.[228] Das bedeutet, dass durch die Programmierung bewusst oder unbewusst Ergebnisse herbeigeführt werden können, die der Rechtsordnung widersprechen und korrekturbedürftig sind.

Gelegentlich wird die Frage aufgeworfen, ob es sich bei der automatischen Vollziehung durch einen Smart Contract um verbotene Eigenmacht i. S. v. § 858 Abs. 1 BGB handelt.[229] Diese Frage ist insbesondere dann zu stellen, wenn durch den Smart Contract der Zugriff auf oder die Nutzung einer Sache gesperrt werden kann (z. B. der geleaste Wagen, der sich bei Nichtbegleichung der Leasingraten nicht mehr starten lässt oder das Smart Lock, das den Zutritt zu einer Wohnung bis zur Zahlung der Miete verhindert). In solchen Fällen ist zu prüfen, ob eine Beeinträchtigung des Besitzes vorliegt, die als verbotene Eigenmacht zu qualifizieren ist. Zudem sind spezifische Überlegungen im Zusammenhang mit dem jeweiligen Vertragsverhältnis anzustellen, z. B. was den Schutz von Wohnraummietern angeht. Bei den in diesem Gutachten betrachteten Fällen im Mobilitätsbereich ist dieses Thema aber weniger relevant, da der Einsatz von Smart Contracts lediglich die Zahlungsabwicklung betrifft. Bei den hierfür eingesetzten Token handelt es sich nicht um Sachen gem. § 90 BGB, sodass maximal eine analoge Anwendung von § 858 BGB in Betracht käme. Zudem ist die Zahlungsabwicklung über einen Smart Contract eher so ausgestaltet, dass der Zahlende in Vorleistung geht (s. u. 6.1.4.1.1). Er gibt bereits im Vorfeld die Kontrolle über einen bestimmten Betrag freiwillig ab, indem er eine entsprechende Transaktion an den Smart Contract autorisiert. Damit kommt es bei einer Auslösung der Zahlung durch den Smart Contract nicht zu einem Zugriff auf einen Wert, der sich im Herrschaftsbereich des Zahlenden befindet. Deswegen ist nicht davon auszugehen, dass der Empfänger hier verbotene Eigenmacht übt.

6.1.4.1 Inhaltskontrolle, §§ 307-309 BGB

Soll der Smart Contract Willenserklärungen ausdrücken (s. o. 6.1.3.2) und enthält er Bedingungen, die für eine Vielzahl von Verträgen vorformuliert sind und vom Verwender einseitig gestellt werden (§ 305 Abs. 1 BGB), unterliegen diese den Beschränkungen des AGB-Rechts und damit auch der Inhaltskontrolle nach §§ 307-309 BGB.[230] Hier ergeben sich keine Besonderheiten gegenüber der Inhaltskontrolle sonstiger Verträge, da es sich lediglich um den Ausdruck von Vertragsbedingungen in einer Programmiersprache handelt. Dies ist lediglich im Geschäftsverkehr mit Unternehmern relevant (§ 310 Abs. 1 S. 1 BGB), da der Einsatz von Programmcode als Vertragssprache gegenüber Verbrauchern nicht zulässig ist (s. o. 6.1.3.2).
Soweit der Einsatz eines Smart Contracts als Abwicklungsmodalität vereinbart wird (s. o. 6.1.3.1), wird dies regelmäßig durch AGB geschehen. Zu untersuchen ist daher, inwiefern die Bestimmung der automatisierten Vertragsabwicklung in AGB der Inhaltskontrolle standhält.[231]

6.1.4.1.1 Verstoß gegen § 309 Nr. 2 BGB

Zunächst könnte die automatisierte Ausführung einen Verstoß gegen § 309 Nr. 2 BGB begründen. § 309 Nr. 2 a) BGB verbietet den Ausschluss oder die Einschränkung eines bestehenden Leistungsverweigerungsrechts aus § 320 BGB, während § 309 Nr. 2 b) BGB das Zurückbehaltungsrecht aus § 273 BGB (soweit es auf demselben Vertragsverhältnis beruht) der Disposition durch AGB entzieht. Da der Ablauf eines Smart Contracts in der

[228] *Paulus/Matzke,* ZfPW 2018, 431 (437).
[229] *Djazayeri*, jurisPR-BKR 12/2016 Anm. 1; vgl. auch *C. Paulus/Matzke, CR 2017, 769.*
[230] *Kaulartz/Heckmann,* CR 2016, 618 (622).
[231] Vgl. *Bertram,* MDR 2018, 1416 (1420); vgl. *Schrey/Thalhofer,* NJW 2017, 1431 (1436).

Regel nicht aufgehalten werden kann, wird dem Nutzer faktisch die Möglichkeit genommen, ein ihm zustehendes Leistungsverweigerungs- oder Zurückbehaltungsrecht geltend zu machen. Anders als bspw. bei einer Einzugsermächtigung, besteht bei DLT-Transaktionen auch keine Möglichkeit, gegenüber einer Bank der Belastung zu widersprechen oder eine Wiedergutschrift zu verlangen.[232]

Allerdings weist die automatisierte Ausführung eine gewisse Ähnlichkeit zur Vereinbarung einer Vorleistungspflicht auf. Eine Vorleistungspflicht führt dazu, dass die Fälligkeit der eigenen Leistung vor der Fälligkeit der Leistung des anderen Teils eintritt.[233] Der Einsatz eines Smart Contracts begründet zwar gerade nicht die Pflicht, eine Leistung vorab, d. h. vollständig vor Erhalt der Gegenleistung, zu erbringen. Dessen ungeachtet gibt der Nutzer die Kontrolle über seine Mittel schon im Vorfeld ab und kann die Erbringung der eigenen Leistung im Regelfall nicht mehr einseitig verhindern. § 309 Nr. 2 BGB zielt jedoch nicht darauf ab, die Vereinbarung von Vorleistungspflichten generell zu verbieten. Die Inhaltskontrolle solcher Vereinbarungen richtet sich daher nicht nach § 309 Nr. 2 BGB, sondern nach § 307 BGB.[234]

6.1.4.1.2 Unangemessene Benachteiligung, § 307 Abs. 1 S. 1 BGB

Die Vereinbarung der automatisierten Vertragsabwicklung könnte eine unangemessene Benachteiligung i. S. v. § 307 Abs. 1 S. 1 BGB darstellen. Eine unangemessene Benachteiligung liegt vor, wenn der Verwender Interessen einseitig verfolgt und von vornherein keine hinreichende Rücksicht auf berechtigte Belange seines Vertragspartners nimmt.[235]

Als Ausgangspunkt für die Bewertung einer Klausel, durch die ein Smart Contract in einem Verbrauchervertrag (§ 310 Abs. 3 BGB) als Abwicklungsmodalität vorgesehen wird, können wiederum die Wertungen zur Vorleistungspflicht dienen. Für deren Vereinbarung wird ein sachlicher Grund gefordert, der das Verlangen gegenüber den für den Kunden entstehenden Nachteilen zu rechtfertigen vermag.[236] Besonders das Recht aus § 320 BGB stellt ein Druckmittel dar, um den Vertragspartner zur Erbringung der geschuldeten Leistung zu bewegen und soll ferner vor dessen Insolvenzrisiko schützen.[237] Dieser Schutz ist jedoch nicht immer notwendig. So wird der Einsatz von Vorleistungsklauseln bei alltäglichen Massengeschäften als zulässig angesehen, die einen geringen Geschäftswert und Gewährleistungsbelang haben bzw. wo die Vorleistungspflicht den technischen Erfordernissen der Vertragsabwicklung entspricht.[238]

Zu beachten ist zusätzlich, dass der Einsatz eines Smart Contracts für den Nutzer weniger belastend ist als eine eigentliche Vorleistungspflicht. Bei einer solchen wäre er nämlich verpflichtet, seine Leistung noch vor Erhalt der Gegenleistung vollständig zu erbringen. Ein Smart Contract dient allerdings gerade dazu, Vorleistungsrisiken für beide Parteien

[232] Vgl. BeckOGK/*Weiler*, Stand: 01.01.2019, BGB § 309 Nr. 2 Rn. 74.
[233] Jauernig/Stadler, § 320 Rn. 21.
[234] BeckOGK/*Weiler*, Stand: 01.01.2019, BGB § 309 Nr. 2 Rn. 28 ff.; vgl. BeckOK BGB/*Becker*, Stand: 01.11.2018, § 309 Nr. 2 Rn. 8; Jauernig/*Stadler*, § 309 Rn. 3; MüKoBGB/*Wurmnest*, § 309 Nr. 2 Rn. 13; Palandt/*Grüneberg*, § 309 Rn. 13; Schulze/*Schulte-Nölke*, § 309 Rn. 13; Staudinger/*Coester-Waltjen*, § 309 Nr. 2 Rn. 7.
[235] Ulmer/Brandner/Hensen/*Fuchs*, § 307 BGB Rn. 96.
[236] BeckOGK/*Zschieschack*, Stand: 01.12.2018, BGB § 307 Vorauszahlungsklauseln Rn. 22; vgl. BeckOK BGB/*Becker*, Stand: 01.11.2018, § 309 Nr. 2 Rn. 9; MüKoBGB/*Wurmnest*, § 309 Nr. 2 Rn. 13; Schulze/*Schulte-Nölke*, § 309 Rn. 13; Staudinger/*Coester-Waltjen*, § 309 Nr. 2 Rn. 7.
[237] BeckOGK/*Zschieschack*, Stand: 01.12.2018, BGB § 307 Vorauszahlungsklauseln Rn. 23.
[238] BeckOGK/*Zschieschack*, Stand: 01.12.2018, BGB § 307 Vorauszahlungsklauseln Rn. 26; BeckOK BGB/*Becker*, Stand: 01.11.2018, § 309 Nr. 2 Rn. 10.

zu verringern und nur tatsächlich erbrachte Leistungen abzurechnen. Die automatisierte Abwicklung soll dem Nutzer schließlich auch die Leistung des Anbieters garantieren. Dass eine Situation entsteht, in der ein Interesse am Zurückhalten der eigenen Leistung besteht, ist primär bei technischen Fehlfunktionen zu erwarten. Diesen, sowie mutwilligen Manipulationen der Abrechnungsinfrastruktur, könnte durch eine Zertifizierung von Smart Contracts und Oracles entgegengewirkt werden. In der automatisierten Vertragsdurchführung liegt also grundsätzlich keine einseitige Interessendurchsetzung des Anbieters vor, sondern sie gibt dem Nutzer ausreichend Aussicht auf den Erhalt einer angemessenen Gegenleistung[239], sodass der Verlust des Druckmittels nicht als unangemessene Benachteiligung erscheint[240].

Die voranstehenden Ausführungen lassen sich auf den unternehmerischen Geschäftsverkehr übertragen, sofern auch hier ein sachlicher Grund für die Vereinbarung von Vorleistungspflichten verlangt wird[241].

6.1.4.2 Verbraucherverträge und besondere Vertriebsformen

Im Zusammenhang mit Mobilitätsangeboten sind auch Normen bezüglich besonderer Vertriebsformen zu beachten. Welche Normen konkret einschlägig sein werden, hängt von der Ausgestaltung im Einzelfall ab. An dieser Stelle soll dennoch ein Hinweis auf einige Vorschriften erfolgen, denen bei DLT-basierten Mobilitätslösungen wahrscheinlich Relevanz zukommen wird.

Der Vertragsschluss in den vorgestellten Szenarien wird in elektronischer Form erfolgen und zwar über Websites, Apps oder an elektronischen Self-Service-Punkten (Letztere sind insbesondere für eine elektrische Ladeinfrastruktur von Bedeutung). Folglich sind die Pflichten im elektronischen Geschäftsverkehr nach §§ 312i, j BGB einzuhalten. Die allgemeinen Pflichten nach § 312i BGB gelten gegenüber allen Kunden eines Unternehmers, also auch im B2B-Bereich. § 312j BGB enthält spezifische Pflichten gegenüber Verbrauchern. Der Anbieter muss sich zum Vertragsschluss Telemedien i. S. v. § 1 Abs. 1 TMG bedienen. Es müssen also Dienste eingesetzt werden, die der Übermittlung der Willenserklärungen von Anbieter und Kunde dienen oder dem Kunden zumindest erlauben, eine Bestellung in elektronischer Form abzugeben.[242] Dies erfasst insbesondere auch den Vertragsschluss im Rahmen des M-Commerce, bei welchem Mobiltelefone als mobile Endgeräte genutzt werden, also z. B. über mobile Browser oder per App.[243] Der Begriff der Dienstleistung ist weit auszulegen und geht über das Verständnis des § 611 BGB hinaus. Erfasst ist vielmehr jede Leistung des Unternehmers, die nicht in der Lieferung einer Ware besteht.[244] Die vertraglich geschuldete Leistung muss ferner nicht elektronisch erbracht werden.[245] Leistungen im Mobilitätsbereich können den Regelungen der §§ 312i, j BGB mithin unterfallen. Diese Pflichten unterliegen nicht den Beschränkungen des § 312 Abs. 2-6 BGB, sondern gelten immer, wenn ein Vertragsschluss im elektronischen Geschäftsverkehr vorliegt.

[239] Vgl. MüKoBGB/*Wurmnest*, § 309 Rn. 13.

[240] Vgl. BeckOGK/*Zschieschack*, Stand: 01.12.2018, BGB § 307 Vorauszahlungsklauseln Rn. 27.

[241] Graf von Westphalen/*Thüsing*, Vertragsrecht, Vorleistungsklauseln Rn. 15; BeckOGK/*Weiler*, Stand: 01.01.2019, BGB § 309 Nr. 2 Rn. 98; Palandt/*Grüneberg*, § 309 Rn. 16.

[242] BeckOK BGB/*Maume*, Stand: 01.11.2018, § 312i Rn. 15; Hoeren/Sieber/Holznagel/*Föhlisch*, Teil 13.4 Rn. 56; MüKoBGB/*Wendehorst*, § 312i Rn. 31.

[243] Spindler/Schuster/*Schirmbacher*, BGB § 312i Rn. 12.

[244] BeckOK BGB/*Maume*, Stand: 01.11.2018, § 312i Rn. 8; Spindler/Schuster/*Schirmbacher*, BGB § 312i Rn. 7.

[245] BeckOK BGB/*Maume*, Stand: 01.11.2018, § 312i Rn. 17; MüKoBGB/*Wendehorst*, § 312i Rn. 38; Spindler/Schuster/*Schirmbacher*, BGB § 312i Rn. 7.

Gleichzeitig kann ein Vertragsschluss im Fernabsatz nach § 312c BGB vorliegen, sodass §§ 312d ff. BGB eingreifen. Notwendig ist dazu ein Vertragsschluss unter ausschließlicher Verwendung von Fernkommunikationsmitteln, d. h. unter körperlicher Abwesenheit der Parteien im Zeitpunkt der Vertragsanbahnung und des -abschlusses.[246] Der Anbieter muss zudem über ein für den Fernabsatz organisiertes Vertriebs- oder Dienstleistungssystem verfügen, also in personeller und sachlicher Ausstattung innerhalb seines Betriebs die Voraussetzungen geschaffen haben, die notwendig sind, um regelmäßig Geschäfte im Fernabsatz zu tätigen.[247] Auch hier gilt ein weites Verständnis des Dienstleistungsbegriffs, sodass jede entgeltliche Leistung Gegenstand eines Fernabsatzvertrags sein kann.[248] § 312c BGB (ebenso wie § 312a BGB, der allgemeine Pflichten für den Geschäftsverkehr mit Verbrauchern enthält) ist gem. § 312 Abs. 1 BGB nur bei Verbraucherverträgen i. S. d. § 310 Abs. 3 BGB einschlägig. Zudem darf keine Bereichsausnahme gem. § 312 Abs. 2 BGB eingreifen, da dann nur § 312a Absatz 1, 3, 4 und 6 BGB anzuwenden ist.

In Betracht kommt zum einen die Ausnahme des § 312 Abs. 2 Nr. 5 BGB für Verträge über die Beförderung von Personen. Diese gilt sowohl für Taxifahrten und taxiähnliche Leistungen wie Chauffeurservices als auch für Reisen mit anderen Verkehrsmitteln.[249] Nicht ausgenommen sind allerdings Vermittler und Buchungsplattformen.[250] Zum anderen kann in Bezug auf elektrische Ladesäulen § 312 Abs. Nr. 9 Alt. 2 BGB einschlägig sein, da unter den automatisierten Geschäftsraum alle Self-Service-Einrichtungen fallen, bei denen die Leistung des Unternehmers unmittelbar und unter Verwendung eines Automaten ausgeführt wird.[251]

6.1.5 Behandlung von Leistungsstörungen und Rückabwicklungsfragen

6.1.5.1 Leistungsstörungen

Im Fall von Leistungsstörungen kann die automatisierte Abwicklung wiederum an technische Grenzen stoßen. Zunächst lässt sich nicht jede Pflichtverletzung ausreichend durch Software erfassen. Während sich digital vergleichsweise einfach feststellen lässt, ob eine Partei überhaupt nicht, verspätet oder zu wenig leistet, gestaltet sich die Bewertung im Fall von Schlechtleistungen schon schwieriger. So dürfte bspw. die Entscheidung, ob eine Ware mangelhaft ist, heute noch die Fähigkeiten der besten Oracles übersteigen. Schließlich sind die Konstellationen der Verletzung von Schutz- und Rücksichtnahmepflichten so vielgestaltig, dass die Abbildung in einem Wenn-dann-Schema derzeit kaum denkbar erscheint. Auch andere Voraussetzungen sekundärer Rechtsbehelfe, z. B. das Vertretenmüssen in Form des Verschuldens, lassen sich nicht ohne Weiteres digital darstellen oder hängen von Wertungen im Einzelfall ab und können deshalb bisher nicht durch Smart Contracts abgewickelt werden.[252] Selbst wenn eine Konstellation vorliegt, in der eine Abwicklung mithilfe von Software durchgeführt werden kann, muss diese Abwicklungsmöglichkeit von Anfang an bedacht und in der Programmierung angelegt werden. Ansonsten bleibt den Parteien zur Geltendmachung ihrer Rechte nur der Rechtsweg. In

[246] Tamm/Tonner/*Schirmbacher*, § 9 Rn. 31.
[247] Hoeren/Sieber/Holznagel/*Föhlisch*, Teil 13.4 Rn. 39.
[248] Hoeren/Sieber/Holznagel/*Föhlisch*, Teil 13.4 Rn. 33; Tamm/Tonner/*Schirmbacher*, § 9 Rn. 18.
[249] Spindler/Schuster*Schirmbacher*, BGB § 312 Rn. 40.
[250] Hoeren/Sieber/Holznagel/*Föhlisch*, Teil 13.4 Rn. 49; Spindler/Schuster*Schirmbacher*, BGB § 312 Rn. 41.
[251] BeckOGK/*Busch*, Stand: 01.12.2018, BGB § 312 Rn. 52.1; Tamm/Tonner/*Schirmbacher* § 9 Rn. 43.
[252] *Paulus/Matzke,* ZfPW 2018, 431 (463).

praktischer Hinsicht ist der Einsatz von Smart Contracts demzufolge besonders dort sinnvoll, wo nur eine geringe Wahrscheinlichkeit von Leistungsstörungen besteht bzw. wo sich solche ohne wertende Entscheidungen feststellen lassen.

6.1.5.2 Rückabwicklung

Bei jedem Austauschverhältnis kann die Situation eintreten, dass die erbrachten Leistungen zurückgewährt werden müssen. Eine Partei kann vom Vertrag zurücktreten, sodass ein Rückgewährschuldverhältnis[253] entsteht (§ 346 Abs. 1 BGB). Außerdem kann das schuldrechtliche Geschäft nichtig oder infolge von Anfechtung[254] ex tunc als nichtig anzusehen sein (§ 142 Abs. 1 BGB). Dann muss das jeweils Erlangte gem. § 812 Abs. 1 S. 1 Alt. 1 BGB zurückgewährt werden.

Der Einwand, dass die Unveränderlichkeit von Einträgen in DLT-Systemen in Konflikt mit Rückabwicklungskonstellationen stehe, vermag im zivilrechtlichen Kontext nicht zu verfangen.[255] Zutreffend ist zwar, dass sich Einträge über stattgefundene Transaktionen nicht nachträglich entfernen lassen. Allerdings bedeutet die Nichtigkeit eines Vertrags gerade nicht, dass Verfügungen oder Realakte, die der Erfüllung dieses Vertrags dienen, nicht existieren dürfen. Im Fall des Rücktritts gilt dies erst recht, da hier der ursprüngliche Leistungsaustausch der Rechtslage entspricht und erst nachträglich ein Rückgewährschuldverhältnis entsteht. Ferner sind gerade nicht die Transaktionen als solche nichtig, sondern die ihnen zugrunde liegenden Rechtsgeschäfte.

Schließlich besteht auch keine rechtliche Pflicht, jegliche Dokumentation im Zusammenhang mit einem nachträglich rückabgewickelten Geschäft zu vernichten. Findet bspw. eine Zahlung in Form einer Banküberweisung statt und muss der Betrag später zurückgewährt werden, taucht die ursprüngliche Überweisung weiterhin in den Kontoauszügen der Beteiligten auf. Zusätzlich kann ein Vergleich mit dem Grundbuchrecht herangezogen werden: Nach § 46 Abs. 1 GBO findet die Löschung fehlerhafter Einträge nämlich nicht durch deren Entfernung, sondern durch Hinzufügung eines Löschungsvermerks statt.[256]

Dass es zu Wertverschiebungen kommt, die nicht der materiellen Rechtslage entsprechen oder dass Register eine formelle Rechtslage ausweisen, die materiell-rechtlich nicht zutreffend ist, ist keine Besonderheit von DLT.[257] Im Rahmen der Rückabwicklung genügt also die wirtschaftliche Wiederherstellung des materiell-rechtlich korrekten Zustands durch rückwärts gerichtete Transaktionen.[258]

Der Inhalt des bereicherungsrechtlichen Rückgewähranspruchs wird erheblich von der transferierten Token-Art abhängen. Allgemein ist zunächst festzuhalten, dass es sich bei Token um reine Datenbankeinträge handelt, die ausschließlich, einzigartig und nicht ver-

[253] Ebenso beim Widerruf gem. §§ 355, 357 BGB (soweit dieser nicht ausgeschlossen ist), MüKoBGB/*Fritsche*, § 355 Rn. 59.

[254] Weiterführend zur Anfechtung beim Einsatz von Smart Contracts *Kaulartz/Heckmann,* CR 2016, 618 (622); *Paulus/Matzke,* ZfPW 2018, 431 (454 ff.).

[255] So auch *Paulus/Matzke,* ZfPW 2018, 431 (460); a.A. *Schrey/Thalhofer,* NJW 2017, 1431 (1435 f.).

[256] *Saive,* DuD 2018, 764 (767).

[257] *Paulus/Matzke,* ZfPW 2018, 431 (461).

[258] Vgl. *Beck/König,* AcP 215 (2015), 655 (662); vgl. *Bertram,* MDR 2018, 1416 (1420); vgl. MüKoBGB/*Grundmann*, § 245 Rn. 34; *Paulus/Matzke,* ZfPW 2018, 431 (460); vgl. *Saive,* DuD 2018, 764 (766).

vielfältigbar sind. Bei einer Token-Transaktion wird folglich auch keine Datenmenge verschoben, sondern lediglich die Berechtigung über einen Datenbankeintrag geändert.[259] Der Wert von Token entsteht entweder durch Angebot und Nachfrage oder dadurch, dass sie Rechte oder Forderungen abbilden.[260] Durch die Zuordnung zu seiner Wallet erhält der Nutzer die Möglichkeit, durch Eingabe seines Private Keys die dargestellte Menge an Token zu übertragen.[261]

Daraus ergibt sich, dass bereits diese faktische Zugriffsmöglichkeit in Form der Berechtigung am Datenbankeintrag einen vermögenswerten Vorteil i. S. v. § 812 Abs. 1 S. 1 BGB darstellt. In jedem Fall muss also im Rahmen der Rückabwicklung die Zuordnung in der Datenbank wiederhergestellt werden. Bei sogenannten Currency Token oder virtuellen Währungen, die als Zahlungsmittel dienen,[262] ist dies auch ausreichend. Bei ihrer Übertragung handelt es sich um einen bloßen Realakt.[263] Mangels Sachqualität können Token auch nicht gutgläubig erworben werden.[264] Bildet der Token eine Forderung oder ein Recht ab (so bei sogenannten Utility Token, die gegen Dienstleistungen, Waren oder die Nutzung bestimmter Dienste eingetauscht werden können,[265] und teilweise bei sogenannten Asset Backed Token, nämlich wenn diese einen Anspruch auf ein bestimmtes Asset widerspiegeln[266]), kann das Autorisieren der Token-Transaktion als konkludente Abtretungserklärung gem. §§ 398, 413 BGB ausgelegt werden.[267] Bei einem unwirksamen Kausalgeschäft müsste neben der Wiederherstellung des Registereintrags auch die Forderung zurück abgetreten werden.

Repräsentiert ein Asset Backed Token das Eigentum an einer Sache,[268] müsste bei einer Rückabwicklung auch jegliche erlangte Position an dieser Sache herausgegeben werden (Eigentum und/oder Besitz). Es ist allerdings fraglich, ob eine Token-Transaktion für die Übereignung einer Sache ausreichen kann.[269] Im Autorisieren der Transaktion kann durchaus eine konkludente Willenserklärung im Rahmen der dinglichen Einigung liegen. Wird dem Erwerber aber nicht zumindest mittelbarer Besitz an der betroffenen Sache eingeräumt, kommt maximal ein Übergabesurrogat i. S. v. § 931 BGB in Betracht. Ein gutgläubiger Erwerb wäre lediglich unter den Voraussetzungen des § 934 möglich. Da ein (gutgläubiger) Eigentumserwerb an Token mangels Sachqualität ausscheidet (s. o.), würde auch eine Einordnung von Token als Inhaberpapiere den Eigentumserwerb nicht erleichtern.[270]

6.1.5.3 Zugang zu Schiedsstellen/Schaffung von Justizschnittstellen

Zur Anspruchsdurchsetzung sind die Parteien auf den Rechtsweg verwiesen, was grundsätzlich dem Normalfall entspricht. Die Besonderheit bei DLT-Transaktionen besteht darin, dass der Anspruchsinhaber auf die Mitwirkung des Anspruchsgegners angewiesen

[259] *Kaulartz/Matzke,* NJW 2018, 3278; *Paulus/Matzke,* ZfPW 2018, 431 (437).
[260] *Kaulartz/Matzke,* NJW 2018, 3278.
[261] *Kaulartz/Matzke,* NJW 2018, 3278 (3279).
[262] *Kaulartz/Matzke,* NJW 2018, 3278 (3279).
[263] *Heckelmann,* NJW 2018, 504 (508); *Kaulartz/Matzke,* NJW 2018, 3278 (3280); *Paulus/Matzke,* ZfPW 2018, 431 (451).
[264] *Kaulartz/Matzke,* NJW 2018, 3278 (3283).
[265] *Kaulartz/Matzke,* NJW 2018, 3278 (3279).
[266] *Kaulartz/Matzke,* NJW 2018, 3278 (3280).
[267] *Kaulartz/Matzke,* NJW 2018, 3278 (3280).
[268] *Kaulartz/Matzke,* NJW 2018, 3278 (3280).
[269] Schon bei Traditionspapieren, die nach hier vertretener Ansicht durch Token ersetzt werden können, ergibt sich die Eigentumsübertragung nicht ohne Weiteres aus der Übergabe des Papiers, vgl. Baumbach/Hopt/*Merkt*, § 448 Rn. 2, 3.
[270] A. a. wohl *Kaulartz/Matzke,* NJW 2018, 3278 (3281 ff.).

ist, da nur dieser die Transaktion durch das Signieren mit dem privaten Schlüssel durchführen kann. Geht es also um die Durchsetzung eines Anspruchs auf Rückübertragung von Token, müsste der Anspruchsteller im Wege einer Leistungsklage gegen den Empfänger vorgehen, damit dieser zur Vornahme der rückwärts gerichteten Transaktion verurteilt wird.[271] Zugriffsmöglichkeiten einer dritten Instanz, wie bspw. bei Bankkonten, bestehen regelmäßig nicht.[272] Bei der Ausführung einer DLT-Transaktion handelt es sich um eine unvertretbare Handlung i. S. v. § 888 Abs. 1 S. 1 ZPO, die nur durch Zwangsgeld oder Zwangshaft durchgesetzt werden kann.[273] Eine Pfändung[274] von Token ist dagegen nicht möglich.

Zur Vereinfachung der Anspruchsdurchsetzung, möglicherweise aber auch zur Verhinderung des Ablaufs fehlerhafter Smart Contracts, könnte eine Zugriffsmöglichkeit für eine vertrauenswürdige Dritte Stelle geschaffen werden. Denkbar wäre entweder eine Justizschnittstelle[275] oder eine programmierte Schiedsstelle[276]. Durch die Schaffung nachträglicher Manipulationsmöglichkeiten[277] würden DLT-basierte Smart Contracts allerdings einen Teil ihrer technisch gewährleisteten Vertrauenswürdigkeit einbüßen, u. a. auch wegen des Risikos eines Missbrauchs dieser Möglichkeiten durch Unbefugte. Sinnvoll könnte eine Gestaltung in Form einer 3-Personen-Lösung sein. Das Anhalten eines Smart Contracts oder die Auslösung einer rückwärts gerichteten Transaktion würden die Signatur durch zwei von drei Schlüsseln erfordern. Die Schlüssel wären auf die Parteien und einen vertrauenswürdigen Dritten (z. B. eine Schiedsstelle) verteilt. Sollten sich die Parteien nicht einig werden, könnte die dritte Stelle angerufen werden und eine Entscheidung treffen.[278]

6.1.6 Exkurse

6.1.6.1 Aufsichtsrechtliche Fragen

Bei der Ausgestaltung DLT-basierter Bezahlsysteme sind aufsichtsrechtliche Implikationen zu beachten. Unter Umständen können Erlaubnispflichten einschlägig sein, insbesondere

[271] *Saive,* DuD 2018, 764 (766). Ein Vorgehen gegen alle Nodes o. ä. erscheint dagegen nicht praktikabel. Vgl. allerdings Klage auf Einführung einer rescue fork https://www.silvermillerlaw.com/wp-content/uploads/2018/04/2018-4-6-DE-1-CLASS-ACTION-COMPLAINT-1.pdf.

[272] *Paulus/Matzke,* ZfPW 2018, 431 (463).

[273] Vgl. *Kütük/Sorge,* MMR 2014, 643 (645); *Kaulartz,* CR 2016, 474 (479) mit dem Hinweis, dass in entsprechenden Fällen auch die Herausgabe der Datei, in der der private Schlüssel gespeichert ist oder die Übertragung des Herausgabeanspruchs gegen den Wallet-Anbieter möglich ist; *Paulus/Matzke,* ZfPW 2018, 431 (464); *Saive,* DuD 2018, 764 (767).

[274] Vgl. zur Anwendbarkeit des § 244 BGB auf virtuelle Währungen *Beck/König,* AcP 215 (2015), 655 (662 ff.); vgl. auch BeckOGK/*Freitag*, Stand: 01.08.2018, BGB § 244 Rn. 28. Die Vorschrift normiert allerdings eine Ersetzungsbefugnis des Schuldners, Jauernig/*Berger*, § 244 Rn. 16. Eine Anwendung zu Gunsten des Gläubigers scheidet daher eher aus.

[275] *Bertram,* MDR 2018, 1416 (1420); *Kaulartz/Heckmann,* CR 2016, 618 (624); *Simmchen,* MMR 2017, 162 (164).

[276] *Kaulartz/Heckmann,* CR 2016, 618 (624).

[277] Zur technischen Umsetzbarkeit durch sogenannter Chameleon Hashes siehe *Saive,* DuD 2018, 764 (766) m.w.N.

[278] Vgl. zur 3-Personen-Lösung *Werbach,* Berkeley Tech. L.J. 2018, 491 (548); siehe auch oben 4.2.1.

nach § 32 Abs. 1 KWG oder § 10 Abs. 1 ZAG.[279] Laut BaFin kommt es wegen der mannigfaltigen Funktionsweisen von Token immer auf eine Prüfung im Einzelfall an.[280] Zur Orientierung können aber gewisse generelle Aussagen herangezogen werden. Für die Ausgabe sogenannter Utility Token, die nur im Netzwerk des Emittenten im Austausch gegen Waren oder Dienstleistungen genutzt werden können, wird tendenziell eine Erlaubnisfreiheit angenommen. Anders kann die Bewertung allerdings ausfallen, wenn den Token auch eine Zahlungsmittelfunktion zukommt, da dann eine Qualifizierung als Rechnungseinheit und damit als Finanzinstrument i. S. d. KWG wieder näherliegt.[281]

Bitcoins sind von der BaFin als Finanzinstrumente i. S. v. § 1 Absatz 11 Satz 1 KWG in Form von Rechnungseinheiten eingeordnet worden, wobei die Einordnung auch auf andere virtuelle Währungen (oder Currency Token) anwendbar ist. Grundsätzlich sieht die BaFin den Einsatz virtueller Währungen als Zahlungsmittel (als Ersatz für Bar- oder Buchgeld) nicht als erlaubnispflichtige Tätigkeit an. Es können aber zusätzliche Umstände hinzukommen, die eine Erlaubnispflicht auslösen. In Betracht kommen insbesondere Tätigkeiten wie der Betrieb von Plattformen oder Börsen, aber auch der Umtausch zwischen gesetzlichen und virtuellen Währungen.[282]

6.1.6.2 Haftung für die Bereitstellung von Smart Contracts

Eine weitere Frage ergibt sich bezüglich der Haftung für die Bereitstellung fehlerhafter Smart Contracts. Hierbei ist danach zu differenzieren, wer die Programmierung vornimmt. Stammt diese vom Leistungsanbieter selbst und erleidet der Nutzer infolge von Programmierfehlern einen Schaden, greift bei Vorliegen der allgemeinen Voraussetzungen die vertragliche Haftung des Anbieters gegenüber dem Nutzer. Die Pflichtverletzung wird in einer unzureichenden Erfüllung von Sorgfaltspflichten (§ 241 Abs. 2 BGB) zu sehen sein. Bezieht der Anbieter die Software von einem Dritten, haftet Letzterer dem Anbieter ebenfalls aus dem Vertragsverhältnis.[283] Im Verhältnis zwischen dem Anbieter und dem Nutzer kommt wiederum eine vertragliche Haftung in Betracht. Zentral wird aber die Frage sein, ob der Anbieter schuldhaft einen fehlerhaften Smart Contract eingesetzt hat, ob der Fehler für ihn also erkennbar war.

[279] *Bundesanstalt für Finanzdienstleistungsaufsicht (*BaFin), Hinweisschreiben vom 20.02.2018, GZ: WA 11-QB 4100-2017/0010.; vgl. auch *Keding,* WM 2018, 64.

[280] *Fußwinkel/Kreiterling*, Blockchain-Technologie – Gedanken zur Regulierung., abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel.html?nn=11056122#U33; siehe ferner *European Securities and Markets Authority (*ESMA), Advice Initial Coin Offerings and Crypto-Assets., abrufbar unter https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, Rn. 76 f. und *European Securities and Markets Authority (*ESMA), Own Initiative Report on Initial Coin Offerings and Crypto-Assets., abrufbar unter https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf, Rn. 46 ff.; ähnlich *European Securities and Markets Authority (*ESMA), ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements., abrufbar unter https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf, S. 1 f.; *Parhofer/Klöhn/Resas,* ZBB 2018, 89 (102 f.).

[281] *Fußwinkel/Kreiterling*, Blockchain-Technologie – Gedanken zur Regulierung.; vgl. auch *European Securities and Markets Authority (*ESMA), Advice Initial Coin Offerings and Crypto-Assets., Rn. 86.

[282] *Bundesanstalt für Finanzdienstleistungsaufsicht (*BaFin), Virtuelle Währungen/Virtual Currency (VC)., abrufbar unter https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_artikel.html.

[283] Zur Frage, ob es sich bei der Erstellung von Smart Contracts um eine Rechtsdienstleistung oder -beratung handelt *Heckelmann,* NJW 2018, 504 (509); *Kaulartz,* Taeger (Hg.) 2016 – Smart world 2016, 1023 (1033 f.).

Möglicherweise werden Smart Contracts auch öffentlich und unentgeltlich zur Verfügung gestellt. In diesem Fall kommt eine Anwendung des Schenkungsrechts[284] mit entsprechenden Haftungsprivilegierungen in Betracht (§§ 521 ff. BGB). Fraglich ist jedoch, ob in solchen Fällen überhaupt ein Rechtsbindungswille erkennbar ist oder ob es sich bei der Softwareüberlassung um ein Gefälligkeitsverhältnis handelt. Hiergegen sprechen allerdings die in der Regel gegebene wirtschaftliche Bedeutung von Software, etwaige Schadensrisiken und das Interesse des Überlassenden an der Vereinbarung seiner Lizenzbedingungen.[285]

Je stärker die Anbindung an die reale Welt ausfällt, desto wahrscheinlicher erscheint die Verletzung eines durch § 823 Abs. 1 BGB geschützten Rechtsguts durch den Einsatz eines fehlerhaften Smart Contracts.[286] Sind allerdings Token als solche betroffen (z. B. im Falle einer fehlerhaften Transaktion) wird das Problem sichtbar, dass weder das Vermögen als solches noch Forderungen von § 823 Abs. 1 BGB geschützt werden.[287] Eine eingehende Auseinandersetzung mit dem deliktischen Schutz von Token würde den Umfang dieses Gutachtens übersteigen, sodass an dieser Stelle auf weiterführende Literatur verwiesen sei.[288]

6.1.7 Zusammenfassung

Insgesamt lässt sich festhalten, dass die vorhandenen zivilrechtlichen Regelungen geeignet sind, um den Einsatz von Smart Contracts ausreichend zu erfassen. Die technologischen Besonderheiten von DLT stellen das Recht nicht vor unlösbare Herausforderungen.

Trotz dieser Besonderheiten sind die allgemeinen Regeln auch auf Verträge anzuwenden, bei denen in irgendeiner Form ein Smart Contract (im Rahmen des Vertragsschlusses oder lediglich als Abwicklungsmodalität) zum Einsatz kommt. Ob eine Willenserklärung vorliegt, in welchem Verhalten sie erblickt werden kann und welchen Inhalt sie hat, ist durch Auslegung nach §§ 133, 157 BGB zu ermitteln. Der Vertragsschluss wird häufig vollständig außerhalb der DLT-Anwendung liegen. Überdies unterliegen Verträge, die unter Einsatz von DLT geschlossen oder ausgeführt werden denselben Beschränkungen wie alle anderen Verträge. Die Parteien müssen also das geltende Recht respektieren, so bspw. das Recht der allgemeinen Geschäftsbedingungen und das Verbraucherschutzrecht. Ungeachtet der Immutabilität von DLT-Systemen lassen sich Rückabwicklungsfragen zufriedenstellend lösen, da die wirtschaftliche Wiederherstellung des ursprünglichen Zustands ausreicht. Insgesamt ist der erreichbare Grad der Automatisierung durch die Grenzen der technischen Möglichkeiten beschränkt. Rechtliche Entscheidungen bedürfen an vielen Stellen wertender Betrachtungen, die aktuell nicht von Software angestellt werden können. Das betrifft sowohl den Leistungsaustausch, der durch einen Smart Contract durchgeführt werden kann, als auch Fragen des Leistungsstörungsrechts.

[284] Auer-Reinsdorff/Conrad/*Kast*, § 12 Rn. 143, 150; Leupold/Glossner/*von dem Bussche/Schelinski*, Teil 1 Rn. 261; *Redeker*, IT-Recht., Rn. 595a.

[285] *Redeker*, IT-Recht., Rn. 595a.

[286] Zur Frage der Anwendbarkeit des ProdHaftG auf Software siehe BeckOGK/*Rebin*, Stand: 01.05.2018, ProdHaftG § 2 Rn. 49 ff.; BeckOK BGB/*Förster*, Stand: 01.11.2018, ProdHaftG § 2 Rn. 22 ff.; Dauner-Lieb/Langen/*Katzenmeier*, ProdHaftG § 2 Rn. 3; MüKoBGB/*Wagner*, ProdHaftG § 2 Rn. 17 ff.

[287] MüKoBGB/*Wagner*, § 823 Rn. 291, 370.

[288] *Engelhardt/Klein,* MMR 2014, 355 (358); *Kaulartz,* CR 2016, 474 (479); *Paulus/Matzke, ZfPW 2018, 431* (453 f.); *Reiter/Methner* in Taeger, Rechtsfragen digitaler Transformationen, 359 (365); *Seitz* in Taeger, Recht 4.0, 777 (786 f.); *Shmatenko/Möllenkamp,* MMR 2018, 495 (498); *Spindler/Bille,* WM 2014, 1357 (1363).

6.2 Datenschutzrechtliche Bewertung

Die folgende Untersuchung geht der Frage nach, inwieweit durch DLT-Lösungen zur Abwicklung von Transaktionen im Mobilitätssektor personenbezogene Daten nach der EU-Datenschutz-Grundverordnung (DS-GVO) verarbeitet werden. Dabei soll geklärt werden, welche Stellen für die stattfindenden Datenverarbeitungen als datenschutzrechtlich Verantwortliche einzuordnen sind, auf welche Rechtsgrundlagen sie sich dafür stützen und wie sie den Lösch- und Berichtigungspflichten nachkommen können. Die Betrachtung wird auf diejenigen Datenverarbeitungen eingegrenzt, die von den Beteiligten über eine DLT-Plattform durchgeführt werden. Für sonstige Verarbeitungen personenbezogener Daten durch die Beteiligten, die für die jeweilige Durchführung der Mobilitätslösung erforderlich sind, gelten ebenfalls die datenschutzrechtlichen Vorgaben. Diese sollen mangels spezifischer Probleme aber nicht Gegenstand der folgenden Betrachtung sein.

Die folgenden Ausführungen gelten unabhängig vom jeweiligen Einsatz im Einzelfall. Im Rahmen dieses allgemeinen Teils sollen Lösungswege aufgezeigt werden, die grundsätzlich für jede Implementierung der DLT-Technologie im Mobilitätssektor derzeit datenschutzrechtskonform sind. Im besonderen Teil soll dann bei den jeweiligen Ausführungen zu den einzelnen Anwendungsfällen auf die hier gefundenen Ergebnisse verwiesen werden.

6.2.1 Anwendbarkeit der DS-GVO

Die DS-GVO gilt, wenn der für die Datenverarbeitung Verantwortliche seine Niederlassung innerhalb der Union hat. Der Ort der Verarbeitung ist dahingehend irrelevant. Weiter gilt die DS-GVO, wenn die Datenverarbeitung im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen an eine in der Union ansässige betroffene Person vorgenommen wird, auch wenn sich der Verantwortliche für die Datenverarbeitung außerhalb der Europäischen Union befindet.

Soweit durch die hier untersuchten DLT-Lösungen Dienstleistungen zumindest auch an natürliche Personen, die innerhalb der Europäischen Union ansässig sind, angeboten werden, wird man von einer Geltung der DS-GVO für die stattfindenden Datenverarbeitungen ausgehen können. Bei einer Ladeinfrastruktur für elektronische Fahrzeuge oder der Abwicklung von Transaktionen beim Ridesharing richtet sich die Dienstleistung auch an natürliche Personen mit Sitz innerhalb der Europäischen Union. Folglich wird für die in diesem Zusammenhang stattfindenden Datenverarbeitungen die DS-GVO gelten. Wird durch DLT eine Plattform für eine Platooning-Anwendung geschaffen oder die Transaktion elektronischer Traditionspapiere ermöglicht, so stellt dies regelmäßig kein Angebot von Waren oder Dienstleistungen an eine natürliche Person dar. Auch in diesem Fall ist jedoch die DS-GVO anwendbar, soweit der für die Datenverarbeitung Verantwortliche seine Niederlassung innerhalb der Union hat. Die Frage nach dem datenschutzrechtlich Verantwortlichen ist u. a. Gegenstand der folgenden Untersuchung.

6.2.2 Verarbeitung personenbezogener Daten

Nach Art. 1 Abs. 2 DS-GVO ist der Zweck der Datenschutz-Grundverordnung der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere des Rechts auf Schutz personenbezogener Daten. Verarbeitungen von Daten sind daher nicht im Allgemeinen datenschutzrechtlich relevant, sondern nur wenn es sich um „personenbezogene Daten" handelt.[289]

[289] So auch Ehmann/Selmayr/*Klabunde*, Art. 4 Rn. 7; Sydow/*Ziebarth*, Art. 4 Rn. 9; Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 4.

Im Folgenden soll untersucht werden, an welchen Stellen es bei der Umsetzung von Mobilitätskonzepten durch DLT-Anwendungen zur Verarbeitung personenbezogener Daten kommen kann. Zunächst soll dabei festgestellt werden, welche Datenverarbeitungen für die Untersuchung relevant sind. Weiter wird geprüft, ob die dabei verarbeiteten Daten einen Personenbezug aufweisen und wer Verantwortlicher für die Datenverarbeitung ist.

6.2.2.1 Relevante Datenverarbeitungen

Der Begriff der Datenverarbeitung nach der DS-GVO ist weit gefasst. Art. 4 Nr. 2 DS-GVO enthält eine Legaldefinition, wonach „jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte[…] Vorgang oder jede solche Vorgangsreihe, wie das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ von Daten als eine Datenverarbeitung anzusehen ist.

Bei der Übermittlung von Daten über eine DLT-Architektur muss prinzipiell zwischen dem Einpflegen der Daten, den dezentralen Speichervorgängen und dem Auslesen der Daten unterschieden werden. Im Folgenden soll kurz erläutert werden, inwieweit diese Vorgänge unter die Definition der Datenverarbeitung zu subsumieren sind. Die Frage, welche Stellen für die Datenverarbeitungen verantwortlich sind, wird jedoch erst in einem späteren Schritt geklärt werden.[290]

6.2.2.1.1 Einpflegen der Daten in die DLT-Plattform

Jede Information, die dezentral auf der DLT-Plattform gespeichert werden soll, muss initial von einer Stelle eingepflegt werden. Es ist dabei möglich, dass lediglich Teile eines Datensatzes auf den DLT-Layer gelegt werden, andere Teile lokal bei der jeweils einpflegenden Stelle verbleiben. Auf die off-Chain gespeicherten Datensätze kann gleichwohl verlinkt werden. Durch das Einpflegen der Daten werden die Informationen allen Personen zugänglich gemacht, die Lesezugriff auf die Daten erhalten. In einer Public-DLT-Applikation ist das grundsätzlich jedermann, in der Private-DLT-Applikation nur die jeweiligen Teilnehmer. Diese Form der Zugänglichmachung könnte als eine Offenlegung durch Übermittlung oder eine Verbreitung angesehen werden, wenigstens jedoch ist sie als „andere Form der Bereitstellung“ an alle Teilnehmer mit Lesezugriff zu qualifizieren, sodass von einer Datenverarbeitung auszugehen ist.[291]

6.2.2.1.2 Weiterverarbeitung der Daten auf der DLT-Plattform

Die in die dezentrale Datenbank einzuspeichernden Informationen werden von den Teilnehmern des Peer-to-peer-Netzwerks vom Absender entgegengenommen und innerhalb des Netzwerks an alle Teilnehmer verteilt. Diese Verarbeitung kann als „Verbreitung“ von Daten eingeordnet werden. Je nach Konsensverfahren der DLT-Technologie wird die dezentrale Datenbank, gegebenenfalls durch Miner, um die neu erhaltenen Informationen ergänzt. Diese Handlungen, die als „Organisation“, „Ordnen“ und „Speichern“ von Daten eingeordnet werden können, sind ebenfalls Datenverarbeitungen.

6.2.2.1.3 Auslesen der Daten aus der DLT-Plattform

[290] Siehe zur Frage nach dem datenschutzrechtlichen Verantwortlichen ausführlich unter, 6.2.3.
[291] Ebenso für eine Public-Blockchain, *Marnau* in Eibl/Gaedke, INFORMATIK 2017, 1025 (1033).

Die Daten werden von den Teilnehmern des Systems mit Lesezugriff bei Bedarf ausgelesen. Dies betrifft sowohl On-Chain-Daten als auch Off-Chain-Daten, auf die verlinkt wurde. Diese Auslesevorgänge sind ebenfalls Datenverarbeitungen.

6.2.2.2 Personenbezogene Daten

Bei den verarbeiteten Daten müsste es sich um „personenbezogene Daten" handeln. Der Begriff ist in Art. 4 Nr. 1 S. 1 DS-GVO legaldefiniert. Demnach sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Der Begriff des personenbezogenen Datums war bereits Gegenstand der EU-Richtlinie 95/46/EG (Datenschutzrichtlinie) und wurde von der Artikel-29-Datenschutzgruppe näher untersucht.[292] Ein personenbezogenes Datum besteht demnach aus den vier Elementen natürliche Person, Information, Personenbezug und Identifizierung bzw. Identifizierbarkeit. Dies lässt sich für die Auslegung des Begriffs nach der DS-GVO übertragen.[293] Dabei ist stets zu beachten, dass die Elemente beim jeweiligen Betrachter der Daten vorliegen müssen, ein Personenbezug also immer relativ festzustellen ist.

6.2.2.2.1 Natürliche Person

Von der DS-GVO sind nur die Daten natürlicher Personen geschützt. Zu den natürlichen Personen zählen alle Menschen ungeachtet ihrer Staatsangehörigkeit. Erfasst sind aber nur lebende Personen, nicht Daten Verstorbener.[294] Die Mitgliedstaaten können jedoch zum Schutz dieser Daten eigene Regelungen treffen. Zu beachten ist, dass ein Datum, das sich auf eine verstorbene Person bezieht, gleichzeitig auch Informationen über noch lebende Personen enthalten kann.[295] Datenschutzrechtlich irrelevant ist dagegen die Verarbeitung von Informationen über juristische Personen, solange von diesen nicht auf natürliche Personen geschlossen werden kann.

Natürliche Personen, die von den Datenverarbeitungen betroffen sind, können sich zum einen unter den Nutzern finden, zum anderen können die DLT-Anwendungen auch Daten Dritter erfassen.

6.2.2.2.1.1 Nutzer der DLT-Anwendung

Betroffene Personen können in erster Linie die Nutzer der DLT-Anwendung sein. Hinsichtlich der Möglichkeit der datenschutzrechtlich relevanten Verarbeitung von Daten über die Nutzer der Anwendung kann danach differenziert werden, an welchen Personenkreis sich die Anwendung richtet.

6.2.2.2.1.1.1 B2B-DLT-Anwendungen

DLT-Anwendungen können so konzipiert werden, dass sie einer Nutzung durch Privatpersonen nicht offenstehen. Wird eine DLT-Anwendung nur von Unternehmen genutzt, so sind verarbeitete Daten, die sich auf diese Unternehmen beziehen, grundsätzlich nicht datenschutzrechtlich relevant. Eine Ausnahme besteht nur dann, wenn ein Unternehmen mit einer natürlichen Person so verknüpft ist, dass Informationen über das Unternehmen zugleich Informationen über die dahinterstehende natürliche Person beinhalten. Denkbar ist u. a., dass durch die Offenbarung von Vermögensverhältnissen eines Unternehmens

[292] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten".
[293] Ebenso Ehmann/Selmayr/*Klabunde*, Art. 4 Rn. 8.
[294] DS-GVO, Erwägungsgrund 27.
[295] BeckOK DatenschutzR/*Schild*, Art. 4 Rn. 11; *Kühling/BuchnerKlar/Kühling*, Art. 4 Rn. 5; Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 26.

auch Informationen über die Vermögensverhältnisse der mit dem Unternehmen verknüpften natürlichen Personen bekannt werden. Dies wird man insbesondere bei „Ein-Mann-Unternehmen" annehmen können, wobei auch andere Fälle denkbar sind. So könnte bspw. der Name der Firma den Namen des Inhabers tragen. Die Wahrscheinlichkeit, Informationen über hinter dem Unternehmen stehende natürliche Personen zu erhalten, sinkt grundsätzlich mit steigender Unternehmensgröße. Gerade bei kleineren Unternehmen muss die Möglichkeit aber Beachtung finden.

Nehmen an einer DLT-Anwendung als unmittelbare Nutzer hingegen nur Unternehmen teil, bei denen eine mit der Nutzerkennung des Unternehmens verknüpfte Transaktion keine Rückschlüsse auf natürliche Personen erlaubt, so sind diese Datenverarbeitungen datenschutzrechtlich nicht relevant. Erlaubt die jeweilige Mobilitätsanwendung eine Konzeption, bei welcher die durchzuführenden Transaktionen allein von solchen Unternehmen vorgenommen werden, so ist diese aus datenschutzrechtlicher Sicht zunächst vorzugswürdig. Eine solche reine B2B-DLT-Applikation wird regelmäßig eine geschlossene DLT-Plattform erfordern, um zu verhindern, dass ausschließlich Unternehmen teilnehmen, welche die genannten Voraussetzungen erfüllen. Sie ist grundsätzlich auch dann möglich, wenn natürliche Personen, bspw. als Endkunden, an der jeweiligen Mobilitätslösung teilnehmen sollen. Voraussetzung ist dann jedoch, dass diese Personen nicht selbst unmittelbar mit einer eigenen Nutzerkennung auf der DLT-Ebene aktiv werden. Dies wird regelmäßig erfordern, dass die Zahlungsabwicklung zwischen den natürlichen Personen und den Anbietern der jeweiligen Dienstleistung nicht unmittelbar erfolgt. Stattdessen stehen die natürlichen Personen in einem Vertragsverhältnis mit einem Intermediär. Nur dieser wickelt über die DLT-Plattform Transaktionen mit den Dienstleistern ab, während die Zahlung zwischen natürlicher Person und Intermediär off-Chain erfolgt.

6.2.2.2.1.1.2 B2C- und C2C-DLT-Anwendungen

Ist die DLT-Anwendung dagegen so konzipiert, dass Privatpersonen unmittelbar als Nutzer auf der DLT-Ebene aktiv werden, so ist jede Verarbeitung von Daten über die Nutzer datenschutzrechtlich relevant.

6.2.2.2.1.2 Daten Dritter auf der DLT-Plattform

Die DLT-Anwendung dient stets zur Herstellung eines Konsenses zwischen den Parteien über eine Information. Je nach Anwendungsfall ist es nicht ausgeschlossen, dass diese Informationen auch Daten über natürliche Personen enthalten, die nicht Nutzer des Systems sind.
Gelingt es, die Mobilitätsanwendung so zu gestalten, dass nur Unternehmen auf der DLT-Ebene aktiv werden, so sind die Endkunden als natürliche Personen nicht unmittelbare Nutzer des Systems. Die Verarbeitung von Daten auf der DLT-Plattform durch die Unternehmen kann aber auch dann datenschutzrechtlich relevant werden, wenn die on-Chain verarbeiteten Daten Informationen über die Endkunden der Anwendung enthalten.

6.2.2.2.2 Information

Der Begriff der „Information" ist weit gefasst und enthält sowohl objektive Informationen (z. B. Name, Wohnort) als auch subjektive Informationen (z. B. Meinungen, Äußerungen). Der Wahrheitsgehalt der Information spielt dabei keine Rolle. Die Information kann in jedem erdenklichen Format vorliegen.[296]

[296] Ehmann/Selmayr/*Klabunde*, Art. 4 Rn. 9; Sydow/*Ziebarth*, Art. 4 Rn. 41.

Nahezu alle Daten, die im DLT-Verfahren verarbeitet werden, weisen einen mehr oder weniger großen Informationsgehalt auf. In der Regel werden die Nutzer zwar nicht mit ihrem Klarnamen auftreten. Informationen finden sich aber bspw. in den Nutzerkennungen, den Kontoständen oder den Zeitstempeln. Als Information genügt bereits die Tatsache, dass eine Interaktion auf der DLT-Plattform stattgefunden hat.

Eine Information ist den Daten jedoch nur dann zu entnehmen, wenn diese für den jeweiligen Betrachter auch lesbar ist. Verschlüsselte Daten können, auch wenn sie für jedermann einsehbar sind, nur von denjenigen Personen gelesen werden, die über den entsprechenden Schlüssel verfügen. Für Personen ohne Lesezugriff handelt es sich bei verschlüsselten Daten folglich nicht um personenbezogene Daten.[297]

6.2.2.2.3 Personenbezug

Nach Ansicht der Artikel-29-Datenschutzgruppe besteht ein Personenbezug dann, wenn entweder ein Inhalts- oder ein Zweck- oder ein Ergebniselement vorhanden ist. Ein Inhaltselement liegt vor, wenn es sich bei den Informationen um solche über die Person handelt, ein Zweckelement dann, wenn sie „mit dem Zweck verwendet werden bzw. verwendet werden können, um eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen“[298]. Ein Ergebniselement liegt vor, wenn sich die Information auf die Rechte und die Interessen einer bestimmten Person auswirken könnte. Es genügt, wenn die Person aufgrund der Verarbeitung der Information anders behandelt werden könnte als andere Personen.[299] Bei der Untersuchung aller Elemente müssen stets die näheren Begleitumstände des Einzelfalls Beachtung finden.

6.2.2.2.3.1 Daten über die Nutzer der Anwendung

Die Nutzer interagieren regelmäßig über ihre Nutzerkennung. Die Tatsache, dass eine Nutzerkennung einer natürlichen Person zugeordnet ist, stellt bereits eine Information über die Person dar (Inhaltselement). Ebenso verhält es sich mit weiteren Informationen, die mit der Nutzerkennung verknüpft werden können, wie Kontostände, Zeitstempel oder aufgezeichnete Interaktionen der Nutzerkennung. Die Informationen sind für diejenigen Teilnehmer des Netzwerks relevant, die ein Interesse an deren Aufzeichnung haben. Sie können aufgrund der Informationen beurteilen, ob der Nutzer eine erforderliche Interaktion vorgenommen hat. Die Informationen dienen daher auch dem Zweck der gegenseitigen Beurteilung der Nutzer (Zweckelement). Dies wirkt sich wiederum auf die Rechte und Interessen der betroffenen Nutzer aus (Ergebniselement). Die Nutzerkennungen sowie die damit verbundenen Informationen enthalten somit Informationen über den betroffenen Nutzer.

[297] So auch *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE., S. 23, welche deutlich macht, dass keine personenbezogenen Daten vorliegen, wenn durch technische Maßnahmen die Herstellung einer Information ausgeschlossen ist. Diese Differenzierung nimmt der Blockchain Bundesverband nicht vor, indem er pauschal behauptet, dass es sich bei verschlüsselten Daten um pseudonymisierte Daten handelt, *Blockchain Bundesverband*, Blockchain, data protection and the GDPR., S.4, abrufbar unter: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf.

[298] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE., S. 11 f.

[299] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE., S. 13.

6.2.2.2.3.2 Daten über Dritte

Die eingespeicherten Daten können Informationen über Dritte umfassen. Inwieweit dies der Fall sein kann, ist je nach Einzelfall der Anwendung zu entscheiden.

6.2.2.2.4 Identifizierung oder Identifizierbarkeit

Identifiziert ist eine Person dann, wenn sie sich in einer Personengruppe von allen Personen unterscheidet.[300] Nach Art. 4 Nr. 1 S. 2 DS-GVO ist eine Person identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Für die Frage, ob eine Person identifizierbar ist, kommt es immer auf die konkreten Umstände des Einzelfalls an. Dabei sollten nach Erwägungsgrund 26 der DS-GVO alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie bspw. Aussondern. Der EuGH hat dies in der Rechtsprechung zum Personenbezug dynamischer IP-Adressen dahingehend präzisiert, dass ein personenbezogenes Datum für den Verarbeitenden dann vorliegt, wenn dieser entweder selbst über alle erforderlichen Informationen zur Identifikation verfügt oder zumindest über rechtliche Mittel verfügt, um diese Informationen von Dritten zu erlangen.[301]

6.2.2.2.4.1 Direkte Identifikation der Person durch Kenntnis der Identität

Eine direkte Identifikation einer Person erfolgt in der Regel durch Kenntnis ihres Namens.[302] Da dieser jedoch nicht einmalig ist, bedarf es für eine eindeutige Identifikation weiterer Informationen, wie bspw. dem Geburtsdatum, einem Lichtbild oder einer Adresse.[303]
Die Nutzer treten auf dem DLT-Layer nicht mit ihrem Klarnamen auf. Eine direkte Identifikation durch den Namen des Nutzers scheidet folglich aus. Anders kann dies für die betroffenen dritten Personen sein, deren Daten auf dem DLT-Layer gespeichert werden. Werden hier Klarnamen gespeichert, so ist eine direkte Identifikation möglich.

6.2.2.2.4.2 Indirekte Identifikation der Person durch Kenntnis der Verknüpfung zwischen Nutzerkennung und Identität

Zu den personenbezogenen Daten zählen ebenfalls jene, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten (pseudonymisierte Daten).[304] Ein Personenbezug könnte sich daher auch durch die Nutzerkennungen des Systems herstellen lassen.

Jeder Teilnehmer des Netzwerks verfügt über eine eindeutige Nutzerkennung in Form eines öffentlichen Schlüssels. Zu jedem öffentlichen Schlüssel existiert ein privater Schlüssel, der vom jeweiligen Teilnehmer unter Verschluss gehalten wird. Mithilfe des privaten Schlüssels ist es möglich, eine digitale Signatur zu erstellen, die es Dritten ermöglicht zu verifizieren, dass der Signierende über den zum öffentlichen Schlüssel gehörenden privaten Schlüssel verfügt. Dabei muss der Signierende den privaten Schlüssel jedoch nicht

[300] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 01248/07/DE., S. 14.
[301] *EuGH*, Urteil vom 19.10.2016 - C-582/14, Rn. 49.
[302] BeckOK DatenschutzR/*Schild*, Art. 4 Rn. 16; Sydow/*Ziebarth*, Art. 4 Rn. 14.
[303] BeckOK DatenschutzR/*Schild*, Art. 4 Rn. 16; Kühling/Buchner/*Klar/Kühling*, Art. 4 Rn. 18.
[304] DS-GVO, Erwägungsgrund 26.

offenbaren. Ebenso wenig ist es mit den derzeit zur Verfügung stehenden technischen Mitteln möglich aus der digitalen Signatur und dem öffentlichen Schlüssel den privaten Schlüssel zu errechnen.

Will der Teilnehmer einen Datensatz in die dezentrale Datenbank übertragen, so sendet er mit seinem öffentlichen Schlüssel eine entsprechende Nachricht an alle Teilnehmer des Systems. Diese Nachricht signiert er mit seinem privaten Schlüssel. Die übrigen Teilnehmer haben somit die Möglichkeit zu prüfen, ob die Nachricht tatsächlich von demjenigen stammt, der zu der Nutzerkennung den entsprechenden privaten Schlüssel kennt.

Die öffentlichen Nutzerkennungen sind mit Informationen auf der DLT-Plattform verknüpft. Besitzt der Betrachter die Information darüber, welche natürliche Person sich hinter der Nutzerkennung verbirgt, so besitzt er damit auch Informationen über diese natürliche Person. Der Personenbezug besteht so lange, wie der jeweilige Betrachter entweder selbst über die zusätzlichen Informationen verfügt oder die Möglichkeit hat, auf diese Informationen bei Dritten zuzugreifen.

Die Kenntnis des Schlüssels zwischen der natürlichen Person und der Nutzerkennung hat zunächst nur der Betroffene selbst. Dies ist solange datenschutzrechtlich irrelevant, wie nicht Dritte Personen ebenfalls über diesen Schlüssel Kenntnis oder die Möglichkeit erlangen, den Schlüssel vom Betroffenen zu erhalten. Die Teilnehmer der DLT-Anwendung nutzen diese, um den jeweils anderen Teilnehmern das Vorliegen bestimmter Tatsachen nachzuweisen, die für das Verhältnis zwischen den Personen von Bedeutung sind. Soll durch die DLT-Anwendung ein Vertrag zwischen zwei Teilnehmern erfüllt werden, so will der Leistende dem Leistungsempfänger die Vornahme der Leistung nachweisen. Hierfür wird es regelmäßig erforderlich sein, den Vertragspartner darüber in Kenntnis zu setzen, welche Nutzerkennung seiner Person zugeordnet ist. Kennt der Leistungsempfänger die Identität seines Vertragspartners, so kann er alle Informationen auf der DLT-Plattform, die für ihn sichtbar mit der jeweiligen Nutzerkennung verknüpft sind, der Identität seines Vertragspartners zuordnen. Natürliche Personen werden also dadurch identifizierbar, dass sie die Verknüpfung ihrer Identität mit einer Nutzerkennung Dritten offenbaren.

6.2.2.2.4.3 Indirekte Identifikation durch die IP-Adresse des Nutzers

Die Nutzer im Peer-to-peer-Netzwerk interagieren mittels einer ihnen vom eigenen Internet-Service-Provider zugewiesenen IP-Adresse. Wie bereits erörtert, geht der EuGH davon aus, dass eine IP-Adresse alleine aufgrund der Möglichkeit der Geltendmachung eines Auskunftsanspruchs beim jeweiligen Internet-Service-Provider ein personenbezogenes Datum für den Verarbeitenden darstellt.[305] Durch die Kenntnis der IP-Adresse könnte der Inhalt einer damit verbundenen Nachricht dem Absender zugeordnet werden.

Beim Versenden einer Transaktion im Netzwerk wird dem Empfänger der Nachricht die IP-Adresse des Senders offenbart. Dabei wird eine Transaktion im Peer-to-peer-Netzwerk jeweils vom Sender zum nächstgelegenen Node übermittelt. Dieser sendet die Nachricht nach Überprüfung im Netzwerk weiter. Auf diese Weise verteilt sich die Nachricht im System, bis schließlich jeder Node die Transaktion erhalten hat. Nicht jeder Node sieht dabei die IP-Adresse des ursprünglichen Senders, sondern lediglich die Adresse desjenigen Nodes, von dem er die Transaktion erhalten hat. Er kann daher nicht sicher sein, dass die IP-Adresse tatsächlich dem Sender der Nachricht gehört. Es besteht jedoch die Möglichkeit, durch Analyse des Nachrichtenverkehrs im Peer-to-peer-Netzwerk Rückschlüsse auf den Absender einer Transaktion zu ziehen. Gelingt den Teilnehmern eine solche Analyse und wird eine solche von den Teilnehmern nach allgemeinem Ermessen

[305] *EuGH*, Urteil vom 19.10.2016 - C-582/14, Rn. 49.

wahrscheinlich genutzt, so stellen die mit der IP-Adresse verknüpften Transaktionen personenbezogene Daten dar.

6.2.2.2.4.4 Indirekte Identifikation durch Gesamtschau der Informationen

Für eine Identifizierbarkeit ist nicht zwingend erforderlich, dass der Betrachter den Schlüssel zur Herstellung der Verbindung der Nutzerkennung mit einer natürlichen Person kennt. Eine indirekte Identifizierung ist auch dann möglich, wenn eine „einzigartige Kombination"[306] an Informationen vorliegt, die in ihrer Gesamtheit nur auf eine bestimmte natürliche Person zutreffen kann, obwohl die einzelnen Informationen noch keine Rückschlüsse erlauben. Hierzu zählen auch die von Art. 4 Nr. 1 S. 2 DS-GVO genannten besonderen Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sind. Je dichter der Datensatz an Informationen über die Person, desto wahrscheinlicher wird deren Identifizierbarkeit.[307]

Der Absender der Nachricht versendet diese, um bestimmte Informationen fälschungssicher in der dezentralen Datenbank abzulegen. Je nach konkretem Anwendungsfall kann aufgrund dieser Informationen auf den Absender der Nachricht geschlossen werden. Dies kann auch dann möglich sein, wenn der Betrachter den Schlüssel zur Verknüpfung zwischen der Nutzerkennung und der Identität nicht kennt. Möglich erscheint dies in Fällen, in denen der Inhalt der Nachricht denklogisch nur von einer bestimmten natürlichen Person stammen kann. Dieser Rückschluss muss nicht zwingend jedermann möglich sein. In Einzelfällen kann dieser Schluss nur von Personen mit dem notwendigen Sonderwissen geschlossen werden. Ist bspw. einem Leistungsempfänger zwar der Schlüssel zur Verknüpfung der Nutzerkennung mit einer natürlichen Person nicht bekannt, weiß dieser jedoch, dass die Interaktion aufgrund des Zeitpunkts und der Umstände nur von seinem Vertragspartner stammen kann und kennt er diesen, so kann er einen Personenbezug herstellen.

Auch wenn der Betrachter den Inhalt der signierten Nachricht nicht einsehen kann, sind Fälle denkbar, in denen er aufgrund der Gesamtschau aller von einer Nutzerkennung versendeten Nachrichten Rückschlüsse auf die dahinterstehende natürliche Person schließen kann. Dies kann dann der Fall sein, wenn eine Nutzerkennung zu spezifischen Zeiten Informationen in die Datenbank einspeist und dabei wiederholt dieselbe Nutzerkennung verwendet wird. Ob sich hieraus Rückschlüsse auf die dahinterstehende natürliche Person ziehen lassen, hängt jeweils vom Einzelfall, insbesondere von der Anzahl der Teilnehmer und der üblichen Frequenz von Speichervorgängen ab.

6.2.2.3 Zwischenergebnis

Bei der Implementierung von DLT-Anwendungen (im Mobilitätsbereich) kommt es sowohl beim Einpflegen, Auslesen und Weiterverarbeiten der Daten auf dem DLT-Layer zu Datenverarbeitungen. Die dabei verarbeiteten Daten sind personenbezogene Daten, wenn sie aus der Perspektive des jeweiligen Betrachters Informationen über eine natürliche Person enthalten. Dies kann dann der Fall sein, wenn der Inhalt eines einzuspeichernden Datensatzes Informationen über eine natürliche Person enthält. Dabei kann es sich um die Nutzer des Systems, aber auch um (unbeteiligte) Dritte handeln. Zudem können die mit einer signierten Nachricht verbundenen Transaktionsdaten Informationen über die Nutzer des Systems beinhalten. Dies ist dann der Fall, wenn die Nutzerkennung vom Betrachter dem Nutzer zugeordnet werden kann und es sich bei dem Nutzer um eine natürliche Person handelt oder es sich bei dem Nutzer zwar um keine natürliche Person

[306] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 01248/07/DE., S. 16.

[307] BeckOK DatenschutzR/*Schild*, Art. 4 Rn. 16; Sydow/*Ziebarth*, Art. 4 Rn. 17, 21.

handelt, die hinter dem Nutzer tätigen natürlichen Personen vom Betrachter der Daten aber ebenfalls zugeordnet werden können. Eine Zuordnung ist dem Betrachter dann möglich, wenn er den Schlüssel zwischen Nutzerkennung und Identität des Nutzers kennt oder auf diesen durch zusätzlich für ihn verfügbare Informationen schließen kann. Zu diesen Informationen kann die IP-Adresse des Nutzers oder eine Gesamtschau der mit einer Nutzerkennung verknüpften und für den Betrachter einsehbaren Informationen gehören.

Da zumindest die Existenz von Nutzerkennung für eine DLT-Plattform unverzichtbar ist, werden im Regelfall Daten verarbeitet werden, die zumindest für einen bestimmten Kreis von Betrachtern Personenbezug aufweisen. Eine Ausnahme gilt nur dann, wenn die Nutzer des Systems keine natürlichen Personen sind und auch nicht auf die hinter den Nutzern tätig werdenden natürlichen Personen geschlossen werden kann und zudem im System keine Daten von Dritten verarbeitet werden. Alle anderen Fälle bedürfen einer Identifizierung der für diese Datenverarbeitungen verantwortlichen Stelle.

6.2.3 Verantwortlicher für die Datenverarbeitung

Adressat der Pflichten aus der DS-GVO ist grundsätzlich der für die Verarbeitung der Daten Verantwortliche.[308] Ausschließlich dieser wird durch eine Rechtsgrundlage zur Datenverarbeitung legitimiert. Für den von der Datenverarbeitung Betroffenen ist der Verantwortliche Anspruchsgegner zur Erfüllung der datenschutzrechtlichen Pflichten. Der Verantwortliche hat gegenüber dem Betroffenen nach den Art. 12-14 DS-GVO transparent über die Datenverarbeitung zu informieren. Dem Betroffenen steht weiter nach Art. 14 DS-GVO das Recht auf Auskunft über die über ihn verarbeiteten personenbezogenen Daten zu. Nach den Art. 16-19 DS-GVO hat der Verantwortliche unrichtige oder nicht mehr erforderliche Daten zu berichtigen oder zu löschen. Aus diesen Gründen ist die Feststellung des Verantwortlichen von besonderer Bedeutung. Dabei ist neben der alleinigen Verantwortlichkeit einer Stelle auch eine geteilte Verantwortlichkeit mehrerer Stellen nach Art. 26 DS-GVO möglich. Der Verantwortliche kann sich zudem Auftragsverarbeitern (Art. 28 DS-GVO), die nach Weisung des Verantwortlichen tätig werden, bedienen.

6.2.3.1 Begriff der Verantwortlichkeit

Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für die Frage, wer „entscheidet", kommt es darauf an, wer tatsächlichen Einfluss auf die Entscheidung nimmt. Einer formalen rechtlichen Benennung eines Entscheidungsträgers kommt dabei nur Indizwirkung zu.[309]

Mit der Entscheidung über den Zweck ist diejenige über das erwartete oder geplante Ergebnis der Verarbeitung gemeint, die Entscheidung über die Mittel ist diejenige über die Art und Weise, wie dieses Ergebnis erreicht wird.[310] Der Begriff des Mittels umfasst dabei u. a. die Entscheidung über die technischen Methoden und den Umfang der Verarbeitung, die Zugangsberechtigung zu den Daten oder die Löschfristen.[311]

6.2.3.2 Verantwortlicher für das Einpflegen der Daten

[308] Sydow/*Raschauer*, Art. 4 Rn. 114.
[309] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 00264/10/DE., S. 15.
[310] Ebd., S. 16.
[311] Ebd., S. 17.

Alle Daten werden initial von den Teilnehmern an die anderen Teilnehmer zur Weiterverarbeitung übermittelt. Über die Zwecke und Mittel dieser Übermittlung entscheidet allein der jeweils Einpflegende. Solange der Einpflegende selbst Betroffener der eingepflegten personenbezogenen Daten ist, ist seine Handlung datenschutzrechtlich nicht relevant. Enthalten die Datensätze jedoch auch personenbezogene Daten anderer Teilnehmer oder Dritter, so bedarf es hierfür einer Rechtfertigung. Rechtfertigungsbedürftig sind dabei stets nur diejenigen Übermittlungen von Daten, die auch für den Adressaten der Daten Personenbezug aufweisen. Adressaten der Datenverarbeitung sind zunächst alle Teilnehmer des Systems mit Lesezugriff.

6.2.3.3 Verantwortlicher für das Auslesen der Daten

Beim Auslesen der Daten entscheidet allein die auslesende Stelle darüber, ob und welche Daten ausgelesen werden. Folglich ist es alleine sie, die über Zwecke und Mittel der Datenverarbeitung entscheidet. Wie beim Einpflegen, ist die auslesende Stelle nur für diejenigen Verarbeitungen von Daten verantwortlich, die andere Teilnehmer oder Dritte betreffen. Eine Verantwortlichkeit setzt zudem voraus, dass der Auslesende den Informationen einen Personenbezug entnehmen kann. Für die Verarbeitung des Auslesens ist er dann der alleinige Verantwortliche.

6.2.3.4 Verantwortlicher für die Speichervorgänge auf dem DLT-Layer

Eine Herausforderung kann die Bestimmung des Verantwortlichen für diejenigen Datenverarbeitungen, die von den Teilnehmern des dezentralen Netzwerks zur Erstellung und Fortführung der dezentralen Datenbank vorgenommen werden, sein. Für die Frage, wer tatsächlichen Einfluss auf die Datenverarbeitungsvorgänge nimmt, muss zunächst zwischen den Gestaltungsformen der „permissioned DLT-Applikation“ und der „permissionless DLT-Applikation“ differenziert werden.

6.2.3.4.1 Permissioned DLT-Applikation („Zentrale Lösung“)

In einer permissioned DLT-Applikation werden der Zugang sowie Lese- und Schreiberechte der Beteiligten durch eine Zentralinstanz festgelegt. Die Zentralinstanz kann auch aus einer Gruppe von Personen bestehen, die sich zum Betrieb des Systems zusammenschließen. Diese Zentralstelle legt ein Rechte- und Rollensystem an und bestimmt dadurch, welche Personen Zugriff auf welche Daten haben sollen. Ein Zugriff auf die Datenbank ist nur durch das übergelagerte System der Zentralstelle möglich. Die Zentralstelle legt die Regeln fest, nach denen die Daten nach dem Einpflegen durch die Teilnehmer des Netzwerks verarbeitet werden. Die Nodes und gegebenenfalls Miner der darunterliegenden DLT-Plattform sind entweder selbst Teil der Gruppe der Zentralstelle oder werden nach deren Weisungen tätig, indem sie die dezentrale Datenbank nach den von der Zentralstelle definierten Regeln führen.
In einem derartigen Szenario übernimmt die Zentralstelle die tatsächliche Kontrolle über die stattfindenden Datenverarbeitungen. Sie entscheidet über Zwecke und Mittel der Datenverarbeitung und kann daher als datenschutzrechtlich Verantwortlicher angesehen werden.[312] Nodes und Miner werden, wenn sie nicht bereits Teil der Gruppe der Personen sind, welche die Zentralstelle bilden, weisungsabhängig tätig und können folglich Auftragsdatenverarbeiter der Zentralstelle nach Art. 28 DS-GVO sein.[313] Voraussetzung ist, dass zwischen der Zentralstelle und den Nodes und Minern ein Vertrag zur Auftragsdatenverarbeitung geschlossen wird. Dieser Vertrag schreibt vor, wie die Datenverarbeitung zu erfolgen hat. Dabei kann bspw. festgelegt werden, dass die Verarbeitung nur nach den Regeln der bereitgestellten Software erfolgen darf.

[312] *Bitkom*, Blockchain und Datenschutz – Faktenpapier., S. 30; *Blockchain Bundesverband*, Blockchain, data protection and the GDPR., S. 7.
[313] *Martini/Weinzierl,* NVwZ 2017, 1251 (1254).

Der Einsatz einer permissioned DLT-Applikation kann die Suche nach einem datenschutzrechtlich Verantwortlichen vereinfachen. Nachteil einer solchen Lösung ist jedoch, dass eine Zentralstelle gebildet werden muss, welche entscheidenden Einfluss auf die stattfindenden Datenverarbeitungen nimmt. Das Ziel der Schaffung einer dezentralen Austauschplattform unter Verzicht auf zentrale Intermediäre kann dadurch, zumindest nicht in Reinform, erreicht werden. Es bedarf daher einer Untersuchung, inwieweit die Rolle des datenschutzrechtlich Verantwortlichen auch in einer zulassungsfreien DLT-Applikation zugewiesen werden kann.

6.2.3.4.2 Permissionless DLT-Applikation

Die Suche nach einem datenschutzrechtlich Verantwortlichen gestaltet sich bei zulassungsfreien DLT-Systemen zunächst schwierig, da unmittelbar keine Zentralinstanz als Kontrollstelle der stattfindenden Datenverarbeitungen identifiziert werden kann. Zu Teilen wird daher vertreten, dass sämtliche Nodes als verantwortliche Stellen einzuordnen sind, da diese Daten weitergeben und in die von ihnen vorgehaltene Kopie der Datenbank übertragen.[314] Andere Stimmen sehen alle Teilnehmer eines offenen DLT-Systems gleichermaßen als für die stattfindenden Datenverarbeitungen Verantwortliche an.[315] Es hat jedoch den Anschein, dass Letztere den Begriff des Teilnehmers und des Nodes gleichsetzen. Als Voraussetzung für die Verantwortlichkeit wird die Weitergabe der Transaktionen im Netzwerk und das Einpflegen der Daten in die eigene Kopie der Datenbank nach den Regeln des Systems genannt. Dies entspricht der Rolle der Nodes. Die Nodes entscheiden sich dafür, die Daten nach den Regeln der von ihnen genutzten Software zu verarbeiten. Jeder Node hätte grundsätzlich die Möglichkeit die Daten gar nicht oder nach anderen Regeln zu verarbeiten. Folglich entscheidet jeder Node über die Zwecke und Mittel der bei ihm stattfindenden Datenverarbeitungen.

Da die Nodes in ihrer Gesamtheit die Infrastruktur der DLT-Plattform bereitstellen, könnte man davon ausgehen, dass sie die Datenverarbeitung als gemeinsam Verantwortliche nach Art. 26 DS-GVO vornehmen. Eine gemeinsame Verantwortlichkeit würde jedoch erfordern, dass die Entscheidung über Zwecke und Mittel der Datenverarbeitung von allen Nodes gemeinsam getroffen wird. Tatsächlich kommt es in einer zulassungsfreien DLT-Applikation aber regelmäßig nicht zu einer Absprache zwischen den Nodes. Jeder entscheidet autonom über die eigene Datenverarbeitung. Folglich wird man davon ausgehen müssen, dass alle Nodes für sich unabhängige Verantwortliche sind.

Ein solches Ergebnis wird nicht zwingend den Interessen der an der DLT-Applikation Beteiligten gerecht. Unter Umständen sind daher Anpassungen der Architektur der DLT-Plattform erforderlich. In der Folge soll danach differenziert werden, ob ein Interesse aller Teilnehmer an allen On-Chain-Daten besteht oder ob nur ausgewählte Teilnehmer an jeweils konkreten On-Chain-Daten ein Interesse haben. Für die jeweilige Interessenslage soll dabei eine Lösung für die Rolle des Verantwortlichen de lege lata vorgestellt werden.

6.2.3.4.2.1 Alle Teilnehmer haben an allen On-Chain-Daten ein Interesse („Offene Lösung“)

Der Anwendungsfall kann so gestaltet sein, dass alle Teilnehmer eines DLT-Netzwerks an allen on-Chain verarbeiteten Daten ein Interesse haben. Dies betrifft Fälle, in denen eine dezentrale Datenbank im Interesse aller Beteiligten zwischen allen offen geführt werden soll. Eingespeicherte Informationen sollen zwischen den Beteiligten nicht geheim bleiben. Stattdessen sollen alle von den Informationen profitieren. Eine solche Lösung wird

[314] *Martini/Weinzierl,* NVwZ 2017, 1251 (1253 f.); *Bitkom*, Blockchain und Datenschutz – Faktenpapier., S. 28 f.

[315] *Schrey/Thalhofer,* NJW 2017, 1431 (1433 f.); *Bechtolf/Vogt,* ZD 2018, 66 (69).

in aller Regel eine geschlossene DLT-Applikation notwendig machen, die lediglich von den Beteiligten eingesehen werden kann. Im Umkehrschluss wird jedoch nicht jede geschlossene DLT-Applikation die genannten Voraussetzungen erfüllen, da es durchaus auch in einer geschlossenen DLT-Applikation ein Interesse daran geben kann, nicht alle Informationen mit allen Teilnehmern zu teilen. Für letzteren Fall muss auf die unten stehenden Ausführungen verwiesen werden.

Haben alle Beteiligten an den verarbeiteten Daten ein berechtigtes Interesse, so eröffnet dies die Möglichkeit zur Verteilung der Verantwortlichkeit auf alle Nodes. Das zuvor gefundene Ergebnis zur Verantwortlichkeit ist in diesem Fall praktisch umsetzbar. Zwischen den Nodes kann eine Kooperation entstehen, die auch die Vereinbarung einer gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO ermöglicht.

6.2.3.4.2.2 Nur ausgewählte Teilnehmer haben an den On-Chain-Daten ein Interesse („Anonymisierungslösung")

Der Fall einer zwischen allen Teilnehmern offen geführten Datenbank wird regelmäßig die Ausnahme bleiben. Oft werden die Teilnehmer ein Interesse daran haben, Informationen ausschließlich mit ausgewählten Teilnehmern zu teilen. Will man diesen Interessen auf einer zulassungsfreien DLT-Plattform gerecht werden, so stellt dies die größten datenschutzrechtlichen Herausforderungen dar. Ein Problem entsteht dann, wenn die on-Chain verarbeiteten Daten für alle Teilnehmer der DLT-Plattform einen Personenbezug aufweisen. Haben nicht alle beteiligten Teilnehmer ein berechtigtes Interesse an der Kenntnis dieser Daten, so wird sich der Einpflegende mit der Übermittlung von personenbezogenen Daten Dritter an alle Teilnehmer des Netzwerks nicht datenschutzkonform verhalten können, da er keine Rechtsgrundlage für diese weitreichende Datenübermittlung hat.[316] Weiter wären, wie voranstehend bereits gezeigt, alle Nodes des Netzwerks für die Verarbeitung dieser Daten als datenschutzrechtlich Verantwortliche einzustufen. In einem offenen Netzwerk wird eine Kooperation dieser Personen jedoch schwerfallen. Es ist nicht davon auszugehen, dass diese ihre datenschutzrechtlichen Pflichten effizient erfüllen können.[317]

Die Verteilung der Verantwortung auf alle Nodes des Netzwerks ist hier nicht interessensgerecht. Stattdessen muss eine Lösung gefunden werden, bei der die Verantwortung auf diejenigen Personen beschränkt wird, die ein tatsächliches Interesse an der konkreten Transaktion haben. Ein derartiges Ergebnis ließe sich durch eine Anpassung der Architektur der DLT-Plattform erreichen. Dabei wird der Grundsatz fruchtbar gemacht, dass ein Personenbezug stets nur relativ durch den jeweiligen Betrachter hergestellt werden kann. Auch die Rolle des Verantwortlichen erfordert, dass die verarbeiteten Daten für den Verantwortlichen einen Personenbezug aufweisen. Werden lediglich Daten verarbeitet, die zwar für Dritte aufgrund von Zusatzinformationen personenbezogene Daten darstellen, für die Verarbeitenden aber keine Möglichkeit besteht den Betroffenen zu identifizieren, so kann der Verarbeitende nicht Verantwortlicher sein. Ziel der Architektur muss daher sein, dass die On-Chain-Daten ohne notwendige Zusatzinformationen keiner natürlichen Person zugeordnet werden können. Ist dies erreicht, so werden auf dem DLT-Layer durch die Nodes keine personenbezogenen Daten verarbeitet. Dies hat zur Folge, dass sie für die stattfindenden Datenverarbeitungen nicht datenschutzrechtlich Verantwortlicher sein können. Eine Verantwortung für die On-Chain-Datenverarbeitungen gäbe es dann nicht. Die Verantwortung läge stattdessen bei denen, die über die notwendigen Zusatzinformationen verfügen, um die On-Chain-Daten einer Person zuzuordnen.

[316] Siehe zur Rechtsgrundlage für die Datenverarbeitung 6.2.4.

[317] Problematisch ist insbesondere die Pflicht zur Berichtung und Löschung von Daten. Siehe hierzu näher unter 6.2.5.

6.2.3.4.2.2.1 Aufhebung des Personenbezugs für Informationen über Dritte

Sollen on-Chain Informationen über Dritte gespeichert werden, so muss sichergestellt werden, dass diese nur von den Personen gelesen werden können, welche ein berechtigtes Interesse an den Informationen haben.

6.2.3.4.2.2.1.1 Verschlüsselung der Informationen

Ein personenbezogenes Datum, welches sicher verschlüsselt ist, stellt nur für diejenigen Stellen ein personenbezogenes Datum dar, welche über den Schlüssel zur Entschlüsselung des Datums verfügen. Der Schlüssel darf nur denjenigen Stellen bekannt sein, welche die verschlüsselten Informationen zwingend benötigen. Durch Verschlüsselung kann der Kreis der Personen, für welche das gespeicherte Datum einen Personenbezug aufweist, auf diejenigen Personen reduziert werden, die ein berechtigtes Interesse an der Kenntnis des Datums haben. Die on-Chain verschlüsselt gespeicherten Informationen stellen in einer öffentlichen DLT-Applikation für jedermann Daten ohne Informationsgehalt dar. Erst durch den Schlüssel werden sie zu einem personenbezogenen Datum. Die Verantwortung für die Datenverarbeitung könnte damit von den Teilnehmern der öffentlichen DLT-Applikation auf den Halter des Schlüssels verlagert werden. Nicht die Nodes des DLT-Netzwerks sind dann für die Datenverarbeitung verantwortlich, sondern diejenigen, die den Schlüssel halten. Im Falle einer Löschverpflichtung muss der Schlüssel gelöscht werden. Dadurch werden die On-Chain-Daten anonymisiert und sind datenschutzrechtlich nicht relevant.

Nach Art. 25 und 32 DS-GVO ist der Verantwortliche verpflichtet, durch entsprechende Technikgestaltung die Rechte der betroffenen Person hinreichend zu schützen. Die Übermittlung personenbezogener Daten zur Verarbeitung auf einer DLT-Plattform könnte diesen Anforderungen auch in verschlüsselter Form nicht genügen. Die Daten werden auf der DLT-Plattform von den Nodes potenziell ad infinitum gespeichert. Eine heute als sicher geltende Verschlüsselung könnte durch künftige Computertechnik aufgebrochen werden. Ist dies möglich, so liegen die personenbezogenen Daten für jedermann sichtbar in der öffentlichen DLT-Applikation. Die gewählte Verschlüsselung muss daher entweder so sicher sein, dass eine Entschlüsselung während der Zeit des Bestehens der DLT-Plattform mit hoher Wahrscheinlichkeit ausgeschlossen ist oder es muss von einer reinen Verschlüsselungslösung abgesehen werden.

6.2.3.4.2.2.1.2 Off-Chain-Speicherung mit Hashwert-Verknüpfung

Um diesem Problem zu begegnen, kann es sinnvoll sein, die Datenspeicherung weitestmöglich off-Chain stattfinden zu lassen. Personenbezogene Daten werden verschlüsselt und off-Chain unter Kontrolle des jeweils Einpflegenden gespeichert. Von diesen Daten wird ein Hashwert gebildet. Zusammen mit einer Verlinkung auf die Off-Chain-Daten wird der zugehörige Hashwert on-Chain eingepflegt. Für die Teilnehmer des Netzwerks weisen diese Daten ohne Weiteres keinen Personenbezug auf. Diesen können nur diejenigen mit den Zugriffsrechten auf die Off-Chain-Daten herstellen. Durch den Hashwert wird sichergestellt, dass die Daten seit der Einspeicherung auf die DLT-Plattform nicht manipuliert worden sind. Die off-Chain gespeicherten Daten liegen stets unter der Kontrolle des Einpflegenden und können jederzeit vom ihm gelöscht werden.

6.2.3.4.2.2.2 Aufhebung des Personenbezugs für Informationen über Nutzer des Systems

Die Off-Chain-Speicherung und Hashwert-Verknüpfung kann nicht für alle Daten eine gangbare Lösung darstellen. Bestimmte Informationen müssen allen Nodes des Systems bekannt sein. Nutzerkennungen, Zeitstempel und Kontostände können auf diese Weise nicht gespeichert werden. Werden sie auf diese Weise gespeichert, so bräuchten alle

Nodes zur Kontrolle Zugriff auf die Informationen und eine nachträgliche Löschung würde eine Überprüfung der Validität neuer Transaktionen unmöglich machen. Das eigentliche Ziel der Off-Chain-Speicherung, die Informationen nur ausgewählten Personen zugänglich zu machen, könnte nicht mehr erreicht werden.

Wenn nicht alle Daten off-Chain gespeichert oder zumindest verschlüsselt werden können, so darf den on-Chain gespeicherten Informationen ein Bezug zu den Nutzern nur dann zu entnehmen sein, wenn der jeweilige Betrachter der Daten hieran ein berechtigtes Interesse hat. Es kann zwar nicht kontrolliert werden, welche Personen in einer öffentlichen DLT-Applikation die On-Chain-Daten einsehen. Es kann jedoch durch eine Anpassung der DLT-Architektur erreicht werden, dass die On-Chain-Daten ohne Zusatzinformationen für die Teilnehmer keinen Personenbezug aufweisen.

Auch wenn Nutzerkennungen, Kontostände und durchgeführte Transaktionen on-Chain sichtbar sind, so weisen diese nur dann einen Personenbezug auf, wenn es gelingt, die Nutzerkennung einer natürlichen Person zuzuordnen. Die Kenntnis vom Schlüssel zwischen Nutzerkennung und Identität hat anfänglich nur der jeweilige Inhaber der Nutzerkennung. Er kann diese Information mit ausgewählten Dritten teilen, vor allen anderen jedoch verbergen. Durch Kontrolle der Kenntnis dieses Schlüssels kann so verhindert werden, dass jedermann den On-Chain-Daten Informationen über konkrete Nutzer entnehmen kann. Hierzu ist erforderlich, dass die On-Chain-Daten ohne Kenntnis des Schlüssels für den Betrachter keine personenbezogenen Daten darstellen. Um ein solches System zu etablieren bedarf es Vorkehrungen. Es muss sichergestellt werden, dass der Personenbezug tatsächlich nur von denjenigen hergestellt werden kann, die Kenntnis vom Schlüssel haben.

6.2.3.4.2.2.2.1 Einmaliger Einsatz von Nutzerkennungen

Es muss zunächst sichergestellt werden, dass die Transaktion keine Inhalte aufweist, die einen Rückschluss auf die Personen hinter den darin enthaltenen Nutzerkennungen ermöglicht. In Extremfällen kann ein solcher Rückschluss bereits dadurch gezogen werden, dass eine Nutzerkennung zu einem bestimmten Zeitpunkt aktiv wurde. Je nach Größe des infrage stehenden Nutzerkreises und der Gegebenheiten des Einzelfalls könnten sich bereits aus dieser Tatsache Rückschlüsse auf eine natürliche Person hinter der Nutzerkennung ziehen lassen. Ist der potenzielle Nutzerkreis hingegen hinreichend groß, so wird man in der Regel davon ausgehen können, dass die alleinige Interaktion einer Nutzerkennung mit einer anderen noch keine Rückschlüsse auf die Betroffenen zulässt.

Grundsätzlich erscheint es möglich, dass die Nutzer für jede Interaktion auf der DLT-Plattform eine eigene Nutzerkennung generieren. Jede Transaktion ist dann mit einer einmaligen Kennung verknüpft. Den Schlüssel zwischen Kennung und Identität kennt nur der Betroffene. Er kann diesen mit denjenigen teilen, die an der Transaktion ein Interesse haben. Regelmäßig wird man davon ausgehen können, dass bei einmaliger Nutzung einer Kennung keine Rückschlüsse auf den Nutzer möglich sind. Eine Ausnahme gilt nur in solchen Szenarien, in denen aufgrund der Umstände des Einzelfalls aus der Gesamtschau der Umstände auch aus der einmaligen Interaktion einer Kennung zu einer bestimmten Zeit auf eine einzelne natürliche Person geschlossen werden kann. Sobald jedoch die Anwendung eine gewisse Größe erreicht, sollte ein solcher Rückschluss nicht mehr möglich sein.

Die Generierung einer neuen Nutzerkennung für jede Interaktion stößt jedoch an Grenzen, wenn mit einer Nutzerkennung Werte (z. B. Token) verknüpft sind und zwischen den Nutzern übertragen werden sollen. Will der Nutzer die Werte zusammenführen, weiterverbreiten oder sich auszahlen lassen, so wird er erneut mit der Nutzerkennung aktiv werden müssen. Durch mehrmalige Interaktion einer Nutzerkennung könnten für Außenstehende Muster sichtbar werden, die wiederum Rückschlüsse auf die beteiligten

Personen erlauben. Unter welchen Umständen solche Erkenntnisse durch Datenanalyse möglich werden, lässt sich pauschal schwer beantworten. Vorzugswürdig ist daher eine Lösung, die ein mehrmaliges Auftreten einer Nutzerkennung gar nicht vorsieht. Es bedarf demgemäß weiterer Anpassungen, die Rückschlüsse auf den Nutzer ausschließen. Hierfür kommen grundsätzlich unterschiedliche Lösungen in Betracht. Diese können je nach Einzelfall auch in Kombination eingesetzt werden. Im Folgenden soll beispielhaft die Off-Chain-Saldierung und der Einsatz von Zero-Knowledge-Proofs sowie von Stealth-Adressen in Kombination mit Ring-Signaturen kurz vorgestellt werden.

6.2.3.4.2.2.2.2 Off-Chain-Saldierung von Transaktionen

Ein Ansatz, der insbesondere bei einer B2B-DLT-Lösung, bei denen Rückschlüsse auf hinter dem Unternehmen stehende natürliche Personen nicht von vornherein ausgeschlossen sind, möglich erscheint, ist eine Off-Chain-Saldierung der Transaktionen durch die Teilnehmer des Netzwerks. Anstatt jede fällige Transaktion direkt in die DLT-Plattform zu übertragen, führt jede Partei zunächst ein eigenes Konto, auf dem fällige Transaktionen saldiert werden. In regelmäßigen Abständen wird von allen Parteien eine Ausgleichszahlung auf der Plattform vorgenommen. Durch dieses Vorgehen werden die Häufigkeit und die zeitliche Verteilung der Aktivitäten der Teilnehmer vereinheitlicht. Rückschlüsse auf einzelne unternehmensinterne Vorgänge und damit in Verbindung stehende Personen sind dann schwieriger. Eine Identifizierung von Mustern durch Analyse der Daten wird ebenfalls erschwert.

Ein gewichtiger Nachteil der Saldierung liegt im Verlust von Transparenz. Die Bildung der Salden nehmen die Teilnehmer in eigener Regie vor. Da zwischenzeitlich keine Eintragung in der dezentralen Datenbank erfolgt, bleibt auch eine vorzeitige Kontrolle der Verrechnung durch die anderen Teilnehmer aus. In Situationen, in denen dieses Risiko jedoch hinnehmbar und möglicherweise durch entsprechende Vorkehrungen, wie Stichprobenkontrollen, kontrollierbar bleibt, kann die Saldierung eine gangbare Methode zur Anonymisierung der Datensätze sein.

6.2.3.4.2.2.2.3 Einsatz von Zero-Knowledge-Proofs

Durch den Einsatz von Zero-Knowledge-Proofs erscheint es für den Absender einer Transaktion möglich, diese an das Netzwerk zu senden, ohne dabei seine eigene Nutzerkennung, die Nutzerkennung des Empfängers oder den zu sendenden Betrag zu offenbaren.[318] Die Nodes können die Validität der Transaktion überprüfen, ohne dabei Kenntnis von Sender, Empfänger oder übermittelten Betrag zu erhalten. Die Daten weisen damit für die Teilnehmer des Netzwerks keinen Personenbezug auf. Die Nodes sind für die stattfindenden Datenverarbeitungen dann nicht verantwortlich. Eine sichere technische Implementierung der Zero-Knowledge-Proofs vorausgesetzt, kann deren Einsatz ein vielversprechender Ansatz für eine datenschutzkonforme offene DLT-Lösung sein.

6.2.3.4.2.2.2.4 Einsatz von Stealth-Adressen in Kombination mit Ring-Signaturen[319]

Um zu verhindern, dass Transaktionen, die einem Nutzer gesandt werden, mit dessen öffentlicher Nutzerkennung verknüpft werden können, kann für jede Transaktion eine „Stealth-Adresse" als Empfangsadresse für Transaktionen generiert werden. Die Generierung nehmen Sender und Empfänger mithilfe eines Schlüssel-Austauschs selbst vor. An eine Stealth-Adresse können Transaktionen gesandt werden, ohne dass für die Teilnehmer des Netzwerks ersichtlich ist, zu welcher öffentlichen Nutzerkennung diese ge-

[318] Vorgestellt von *Sasson/Chiesa/Garman/Green* et al. in The Institute of Electrical and Electronics Engineers, IEEE Symposium on Security and Privacy, 459-474.

[319] So umgesetzt im Cryptonote Protokoll, *Saberhagen*, CryptoNote v 2.0.

hört. Lediglich der Empfänger kann durch Verwenden eines geheimen Schlüssels ermitteln, welche Stealth-Adressen seiner Nutzerkennung zugeordnet sind. Durch einen ebenfalls geheimen Schlüssel hat er die Möglichkeit, über die dort hinterlegten Werte zu verfügen.

Die Nutzung von Stealth-Adressen verschleiert zunächst den Empfänger einer Transaktion. Die Sender sind jedoch weiter sichtbar. Auch Transaktionen von einer Stealth-Adresse könnten weiter beobachtet und Rückschlüsse könnten gezogen werden. Um zu verschleiern, von welcher Adresse Transaktionen ausgeführt werden, können Ring-Signaturen eingesetzt werden. Ring-Signaturen fassen mehrere Inputs und Outputs zusammen und verbergen so, welche Transaktionen von welchem Sender an welchen Empfänger gesendet worden sind. Auf einer zweiten Ebene können die Transaktionen so zusammengefasst werden, dass auch der übermittelte Betrag der einzelnen Transaktion nur für Sender und Empfänger ersichtlich ist. Die Kombination von Stealth-Adressen und Ring-Signaturen könnte somit eine Möglichkeit bieten, die Verknüpfung zwischen Nutzerkennung und Identität für die Teilnehmer des Systems aufzuheben. Die gespeicherten Transaktionen wären dann für die Teilnehmer, welche nicht über die notwendigen Schlüssel zur Zuordnung verfügen, anonymisiert.

Bei einer technischen Anonymisierung, unabhängig davon ob diese durch Zero-Knowledge-Proofs, Ring-Signaturen und Stealth-Adressen oder auf anderem Wege geschaffen wird, dürfen die damit verbundenen Konsequenzen nicht aus den Augen verloren werden. Soll mit der DLT-Plattform ein Zahlungssystem geschaffen werden, können von der Anonymisierung auch illegal agierende Akteure profitieren. Wie der Vergleich mit dem Bargeldverkehr zeigt, spricht zwar zunächst nichts gegen eine weitgehend anonyme Möglichkeit der Zahlungsabwicklung. Ein digitales Bargeldäquivalent birgt jedoch weitaus größere Risiken, da der Austausch grundsätzlich für jeden orts- und zeitungebunden ermöglicht wird. Das Ziel des Datenschutzes steht teilweise in Spannung mit dem Bedürfnis nach (staatlicher) Kontrolle des Zahlungsverkehrs. Sind in einem digitalen Zahlungsverkehrs-System alle Beteiligten anonym, erschwert dies u. a. die Verbrechensbekämpfung. Wird von staatlicher Seite der Einsatz einer DLT-Plattform mit technischer Anonymisierungslösung gefördert, so sind diese Folgen einzukalkulieren.

6.2.3.4.2.2.3 Risiko des Regelverstoßes durch Teilnehmer der Plattform

Die Anonymisierungslösung strebt die vollständige Verbannung von personenbezogenen Daten auf dem DLT-Layer an. Außer den Beteiligten einer Transaktion soll kein Dritter den On-Chain-Daten einen Personenbezug entnehmen können. Die beschriebenen Maßnahmen zur Erreichung dieses Zustands sind mit bedeutenden Herausforderungen verbunden. Sollten (ungeplant) Daten auf den DLT-Layer gelangen, denen auch die Nodes des Netzwerks Informationen über natürliche Personen entnehmen können, so sind diese, wie oben bereits erläutert, für die Verarbeitung dieser Informationen verantwortlich. Es stellt sich dann für diese Informationen die schwer zu lösende Herausforderung der Geltendmachung der Betroffenenrechte. Eine Zentralstelle, die nachträglich korrigierend eingreifen könnte, ist nicht vorhanden. Will man auf eine solche Zentralstelle verzichten, darf die Software der DLT-Plattform, welche von den Nodes genutzt wird, eine Situation, in der die Nodes zu Verantwortlichen werden, nicht zulassen. Die Software muss daher so ausgestaltet sein, dass sie Informationen, die von den Nodes verarbeitet werden, nur in einem Format erlaubt, das einen Personenbezug der On-Chain-Daten ausschließt.

6.2.3.5 Zwischenergebnis

Verantwortlicher für das Einpflegen und Auslesen der Daten ist der jeweils tätige Teilnehmer. Die Verantwortung für die On-Chain-Verarbeitungen tragen – ohne weitere Anpassungen der Architektur – alle Nodes des Netzwerks. Für den Fall, dass alle Nodes

des Netzwerks auch ein berechtigtes Interesse an allen verarbeiteten Daten haben, kann dies grundsätzlich eine gangbare Lösung (offene Lösung) sein.

In der Regel wird es jedoch so sein, dass nicht alle Teilnehmer einer DLT-Plattform an allen verarbeiteten Informationen ein berechtigtes Interesse haben. Die gesetzliche Zuweisung der Verantwortlichkeit an alle Teilnehmer führt in diesem Fall zu ungewünschten Ergebnissen. Aufgrund der mit der Verantwortlichkeit verbundenen Verpflichtungen wird die Rolle des Nodes unattraktiv. Den Verpflichtungen des Verantwortlichen können die Nodes nur schwer oder, im Falle der Verpflichtung zur Berichtung und Löschung, gar nicht nachkommen. Zudem würde jedes Einpflegen von personenbezogenen Daten in die DLT-Plattform eine Übermittlung an einen unüberschaubaren Personenkreis bedeuten. Für diese weitreichende Übermittlung fehlt es dem Einpflegenden an einer Rechtsgrundlage.

Es müssen demzufolge alternative Lösungswege für die Verteilung der Verantwortlichkeit geschaffen werden. Dies erfordert eine Anpassung der Architektur der DLT-Plattform. Haben nicht sämtliche Teilnehmer ein berechtigtes Interesse an allen verarbeiteten Daten, so muss entweder durch Einsatz einer permissioned DLT-Applikation eine verantwortliche Zentralstelle geschaffen werden (zentrale Lösung) oder im Falle einer offenen DLT-Applikation die Aufhebung des Personenbezugs für alle on-Chain verarbeiteten Daten bewerkstelligt werden (Anonymisierungslösung).

6.2.4 Rechtsgrundlagen für die Datenverarbeitung

Der Verantwortliche unterliegt nach der DS-GVO bezüglich der Datenverarbeitung einem grundsätzlichen Verbot mit Erlaubnisvorbehalt. Personenbezogene Daten dürfen von ihm nur verarbeitet werden, wenn er für die Verarbeitung eine Rechtsgrundlage vorweisen kann. Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten finden sich in der DS-GVO vorrangig in Art. 6 DS-GVO. Im Folgenden sollen für das Einpflegen und Auslesen sowie die On-Chain-Verarbeitung passende Rechtsgrundlagen gefunden werden.

6.2.4.1 Rechtfertigung des Einpflegens und Auslesens der Daten

Zunächst müssen die einpflegenden und auslesenden Teilnehmer für die von ihnen verantwortete Datenverarbeitung des Einpflegens und des Auslesens personenbezogener Daten eine Rechtsgrundlage vorweisen können. Dabei kann danach differenziert werden, ob es sich bei den verarbeiteten Daten um personenbezogene Daten des jeweils korrespondierenden Teilnehmers der konkreten Transaktion handelt oder ob auch Daten Dritter verarbeitet werden.

6.2.4.1.1 Verarbeitung personenbezogener Daten der korrespondieren Teilnehmer der Transaktion

Unabhängig vom konkreten Anwendungsfall lässt sich konstatieren, dass das Einpflegen und Auslesen der Daten zur Erfüllung einer vertraglichen Verpflichtung mit dem jeweiligen Transaktionspartner erfolgt. Nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO ist eine Verarbeitung personenbezogener Daten zulässig, wenn diese für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Der Begriff „Vertrag“ erfasst dabei alle rechtsgeschäftlichen oder rechtsgeschäftsähnlichen

Schuldverhältnisse.[320] Erfasst sind Leistungs-, Neben- und Rücksichtspflichten die notwendigerweise mit dem Schuldverhältnis einhergehen.[321] Erforderlich ist die Datenverarbeitung dann, wenn der Vertrag ohne die Datenverarbeitung nicht so erfüllt werden könnte, wie sich die Parteien auf die Erfüllung geeinigt haben.[322]

In jedem Anwendungsfall stehen die jeweiligen Transaktionspartner in einem (unterschiedlich ausgestalteten) Vertragsverhältnis. Die Teilnehmer nutzen die DLT-Architektur, um Informationen zur Durchführung ihrer gegenseitigen vertraglichen Verpflichtung untereinander manipulationssicher auszutauschen. Soweit sich die hierbei verarbeiteten Daten auf diejenigen beschränken, die zur Durchführung ihres Vertrags erforderlich sind, dient ihnen Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO als Rechtsgrundlage für die stattfindenden Datenverarbeitungen.

6.2.4.1.2 Verarbeitung personenbezogener Daten Dritter

Etwas anderes gilt nur in den Fällen, in denen die Transaktionen neben den Daten der jeweiligen Teilnehmer der Transaktion gleichfalls Daten über unbeteiligte Dritte enthalten. Hier kann nicht auf die Rechtsgrundlage der Erfüllung eines Vertrags abgestellt werden, da die von der Datenverarbeitung betroffene Person hierfür selbst Vertragspartei sein muss. Stattdessen müssen andere Rechtsgrundlagen in Betracht gezogen werden. Hier kommen vorrangig die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten oder die Verarbeitung nach Einholung einer Einwilligung des Betroffenen in Betracht.

6.2.4.1.2.1 Erfüllung einer rechtlichen Verpflichtung, Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO

Möglich erscheint es zunächst, dass die Daten Dritter zur Erfüllung einer rechtlichen Verpflichtung eingepflegt und ausgelesen werden. Nach Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO ist eine Datenverarbeitung zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist. Nach Art. 6 Abs. 3 UAbs. 1 DS-GVO kann sich diese Verpflichtung aus dem Unionsrecht oder dem Recht der Mitgliedstaaten ergeben. Es muss sich dabei um eine Rechtsvorschrift handeln, deren normierte Verpflichtung sich unmittelbar auf die Datenverarbeitung bezieht. Es genügt mithin nicht, wenn sich der Verantwortliche auf irgendeine rechtliche Verpflichtung beruft und zu diesem Zweck Datenverarbeitungen vornimmt.[323]

6.2.4.1.2.2 Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO

Nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist eine Datenverarbeitung auch dann zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Zu den berechtigten Interessen zählen nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche und ideelle.[324] Grundsätzlich ist von einer Schutzwürdigkeit der betroffenen Person auszugehen. Im Rahmen der Abwägung sind die näheren Umstände

[320] BeckOK DatenschutzR/*Albers/Veit,* Art. 6 Rn. 30.
[321] BeckOK DatenschutzR/*Albers/Veit,* Art. 6 Rn. 31.
[322] Kühling/Buchner/*Buchner/Petri*, Art. 6 Rn. 40; Paal/Pauly/*Frenzel*, Art. 6 Rn. 14.
[323] Kühling/Buchner/*Buchner/Petri*, Art. 6 Rn. 76.
[324] Kühling/Buchner/*Buchner/Petri*, Art. 6 Rn. 146.

der konkreten Datenverarbeitung zu berücksichtigen. Dabei sind die Aufgaben und Zwecke, die der Verantwortliche mit der Datenverarbeitung verfolgt, ebenso zu beachten, wie die Sensibilität der Daten für die Persönlichkeitsrechte des Betroffenen.

6.2.4.1.2.3 Einwilligung des Betroffenen, Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO

Schließlich kommt für eine Rechtfertigung der Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO die Einwilligung der betroffenen Person zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke in Betracht. Die Einwilligung muss dabei ausdrücklich erfolgen und sich auf den konkreten Zweck der Datenverarbeitung beziehen. Sie muss freiwillig, in informierter Weise und unmissverständlich abgegeben werden. Nach Art. 7 Abs. 1 DS-GVO hat der Verantwortliche die Einholung der Einwilligung nachzuweisen. Nach Art. 7 Abs. 3 DS-GVO hat die betroffene Person jederzeit die Möglichkeit, eine einmal erteilte Einwilligung zu widerrufen. Bis dahin vorgenommene Datenverarbeitungen bleiben zwar rechtmäßig, künftige Datenverarbeitungen müssen dann aber unterbleiben. Nicht zuletzt wegen der jederzeitigen Widerrufsmöglichkeit und erforderlichen Dokumentationspflichten sollte auf die Einwilligung nur dann zurückgegriffen werden, wenn keine andere Rechtsgrundlage einschlägig ist.

6.2.4.2 Rechtfertigung der On-Chain-Verarbeitung

Die Frage nach der Rechtsgrundlage für die On-Chain-Verarbeitung hängt von der gewählten Lösung zur Verteilung der Verantwortlichkeit ab. Im Falle der oben beschriebenen „Anonymisierungs-Lösung" ist eine Rechtfertigung für die On-Chain-Verarbeitung nicht erforderlich. Haben nur ausgewählte Teilnehmer an den On-Chain-Daten ein Interesse, so ist, wie oben gezeigt, eine Architektur notwendig, in der die On-Chain-Daten für die Teilnehmer des Netzwerks keinen Personenbezug aufweisen. Ist dies der Fall, sind diese nicht datenschutzrechtlich verantwortlich und benötigen folglich für die Datenverarbeitungen keine Rechtsgrundlage.
Anders verhält es sich bei der „offenen Lösung" und der „zentralen Lösung". Für diese soll im Folgenden eine Rechtfertigung der stattfindenden Datenverarbeitungen diskutiert werden.

6.2.4.2.1 Rechtsgrundlage für die Verarbeitung bei der „offenen Lösung"

Haben alle Teilnehmer an allen On-Chain-Daten ein Interesse und ist die DLT-Applikation dementsprechend offen gestaltet, so sind alle Teilnehmer gleichermaßen, gegebenenfalls nach Art. 26 DS-GVO gemeinsam für die Datenverarbeitung verantwortlich. Hier kann zwischen den Teilnehmern ein Vertrag zur gemeinsamen Führung der Datenbank und der Speicherung der Daten geschlossen werden. Die Verarbeitungen finden dann zur Erfüllung dieses Vertrags statt. Wird kein Vertrag geschlossen, so kann die Datenverarbeitung im berechtigten Interesse der gemeinsam Verantwortlichen erfolgen. Da alle Beteiligten ein Interesse an der Datenverarbeitung haben, wird die Verarbeitung der gegenseitigen personenbezogenen Daten einer Interessenabwägung aller Voraussicht nach standhalten. Für die Verarbeitung von personenbezogenen Daten Dritter müssten die Beteiligten ebenfalls über eine Rechtsgrundlage verfügen. Hier könnte ebenfalls ein Vertrag zwischen dem Dritten und den Verarbeitenden vorliegen, zu dessen Erfüllung die Verarbeitung in der verteilten Datenbank erforderlich ist. Alternativ könnte auch hier ein berechtigtes Interesse der Teilnehmer vorliegen. Schließlich erscheint es möglich, sich von den Dritten jeweils eine Einwilligung in die Datenverarbeitung einzuholen.

6.2.4.2.2 Rechtsgrundlage für die Verarbeitung bei der „zentralen Lösung"

In der permissioned DLT-Applikation ist eine Zentralstelle für die stattfindenden Datenverarbeitungen verantwortlich. Regelmäßig werden die Nodes als Auftragsverarbeiter der Zentralstelle tätig. Auch die Zentralstelle muss für die On-Chain-Verarbeitungen eine Rechtsgrundlage vorweisen. Hier ist zunächst ebenfalls naheliegend, dass die Zentralstelle einen Vertrag mit den Teilnehmern schließt. Inhalt des Vertrags ist der Betrieb des dezentralen Netzwerks durch die Zentralstelle. Die stattfindenden Datenverarbeitungen sind dann für die Erfüllung des Vertrags erforderlich. Werden Daten Dritter in der Datenbank verarbeitet, so kommen als Rechtsgrundlagen eine Verpflichtung aus dem Vertrag zwischen Zentralstelle und Dritten, ein berechtigtes Interesse der Zentralstelle oder eine Einwilligung des Dritten in Betracht. In diesem Rahmen ist jedoch stets zu prüfen, ob die Daten Dritter zwingend on-Chain verarbeitet werden müssen oder ob nicht eine Off-Chain-Speicherung der Daten mit Hashwert-Verknüpfung möglich ist.[325] Hierfür spricht auch die Tatsache, dass trotz Verantwortlichkeit einer zentralen Stelle die Daten nicht zwingend nachträglich gelöscht werden können.[326]

6.2.5 Umsetzung des Rechts auf Berichtigung und Löschung

Eine Herausforderung der Datenverarbeitung auf einer DLT-Plattform ist die Wahrung der in der DS-GVO normierten Betroffenenrechte. Während sich für die Informations- und Auskunftspflichten nach Art. 13-15 DS-GVO durch den DLT-Einsatz vergleichsweise wenig Besonderheiten ergeben, können insbesondere das Recht auf Berichtigung (Art. 16 DS-GVO) und das Recht auf Löschung (Art. 17 DS-GVO) problematisch sein. Diese sollen daher im Folgenden näher untersucht werden.

Der Betroffene hat nach Art. 16 S. 1 DS-GVO das Recht, dass ihn betreffende unrichtige personenbezogene Daten unverzüglich berichtigt werden. Zudem hat er das Recht, dass die Daten auf seinen Wunsch unverzüglich gelöscht werden, soweit hierfür ein in Art. 17 Abs. 1 DS-GVO aufgezählter Löschungsgrund vorliegt. Demnach kann im hier betrachteten Verfahren eine Löschung verpflichtend sein, wenn die Daten für die Zwecke ihrer Erhebung nicht mehr erforderlich sind, der Betroffene eine von ihm gegebene Einwilligung zur Verarbeitung der Daten widerruft und keine andere Rechtsgrundlage für die Verarbeitung mehr besteht, der Betroffene rechtmäßig von seinem Widerspruchsrecht gegen die Verarbeitung der Daten Gebrauch macht, die Datenverarbeitung unrechtmäßig erfolgte oder die Löschung der Daten zur Erfüllung einer rechtlichen Verpflichtung aus dem Unionsrecht oder dem Recht der Mitgliedstaaten, welcher der Verantwortliche unterliegt, erforderlich ist.

Für die Umsetzung der Löschpflichten muss erneut zwischen der „Anonymisierungslösung", der „offenen Lösung" und der „zentralen Lösung" unterschieden werden.

6.2.5.1 Löschung bei der „Anonymisierungslösung"

Den Löschpflichten kann bei Wahl der „Anonymisierungslösung" vergleichsweise einfach genügt werden. Verantwortlich sind nicht alle Teilnehmer des Systems, sondern nur diejenigen, die zur jeweiligen Transaktion den Schlüssel zwischen Nutzerkennung und Identität bzw. die Kontrolle über die off-Chain gespeicherten personenbezogenen Daten halten. Werden Daten off-Chain gespeichert und mittels eines Hashwerts auf der DLT-Ebene verknüpft, so können die off-Chain gespeicherten Daten vom Verantwortlichen jederzeit gelöscht werden. Der on-Chain verbleibende Verweis auf die Off-Chain-Daten führt ins Leere. Die so verbleibenden Daten weisen keinen Personenbezug auf. Ein Personenbezug besteht für diejenigen Daten, die mittels der Kenntnis des Schlüssels zwi-

[325] Siehe zu dieser Möglichkeit bereits unter 6.2.3.4.2.2.1.2 und allg. zu Hashfunktionen unter 4.1.4.
[326] Siehe zu den Löschpflichten bei Wahl der zentralen Lösung unter 6.2.5.2.

schen Nutzerkennung und Identität einer natürlichen Person zugeordnet werden können. Den Schlüssel halten jeweils die für die Datenverarbeitung Verantwortlichen. Trifft diese eine Löschungspflicht für das entsprechende Datum, so werden nicht die On-Chain-Daten, dafür aber der Schlüssel zur Herstellung der Verknüpfung zwischen Nutzerkennung und Identität gelöscht. Die Identifikation der natürlichen Person alleine mit den on-Chain verbleibenden Daten ist auch dem Verantwortlichen nicht mehr möglich. Die Daten sind folglich dauerhaft anonymisiert. Dies kommt einer Löschung der Daten gleich.[327]

6.2.5.2 Löschung bei der „offenen Lösung" und der „zentralen Lösung"

Bei Wahl der offenen Lösung sind sämtliche Teilnehmer gemeinsam verantwortlich und gegebenenfalls zur Löschung verpflichtet. Die zentrale Lösung weist die Verantwortung dagegen einer vorher bestimmten Zentralstelle zu. Dies offenbart eine weitere Herausforderung der beiden Lösungsansätze. Zwar lässt sich die Rolle des Verantwortlichen allen gemeinsam oder einer Zentralstelle zuweisen, die Löschpflichten müssen jedoch auch von allen gemeinschaftlich oder der Zentralstelle erfüllt werden können. Grundsätzlich kann aber auch bei diesen Lösungsmodellen der Inhalt eines Blocks nicht nachträglich von den Teilnehmern manipuliert werden. Auch hierfür müssen daher Lösungsmöglichkeiten vorgesehen werden.
Grundsätzlich hat eine Löschung der Daten nicht zu erfolgen, solange diese für den Zweck ihrer Verarbeitung weiterhin erforderlich sind. Wird zwischen der Zentralstelle oder den Teilnehmern einer offenen Lösung ein Vertrag über die Datenverarbeitung auf der DLT-Plattform geschlossen, so sind Datenverarbeitungen, die sich auf diesen Vertrag stützen solange rechtmäßig, wie sie zur Erfüllung des Vertrags erforderlich sind, Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO. Sieht der Vertrag die manipulationssichere Speicherung von Daten der Teilnehmer auf einer DLT-Plattform vor, so ließe sich argumentieren, dass diese Speicherung aufgrund der Architektur der DLT grundsätzlich zeitlich unbegrenzt erforderlich bleibt. Eine nachträgliche Manipulation der Daten würde die Kette unterbrechen und den Vertragszweck gefährden. Für die zentrale und offene Lösung könnte daher auf eine Löschung personenbezogener Daten der Teilnehmer verzichtet werden, soweit alle Teilnehmer untereinander oder mit der Zentralstelle vor der Teilnahme am DLT-Projekt eine vertragliche Bindung eingegangen sind. Vertragsinhalt müsste die Führung einer grundsätzlich unveränderbaren DLT-Plattform durch die Zentralstelle oder alle Teilnehmer des Systems sein, wobei die dabei verarbeiteten Daten eindeutig kenntlich gemacht und soweit wie möglich zu begrenzen wären. Nicht erfasst blieben jedoch auch in diesem Fall Daten Dritter. Werden neben den Daten der unmittelbaren Teilnehmer des Systems, die durch Nutzerkennungen auf der DLT-Plattform aktiv werden, auch Daten Dritter verarbeitet, so müsste auch mit diesen jeweils ein Vertrag geschlossen werden, der die unveränderliche Speicherung der Daten beinhaltet.

Auch wenn eine solche vertragliche Vereinbarung zwischen den Beteiligten besteht, müsste weiter ausgeschlossen sein, dass es zu unrechtmäßigen Datenverarbeitungen kommt. Gem. Art. 17 Abs. 1 lit. d DS-GVO sind nämlich unrechtmäßig erhobene Daten auch dann zu löschen, wenn diese aufgrund einer vertraglichen Vereinbarung verarbeitet wurden. Eine Unrechtmäßigkeit der Verarbeitung kann vornherein jedoch nicht ausgeschlossen werden. So könnte bspw. der Vertrag zwischen den Beteiligten aufgrund von Mängeln nichtig sein. Der Verantwortliche kann sich dann für die Datenverarbeitung nicht mehr auf die vertragliche Vereinbarung stützen. Folglich wird man de lege lata davon ausgehen müssen, dass bei der zentralen oder offenen Lösung Möglichkeiten einer nachträglichen Manipulation der Kette vorgesehen werden müssen. Diese sollen im Folgenden kurz diskutiert werden.

[327] So auch *Martini/Weinzierl,* NVwZ 2017, 1251 (1256).

6.2.5.2.1 Redactable Blockchain

Zumindest für Blockchain-Lösungen kann eine Möglichkeit, den Lösch- und Berichtigungspflichten von On-Chain-Daten nachzukommen, die Verwendung einer weiter entwickelten „Chameleon-Hashfunktion" in einer „Redactable Blockchain" sein.[328] Die „Chameleon-Hashfunktion" wird statt der gewöhnlichen Hashfunktion zur Verknüpfung der einzelnen Blöcke verwendet und beinhaltet eine „Falltür". Mithilfe eines geheimen Schlüssels ist es möglich, für einen veränderten Input denselben Hashwert zu erzeugen. Auf diese Weise kann der Inhalt eines Blocks nachträglich manipuliert werden, die Kette bleibt hingegen intakt. Die Besonderheit der weiter entwickelten Hashfunktion in einer „Redactable Blockchain" ist, dass Kollisionen der Hashfunktion auch nach Veröffentlichung des veränderten Blocks nur mit Kenntnis des Schlüssels gefunden werden können. Somit bleibt die Blockchain trotz der Veränderungen für Dritte unangreifbar. Werden Veränderungen vorgenommen, so sind diese dennoch durch die Teilnehmer des Netzwerks nachvollziehbar. Der Besitzer des Schlüssels kann daher keine unbemerkten Änderungen vornehmen. Der Schlüssel kann von einer Zentralstelle unter Verschluss gehalten und bei Bedarf eingesetzt werden. Alternativ ist es möglich, den Schlüssel unter mehreren Instanzen aufzuteilen und eine Veränderung der Blockchain nur durch die Mitwirkung aller Schlüsselinhaber zu ermöglichen.[329] Bei der zentralen Lösung kann die Verwaltung des Schlüssels von der Zentralstelle vorgenommen werden. Bei der offenen Lösung ist denkbar, den Schlüssel auf alle Teilnehmer des Systems aufzuteilen oder innerhalb des Systems eine Gruppe von „Verwaltern" zu bestimmen, die dieser Aufgabe nachkommt.

6.2.5.2.2 Forks

Arbeiten in einer offenen Lösung sämtliche Teilnehmer zusammen, so erscheint, dass sich alle Nodes im Falle einer Löschverpflichtung auf einen entsprechenden Fork einigen. Eine Zentralstelle könnte die Nodes als Auftragsverarbeiter zur Durchführung eines Forks anweisen. Auf diese Weise werden die Regeln der DLT-Plattform geändert. Alte Datensätze mit zu löschendem Inhalt könnten aus der DLT-Plattform entnommen, von den Nodes künftig ignoriert und gelöscht werden. Da entweder alle Nodes gemeinsam verantwortlich sind oder als Auftragsverarbeiter einer Zentralstelle tätig werden, erscheint ein solches Vorgehen grundsätzlich denkbar.

6.2.5.2.3 Off-Chain-Speicherung und einmalige Vergabe von Nutzerkennungen

Stellen die aufgezeigten Lösungswege keinen gangbaren Weg dar, so kann auch bei der offenen und zentralen Lösung grundsätzlich eine Gestaltung vergleichbar mit der Anonymisierungslösung vorgenommen werden. Nutzerkennungen werden einmalig vergeben und Daten, die einen Personenbezug ermöglichen, werden off-Chain gespeichert und mittels Hashwerten on-Chain verknüpft. Den Löschpflichten kann dann wie bei der Anonymisierungslösung nachgekommen werden. Den Schlüssel zwischen Nutzerkennung und Identität verwalten, im Falle der zentralen Lösung, die Zentralstelle oder, im Falle der offenen Lösung, alle Teilnehmer des Systems. Bei Bedarf kann er von den jeweils Verantwortlichen gelöscht werden, um damit eine dauerhafte Anonymisierung der Daten durchzuführen.

6.2.6 Zusammenfassung

[328] Das Konzept der Redactable Blockchain wurde vorgestellt von *Ateniese/Magri/Venturi/Andrade*, 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 111-126. Ebenfalls vorgeschlagen wird es von *Martini/Weinzierl,* NVwZ 2017, 1251 (1256 f.); *Marnau* in Eibl/Gaedke, INFORMATIK 2017, 1025 (1030); *Bechtolf/Vogt,* ZD 2018, 66 (70); *Finck,* EDPL 2018, 17 (31).

[329] *Ateniese/Magri/Venturi/Andrade*, 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 111 (117).

Die beim Einsatz einer DLT-Lösung stattfindenden Datenverarbeitungen erfolgen entweder im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen an eine in der Europäischen Union ansässige betroffene Person oder durch einen Verantwortlichen, der seine Niederlassung innerhalb der Europäischen Union hat. Mithin ist die DS-GVO für die hier zu untersuchenden Datenverarbeitungen anwendbar.

Für die Frage, ob bei der jeweiligen Mobilitätslösung personenbezogene Daten auf der DLT-Ebene verarbeitet werden, kann zwischen der reinen B2B-Lösung ohne Identifizierbarkeit natürlicher Personen als Nutzer des Systems und allen sonstigen Fällen differenziert werden.

6.2.6.1 Reine B2B-DLT-Applikation

Von den Datenverarbeitungen betroffene Personen können sowohl die Nutzer des Systems als auch Dritte sein. Wird die DLT-Applikation unmittelbar nur von Unternehmen genutzt, deren Aktivität keine Rückschlüsse auf hinter dem Unternehmen stehende natürliche Personen erlaubt, so sind die Verarbeitungen der Daten über die Nutzer des Systems datenschutzrechtlich nicht relevant. Macht die jeweilige Anwendung den Austausch von Daten über Dritte, z. B. die Endkunden der Anwendung, zwischen den teilnehmenden Unternehmen notwendig, so sind diese Daten off-Chain zu speichern. Auf diese Weise werden keine personenbezogenen Daten auf der DLT-Ebene verarbeitet. Folglich sind die stattfindenden Datenverarbeitungen datenschutzrechtlich nicht relevant. Erlaubt die jeweilige Mobilitätslösung eine solche Konzeption, so ist diese de lege lata aus datenschutzrechtlicher Sicht vorzugswürdig. Herausforderung dieser Lösung ist der Ausschluss einer Identifizierbarkeit von natürlichen Personen hinter dem teilnehmenden Unternehmen. Diese ist auch bei größeren Unternehmen nicht zwingend ausgeschlossen. Es bedarf daher einer sorgfältigen Prüfung im Einzelfall.

6.2.6.2 Sonstige Fälle

Ist eine reine B2B-Lösung, wie zuvor beschrieben, nicht möglich oder erwünscht, wird die Anwendung regelmäßig die Verarbeitung von personenbezogenen Daten notwendig machen. Bei den Nutzern des Systems handelt es sich im Falle von B2C- und C2C-Anwendungen meist um natürliche Personen. Auch im Falle von B2B-Anwendungen können natürliche Personen betroffen sein, wenn die hinter dem Unternehmen stehenden Personen bekannt sind.
Die Personen sind selten direkt durch Klarnamen in den gespeicherten Datensätzen, stets jedoch indirekt durch eine Kenntnis des Schlüssels zwischen Identität und verwendeter Nutzerkennung identifizierbar. Zudem ist eine Identifizierbarkeit auch ohne Kenntnis des Schlüssels durch eine Gesamtschau aller verfügbaren on-Chain gespeicherten Informationen nicht ausgeschlossen.

Verantwortlicher für das Einpflegen und Auslesen der Daten ist die jeweils tätige Stelle. Handelt es sich dabei um Daten über den jeweiligen Transaktionspartner, so wird regelmäßig Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO eine taugliche Rechtsgrundlage für die Datenverarbeitung sein. Handelt es sich um Daten Dritter, können diese zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrung berechtigter Interessen oder nach Einwilligung durch den betroffenen Dritten eingepflegt und ausgelesen werden.

Die Verantwortung für die On-Chain-Verarbeitungen tragen – ohne weitere Anpassungen der Architektur – alle Nodes des Netzwerks. Für den Fall, dass alle Nodes des Netzwerks auch ein berechtigtes Interesse an allen verarbeiteten Daten haben, kann dies grundsätzlich eine gangbare Lösung (offene Lösung) sein. Haben nicht alle Teilnehmer ein berechtigtes Interesse an allen verarbeiteten Daten, so muss entweder durch Einsatz einer permissioned DLT-Applikation eine verantwortliche Zentralstelle geschaffen werden (zentrale Lösung) oder im Falle einer offenen DLT-Applikation die Aufhebung des

Personenbezugs für alle on-Chain verarbeiteten Daten bewerkstelligt werden (Anonymisierungslösung). Im Falle der Anonymisierungslösung ist eine Rechtsgrundlage für die on-Chain verarbeiteten Daten mangels Personenbezugs nicht erforderlich. Eine erhebliche Herausforderung der Anonymisierungslösung besteht jedoch darin, dafür zu sorgen, dass die verwendete Software der Nodes einen Personenbezug der On-Chain-Daten nicht zulässt. Im Falle der offenen oder zentralen Lösung können die personenbezogenen Daten der Nutzer aufgrund Vertrags, die Daten Dritter ebenfalls aufgrund Vertrags, zur Wahrung eines berechtigten Interesses oder nach Einwilligung der Betroffenen verarbeitet werden.

Flaschenhals für die einzelnen Lösungsmodelle ist die Umsetzung des Rechts auf Berichtigung und Löschung. Während sich dieses bei Wahl der Anonymisierungslösung vergleichsweise einfach durch Löschung des Schlüssels und der Off-Chain-Daten bewerkstelligen lässt, sind für die offene und zentrale Lösung weitere Anpassungen erforderlich. Wenn der Einsatz einer Redactable Blockchain, von Forks oder vergleichbaren Instrumenten zur nachträglichen Manipulation des DLT-Layers keine gangbare Lösung darstellt, kann auch in diesem Fall den Löschpflichten de lege lata nur durch Wahl der Anonymisierungslösung, also den Verzicht auf die Speicherung personenbezogener Daten auf dem DLT-Layer, begegnet werden.

6.2.7 Ausblick de lege ferenda

Die Untersuchung zeigt, dass die Implementierung von DLT-Anwendungen zur Umsetzung von Mobilitätsvorhaben grundsätzlich DS-GVO-konform möglich ist. Je nach Anwendungsfall erfordert der Einsatz von DLT aber weitreichende Anpassungen der Architektur, um den von der DS-GVO normierten Löschpflichten nachkommen zu können. Dies kann im Einzelfall einen nicht unbedeutenden technischen Aufwand erfordern.

Datenschutzrechtliches Hindernis für den Einsatz von DLT-Applikationen ist in erster Linie die unbefriedigende Zuweisung der Rolle des datenschutzrechtlich Verantwortlichen auf alle Nodes der DLT-Plattform sowie mangelnde oder impraktikable Möglichkeiten zur nachträglichen Löschung von eingespeicherten Informationen. Optimal wäre folglich eine Regelung, welche die Verantwortung für die on-Chain verarbeiteten Informationen klar zuweist und eine Löschung von eingepflegten Informationen überflüssig macht.

Dieses Ziel könnte de lege ferenda dadurch erreicht werden, dass die Rolle des Verantwortlichen für die Verarbeitung von personenbezogenen Daten auf DLT-Plattformen den jeweiligen Beteiligten einer konkreten Transaktion zugewiesen wird. Die Nodes des Netzwerks agieren alleine als Datenmittler und haben an den verarbeiteten Informationen kein Interesse. Sie entscheiden zwar tatsächlich über Zwecke und Mittel der Datenverarbeitung ihrer Kopie der Datenbank. In einer Gesamtschau sind sie jedoch vielmehr Werkzeuge der Nutzer der DLT-Applikation, die sich dieses Instruments zum gegenseitigen Datenaustausch und zur Datenaufbewahrung bedienen.[330] Eine gesetzliche Regelung könnte daher vorsehen, dass Verantwortlicher für die Verarbeitung von Informationen in DLT-Applikationen, die mit einer Nutzerkennung verknüpft sind, diejenigen Teilnehmer sind, denen die jeweiligen Nutzerkennungen zuzuordnen sind und die sich nach ausführlicher Information freiwillig zur Nutzung der DLT-Applikation entschieden haben. Beinhaltet eine Transaktion neben der eigenen Nutzerkennung des Einpflegenden auch Nutzerkennungen weiterer Teilnehmer, so sind diese in der Folge ebenfalls für die in dieser Information eingepflegten personenbezogenen Daten in Gestalt der betroffenen Nutzerkennungen verantwortlich.

[330] So argumentiert auch der *Blockchain Bundesverband*, Blockchain, data protection and the GDPR., S. 6.

Es entstünde durch diese Gestaltung eine Situation, in der die Betroffenen selbst zu (gemeinsam) Verantwortlichen der sie betreffenden Datenverarbeitungen werden. Vereinigt sich die Rolle des Betroffenen und des Verantwortlichen in einer Person, so werden die datenschutzrechtlichen Pflichten durch Konfusion aufgehoben. Eine Löschung der Daten ist ausdrücklich nicht vorgesehen. Dies war den Beteiligten aber im Vorfeld bekannt. Durch ihre Teilnahme stimmen sie diesem Umstand zu. Der gemeinsame Zweck der Beteiligten der Verwendung einer DLT-Plattform zum Austausch von Informationen setzt die dauerhafte Speicherung der Informationen auf der DLT-Plattform voraus. Hierdurch könnte eine Möglichkeit geschaffen werden, um DLT-Applikationen datenschutzrechtlich sicher umzusetzen.

Ein solcher Ansatz darf jedoch nicht übersehen, dass das Datenschutzrecht als Ausprägung des allgemeinen Persönlichkeitsrechts einen hohen Stellenwert besitzt. Einschränkungen des Datenschutzrechts zur Ermöglichung von Technologien zur effizienteren Durchführung von Werttransaktionen sind daher stets kritisch zu betrachten. In jedem Fall ist ausgeschlossen, dass durch eine solche Regelung auch die Verarbeitung von Daten Dritter gerechtfertigt wird, welche selbst nicht Teilnehmer des Netzwerks sind. Deren personenbezogene Daten sind zwingend off-Chain zu speichern. Auch nach einer Gesetzesänderung müssten die On-Chain-Daten auf das absolute Minimum beschränkt bleiben, sodass sich regelmäßig neben der Nutzerkennung und einer Werttransaktion keine weiteren Informationen auf dem DLT-Layer befinden sollten. Teilnehmer der DLT-Applikation müssten im Vorfeld ausführlich über die Folgen des Vertragsschlusses, insbesondere über die dauerhafte Speicherung der mit ihrer Nutzerkennung verbundenen Informationen, informiert werden.

Eine derartige Gesetzesänderung ist mit nicht unerheblichen Hürden verbunden. Zunächst ist der Begriff des datenschutzrechtlich Verantwortlichen ein unionsrechtlicher Begriff. Es liegt nicht in der Hand der Mitgliedstaaten diesen eigenständig auszulegen oder zu normieren. Folglich bedürfte eine Anpassung des Begriffs des Verantwortlichen einer Änderung der DS-GVO auf Unionsebene. Weiter sind die Risiken der Verlagerung der Verantwortung auf die jeweiligen Teilnehmer einer Transaktion zu beachten. Die Teilnahme an einer DLT-Plattform würde für den Nutzer zu einem teilweisen Verzicht auf sein Datenschutzrecht führen. Es darf dabei jedoch keine Situation entstehen, in denen die Bürger durch eine unbedachte oder (faktisch) aufgezwungene Teilnahme an einem DLT-Projekt der Verfügungsmacht über ihre personenbezogenen Daten beraubt werden. Da die Interessierten vor der Teilnahme an der DLT-Plattform über die bevorstehenden Datenverarbeitungen umfassend informiert werden müssten, stellt sich weiter die Frage, welche Stelle die Pflicht zur Information trifft. Denkbar erscheint es hier, dass eine gesetzliche Regelung die Einbettung der Informationen in die Software der DLT-Plattform vorsieht. Bei DLT-Applikationen, die diese Voraussetzungen nicht erfüllen und die personenbezogene Daten verarbeiten, würde dann ein Datenschutzverstoß aller Teilnehmer vorliegen.

Eine weitere Problematik kann dadurch entstehen, dass einzelne Teilnehmer vorsätzlich, fahrlässig oder aufgrund technischer Mängel personenbezogene Daten in das DLT-Netzwerk einpflegen, die nicht den Vorgaben des Systems entsprechen. Auf diese Weise können bspw. personenbezogene Daten Dritter oder Daten der Teilnehmer, die über das notwendige Minimum hinausgehen, dauerhaft veröffentlicht werden. Zwar könnte man die Verantwortung hierfür dem jeweils Einpflegenden zuweisen. Den notwendigen Löschpflichten kann dieser aber nicht nachkommen. Es müssten dann zumindest Kompensationsansprüche geschaffen werden. Es ist jedoch höchst fraglich, ob ein System, welches eine solche Möglichkeit des bewussten oder unbewussten Missbrauchs eröffnet, den Datenschutzgrundsätzen des Art. 5 DS-GVO und den Anforderungen an Privacy by design und Privacy by default des Art. 25 DS-GVO gerecht werden kann. Eine Lösung könnten hier zertifizierte DLT-Plattformen bieten, deren technische Grundeinstellung einen solchen Missbrauch verhindert, etwa dadurch, dass die verwendete Software nur

Datensätze akzeptiert, bei denen die Einspeicherung unerwünschter personenbezogener Daten ausgeschlossen ist.

6.3 Vorhandene Regulierungsansätze

6.3.1 International[331]

6.3.1.1 USA

In den USA überwacht die U.S. Securities and Exchange Commission (SEC) ICOs und den Handel mit Kryptowährungen und Token.[332] Eine übergreifende, bundesstaatliche Gesetzgebung ist nicht vorhanden.[333] Verschiedene Staaten haben eigene Gesetze erlassen. Das wohl bekannteste ist das Regelungsregime BitLicense[334] (New York), das für unternehmerische Tätigkeiten im Zusammenhang mit virtuellen Währungen gilt.[335]

Zu Beginn des Jahres 2019 haben mehrere Gesetzesinitiativen[336] vorgelegen, die im Zusammenhang mit der DLT-Technologie stehen. Ein Großteil bezieht sich auf die Regulierung virtueller Währungen, allerdings sollen auch die Vorteile des Einsatzes von DLT-Technologien durch die Regierung untersucht und Regeln zur Durchsetzbarkeit von Smart Contracts eingeführt werden.

6.3.1.2 Schweiz

In der Schweiz stehen virtuelle Währungen und andere DLT-Anwendungen (u. a. Smart Contracts) unter Beobachtung der Eidgenössischen Finanzmarktaufsicht (FINMA), die für bestimmte Tätigkeiten aufsichtsrechtliche Bewilligungspflichten annimmt.[337] Zudem hat die FINMA eine Wegleitung veröffentlicht, in der Hinweise zur Behandlung von Unterstellungsanfragen betreffend ICOs gegeben werden.[338]
Anfang 2018 wurde vom Staatssekretariat für internationale Finanzfragen die Arbeitsgruppe Blockchain/ICO ins Leben gerufen, die den regulatorischen Rahmen in der Schweiz überprüfen und etwaigen Handlungsbedarf aufzeigen sollte. Ziele waren u. a.

[331] Aufgeführt ist eine Auswahl gesetzlicher Regelungen und Initiativen. Eine Übersicht über internationale Regulierung in Bezug auf virtuelle Währungen (mit regelmäßigen Aktualisierungen): https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html.

[332] Siehe bspw. *Securities and Exchange Commission*, Statement on Digital Asset Securities Issuance and Trading., abrufbar unter https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading.

[333] Vgl. auch *Hofert*, Regulierung der Blockchains., S. 208 f.

[334] Abrufbar unter https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

[335] Siehe weiterführend *Hofert*, Regulierung der Blockchains., S. 205, 216 ff.

[336] Überblick bei https://www.virtualcurrencyreport.com/2019/01/blockchain-week-in-review-week-of-january-14-18-2019/#more-3837.

[337] *FINMA*, Faktenblatt Virtuelle Währungen, Stand 30.08.2018., abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaetter/faktenblatt-virtuelle-waehrungen.pdf?la=de.

[338] *FINMA*, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16.02.2018., abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de&hash=6518A4B3067554A0E22600E167601EF59AA20542.

die Erhöhung der Rechtssicherheit und die Sicherstellung einer technologieneutralen Regulierung.[339] In einem aktuellen Bericht des Bundesrats wird ein gewisser gesetzgeberischer Handlungsbedarf adressiert. Zum einen empfiehlt der Bundesrat eine Anpassung des Wertpapierrechts, um eine rechtssichere und möglichst technologieneutrale Ausgestaltung des Übergangs von Wertrechten durch Buchungen in dezentralen Registern zu ermöglichen.[340] Weiterer Anpassungsbedarf wird im Insolvenzrecht gesehen. So soll die Aussonderung kryptobasierter Vermögenswerte aus der Konkursmasse gesetzlich abschließend geklärt werden.[341] Das Finanzmarktrecht wird als grundsätzlich ausreichend technologieneutral angesehen, sodass keine grundlegenden Anpassungen für nötig erachtet werden.[342]

6.3.1.3 Malta, Liechtenstein

Das maltesische Parlament hat im Jahr 2018 drei Gesetze verabschiedet, die spezifische Regulierung für DLT-Anwendungen beinhalten. Durch den Malta Digital Innovation Authority Act (MDIA Act)[343] wurde eine Behörde (Malta Digital Innovation Authority) geschaffen, zu deren Aufgaben die Überwachung und Regulierung innovativer Technologien gehören soll. Das Gesetz bezieht ausdrücklich DLT-Technologien und Smart Contracts ein. Der Innovative Technology Arrangement and Services Act (ITAS Act)[344] betrifft die Zertifizierung von DLT-Anwendungen. Der Virtual Financial Assets Act (VFA Act)[345] enthält schließlich Normen im Zusammenhang mit virtuellen Währungen, ICOs etc.

Liechtenstein[346] hat einen Gesetzentwurf vorgelegt, mit dem ein sicherer Rechtsrahmen für DLT geschaffen werden soll.

6.3.1.4 Japan[347]

In Japan sind im Jahr 2017 Reformen mehrerer Gesetze 2017 in Kraft getreten, im Zuge derer spezielle Normen in Bezug auf virtuelle Währungen erlassen wurden. In Art. 2 (5) Payment Service Act ist eine Legaldefinition des Begriffs „virtuelle Währung" enthalten. Zudem besteht eine Registrierungspflicht für Anbieter, die Tauschbörsen für virtuelle Währungen betreiben wollen. Als Maßnahme im Kampf gegen Geldwäsche und Terrorismusfinanzierung müssen Betreiber von Tauschbörsen die Identität ihrer Kunden feststellen. Schließlich wurden ebenfalls neue verbraucherschützende Normen geschaffen.

[339] *Schweizer Bundesrat*, Medienmitteilung vom 18.01.2018., abrufbar unter https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69539.html.

[340] *Schweizer Bundesrat*, Bericht Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz., abrufbar unter https://www.mme.ch/fileadmin/files/documents/Publikationen/2018/181207_Bericht_Bundesrat_Blockchain.pdf, S. 67 f.

[341] Bericht des Bundesrates, S. 72.

[342] Bericht des Bundesrates, S. 9 f.

[343] Abrufbar unter http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1.

[344] Abrufbar unter http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1.

[345] Abrufbar unter http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1.

[346] Mitteilung vom 29.08.2018, abrufbar unter https://www.liechtenstein.li/en/news-detail/article/liechtenstein-preparing-blockchain-act/.

[347] Dazu *Danwerth,* ZVglRWiss 2018, 117.

6.3.2 Nationale und europäische Ebene

Auf nationaler Ebene existiert bisher keine DLT-spezifische Regulierung. Im Zentrum der derzeit stattfindenden Diskussion stehen Fragen des Finanz- und Kapitalmarktrechts, insbesondere die Einordnung von Token als Wertpapiere und damit zusammenhängende aufsichtsrechtliche Implikationen. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat mehrfach zu Fragen virtueller Währungen, Token und ICOs Stellung bezogen.[348] So hat sie insbesondere virtuelle Währungen als Rechnungseinheiten i. S. v. § 1 Abs. 11 S. 1 Nr. 7 KWG qualifiziert.[349] Die Prüfung erfolgte stets anhand der Rechtslage de lege lata.

Auf Ebene der Europäischen Union ist im Dezember 2017 die erste Vorschrift in Bezug auf virtuelle Währungen ergangen. Der Begriff der „virtuellen Währung" taucht seitdem in Art. 1 (2) (d) der 5. Geldwäscherichtlinie auf. Im Europäischen Parlament wurde im August 2018 ein Antrag zur Ausweitung der Regelungen zum Crowdfunding auf ICOs eingebracht.[350] Die Europäische Union erwägt weitere Maßnahmen im Zusammenhang mit der Schaffung eines wettbewerbsfähigen und innovativen Finanzmarkts, auch unter Einbeziehung der Blockchain-Technologie.[351] Insgesamt liegt der Schwerpunkt auch hier auf finanz- und kapitalmarktrechtlichen Fragen, insbesondere bezüglich des Anlegerschutzes.[352]

[348] *Bundesanstalt für Finanzdienstleistungsaufsicht (*BaFin), Hinweisschreiben vom 20.02.2018, GZ: WA 11-QB 4100-2017/0010.; *Bundesanstalt für Finanzdienstleistungsaufsicht (*BaFin), Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs)., abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html?nn=11056122; *Fußwinkel/Kreiterling*, Blockchain-Technologie – Gedanken zur Regulierung.

[349] *Bundesanstalt für Finanzdienstleistungsaufsicht (*BaFin), Merkblatt Finanzinstrumente vom 20.12.2011, geändert am 26.07.2018., abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html; a.A. KG Berlin, Urteil com 25.9.2018 – (4) 161 Ss 28/18 (35/18), NJW 2018, 3734.

[350] Vgl. Europäisches Parlament, 2018/0048(COD), abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-626.662&format=PDF&language=DE&secondRef=02.

[351] Vgl. *Europäische Kommission*, COM(2018) 109 final., abrufbar unter https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-109-F1-DE-MAIN-PART-1.PDF; *Europäische Kommission*, Blockchain Technologies., abrufbar unter https://ec.europa.eu/digital-single-market/en/blockchain-technologies.

[352] *European Securities and Markets Authority (*ESMA), Advice Initial Coin Offerings and Crypto-Assets., Rn. 14 ff.

7 Frachtpapiere

7.1 Ökonomisch-technischer Teil

7.1.1 Definition und Beschreibung des Anwendungsbeispiels

Beim Bill of Lading (BoL)[353] handelt es sich um ein besonders im internationalen Transport- und Logistikbereich zentrales Dokument. Das BoL ist ein spezielles Schiffsfrachtpapier, das gleichzeitig auch ein Warenwertpapier ist. Es wird üblicherweise vom Spediteur (Frachtunternehmen, Verfrachter) zunächst als Beleg für die Annahme der Fracht vom Exporteur (Belader) zur Verschiffung erstellt. Es umfasst zentrale Daten über die Art der verladenen Güter sowie die entsprechenden Transportmodalitäten und wird dem Importeur (Entlader) typischerweise nach Unterzeichnung durch Exporteur und Spediteur sowie der Bezahlung der Ware übermittelt. Im internationalen Handel erhält das BoL besonders aus dem Internationalen Abkommen zur Vereinheitlichung von Regeln über Konnossemente von 1924[354] seine Bedeutung.

Das BoL übernimmt demnach dreierlei Aufgaben[355]: Es dient dem Belader als Beleg für die Annahme der Ladung durch den Spediteur, als Beweis für den zwischen Exporteur und Spediteur geschlossenen Frachtvertrag sowie als verbriefter Rechtsanspruch auf die Ware. Letzteres bedeutet, dass der Eigentümer des BoL somit stets das Eigentum an der Fracht und folglich den rechtmäßigen Anspruch auf Herausgabe der Ware besitzt bzw. kraft BoL den Übergang des Eigentums der Ware auf einen anderen Beteiligten in der Lieferkette herbeiführen kann.[356]

Das BoL ist im weltweiten Schiffsfrachtbetrieb von Relevanz und international anerkannt. Im internationalen Handel benötigen Importeur und Exporteur wegen des Mangels an gegenseitigem Vertrauen, der z. B. durch unterschiedliche Rechtsordnungen in ihren Herkunftsländern bedingt ist, zusätzliche Sicherheiten im Warenhandel. So möchte der Exporteur im Idealfall seine Ware erst dann herausgeben, wenn er die Zahlung vom Importeur erhalten hat. Andererseits hat der Importeur vor der Zahlung ein berechtigtes Interesse an einer Bestätigung, dass er die Ware im vereinbarten Zustand erhalten wird. Um diesen Interessenkonflikt zu lösen, wird das BoL eingesetzt. Im Zuge des Beladens erhält der Exporteur das BoL vom Verfrachter als Quittung. Es dient ihm als Garantie am Eigentum der Ware, auch wenn sich diese nicht mehr physisch in seinem Besitz befindet. Als Nachweis für den Versand der Ware wird oftmals bereits eine Kopie des BoL an den Importeur versendet. Nach Zahlung der Ware durch den Importeur versendet der Exporteur das BoL, d. h., er schickt es physisch per Post an den Importeur bzw. den von diesem beauftragten Empfänger, der dann gegen Übergabe des BoL an den Verfrachter (und nur gegen physische Übergabe) die Ware ausgeliefert bekommt. Mittels Abbildung 22 soll dieser Vorgang veranschaulicht werden:

[353] Im deutschen HGB Konnossement, siehe dazu die Ausführungen im rechtlichen Teil.
[354] Auch bekannt als Haager Regeln.
[355] *Beecher,* The International Lawyer 2006, 627.
[356] Sogenannte Traditionswirkung, siehe 6.

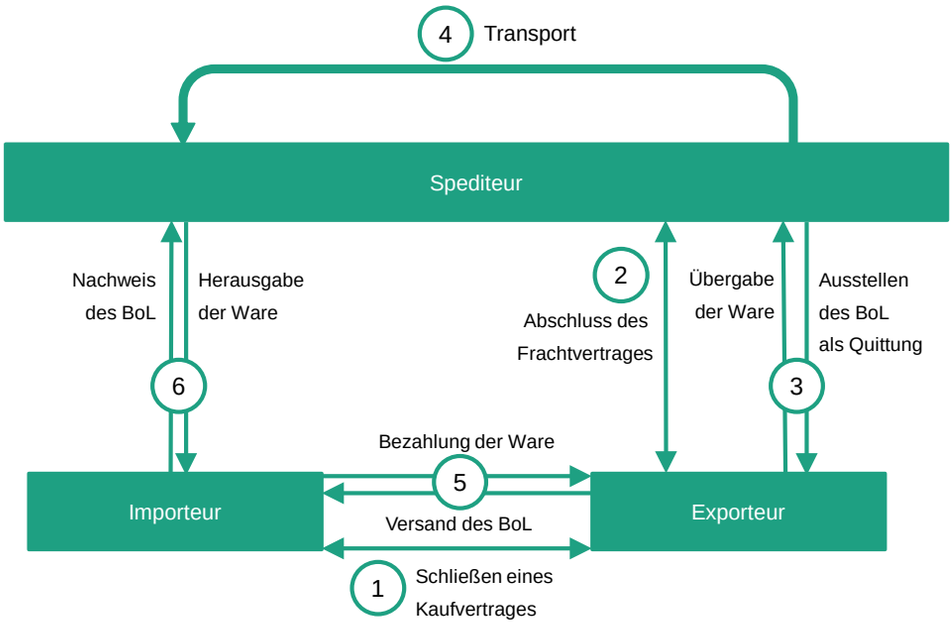


Abbildung 22: Vereinfachte Darstellung der Rolle eines BoL im internationalen Seehandel

Das BoL beinhaltet typischerweise folgende Informationen[357]:

- Daten des Exporteurs sowie des Importeurs (Name/Unternehmen, Kontaktinformationen)
- Gegebenenfalls Kontaktinformationen von Dritten, die über den aktuellen Status des Versands informiert werden müssen
- Daten des Spediteurs (Unternehmen, Logo, Adresse, Kontaktinformationen und Beförderungsbedingungen)
- BoL-Nummer (eindeutige Zahl, die von der Spedition oder von der Schifffahrtsgesellschaft erstellt wird)
- Name des Schiffs/Fahrzeugs und Nummer der Fahrt
- Empfangsort, Beladehafen, Entladehafen, Ort der Übergabe, Zielort
- Containernummer, Siegelnummer, Kennzeichen
- Beschreibung der Ware (Gesamtgewicht, Volumen …)
- Spezifikation der Incoterms[358] (internationale Handelsklauseln)
- Ort und Datum des Versands und Unterschriften von Exporteur, Spediteur sowie Importeur
- Beförderungsbedingungen, gegebenenfalls Spezifizierung von Transportmodalitäten, wie etwa „Port-to-port“ oder „Combined Transport“

Zudem kann das BoL besondere Vereinbarungen zwischen dem Exporteur und dem Spediteur beinhalten, die von den allgemeinen Transportbedingungen des Verfrachters abweichen.[359]

[357] § 515 HGB.
[358] Die International Commercial Terms sind eine Reihe freiwilliger Klauseln zur Auslegung handelsüblicher Vertragsformeln im internationalen Warenhandel.
[359] *Beecher,* The International Lawyer 2006, 627.

Wegen der im BoL enthaltenen umfassenden Dokumentation der Transportbestimmungen sowie seiner rechtlichen Stellung als Traditionspapier wird das BoL bevorzugt bei den im internationalen Warenhandel stattfindenden Akkreditivgeschäften[360] (Letter of Credit, LoC) eingesetzt. Die Standards für die Nutzung von Akkreditiven werden in den ERA 600 der internationalen Handelskammer[361] festgelegt. Dort wird ein Akkreditiv wie folgt beschrieben:

Das (Dokumenten-)Akkreditiv bezeichnet ein Zahlungsinstrument im internationalen Handel. Dabei sichert die Bank des Importeurs (eröffnende Bank) dem Exporteur einer Ware die Zahlung des Gegenwerts zu, wenn bestimmte, zuvor definierte Dokumente vollständig und korrekt vorgelegt werden. Der Akkreditivprozess ist in Abbildung 23 vereinfacht visualisiert:[362]

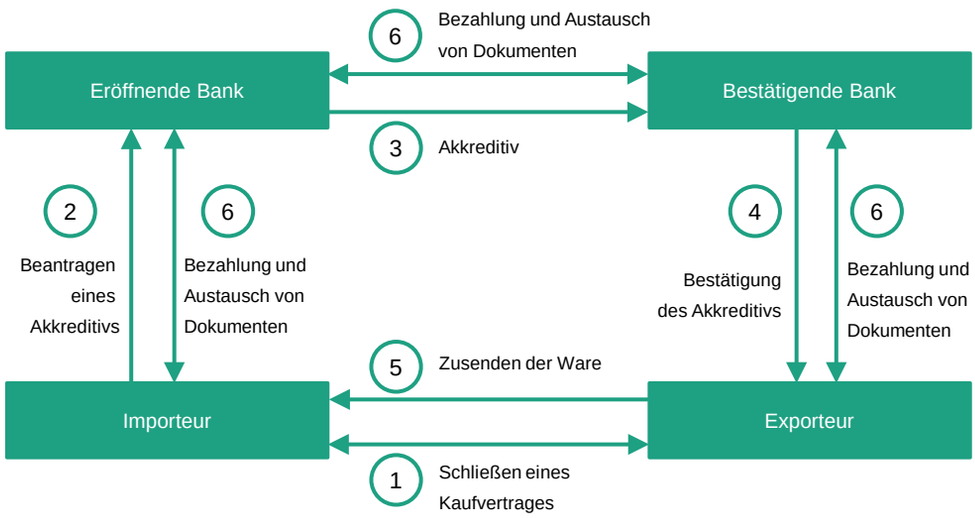


Abbildung 23: Vereinfachte Darstellung eines Akkreditivprozesses

Beim Akkreditivprozess sind somit in der Regel vier teilnehmende Parteien involviert: Importeur und Exporteur sowie zwei Banken, die eröffnende Bank und die avisierende Bank. Dem Akkreditiv liegt stets der Kaufvertrag für ein bestimmtes Gut zugrunde (1), in dem das Akkreditiv als Zahlungsinstrument vereinbart wird. Das Akkreditiv selbst ist jedoch anschließend von diesem Kaufvertrag losgelöst. Nur die im Akkreditivvertrag festgelegten Bedingungen an die einzureichenden Dokumente sind maßgeblich für die Prozessdurchführung.

Der Importeur beantragt nach dem Schließen des Kaufvertrags (1) zunächst die Eröffnung eines Akkreditivs (2) bei seiner Bank (eröffnende Bank/Akkreditivbank), bevor diese das Akkreditiv über die avisierende Bank eröffnet (3). Anschließend avisiert diese Bank das Akkreditiv an den Exporteur (4). Nun versendet der Exporteur die Ware an den Importeur (5) und reicht daran anschließend alle zuvor definierten Dokumente (z. B. das Konnossement) bei seiner Bank ein (6). Die avisierende Bank überprüft diese Dokumente auf Vollständigkeit und inhaltliche Richtigkeit. Häufig erfolgt diese Prüfung manuell anhand papierbasierter Dokumente. Im Falle korrekt vorliegender Dokumente werden diese an die Akkreditivbank weitergegeben. Diese führt die gleichen Prüfungen erneut durch.

[360] Es existieren viele verschiedene Ausprägungen von Akkreditiven, hier soll aber auf die Abwicklung von Dokumentenakkreditiven Bezug genommen werden.

[361] Einheitliche Richtlinien und Gebräuche für Dokumenten-Akkreditive, international UCP 600 (Unifirm Customs and Practice for Documentary Credits).

[362] Eine detaillierte Beschreibung des LoC-Prozesses findet sich bspw. in *Grassi,* 7 Pace Int'l Rev. 1995, 81.

Sobald auch diese Bank die Dokumente als korrekt einstuft, wird die Zahlung an den Exporteur ausgelöst.

In diesem Anwendungsfall sollen das BoL, stellvertretend für alle Arten von Dokumenten im internationalen Warenhandel, genauer betrachtet sowie die damit oft verbundenen (Dokumenten-)Akkreditivgeschäfte näher analysiert und auf mögliche Einsätze der DLT hin überprüft werden. Zusätzlich sollen außerdem die eng damit verbundenen Implikationen für Supply-Chain-Prozesse analysiert werden.

7.1.2 Status quo und Herausforderungen

Im Jahr 2017 sind Waren im Wert von insgesamt knapp 18 Billionen US-Dollar auf internationalen Märkten gehandelt worden[363], von denen etwa 90 Prozent im internationalen Schiffsfrachtverkehr transportiert worden sind.[364] Der Handel und die damit verbundenen Logistikprozesse sind dabei in zunehmendem Maße abhängig von hochkomplexen und -spezialisierten Supply-Chain-Prozessen, die wiederum häufig nur durch Einführung bzw. unter Verwendung moderner Kommunikations- und Informationstechnologien möglich sind. Heute findet jedoch ein Großteil der Prozessdokumentation nach wie vor über traditionelle Papierdokumente, wie etwa das BoL, statt.

Die Verwendung papierbasierter Dokumente zeigt verschiedene Nachteile. Der wohl größte Nachteil besteht darin, dass papierbasierte Dokumente physisch transportiert werden müssen. Der Importeur benötigt das papierhafte, originale BoL, um die Herausgabe der Fracht vom Verfrachter herbeiführen und so das Eigentum an der Fracht erlangen zu können. Im Idealfall kann der Exporteur der Ware das BoL bereits zeitnah (z. B. einen Tag nach dem Verfrachten der Ware bzw. dem Ablegen des Schiffs) vom Frachtunternehmen erhalten. Durchschnittlich wartet ein Exporteur jedoch etwa drei Tage lang, manchmal ist das BoL sogar eine Woche nach Versand noch nicht ausgestellt.[365] Das BoL muss dann an den Empfänger der Ware (bzw. einen Vertreter, der mit der Entgegennahme der Ware beauftragt ist) gesendet werden. Die Übersendung der Dokumente benötigt selbst per Expressmail (Luftpost) im Mittel weitere vier bis sieben Tage. Der Empfänger muss das BoL nun wiederum dem Frachtunternehmen vor Ort aushändigen, was erneut bis zu zwei Tage in Anspruch nimmt, da sich die Kundenservicestellen der meisten Schifffahrtsunternehmen nicht in der Nähe eines Hafens befinden.[365] Hinzu kommt, dass selbst in die unkompliziertesten Transporte im internationalen Warenhandel eine Vielzahl von Beteiligten involviert ist.[366]

Die Problematik verkompliziert sich zusätzlich dadurch, dass etwa im Rahmen eines Akkreditivs auch noch Banken am Prozess beteiligt sind. Der Exporteur muss diesen das BoL und weitere Dokumente zum Abgleich mit den Akkreditivbedingungen zur Verfügung stellen. Die Dokumente werden in diesem Prozess wiederum physisch (z. B. per Kurier oder Luftpost) an die jeweils nächste Partei im Prozess weitergeleitet. Zudem müssen die Dokumente im Akkreditivprozess, also u. a. das BoL, auf die Einhaltung der Akkreditivbedingungen geprüft werden. Diese Überprüfung geschieht oft mühsam per Hand durch Bankmitarbeiter.

Daraus resultiert, dass der Versand der Dokumente häufig länger dauert als der der Ware, was letztlich den Empfänger daran hindert, seine Ware fristgerecht am Zielhafen abzuholen, da dies nur mit dem originalen BoL möglich ist. Der Importmanager eines großen

[363] *Statista*, Trends in global export volume of trade in goods from 1950 to 2017.
[364] *International Chamber of Shipping*, Shipping and World Trade Shipping and World Trade.
[365] *Beecher,* The International Lawyer 2006, 627 *Beecher,* The International Lawyer 2006, 627.
[366] Die Angaben variieren je nach Quelle, typischerweise werden als untere Grenze 10 – 30 Beteiligte genannt.

Zollspediteurs fand im Zuge einer Studie heraus, dass etwa 25 Prozent der Warensendungen, für die ein Akkreditivgeschäft abgeschlossen wurde, mit Liegegebühren, also Vertragsstrafen für nicht fristgerecht abgeholte Ware, belegt wurden.[365] Das Problem verschärft sich zusätzlich dadurch, dass die für die Zustellung des BoL zur Verfügung stehende Zeit wegen der sinkenden Überfahrtsdauer von Frachtschiffen im Allgemeinen während der letzten Jahre gesunken ist – bspw. kann ein Transport von Bremen nach New York mittlerweile in nur neun Tagen durchgeführt werden. Außerdem ist die Überfüllung von Häfen aufgrund des stetig wachsenden Warenhandels in den letzten Jahren zu einem ernst zu nehmenden Problem herangewachsen, das Frachtunternehmen dazu zwingt, die Ware möglichst schnell vom Pier zu räumen.

Der stark papierbasierte Prozess verlangsamt also nahezu alle Arbeitsschritte und verursacht zudem eine hohe Fehleranfälligkeit durch das häufige, manuelle Übertragen von Informationen.[367] Die fehlende Prozessdigitalisierung und die damit ebenso fehlende Automatisierung führen oft zu einem Mangel an Informationen, etwa beim Tracking von Waren, und machen so insgesamt Supply-Chain-Prozesse unflexibel. Dies impliziert bspw. die Notwendigkeit größerer Rohstoffreserven bei Unternehmen und verursacht demzufolge weitere Kosten. Insgesamt bedingt das heutige, analoge System Schätzungen zufolge Kosten in Höhe von 5-10 Prozent des Werts der jährlich international gehandelten Waren[368] und liegt somit in der Größenordnung von etwa einer Billion US-Dollar. Diese vereinfachte Schätzung unterstellt, dass der internationale Warenverkehr vollständig durch DLT realisiert wird. Dies Schätzung weicht von dedizierten Studien wie z.B. von Gartner ab, indem darin Marktdurchdringung explizit modelliert wird. In den letzten Jahrzehnten wurde intensiv daran geforscht, den internationalen Handel zu digitalisieren und somit u. a. das dafür zentrale BoL durch einen geeigneten elektronischen Prozess mit derselben Funktionalität zu ersetzen. Eine solche elektronische Alternative, die im Folgenden als E-BoL bezeichnet wird, könnte nicht nur die benötigte Prozesszeit für die Verarbeitung der Dokumente signifikant reduzieren, sondern auch die Sicherheit durch Verschlüsselung und digitale Signaturen erheblich erhöhen. Außerdem könnte die Effizienz durch das Ausschließen der genannten Fehler beim Ab- und Umschreiben von Informationen reduziert werden. Allein durch die schnellere Bereitstellung von Informationen und aus den damit effizienteren Logistikprozessen resultierenden Zeiteinsparungen zwischen Prozessschritten könnten Schätzungen von IBM zufolge bereits bis zu 40 Prozent der Transportkosten auf See eingespart werden, was pro Container mehrere Tausend Dollar ergeben kann.

Der Status quo und seine Herausforderungen haben die Suche nach Verbesserungen und Alternativen initiiert. In den letzten Dekaden hat sich dabei der Sea Waybill als praktische Variante angeboten.[369] Dieser wird im Gegensatz zum BoL nicht als Traditionspapier angesehen, sodass zum Übergang des Eigentums gerade nicht die physische Übergabe erforderlich ist. Vielmehr genügt etwa eine Kopie des Sea Waybill als Nachweis für die Berechtigung zur Abholung der Ware. Dies ermöglicht zumindest eine Digitalisierung des Informationsflusses, jedoch keine Digitalisierung der mit der Übergabe der BoL verbundenen Übereignungsprozesse. Dennoch ist das BoL als rechtlich umfassendes und universell einsetzbares Instrument weiter sehr verbreitet.

Mit herkömmlichen digitalen Technologien könnten die technischen Anforderungen an eine digitale BoL durchaus erfüllt werden. Dabei sorgt eine Public-Private-Key-Infrastruk-

[367] Schätzungen zufolge enthält jedes zweite Dokument mindestens einen Fehler, der von falschem Abschreiben von Informationen stammt.

[368] *Todd,* Journal of International Banking Law 2000, 410.

[369] *Boom,* European Transport Law (ETL) 1997, 9.

tur für Autorisierung, Verschlüsselung und für Integrität (SSL/TLS), und in einem zentralen Register kann der Regulator sicherstellen, dass es immer nur eine gültige E-BoL zu einem Vorgang gibt.

Der erste ernstzunehmende Ansatz zur Etablierung eines auf diesen Prinzipien beruhenden elektronischen BoL war BOLERO[370], ein zentrales, privates Registrierungs- und Kommunikationssystem, das von einem Konsortium aus mehreren Frachtunternehmen, Banken, Versicherungen sowie Kommunikationsunternehmen unterstützt wurde. Beteiligte an einem Frachtprozess – und nur diese – können sich darin einbringen und Transaktionen lesen oder bearbeiten. Dabei wurden bereits kryptografische Methoden zur Verschlüsselung verwendet. Die Plattform bietet ebenfalls die Möglichkeit zur Kommunikation zwischen den Parteien.

Problematisch war hierbei die international nicht anerkannte elektronische Form des BoL (bzw. die mangelnde Gesetzeslage). Mittels der Geschäftsbedingungen der Plattform wurde versucht, dieses Problem zu umgehen. Es blieb jedoch unklar, inwiefern damit das Recht des Eigentümers des BoL auf Herausgabe der Ware nach dem jeweiligen nationalen Recht tatsächlich vermittelt wurde. Unabhängig davon, ob das Regelwerk dies ermöglichen soll oder nicht, ist es fraglich, ob ein elektronisches BoL dies ermöglichen kann. An diesem Punkt könnte nämlich die Vertragsfreiheit sehr wohl mit den berechtigten Interessen von Dritten, etwa Kreditgebern von am Transfer beteiligten Akteuren, kollidieren. Die meisten Autoren gehen davon aus, dass nach geltendem Recht ein elektronisches BoL kein Dokument ist, das das Eigentum an der Ware und damit Recht und Pflichten übertragen kann[371]. Insgesamt konnte sich BOLERO am Markt nicht durchsetzen, auch sonst konnte sich noch keine zentrale Plattform durchsetzen.

In den letzten Jahren entwickelte sich jedoch eine gewisse Dynamik. In einem neuen Versuch begannen IBM und Maersk Ende 2017 mit der Entwicklung von TradeLens, einem Blockchain-Prototypen, basierend auf Hyperledger Fabric, um die Supply Chain für Containerverschiffung zu verwalten. Dabei können alle am Prozess beteiligten Dokumente digitalisiert und die Container nachverfolgt werden. Mittlerweile sind nach Angaben von IBM 92 Unternehmen, darunter Frachtunternehmen (Maersk, Pacific International) sowie Hafenbetreiber (Rotterdam, Singapur), mit über 200 Docks beteiligt, die etwa 20 Prozent des weltweiten internationalen Warenumsatzes transportieren und etwa denselben Anteil an Docks (~235) betreiben. Bisher sollen mehr als 250 Millionen „Shipping Events" über TradeLens abgewickelt[372] worden sein. Dabei ist zu bemerken, dass aktuell keine Möglichkeit, Eigentum an dem E-BoL zu übertragen, implementiert ist, sodass TradeLens bislang ausschließlich der nachvollziehbaren Dokumentation von Supply-Chain-Prozessen für alle an einem Versand beteiligten Akteure dient. Einige nationale Behörden, wie etwa die saudi-arabische Zollbehörde, sehen überdies die Integration von TradeLens in ihrer Zollbehörde vor[373]. Allerdings verlangen IBM und Maersk für den Zugang zum TradeLens-System Gebühren, über deren Höhe aber aktuell noch kaum Informationen vorhanden sind. Darüber hinaus beanspruchen sie aus dem Projekt entstehende Intellectual Property Rights für sich. Dadurch wird de facto die Dezentralisierung der Lösung wieder aufgehoben. Der langfristige Erfolg und die Konkurrenzfähigkeit gegen eine komplett offene Lösung bleiben daher trotz des bisher starken Wachstums fraglich.

Vermutlich als Konsequenz daraus haben erst Ende 2018 einige weitere der weltweit größten Frachtunternehmen und Terminalbetreiber ein weiteres Konsortium zum Entwi-

[370] Bill of Lading Electronic Registry Organization, seit 1998.
[371] *Beecher,* The International Lawyer 2006, 627.
[372] *Tradelens*, The Power of the Ecosystem.
[373] *Customs*, Saudi Customs Pilot Sees the Integration of Customs Tracking Feature with IBM and Maersk TradeLens Blockchain Solution.

ckeln einer DLT-basierten Plattform für ein weltweites Handelsökosystem, genannt Global Shipping Business Network (GSBN), gegründet. Zunächst sollen dabei die Digitalisierung und Automatisierung von Dokumentation und Prozessen rund um Gefahrgüter ermöglicht werden, die in der Regel von einer Reihe an Regularien betroffen sind. Letztlich soll aber ein nahtloses Teilen von Dokumenten und Daten über den gesamten Lebenszyklus eines Seetransports ermöglicht werden.

Das israelische Start-up Wave, das 2016 gemeinsam mit Barclays die weltweit erste Live-Blockchain-Transaktion im Handelsbereich durchgeführt haben will[374], arbeitet bereits an einer kommerziellen Lösung für eine mittels DLT digitalisierte Bill of Lading. Aktuell testet die Firma gemeinsam mit mehreren Frachtunternehmen verschiedene Pilotimplementierungen[375]. Das Start-up CargoX mit Sitz in Slowenien hat Ende 2018 angekündigt, dass seine DLT-basierte Lösung für ein elektronisches BoL ab sofort kommerziell verfügbar ist. Diese ermöglicht das Ausstellen und den Transfer eines elektronischen BoL auf einer öffentlichen Blockchain. Im Januar 2018 hatte CargoX über 7 Mio. USD in einem ICO eingesammelt, um in der zweiten Jahreshälfte mit mehreren Logistikanbietern Pilotprojekte durchzuführen; diese nutzen nun auch die Plattform. Unter anderem sind dies die Schweizer Fracht AG, Sprint International Express, Globalink, Global Value Network und Freightalia. Laut Start-up können die Benutzer für 15 US-Dollar und innerhalb weniger Minuten die Ausstellung und den Transfer eines BoL ausführen.

Ein weiteres Pilotprojekt wird derzeit unter der Leitung des Hafens von Rotterdam bzw. des von ihm gegründeten BlockLabs durchgeführt.[376] In diesem Projekt, an dem u. a. Samsung SDS sowie ABN AMRO beteiligt sind, soll mittels der DLT eine papierlose Integration aller physikalischen, administrativen, beobachtenden sowie finanzierenden Prozesse und Services behandelt werden.

7.1.3 Mögliche Lösungsansätze und Rolle von DLT

Ein E-BoL muss die drei einleitend genannten Funktionen des BoL implementieren. Insbesondere muss es die Beförderungsbedingungen festlegen, eine Bestätigung für die Entgegennahme der Ware durch den Spediteur darstellen und Zugang zum Eigentum ermöglichen. Zudem sollte sich ein E-BoL durch einen geringen Preis sowie hohe Fälschungssicherheit auszeichnen. Damit sich ein solcher E-BoL in der Praxis durchsetzen kann, muss er zudem mit verhältnismäßig geringen Kosten eingeführt und genutzt werden können. Gleichzeitig muss natürlich gewährleistet sein, dass lediglich Personen mit gerechtfertigtem Interesse an den Vorgängen Zugang zu den in einem E-BoL enthaltenen Daten erhalten.

Bereits Mitte der 1990er-Jahre wurde die rechtliche Perspektive für eine Digitalisierung des BoL von der Kommission der Vereinten Nationen für internationales Handelsrecht (UNCITRAL) aufgegriffen. Als Hauptproblem identifizierte diese die bereits diskutierte „Garantie der Einzigartigkeit", die jede elektronische Realisierung eines BoL erfüllen muss.[377]

[374] *Reuters*, Barclays says conducts first blockchain-based trade-finance deal.

[375] *Gtreview*, New blockchain shipping consortium to rival Maersk and IBM's TradeLens. *Gtreview*, New blockchain shipping consortium to rival Maersk and IBM's TradeLens.

[376] *Port of Rotterdam*, ABN AMRO, Samsung SDS and the Port of Rotterdam Authority are launching a container logistics blockchain pilot.

[377] Artikel 17(3) des Model Law von UNCITRA lautet: [I]f a right is to be granted to, or an obligation is to be acquired by, one person and no other person and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

Zentrale, von einem Intermediär betriebene Plattformen wie BOLERO, die bis vor kurzem die einzige Möglichkeit für die technische Realisierung eines elektronischen BoL (E-BoL) boten, weisen jedoch für die beteiligten Akteure Nachteile und Risiken auf. So bietet eine zentrale Plattform stets einen Single Point of Failure und somit ein potenzielles Angriffsziel. Gezielte Manipulationen, entweder durch Angriffe oder auch durch den Intermediär sind möglich. Insbesondere besteht jedoch, wie bei vielen B2B-Situtationen, in denen für die Digitalisierung eines Prozesses organisationsübergreifende Kooperation nötig ist, die Problematik, dass in der Regel gegenüber anderen Unternehmen der gleichen Wertschöpfungskette eine Wettbewerbssituation und demzufolge kein Vertrauen besteht. Die potenzielle Marktmacht, die ein zentraler Plattformbetreiber über eine aus der Kontrolle über die Plattform resultierende Monopolsituation erhalten könnte, ist ebenfalls bei Unternehmen außerhalb der jeweiligen Wertschöpfungskette ein erhebliches wirtschaftliches Risiko für die Wettbewerber. Zudem ist es gut möglich, dass wegen der großen wirtschaftlichen und damit strategischen Rolle des internationalen Seehandels auch aus nationaler Perspektive Vorbehalte gegen eine Plattform bestehen könnten, die von einem in einem anderen Land ansässigen Monopolisten kontrolliert wird. Dies führt dazu, dass Kollaboration auf einer zentralen Plattform in der Regel kaum Unterstützer findet.

Wie bereits im Grundlagenteil ausgeführt, kann die DLT diese Punkte adressieren und gerade in solchen Situationen als grundlegende IT-Infrastruktur die Kooperation von Unternehmen ermöglichen. Bei der Implementierung einer solchen Lösung gibt es mehrere Herausforderungen für die Anerkennung eines E-BoL. Neben dem Verwenden von digitalen Signaturen als Äquivalent zur händischen Unterschrift muss sichergestellt sein, dass der Frachtbrief auch in einem verteilten System nicht kopiert werden kann. Die Verwendung von digitalen Signaturen ist in Deutschland und auch vielen anderen Ländern bereits weit verbreitet, sodass an dieser Stelle keine technischen Neuerungen nötig sind. Grundsätzlich kann man das Kopieren eines elektronischen Dokuments in einem verteilten System technisch zwar nicht verhindern. In einem DLT-System kann aber über die Konsensmechanismen verhindert werden, dass innerhalb des Systems E-BoL mehrfach in gültiger Instanz existieren oder mehrmals gültig eingesetzt werden können. Die Grundidee bei der Digitalisierung des BoL ist somit, den Frachtbrief als „Asset Backed Token“[378] zu modellieren und durch die Governance in der DLT sicherzustellen, dass dieser per Konstruktion nur einmal verwendet werden kann. Durch die in der DLT meist inhärente PKI[379] sind die für elektronische Unterschriften unter einem E-BoL erforderlichen digitalen Signaturen in einer DLT-Lösung ohnehin implementiert. Die fälschungssichere Prozessdokumentation mittels DLT ermöglicht zudem Auditierbarkeit[380] und Rechtssicherheit im Falle von Disputen.

Als Erweiterung eines E-BoL könnten dann auch die Akkreditivgeschäfte stärker automatisiert werden. Hierbei könnten mittels eines Treuhand-Smart-Contracts[381] der vom Importeur zu bezahlende Betrag bei Erstellung des E-BoL eingefroren werden. Beim Entladevorgang kann dann der Token für den E-BoL vom Exporteur auf den Importeur übertragen werden und dadurch die Auflösung des Treuhand-Smart-Contracts ausgelöst werden, was den eingefrorenen Betrag an den Exporteur freigibt. Weiterführende Effekte, die sich in einem solchen System ergeben, wie bspw. eine damit einhergehende Kapitalbindung, sind in der Zukunft genauer zu analysieren.

[378] Siehe auch Abschnitt 5.2.5.6.

[379] Siehe auch Abschnitt 4.1.2.

[380] Ein Audit ist ein Vorgang, bei dem untersucht wird, ob Prozesse etwa in Unternehmen bspw. gesetzlich oder unternehmerisch geforderten Standards genügen. Solche Verfahren erfolgen etwa im Rahmen von Wirtschaftsprüfungen oder im Qualitätsmanagement.

[381] Engl. Escrow Smart Contract, siehe auch Abschnitt 4.2.1.

7.1.4 Prozessbeschreibung

Durch die folgende technische Architektur, die für jeden aktuell analogen Schritt einen digitalen Zwillingsvorgang durchführt, könnte das Frachtpapier unter Berücksichtigung der zuvor beschriebenen Anforderungen digitalisiert werden.

- Wie auch im herkömmlichen System werden bereits vor Versand der Ware ein Kaufvertrag zwischen Importeur und Exporteur sowie ein Transportvertrag zwischen Exporteur/Importeur und Spediteur geschlossen, etwa durch gegenseitiges digitales Signieren entsprechender elektronischer Vertragsdokumente.
- Ein E-BoL, das die für ein BoL nötigen Daten[382] enthält, wird im Moment der Befrachtung vom Spediteur erstellt sowie von ihm und dem Exporteur digital signiert. Anschließend erhalten alle an dem Logistikprozess beteiligten Akteure Informationen über die Inhalte dieses BoL. Durch Implementierung des E-BoL als Asset Backed Token[383], der anfangs dem Exporteur zugeschrieben wird, können die Eigentumsverhältnisse eindeutig repräsentiert werden.
- Dieser Token unterscheidet sich prinzipiell nicht von einem Smart Contract, also einer DLT-Adresse, die durch Nachrichten angesprochen und deren Inhalt gemäß bestimmten Regeln, über die im Netzwerk ein Konsens herrscht, verändert werden kann.
- Die Eigentumsverhältnisse am Token können dadurch abgebildet werden, dass für den entsprechenden Smart Contract ein Eintrag „Besitzer" definiert wird, der den Public Key des Eigentümers enthält. Zum Ändern dieses Feldes ist dann zwingend der private Key des Eigentümers nötig.

Eine mögliche Variante des via E-BoL digitalisierten Prozesses ist schematisch in Abbildung 24 aufgezeigt.

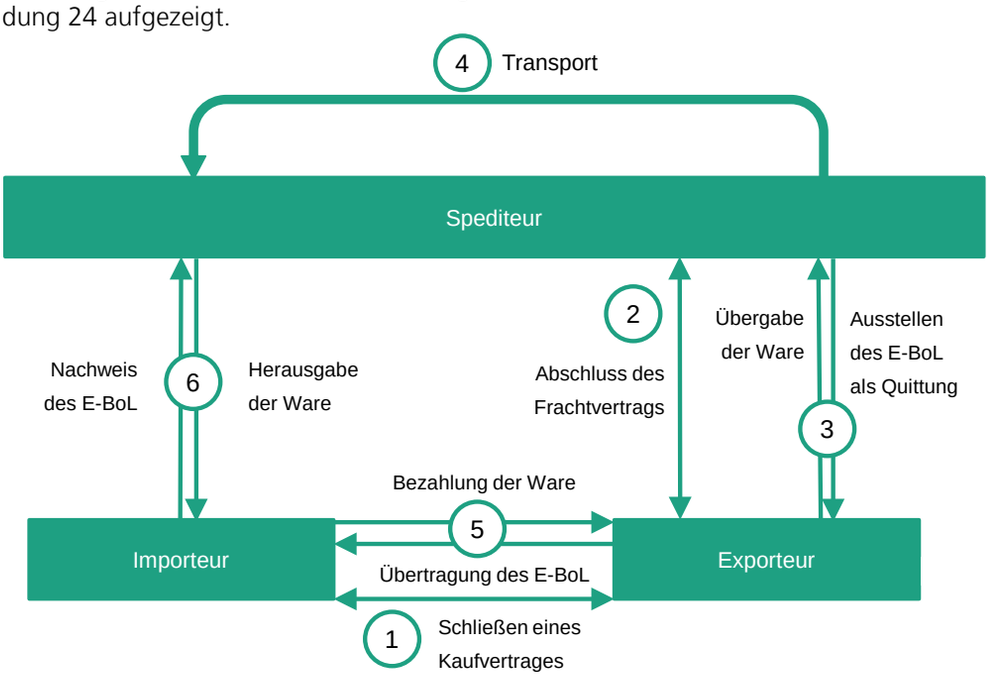


Abbildung 24: Schematische Darstellung des internationalen Handels auf Basis eines E-BoL

[382] Siehe auch Abschnitt 7.1.1.
[383] Siehe auch Abschnitt 5.2.5.6.

Es ist zu beachten, dass für eine solche Implementierung eine Smart-Contract-fähige DLT benötigt wird. Eine Möglichkeit, die bspw. bei TradeLens genutzt wird, ist die Implementierung in Hyperledger Fabric. Innerhalb solcher Lösungen gibt es außerdem Architekturen, die für das Abbilden des mit dem BoL verbundenen Prozesses besonders geeignet sind. Für TradeLens gibt es z. B. mehrere REST-APIs[384], etwa eine API zum Hinzufügen oder Entfernen von am Prozess beteiligten Instanzen (Häfen, Speditionen …), eine API zum Teilen von Dokumenten sowie eine API, mit deren Hilfe Ereignisse in die TradeLens-Plattform eingetragen werden können, wie etwa voraussichtliche Ankunftszeiten, die dann automatisiert an die beteiligten Nodes und damit Prozessbeteiligten weitergeleitet werden. Für die TradeLens-Plattform steht also mittlerweile eine Vielzahl von umfassenden APIs zur Verfügung, anhand derer direkt am Transport eines Containers bzw. einer Ware beteiligte Unternehmen oder Autoritäten Eintragungen vornehmen können. Eine Funktionalität für die Übermittlung des E-BoL gibt es hierbei offenbar noch nicht, jedoch besteht die Möglichkeit, ein E-BoL zu Dokumentationszwecken zu erstellen sowie allgemein Dokumente, wie etwa Scans von Papieren, zur Verfügung zu stellen. Hierbei ist hervorzuheben, dass durch eine entsprechende Implementierung, bspw. in Hyperledger Fabric[385], umfassende Möglichkeiten zur Verfügung stehen, um die Firmengeheimnisse zu wahren:

- Durch die Implementierung in einer privaten Blockchain ist die Anzahl an Nodes, die auf die Daten zugreifen können, per se äußerst begrenzt. Teilnehmende Nodes sind neben den Frachtunternehmen auch zuliefernde Speditionen oder Großkunden sowie Häfen oder Landesbehörden (Autoritäten), etwa der Zoll.
- Weiter ist bspw. Hyperledger Fabric eine Blockchain, die umfassende Funktionen für Datensicherheit beinhaltet. So können mehrere private Blockchains, an der jeweils eine Teilmenge der Nodes teilnimmt, verwaltet werden. Man kann sich Architektur hinter TradeLens somit als eine Vielzahl von Blockchains vorstellen, sodass an jedem Transport etwa eines Containers nur diejenigen Nodes Lese- und Schreibrechte besitzen, die aktiv, etwa durch den Ersteller des E-BoL, in den Prozess eingebunden werden.
- Zusätzlich besteht auch innerhalb einer dieser DLT die Möglichkeit, Daten vollständig privat zu halten. Soll etwa der Inhalt des Containers oder die Identität eines Unternehmens geheim gehalten werden, so werden die Daten nur für die dafür bestimmten Nodes freigegeben. Die gleiche Möglichkeit besteht ebenso für Input- oder Outputwerte für bzw. aus einem Smart Contract (Chaincode).

Im Bereich der Akkreditive ist auf Basis eines E-BoL eine vollständige Automatisierung des zuvor beschriebenen analogen Prozesses mittels der DLT denkbar, z. B. wie in Abbildung 25 dargestellt.

[384] Eine API (application programming interface) ist eine Programmierschnittstelle eines IT-Systems, d. h. ein Programmteil, mit dem man andere Programme an das System anbinden kann. Eine REST-API ist dabei ein Standard für APIs, dem besonders hohe Zuverlässigkeit zugesprochen wird. Eine API zum Einstellen von Prozessschritten bzw. Ereignissen im internationalen Seehandel („shipping events") findet man etwa unter https://platform-sandbox.tradelens.com/documentation/swagger/?urls.primaryName.

[385] Siehe auch auch 1.2.1.

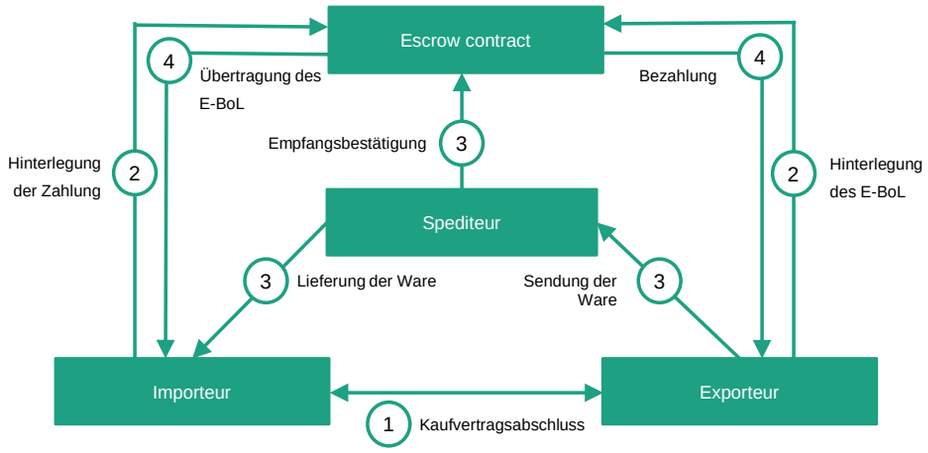


Abbildung 25: Akkreditivprozess basierend auf einem Treuhand-Smart-Contract[386]

Der Prozess könnte dabei grundsätzlich ohne Beteiligung von Banken abgewickelt werden. Dabei werden gegebenenfalls zunächst weitere, neben dem E-BoL für das Akkreditiv benötigte Dokumente festgelegt. Noch vor dem Befrachten der Ware wird dann der zu zahlende Betrag vom Importeur in einem sogenannten Treuhand-Smart-Contract[387] hinterlegt. Hat eine zuvor definierte, vertrauenswürdige Partei[388] (z. B. ein Kurier) den Warenversand/-eingang digital bestätigt[389] sowie die entsprechenden Bedingungen geprüft, kann der Geldtransfer an den Exporteur ausgelöst werden. Der Treuhand-Smart-Contract übernimmt also neben der Prüfung[390] der Bedingungen, etwa ob bestimmte Fristen eingehalten wurden, die Zahlungssicherung und ersetzt für diese die Funktion der Bank(en). Hierbei stellt sich die Frage, ob diese Zahlung direkt mittels DLT durchgeführt werden kann (z. B. mittels Token) oder ob der Smart Contract lediglich eine auslösende Funktion hat und die Zahlung über andere, bestehende Kanäle erfolgt.

Zudem übernimmt ein Akkreditiv neben der Transaktionsfunktion jedoch insbesondere auch eine Finanzierungsfunktion für den Exporteur über sogenanntes Reverse Factoring, die in einem Prozess auf Basis von Treuhand-Smart-Contracts signifikant eingeschränkt wird. Da in diesem Prozess (ohne Banken) Liquidität im Smart Contract gebunden wird, ist in Zukunft eine Diskussion der rechtlichen Bewertung von in Smart Contracts treuhänderisch verwaltetem Kapital nötig.

Insgesamt zeigt sich anhand der Abläufe sehr deutlich, dass der Fluss von Informationen Voraussetzung für die Digitalisierung des BoL sowie von Akkreditiven bildet. Die Funktionalitäten für Real-time-Tracking sowie manipulationssichere Speicherung der Daten sollten so in jedem DLT-basierten Ökosystem für Dokumente wie das BoL inhärent sein. Dies wird dadurch bestätigt, dass mit TradeLens in der Tat zunächst eine Plattform für den Austausch und die manipulationssichere Speicherung von Informationen über die am Transport beteiligten Dokumente geschaffen worden ist. Es ist davon auszugehen, dass dort und auch bei den momentan im Markt entstehenden Alternativen nach und nach zusätzliche Möglichkeiten, wie die Nutzung eines E-BoL oder eines vollständig digitalisierten Akkreditivs, entstehen.

[386] In der englischsprachigen Literatur: Escrow Smart Contract oder Escrow Contract.
[387] Siehe Abschnitt auch 1.2.1.
[388] Diese ist kein Plattformbetreiber, sodass keine Probleme mit Monopolbildung etc., die letztlich die Argumente für den Verzicht auf Intermediäre liefert, entstehen.
[389] Siehe auch 4.2.5 im allgemeinen technischen Teil.
[390] Auch hier stellt sich wieder die allgemeine Frage, wie eine automatisierte Prüfung durch einen Smart Contract im Disputfall zu behandeln ist, siehe 1.2.3.

7.1.5 Fazit und Handlungsempfehlungen

Die Ursachen dafür, dass die Digitalisierung im internationalen Handel, insbesondere im Zusammenhang mit dem BoL, noch nicht weit fortgeschritten ist, sind vielfältig. Die hohe Komplexität und Diversität im internationalen Handel, verschiedene Rechtsräume und der Mangel an geeigneter, länderübergreifender Infrastruktur sind einige der Gründe, dass sich bisher keine einheitliche, digitale Lösung etablieren konnte. Als Begründung, warum der Logistiksektor im Vergleich zu etwa dem Finanzsektor einen geringen Digitalisierungsgrad besitzt, wird oftmals angeführt, dass dort die Gesetze von mehreren Ländern zusammentreffen Auch die Skepsis gegenüber einem zentralen Intermediär als Vertrauen stiftender Institution ist eher groß in einer Branche, in der traditionell eher wenig Kontrolle stattfindet. Hinzu kommt die Tatsache, dass zentrale Plattformen in der Regel von einem einzigen Betreiber vorangetrieben werden und zu Monopolzuständen führen. Dies verhindert die Adaption einer zentralen Lösung im B2B-Kontext. Die Wettbewerber haben keinen Anreiz, an der Plattform der direkten Konkurrenz teilzunehmen.

Zudem bestehen Ressentiments gegenüber digitalen Lösungen, etwa, weil schlechter nachvollziehbar ist, wer gegebenenfalls vertrauliche Daten einsehen kann und Informationsverlust aufgrund von Programmierfehlern oder Angriffen befürchtet wird. Auch hohe Versicherungskosten wegen unbekannter Programme und Risiken sowie anfangs geringe Nutzenpotenziale bei hohem Investment (Plattformeffekt erst spät spürbar) werden als Hinderungsgründe genannt. Für kleinere Unternehmen ist es zumeist schwierig, da sie am selben Ökosystem wie Großkonzerne teilnehmen müssen, um die Vorteile einer digitalen Lösung zu genießen, gleichzeitig aber trotzdem hohe Investitionen z. B. in die Integration der entsprechenden APIs in ihre Systeme tragen müssen. Bei einer Befragung Anfang der 2000er-Jahre war der meistgenannte Grund, dass die Infrastruktur, der Markt oder die Handelspartner noch nicht für eine solche Lösung bereit seien (51 Prozent), gefolgt von Bedenken hinsichtlich der Gesetzgebung (44 Prozent). Gefahren in ungenügender Sicherheit (25 Prozent), zu hohe Kosten (12 Prozent) oder Vertraulichkeit (10 Prozent) spielen hingegen eher eine untergeordnete Rolle.[391] Im Falle von BOLERO hatten die Unternehmen im Logistikbereich offenbar keinen hinreichenden Anreiz, zugunsten digitaler Lösungen von altbewährten Prozessen abzuweichen.

Wie beschrieben, kann sowohl auf Basis einer zentralen Instanz als auch auf Basis einer DLT-Lösung von technischer Seite ein digitales Äquivalent zum BoL implementiert werden. Lösungen über eine zentral koordinierte Plattform sind bereits seit Langem technisch möglich, haben sich aber nicht durchsetzen können. Die in den letzten Monaten in starkem Maße zunehmenden Bemühungen, DLT-basierte Lösungen am Markt zu etablieren, legen die Deutung nahe, dass die DLT neue, von den beteiligten Akteuren als vielversprechend angesehene Möglichkeiten schaffen kann.

Ein elektronisches System, egal ob DLT-basiert oder nicht, würde zunächst eine diesbezügliche Standardisierung der internationalen Gesetzgebungen erfordern[392]. Eine Zusammenarbeit der zuständigen Stellen muss somit eine erste Handlung in diesem Bereich sein. Wenn eine solche Infrastruktur verfügbar wäre, ist die umfassende und am Markt akzeptierte Verwendung von E-BoL denkbar.

Bei sämtlichen Initiativen sollte dabei jedoch nicht ausschließlich das BoL fokussiert werden. Dieses sollte eher als exemplarisches, wichtiges Dokument angesehen werden. Auch weitere Dokumente, etwa Versicherungspapiere oder Echtheitszertifikate, die in

[391] *Goldby*, Electronic bills of lading and central registries: what is holding back progress?.
[392] Details hierzu finden sich in Kapitel 6.

diesem und ähnlichen Prozessen von Wichtigkeit sind, sollten einbezogen werden. Gesetzesanpassungen oder Klarstellungen müssen gegebenenfalls sowohl hinsichtlich der Gültigkeit elektronischer Signaturen und digitaler Zertifikate als auch hinsichtlich der Zugänglichkeit und Beweiskraft elektronischer Transaktionen vor Gericht sowie der Unterscheidung von verhandelbaren Papieren (Konnossements) und nicht-verhandelbaren Papieren stattfinden. Zudem benötigt die Frage der Verantwortlichkeit im Falle von Programmier- bzw. Systemfehlern und daraus resultierenden Unklarheiten über Eigentumsverhältnisse an dem elektronischen BoL langfristig einer Klärung.

Anhand verschiedener Beispiele hat sich jedoch auch gezeigt, dass Bemühungen von Regulatoren und Gesetzgebern, elektronische Dokumente zu etablieren, in der Wirtschaft bisher auf wenig Resonanz stoßen. Daher ist es nachvollziehbar, dass der Gesetzgeber sich eher in einer abwartenden Haltung befindet, da die Gesetzgebung traditionell eher reaktiv als proaktiv agiert. Dennoch sollte hier die Politik stets die aktuellen Vorgänge verfolgen, damit etwa deutsche Außenhandelsinteressen nicht durch das Verpassen neuester Trends in technischen Entwicklungen gefährdet sind.

7.2 Rechtlicher Teil

Nach der ökonomisch-technischen Analyse zum Potenzial der Digitalisierung des Bill of Lading und den darauf aufbauenden Erwägungen zu dessen Realisierung mittels DLT gilt es nun den Fokus auf die Einordnung dieses im internationalen Warenverkehr relevanten Frachtpapiers in das deutsche Seehandelsrecht auszurichten. Hieran anschließend wird die Frage des Datenschutzes im Kontext der digitalen Frachtpapiere adressiert.

7.2.1 Traditionspapiere

Das Bill of Lading entspricht im deutschen HGB dem Konnossement (§ 515 HGB). Dieses verbrieft in der Seeschifffahrt einen Herausgabeanspruch auf die verschifften Güter, d. h. bewegliche Sachen. Zugleich repräsentiert es die Ware, sodass über diese allein durch Übergabe des Papiers verfügt werden kann (sogenannte Traditionswirkung[393]). Neben dem Konnossement kennt das deutsche HGB zusätzlich den Ladeschein (§ 443 HGB, insbesondere in der Binnenschifffahrt[394]) und den Lagerschein (§ 475c HGB), die ebenfalls wie das Konnossement Ware repräsentieren und an deren Stelle handelbar sind, weshalb alle drei Wertpapiere auch Traditionspapiere genannt werden. Gemein ist den Traditionspapieren, dass der Gesetzgeber sie vielfach normativ gleich ausgestaltet. Anschaulich wird ebendies anhand der im Grunde wortlautidentischen und für DLT-Anwendungen relevanten digitalen Öffnungsklauseln in den §§ 443 Abs. 3, 475c Abs. 4, 516 Abs. 2, 3 HGB. Diese stellen den vorgenannten bisher papiergestützten Traditionspapieren ihr jeweiliges funktionelles digitales Äquivalent gleich.[395] Zulässig ist danach schon heute der Einsatz digitaler Traditionspapiere auf Basis von DLT, wenn sich über diese alle Funktio-

[393] § 448 HGB für den Ladeschein; § 475g HGB für den Lagerschein; § 524 HGB für das Konnossement; die sachenrechtliche Behandlung ist streitig, siehe hierzu Baumbach/Hopt/*Merkt*, § 448 Rn 2.

[394] Rabe/Bahnsen/*Rabe/Bahnsen,* Vor 481 Rn. 121.

[395] Weitere digitale Öffnungsklauseln finden sich auch für den Frachtbrief in § 408 Abs. 2 HGB und für den Seefrachtbrief in § 526 Abs. 4 HGB. Im Unterschied zu den Traditionspapieren sind sie keine Wertpapiere, sondern (wenn von beiden Parten unterzeichnet) eine bloße Beweisurkunde über den Abschluss und den Inhalt desFrachtvertrags sowie die Übernahme des Guts durch den Frachtführer, Baumbach/Hopt/*Merkt*, § 409 Rn 1.

nen der papiergestützten Traditionspapiere abbilden lassen. Letzteres wird in der Literatur unter einschränkendem Hinweis auf die nachfolgend noch zu schildernden Herausforderungen im Ergebnis positiv beurteilt.[396]

7.2.1.1 Internationaler Anwendungsbereich des dt. Seehandelsrechts

Deutschland hat das Internationale Übereinkommen zur Vereinheitlichung von Regeln über Konnossemente (Haager Regeln) ratifiziert, nicht aber daran anknüpfende spätere Zusatzprotokolle wie etwa die Hague-Visby-Regeln oder die Hamburger Regeln.[397] Auch die späteren Rotterdam Regeln, die erstmals Regeln über „elektronische Beförderungsaufzeichnungen" beinhalten, wurden bislang nicht von Deutschland unterzeichnet.[398] Im Übrigen wurden die Rotterdam Regeln aber auch noch nicht von genügend anderen der bisherigen Unterzeichnerstaaten ratifiziert, sodass sie ohnehin völkerrechtlich bislang noch nicht in Kraft getreten sind.[399] Sie waren dem deutschen Gesetzgeber aber Vorbild für die Aktualisierung des deutschen Seehandelsrechts.[400] Als internationales Recht gelten die Haager Regeln, soweit sie Anwendung finden, vor nationalem Recht, d. h. den §§ 476 ff. HGB.[401] Primär erfolgen im Seehandel Vereinbarungen über das anzuwendende Recht bzw. eine Bestimmung des Gerichtsstands.[402] Im Kollisionsfall, d. h. im Falle einer unterbliebenen oder unwirksamen Vereinbarung, kann deutsches Seehandelsrecht über Art. 5 Abs. 1 Rom I-VO Anwendung finden.

7.2.1.2 Akkreditivgeschäft im Außenhandel

Die Vorteile von DLT-basierten Traditionspapieren werden, wie bereits voranstehend im ökonomisch technischen Teil[403] für BoL im internationalen Kontext veranschaulicht, anhand des Akkreditivgeschäfts im Außenhandel deutlich.[404] In diesem Unterpunkt soll darauf aufbauend nur noch abschließend das Akkreditivgeschäft unter Zugrundelegung des deutschen Rechts vervollständigt werden, bevor die Abbildbarkeit von Traditionspapieren auf Basis von DLT eingehender beleuchtet wird.

Angenommen ein deutscher Importeur (Käufer) kauft Waren eines asiatischen Exporteurs (Verkäufer), so liegt es im Interesse des Exporteurs, die Ware nicht ohne einen Nachweis der Zahlung dem Verfrachter zu übergeben, und im Interesse des Importeurs, nicht ohne Nachweis der Übergabe an den Verfrachter bezahlen zu müssen. Interessengerechte Abhilfe schafft hier wie seitens der Ökonomen bereits unter 7.1.1 geschildert, eine Akkreditivvereinbarung zwischen den Handelsparteien. Nach dieser verpflichtet sich der Käufer die Ware durch Stellung eines Akkreditivs bei einer Bank zu bezahlen.[405] Hierfür erteilt der Käufer seiner Bank einen Akkreditivauftrag (Geschäftsbesorgungsvertrag, § 675 BGB), wonach sich diese verpflichtet, gegenüber dem Verkäufer ein abstraktes Schuldversprechen im Sinne von § 780 BGB zu begründen (ein sogenanntes Akkreditiv, näher ausgestaltet in den Einheitlichen Richtlinien und Gebräuchen für Dokumenten-

[396] *Saive,* TranspR 2018, 234; *Saive,* RdTW 2018, 85.
[397] MüKoBGB/*Martiny*, Rom I-VO Art. 5 Rn. 97.
[398] Siehe Art. 1 und 8 der Rotterdam Regeln (Übereinkommen der Vereinten Nationen über Verträge über die internationale Beförderung von Gütern ganz oder teilweise auf See).
[399] Zum aktuellen Status der Unterzeichnungen und Ratifikationen siehe: http://www.uncitral.org/uncitral/en/uncitral_texts/transport_goods/rotterdam_status.html.
[400] BT-Drs. 17/10309 S. 41f.
[401] *Wieske*, Transportrecht. S. 313.
[402] Rabe/Bahnsen/*Rabe/Bahnsen,* Vor § 481 Rn. 125, 131.
[403] Siehe Abschnitt 7.1.4.
[404] *Saive,* TranspR 2018, 234 (236).
[405] Baumbach/Hopt/*Hopt*, BankGesch K/1.

Akkreditive der Internationalen Handelskammer, kurz: ERA 600, die nach h. M. AGB[406] darstellen).[407] Der Verkäufer erlangt dadurch einen unmittelbaren und selbstständigen Anspruch gegen die eröffnende Bank auf Zahlung gegen Aushändigung der Warendokumente. Letztere prüft die Akkreditivbank im Rahmen des Akkreditivauftrags mit dem Käufer vor der Anweisung der Zahlung an ihre Kooperationsbank im Ausland/Bank des Verkäufers auf Richtigkeit, insbesondere hinsichtlich Art und Menge der Ware, Verpackung, Versandfristen und Qualitätszertifizierungen. Nur wenn alle Warendokumente den Akkreditivbedingungen auf das Genaueste (Grundsatz der Dokumentenstrenge) entsprechen, wird die Zahlung ausgeführt. Für den Verkäufer bedeutet das Akkreditivgeschäft, dass er einen eigenständigen und von den Interessen des Käufers unabhängigen Zahlungsanspruch gegen die Akkreditivbank erlangt. Für den Käufer wiederum bedeutet das Akkreditivgeschäft, dass er alle Dokumente seitens des Exporteurs erhält, die er benötigt, um die Ware gemäß § 521 Abs. 1 HGB als durch das Konnossement legitimierter Besitzer Zug um Zug gegen Rückgabe des Konnossements gemäß § 521 Abs. 2 HGB vom Verfrachter heraus zu verlangen. In der Praxis können die Dokumentenprüfung und der Versand ebendieser länger dauern als der Transport der Ware (siehe hierzu bereits ausführlich 7.1.2).[408] Um diesem Umstand entgegenzuwirken, bieten sich DLT-basierte Traditionspapiere an, die Datenverwaltung und -auswertung in der Logistik automatisieren könnten.

7.2.1.3 DLT-basierte Traditionspapiere

DLT-basierte Traditionspapiere sind nach den §§ 443 Abs. 3, 475c Abs. 4, 516 Abs. 2 HGB lediglich dann ein Äquivalent zum papiergebundenen Original, wenn sich sämtliche Funktionen der papiergestützten Traditionspapiere digital abbilden lassen und damit Gleichwertigkeit zwischen analogem und digitalem Traditionspapier herrscht. Neben der Begebung des Traditionspapiers sind daher insbesondere auch die Beweis-, Sperr-, Traditions- und Legitimationsfunktion abzubilden.[409] Im Folgenden wird vorrangig beispielhaft auf das Konnossement eingegangen, die Anforderungen gelten aber auch sowohl für den Ladeschein als auch für den Lagerschein.

7.2.1.3.1 Begebung

Traditionspapiere erfordern in der analogen Welt einen Begebungsvertrag[410], durch den das verbriefte Vermögensrecht auf den Inhaber einer ihm zusätzlich zu übereignenden Urkunde übertragen wird. Diese jeweiligen Urkunden müssen die in den §§ 443 Abs. 1 i. V. m. 408 Abs. 1, 475c Abs. 1 - 3 und 515 HGB genannten Informationen abbilden. Gleiches gilt gemäß §§ 443 Abs. 3, 475c Abs. 4, 516 Abs. 2 HGB auch für das jeweilige digitale Äquivalent. In Bezug auf DLT bieten sich Asset Backed Token als Abbild an.[411]

Der Begriff des Tokens steht im Kontext der DLT für einen „Eintrag in einer Datenbank, der ausschließlich, einzigartig und nicht vervielfältigbar ist."[412] Ein Token als solches ist dabei letztlich lediglich ein Smart Contract, der neben weiteren Attributen auch ein Feld „Inhaber" aufweist, das zu jedem Zeitpunkt nur mithilfe des privaten Schlüssels des ak-

[406] Baumbach/Hopt/*Hopt,* ERA vor Art. 1 Rn. 4.
[407] Baumbach/Hopt/*Hopt*, BankGesch K/1.
[408] *Saive,* TranspR 2018, 234 (236).
[409] BT-Drs. 17/10309 S. 93.
[410] Vertrag zwischen Verfrachter und Ablader zugunsten des legitimierten Konnossementinhabers (§ 328 BGB), *von Bernstorff,* RIW 2001, 504 (508).
[411] *Saive,* TranspR 2018, 234 (237).
[412] *Kaulartz/Matzke,* NJW 2018, 3278.

tuellen Berechtigten verändert werden kann. In Bezug auf die Warenlogistik soll ein Token das Eigentum an einem bestimmten real existierenden Asset bzw. im Falle der Traditionspapiere einen Anspruch auf ein bestimmtes real existierendes Asset widerspiegeln und wird daher als Asset Backed Token bezeichnet.[413]

Um einen solchen Asset Backed Token zu erstellen, muss der Lagerhalter, der Frachtführer oder der Verfrachter die erforderlichen Informationen über eine Schnittstelle zu einer DLT-Plattform (API) in einem Token digital zusammenführen. Eingespeist in eine DLT-Plattform ist dieser als Smart Contract, wenn er von allen Nodes validiert und gespeichert wurde.[414] Einmal in eine DLT-Plattform aufgenommen, sind die enthaltenen Informationen irreversibel mit dem Token verbunden. Aufgrund der überschaubaren Anzahl möglicher Nodes, wie etwa Ladungsbeteiligter und Behörden, dürfte sich als Netzwerkstruktur – wie auch im Ökonomischen Teil unter 7.1.4 aufgezeigt – eine private permissioned Blockchain (DLT-Plattform) anbieten.[415]

7.2.1.3.2 Beweisfunktion

Die Beweisfunktion des Konnossements erstreckt sich darauf, dass der Verfrachter die Waren so übernommen hat, wie sie im Konnossement gemäß §§ 515 Abs. 1 Nr. 7, 8, 517 Abs. 1 S. 1 HGB beschrieben sind. Indem alle erforderlichen Informationen via Software im Asset Backed Token digital zusammengeführt werden, kann dieser Funktion Rechnung getragen werden.

7.2.1.3.3 Legitimationsfunktion

In der analogen Welt ist aus dem Konnossement der Eigentümer des Papiers berechtigt, die im Konnossement verbrieften seefrachtvertraglichen Ansprüche geltend zu machen.[416] Gemäß § 519 Abs. 1 S. 2 HGB wird seine Berechtigung vermutet, wenn er das ihn formal legitimierende Papier in Besitz hat. Die Legitimation ist abhängig von der Konnossementart. Zu unterscheiden sind insoweit Inhaber-, Order- und Rektakonnossement.[417] Entsprechend seiner Betitelung ist bei Erstgenanntem gemäß § 519 S. 2 Nr. 1 HGB jeder Besitzer ohne (namentliche) Erwähnung in dem Papier legitimiert, weshalb es mangels Rückverfolgbarkeit der Inhaberhistorie ohne Praxisrelevanz ist.[418] Beim Zweitgenannten ist gemäß § 519 S. 2 Nr. 2 HGB der Besitzer legitimiert, der als Empfänger benannt (mitunter genügt „an Order des Abladers“) oder auf dessen Name eine ununterbrochene Reihe von Indossamenten (Übertragungsvermerke) hinführt.[419] Bei Drittgenanntem ist gemäß § 519 S. 2 Nr. 3 HGB abschließend nur der Besitzer legitimiert, dessen Name als Empfänger auf dem Papier steht. Die Legitimation des jeweiligen Berechtigten wäre im Falle des Einsatzes einer DLT-Applikation für den Verfrachter über einer Benutzerschnittstelle, welche die Zuordnung des Asset Backed Token ersichtlich und nachvollziehbar macht, einsehbar (abhängig von der Ausgestaltung der DLT-Applikation nur über Berechtigte). Im Vergleich zum papierbasierten Konnossement würde dies zugleich den Verfrachter davon entlasten, die Erscheinung des Konnossements jedenfalls auf Anzeichen für eine Fälschung hin prüfen zu müssen.[420]

[413] *Kaulartz/Matzke,* NJW 2018, 3278 (3280).
[414] *Saive,* TranspR 2018, 234 (237).
[415] *Saive,* RdTW 2018, 85 (88).
[416] MüKoHGB/*Herber*, § 519 Rn. 3.
[417] Rabe/Bahnsen/*Rabe/Bahnsen,* § 519 Vor 481 Rn. 119.
[418] MüKoHGB/*Herber*, § 519 Rn. 5.
[419] Rabe/Bahnsen/*Rabe/Bahnsen,* § 519 Vor 481 Rn. 119.
[420] MüKoHGB/*Herber*, § 519 Rn. 9.

7.2.1.3.4 Sperrfunktion

Aus § 519 Abs. 1 S. 1 HGB folgt der Grundsatz, dass neben den im Konnossement verbrieften Ansprüchen nicht gleichzeitig auch Ansprüche aus dem Frachtvertrag geltend gemacht werden können, solange diese durch das Konnossement verbrieft sind.[421] Insoweit sperrt das Konnossement Ansprüche aus dem Frachtvertrag, denn das Konnossement überlagert den Frachtvertrag, der nicht notwendig mit den Rechtsverhältnissen aus dem Konnossement identisch ist.[422] Primär sind im Konnossement die Ansprüche gegen den Verfrachter auf Beförderung zum Bestimmungsort und auf Auslieferung an den Konnossementberechtigten verbrieft, §§ 514 Abs. 1 S. 2, 521 Abs. 1 S. 1 HGB.[423] Sekundär verbrieft es auch Ansprüche auf Schadensersatz wegen Verlusts oder Beschädigung des Guts.[424] Die Sperre des Frachtvertrags durch das Konnossement endet bspw., wenn der Berechtigte die Annahme der Güter ablehnt.[425] Dann darf der Befrachter die Rechte aus dem Frachtvertrag wieder geltend machen.[426] Indem alle Nodes die Existenz des Konnossements über eine DLT-Applikation einsehen können, wissen sie im Übrigen auch um die Sperrwirkung des Konnossements. Sollte in Fortsetzung des vorgenannten Beispiels der Berechtigte die Annahme verweigern, wäre dies etwa durch den Verfrachter auf der DLT-Plattform zu hinterlegen, um die Sperrwirkung insoweit aufzuheben, womit auch diese Funktion abbildbar wäre.

7.2.1.3.5 Traditionsfunktion

Der Eigentumsübergang[427] an der Ladung im Falle der Weiterveräußerung während des Seetransports würde sich als Übertragung eines Tokens an den Importeur/Käufer im Rahmen einer Transaktion auf der DLT-Plattform vollziehen, sobald sie von allen berechtigten Nodes validiert und im verteilten Computernetzwerk festgehalten wäre.[428] Hiernach wären die neuen Eigentumsverhältnisse wie bereits beschrieben transparent.

7.2.1.3.6 Signatur

Die im Grunde wortlautidentischen digitalen Öffnungsklauseln der §§ 443 Abs. 3, 475c Abs. 4, 516 Abs. 2, 3 HGB enthalten alle den Passus „Authentizität und Integrität der Aufzeichnung". Der Begriff der Aufzeichnung resultiert dabei aus der Übersetzung der Rotterdam-Regeln im Kontext des § 516 Abs. 2 HGB und wurde im Sinne der Einheitlichkeit auch in sämtliche weiteren Öffnungsklauseln übernommen.[429] Hierdurch soll verdeutlicht werden, dass es sich gerade nicht um eine Privaturkunde im Sinne des § 416 ZPO handelt.[430] Durch das Erfordernis der dauerhaften Gewährleistung von Authentizität und Integrität der Aufzeichnung wird zudem ausdrücklich von dem Erfordernis abgesehen, dass die Aufzeichnung der elektronischen Form nach § 126a BGB genügen muss.

[421] *Ramming,* RdTW 2018, 45 (50).
[422] MüKoHGB/*Herber*, § 519 Rn. 11.
[423] Rabe/Bahnsen/*Rabe*, § 519 Rn. 7.
[424] Rabe/Bahnsen/*Rabe*, § 519 Rn. 7.
[425] MüKoHGB/*Herber*, § 519 Rn. 17.
[426] MüKoHGB/*Herber*, § 519 Rn. 17.
[427] Zur streitigen sachenrechtlichen Behandlung siehe Baumbach/Hopt/*Merkt*, § 448 Rn 2.
[428] *Saive,* TranspR 2018, 234 (237).
[429] BT-Drs. 17/10309 S. 93.
[430] BT-Drs. 17/10309 S. 52.

Dadurch wird dem Umstand Rechnung getragen, dass das Prozedere rund um die qualifizierte elektronische Signatur nach dem Signaturgesetz (a. F.) sehr aufwendig sowie teuer ist und im Übrigen die jetzige Formulierung mehr Flexibilität gewährt.[431]

7.2.1.3.7 Rückabwicklung

Eine Rückabwicklung von DLT-basierten Transaktionen ist grundsätzlich möglich. Siehe hierzu insbesondere die Ausführungen zu Smart Contracts im Allgemeinen (6.1.1). In Bezug auf das Konnossement würde sie sich dergestalt vollziehen, dass nach einer Rücktransaktion wieder ausschließlich der ursprüngliche Inhaber mit seinem privaten Schlüssel auf den Asset Backed Token zugreifen kann. Der Fortbestand der Transaktionshistorie auf einer DLT-Plattform ist, wie im Grundlagenteil zu Smart Contracts ausgeführt[432], unschädlich.[433] Ein Grund für ein Löschungserfordernis der Transaktionshistorie kann sich im Bereich der Traditionspapiere wohl nur aus dem übereinstimmenden Parteiwillen ergeben, wenn etwa kritische Güter verfrachtet werden. Letzteres steht der grundsätzlichen Äquivalenz DLT-basierter und papiergestützter Traditionspapiere aber nicht entgegen.

7.2.1.3.8 Numerus clausus

Der Kreis der Wertpapiere ist in Deutschland durch den Numerus clausus der Wertpapiere begrenzt, was bis zur Einführung der eingangs genannten Öffnungsklauseln elektronische Traditionspapiere verhinderte. Durch Letztere wollte der Gesetzgeber dieses „Hindernis" beseitigen.[434] Eine einschränkende Wertung ergibt sich auch nicht aus der Ermächtigungsgrundlage nach § 516 Abs. 3 HGB, die sich wortgleich auch in §§ 443 Abs. 3 und 475c Abs. 4 HGB findet. Denn die Bundesregierung führte im Gesetzentwurf hierzu aus, dass die Entscheidung „inwieweit von der Ermächtigung Gebrauch gemacht wird, […] davon abhängen [sollte], ob sich geeignete Formen und Verfahren in der Praxis abzeichnen."[435] Entsprechend ist die Ermächtigungsgrundlage nur darauf ausgerichtet, die Standardisierung der Einzelheiten der Ausstellung, Vorlage, Rückgabe und Übertragung eines elektronischen Konnossements sowie die Einzelheiten des Verfahrens einer nachträglichen Eintragung in ein elektronisches Konnossement in der Praxis sicherstellen zu können.[436]

7.2.1.3.8.1 Vorlage

Der Regelungsgegenstand „Vorlage" in der Ermächtigungsgrundlage des § 516 Abs. 3 HGB impliziert zudem trotz des Wortlauts nicht zwingend eine Urkunde. Letzteres erscheint auf den ersten Blick im Kontext des elektronischen Konnossements, das gerade dem Papiererfordernis abhelfen soll, auch widersinnig. Aufhorchen lässt in diesem Kontext aber das Aktienrecht als spezielles Wertpapierrecht. Nach § 10 Abs. 5 AktG kann zwar der Anspruch des Aktionärs auf Verbriefung seines Anteils in der Satzung eingeschränkt oder ganz ausgeschlossen werden. Neben diesem Ausschluss des individuellen Verbriefungsanspruchs des Aktionärs bleibt die AG jedoch verpflichtet, eine Globalurkunde (§ 9a Abs. 1 S. 1 DepotG) zu begeben und diese zu hinterlegen.[437] Dessen ungeachtet umfasst die weit gefasste Begriffsbestimmung des Wertpapiers in § 2 Abs. 1

[431] BT-Drs. 17/10309 S. 93.
[432] Siehe 6.1.1.
[433] Zu Fragen des Datenschutzes in diesem Zusammenhang siehe 7.2.1.4.
[434] BT-Drs. 17/10309 S. 93.
[435] BT-Drs. 17/10309 S. 93; a.A. Rabe/Bahnsen/*Rabe*, § 516 Rn. 5.
[436] BT-Drs. 17/10309 S. 93.
[437] Henssler/Strohn/*Lange*, AktG § 10 Rn. 15.

WpHG Wertpapiere als solche auch dann, wenn keine Urkunde über sie ausgestellt wurde. Solange ein Wertpapier und damit letztlich auch ein Traditionspapier insoweit die erforderlichen Charakteristika aufweist, ist es auch in digitaler Form, d. h. als Token, gültig.[438]

7.2.1.3.8.2 Nachträgliche Eintragung

Im Gesetzentwurf zum heutigen § 516 HGB benennt die Bundesregierung im Kontext der Verordnungsermächtigung hinsichtlich nachträglicher Eintragungen in ein elektronisches Konnossement ausdrücklich Fälle nach § 517 Abs. 2 HGB, in denen der Verfrachter noch Vorbehalte in das elektronische Konnossement eintragen will.[439] § 517 Abs. 2 HGB kann im Hinblick auf DLT durch einen Smart Contract Rechnung getragen werden, indem dieser dem Verfrachter die Möglichkeit einräumt zusätzliche Informationen nachträglich hinzuzufügen. Für den Betrachter ergibt sich dann das gesamte Traditionspapier auf der DLT-Plattform als eine Kombination aus ursprünglicher Eintragung und späteren Ergänzungen. Ein Eingriff in die DLT-Plattform als solche ist folglich nicht erforderlich.

7.2.1.4 Datenschutz bei digitalen Traditionspapieren mittels DLT

Soll ein Token als Äquivalent zu einem Traditionspapier eingesetzt werden und in der DLT zwischen den Vertragsparteien des Handelsgeschäfts transferiert werden, so muss dabei der Schutz der Daten der betroffenen natürlichen Personen gewährleistet sein.

Als betroffene Personen kommen, wie bei jeder Anwendung, die Nutzer des Systems und mögliche Dritte in Betracht. Als unmittelbare Nutzer des Systems werden Exporteur, Importeur und Spediteur tätig. Diese interagieren über DLT mit dem Smart Contract im Rahmen der Übermittlungsprozesse des Tokens. Dokumentiert werden diese Interaktionen in der DLT. Soweit es sich bei Exporteur, Importeur oder Spediteur um eine natürliche Person handelt, sind diese Datenverarbeitungen datenschutzrechtlich relevant.[440] Handelt es sich dagegen um Unternehmen, bei denen allein durch eine Aktivität der Nutzerkennung Rückschlüsse auf hinter dem Unternehmen stehende natürliche Personen ausgeschlossen sind, sind die Transaktionen durch die Nutzer des Systems nicht datenschutzrechtlich relevant.[441] Es verbleibt jedoch auch hier die Möglichkeit einer Identifizierung von Personen durch den Inhalt des Traditionspapiers. Dieser kann gegebenenfalls auch Daten über Dritte umfassen, die über den Status des Versands informiert werden möchten.[442] Auch ist von vornherein nicht ausgeschlossen, dass durch die Beschreibung der Waren im Papier Rückschlüsse auf damit in Verbindung stehende dritte Personen möglich werden.

Die Abbildung von Traditionspapieren auf einer DLT-Plattform erfordert demgemäß eine entsprechende Anpassung der Architektur. Es muss dabei danach unterschieden werden, ob anhand der Kenntnis der Nutzer der Plattform (Exporteur, Importeur, Spediteur) Informationen über die hinter dem Unternehmen stehenden Personen bekannt werden können.

[438] *Parhofer/Klöhn/Resas,* ZBB 2018, 89 (102).
[439] BT-Drs. 17/10309 S. 93.
[440] Siehe hierzu bereits die Ausführungen im allgemeinen Teil 6.2.2.2.1.1.
[441] Siehe hierzu bereits die Ausführungen im allgemeinen Teil 6.2.2.2.1.1.1.
[442] Verweis auf Ausführungen zum üblichen Inhalt der klassischen Traditionspapiere.

7.2.1.4.1 Keine Information über die hinter den Unternehmen stehenden natürlichen Personen

Es besteht die Möglichkeit, dass natürliche Personen hinter den beteiligten nutzenden Unternehmen nicht identifizierbar sind. In diesem Fall ist die Verarbeitung von Informationen über die beteiligten Unternehmen datenschutzrechtlich nicht relevant. Es muss allerdings auch diesbezüglich sichergestellt werden, dass das digitale Äquivalent zum Traditionspapier selbst keine personenbezogenen Informationen über Dritte beinhaltet. Eine Verarbeitung dieser Daten mittels DLT kann aber durch eine Off-Chain-Speicherung verhindert werden. Die im Traditionspapier hinterlegten Informationen werden nicht im Klartext in der DLT hinterlegt, sondern verbleiben lokal, signiert und verschlüsselt beim jeweiligen Aussteller. Dieser kann den anderen an der Transaktion Beteiligten Zugriff auf das Dokument gewähren. Die Möglichkeit zur Einsicht des Dokuments geht dabei mit der Übergabe des Schlüssels für die verschlüsselten Informationen einher. Der Token auf der DLT-Plattform enthält lediglich einen Hashwert dieser Informationen.[443] Auf diese Weise wird sichergestellt, dass die Informationen nachträglich nicht verändert wurden. Der Hashwert stellt für sich kein personenbezogenes Datum dar, da aufgrund der Eigenarten der Hashfunktion nicht auf den Input geschlossen werden kann. Auf diese Weise ist eine Identifizierung von natürlichen Personen durch die On-Chain-Daten ausgeschlossen.[444]

Falls sichergestellt werden kann, dass nur Unternehmen teilnehmen, bei denen keine Informationen über die hinter dem Unternehmen stehenden natürlichen Personen erlangt werden können, ist technisch sicherzustellen, dass der Inhalt des Traditionspapiers off-Chain gespeichert und lediglich über Hashwerte mit dem DLT-Layer verbunden ist. Auf diese Weise kann eine datenschutzkonforme Umsetzung gelingen. Zu beachten ist jedoch, dass der Ausschluss von Informationen über hinter dem Unternehmen stehende natürliche Personen keinesfalls selbstverständlich ist. Soll die Plattform grundsätzlich offen gestaltet sein und auch Importeuren, Exporteuren und Spediteuren offenstehen, die als kleine Unternehmen agieren und bei denen die Wahrscheinlichkeit der Gewinnung von Informationen über natürliche Personen groß ist,[445] kann diese Lösung nicht genügen. In diesem Fall kann bereits die Interaktion einer Nutzerkennung in Verbindung mit der Übertragung des Traditionspapiers auf dem DLT-Layer einen datenschutzrechtlich relevanten Vorgang darstellen. Es müssen dann alternative Lösungsmöglichkeiten gefunden werden.

7.2.1.4.2 Informationen über die hinter den Unternehmen stehenden natürlichen Personen möglich

Handelt es sich bei Exporteur, Importeur oder Spediteur um natürliche Personen oder um Unternehmen, bei denen dahinterstehende natürliche Personen identifiziert werden können, so stellen sich bei der Interaktion dieser Beteiligten mittels DLT die Herausforderungen, welche bereits im Grundlagenteil diskutiert worden sind. Auch in diesem Fall hat eine Off-Chain-Speicherung mit Hashwert-Verknüpfung zu erfolgen. Zusätzlich sind jedoch Maßnahmen vorzunehmen, die auch der Problematik des Personenbezugs der Nutzerkennungen selbst begegnen.

[443] Siehe zum Begriff des Hashwerts bereits unter 4.1.4.
[444] Siehe zu diesem Lösungsansatz bereits unter 6.2.3.4.2.2.1.2.
[445] Siehe hierzu bereits unter 6.2.2.2.1.1.1.

Eine „offene Lösung“[446] würde erfordern, dass alle am System Beteiligten an allen Informationen ein berechtigtes Interesse haben. An der Übertragung eines einzelnen Traditionspapiers haben jedoch nur die an den jeweiligen Handelsgeschäften involvierten Personen ein berechtigtes Interesse. Eine Einsicht aller Aktivitäten durch alle am System Beteiligten ist deswegen nicht datenschutzkonform. Die „offene Lösung“ ist dementsprechend hier nicht umsetzbar.
Möglich erscheint aber dagegen grundsätzlich eine „zentrale Lösung“[447]. Bei dieser müsste durch eine Zentralstelle eine permissioned Blockchain betrieben werden. Über ein Rechte- und Rollen-System kann von der Zentralstelle gesteuert werden, welche Informationen für die einzelnen Teilnehmer sichtbar sind. Die Zentralstelle wäre dann datenschutzrechtlich Verantwortliche für die On-Chain-Verarbeitungen. Als Rechtsgrundlage für die Verarbeitung kommt nun ein zwischen den Teilnehmern und der Zentralstelle geschlossener Vertrag in Betracht.[448] Die Zentralstelle muss über geeignete Löschkonzepte verfügen. Hier kommen eine „Redactable Blockchain“[449], bei der nachträglich durch die Zentralstelle Änderungen eingebracht werden können, oder Forks[450], bei denen die Nodes dazu verpflichtet werden, ungewünschte Daten aus der dezentralen Datenbank zu löschen, in Betracht.

Ist eine „zentrale Lösung“ nicht möglich oder nicht gewünscht, kann auch eine „Anonymisierungslösung“[451] gewählt werden. Dabei wird eine Saldierung von Transaktionen nicht möglich sein,[452] da jede Übertragung des Traditionspapiers nachvollzogen werden muss. In Betracht kommen daher nur technische Anonymisierungslösungen, wie bspw. Zero-Knowledge-Proofs[453] oder Einsatz von Stealth-Adressen in Kombination mit Ring-Signaturen[454]. Bei einer Anonymisierung finden on-Chain keine datenschutzrechtlich relevanten Datenverarbeitungen mehr statt. Folglich ist hierfür auch keine Rechtsgrundlage erforderlich. Eine Löschung ist ebenfalls nicht nötig.

7.2.2 Fazit und Handlungsempfehlung

Die digitalen Öffnungsklauseln des HGB im Bereich der Traditionspapiere ermöglichen durch das Äquivalenzerfordernis schon heute den Einsatz von DLT-basierten Traditionspapieren. Diese Rechtssetzungstechnik schafft daher Flexibilität, weshalb sie der Gesetzgeber möglicherweise auch in anderen Bereichen fruchtbar machen könnte.

Die datenschutzrechtlichen Vorgaben erfordern eine Differenzierung nach dem Kreis der potenziellen Teilnehmer. Für den Fall, dass es sich bei den Teilnehmern (Exporteuren, Importeuren und Spediteuren) ausschließlich um Unternehmen handelt, bei denen Rückschlüsse auf die hinter den Unternehmen stehenden natürlichen Personen nicht möglich sind, genügt es, auf die Speicherung personenbezogener Daten auf dem DLT-Layer zu verzichten. Die Informationen sind off-Chain zu speichern und mittels eines Hashwerts auf der DLT-Plattform zu verlinken. Eine solche Lösung erfordert jedoch eine vorherige Prüfung der Teilnehmer darauf, ob diese die obenstehenden Herausforderungen erfüllen. Insbesondere kleinere Unternehmen könnten dann wohl nicht am System teilnehmen.

[446] Siehe zur „offenen Lösung“ bereits unter 6.2.3.4.2.1.
[447] Siehe zur „zentralen Lösung“ bereits die Ausführungen unter 6.2.3.4.2.1.
[448] Siehe zu den Rechtsgrundlagen bei Wahl der zentralen Lösung bereits unter 6.2.4.2.2.
[449] Siehe zur Redactable Blockchain bereits unter 6.2.5.2.1.
[450] Siehe zu Forks bereits unter 6.2.5.2.2 und 4.4.3.
[451] Siehe zur „Anonymisierungslösung“ bereits unter 6.2.3.4.2.2.
[452] Zur Saldierung bereits allgemein unter 6.2.3.4.2.2.2.2.
[453] Zu Zero-Knowledge-Proofs siehe bereits unter 6.2.3.4.2.2.2.3 und 5.1.3.
[454] Zu Stealth-Adressen in Kombination mit Ring-Signaturen bereits unter 6.2.3.4.2.2.2.4.

Sollen die DLT-gestützten Traditionspapiere zumindest auch von und an Exporteure, Importeure und Spediteure übertragen werden können, bei denen es sich um natürliche Personen handelt oder die Kenntnis des tragenden Unternehmens auch Informationen über natürliche Personen offenbart, die hinter dem Unternehmen stehen, so ist eine offene DLT-Plattform ohne Anpassung der Architektur aus datenschutzrechtlicher Perspektive nicht denkbar. Die erforderliche Anpassung kann durch die Schaffung einer verantwortlichen Zentralstelle („zentrale Lösung") oder durch die vollständige Anonymisierung der Nutzerkennungen („Anonymisierungslösung") erfolgen.

Digitale Öffnungsklauseln und Datenschutz

Die digitalen Öffnungsklauseln im Handelsgesetzbuch ermöglichen durch das Äquivalenzerfordernis zwischen papiergebundenem Original und DLT-basiertem Abbild schon heute insbesondere im Seehandel (§§ 476 ff. HGB) den Einsatz von DLT-basierten Traditionspapieren. Aufgrund der Flexibilität dieser Regelungstechnik kann der Gesetzgeber sie möglicherweise auch in anderen Bereichen fruchtbar machen. Datenschutzrechtliche Vorgaben sind im Kontext der digitalen Frachtpapiere abhängig vom Kreis der potenziellen Teilnehmer zu beachten.

8 Elektrisches Laden

8.1 Ökonomisch-technischer Teil

8.1.1 Definition und Beschreibung des Anwendungsfalls

Die Elektromobilität bzw. die elektrifizierte Mobilität haben in den letzten Jahren eine rasante technische Entwicklung durchlaufen. Der Fahrzeugbestand und die Anzahl der Neuzulassungen bleiben dennoch hinter den ursprünglichen Erwartungen zurück. Mit ca. 291 000 E-Fahrzeugen (inklusive Hybride) zum 01.01.2018[455] steht Deutschland vor der Herausforderung, die Verkehrswende durch Förderung von Elektromobilität weiter zu beschleunigen. Dass die Erwartungen an die Verbreitung der Elektromobilität mittelfristig wieder erreicht werden, scheint möglich. Unabdingbare Voraussetzung dafür ist u. a. die Bereitstellung einer öffentlich zugänglichen Ladeinfrastruktur. Diese Infrastruktur muss für sämtliche Ladesituationen flächendeckend, bedarfsgerecht sowie einfach anwendbar und abrechenbar gestaltet sein.[456] Die Ladesituationen gestalten sich dabei sehr kontextspezifisch, lassen sich jedoch grundsätzlich in drei wesentlich zu unterscheidende Kategorien einordnen:

a) das „Laden zu Hause“,
b) das „Laden am Zielort“ und
c) das „(Schnell-)Laden unterwegs“.

Während für (a) in der Regel abrechnungs- und benutzerschnittstellenfreies Laden in einer gewohnten Umgebung entweder über den Haushaltsstromanschluss oder über eine Wallbox[457] möglich ist, unterscheiden sich in den Fällen (b) und (c) die Abläufe zur Beladung des E-Fahrzeugs zum Teil sehr deutlich von (a). Gleichzeitig stellen für die Akzeptanz der Elektromobilität und damit einhergehender Hemmnisse wie etwa die sogenannte Reichweitenangst gerade die Ladesituationen (b) und (c) die besonders relevanten Fälle dar.[458] Der Aufbau der Infrastruktur für diese beiden Ladesituationen und die Marktdurchdringung von Elektromobilität sind aneinandergekoppelt. Die noch immer geringen Zulassungszahlen von E-Fahrzeugen stellen für (potenzielle) Ladeinfrastrukturbetreiber ein erhebliches wirtschaftliches Risiko dar. Aufgrund der geringen Anzahl an E-Fahrzeugen ist die Ladeinfrastruktur aktuell häufig zu gering ausgelastet, um rentabel sein zu können. Dies gilt insbesondere für die kapitalintensive Schnellladeinfrastruktur. Auf der anderen Seite gilt der Mangel an ebenjener (Schnell-)Ladeinfrastruktur als einer der wesentlichsten Vorbehalte gegenüber E-Fahrzeugen. Dies hat einen sich gegenseitig negativ verstärkenden Effekt zur Folge.[459]

[455] *Kraftfahrt-Bundesamt*, Pressemitteilung Nr. 06/2018 - Der Fahrzeugbestand am 1. Januar 2018.
[456] *Sächsische Energieagentur – SAENA GmbH*, Kompetenzatlas Elektromobilität Sachsen.
[457] Heimladeeinrichtung an einer Hauswand.
[458] *Sun/Yamamoto/Morikawa,* Transportation Research Part D: Transport and Environment 2016, 26.
[459] *Sun/Yamamoto/Morikawa,* Transportation Research Part D: Transport and Environment 2016, 26.

Reichweitenangst

Reichweitenangst wird in der Verhaltenswissenschaft als eine stressvolle Erfahrung einer gegenwärtigen oder antizipierten Reichweitenproblematik verstanden, wobei die Möglichkeiten effektiv mit der Problematik umzugehen als unzureichend wahrgenommen werden.[460]

Vergleiche

Im Sinne einer grundlegenden Versorgung sollte insbesondere öffentliche Ladeinfrastruktur jedem E-Fahrzeugfahrer zur Verfügung stehen, um diesen „circulus vitiosus" zu durchbrechen. Denn in Deutschland existieren bereits zahlreiche Ladesäulen, die zudem vielfach bereits schnelladefähig[461] sind. In der Vergangenheit und stellenweise sogar noch aktuell (bei älteren Bestandssäulen) existieren Herausforderungen bezüglich der Zugänglichkeit der Ladeinfrastruktur. Damit sich dies ändert, hat der Gesetzgeber bereits Verordnungen erlassen, um diskriminierungsfreien Zugang zu öffentlicher Ladeinfrastruktur sicherzustellen. Diskriminierungsfreier Zugang bedeutet dabei grundsätzlich, dass jede Ladesäule potenziell von jedem E-Fahrzeug bzw. dessen Fahrer genutzt werden kann. Die Anzahl und Schnellladefähigkeit von öffentlich zugänglicher Ladeinfrastruktur ist für eine hohe Marktdurchdringung der Elektromobilität nicht flächendeckend ausreichend. Aus diesem Grund darf diese nicht zusätzlich auch noch partitioniert und fragmentiert werden. Eine Partitionierung kann prinzipiell auf drei Ebenen stattfinden bzw. durch Ausgestaltungsvarianten in diesen Ebenen verursacht werden:

- physische Ebene (z. B. Stecker),
- informatorische Ebene (z. B. Protokolle bzw. IKT-Systeme),
- ökonomische Ebene (Zahlungen bzw. Zahlungsmodalitäten).

Zu beachten ist, dass die informatorische Ebene ihrerseits mehrere Schichten aufweist. So ist die Kommunikation zwischen Ladesäule und Fahrzeug, Ladesäule und Backend-Systemen des Charging Point Operators (CPO) sowie der CPOs mit anderen Markteuren durch jeweils separate Protokolle und Systeme geregelt. Die zuerst genannten werden manchmal auch als Low-Level-Protokolle, Letztere als Higher-Level-Protokolle bzw. -Systeme bezeichnet. Eine umfassende Übersicht aller gängigen Ladeprotokolle und Akteure ist untenstehender Quelle zu entnehmen.[462]

Die Kernherausforderungen der Partitionierung haben sich zunehmend von der physischen zur informatorischen (insb. Higher-Level-Protokolle) und ökonomischen Ebene verlagert. Dies wird in einem späteren Abschnitt dieses Anwendungsfalls ausführlich beleuchtet. Im Folgenden sollen die Relevanz der Partitionierung bzw. die Konsequenzen für die zur Verfügung stehende Ladeinfrastruktur veranschaulicht werden. In Abbildung 26 wird auf Basis von Daten des Ladestationsverzeichnisses Open Charge Map[463] beispielhaft die Zugänglichkeit von Ladeinfrastruktur dargestellt.

[460] *Rauh/Franke/Krems,* Human factors 2015, 177.
[461] D. h., sie bieten mehr als 22 Kilowatt Leistung.
[462] *V2G Clarity*, IEC 63110 – Standardizing the Management of Electric Vehicle (Dis-)Charging Infrastructures.
[463] https://openchargemap.org.

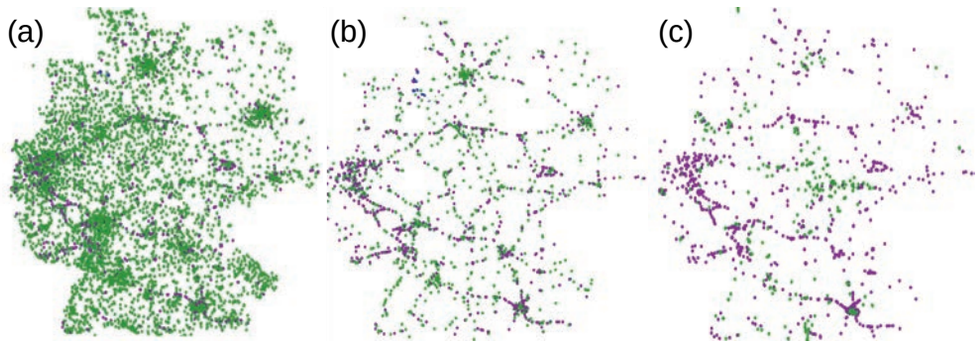


Abbildung 26: Ladestationen in Deutschland: (a) alle öffentlich zugänglichen Ladestationen, (b) alle schnellladefähigen, öffentlich zugänglichen Ladestationen, (c) alle öffentlich zugänglichen Ladestationen aus Sicht eines Fahrstromangebotsnutzers

Aus der Darstellung wird erkenntlich, dass in Deutschland bereits ein vergleichsweise dichtes Netz an Ladestationen errichtet und öffentlich zugänglich gemacht worden ist (a). Zudem wird ersichtlich, dass schnellladefähige Infrastruktur in erheblich geringerem Umfang vorhanden ist und primär entlang Schnellstraßen entsteht (b). Betrachtet man nun das Ladenetz eines deutschlandweit operierenden führenden Anbieters, der selbst keine physische Ladeinfrastruktur betreibt, sondern ausschließlich die Zugänglichkeit und entsprechende einheitliche[464] Tarife für E-Fahrzeugfahrer bzw. für E-Fahrzeugeigentümer bereitstellt, zeichnet sich ein Bild ab, das sehr deutlich zeigt, dass nach wie vor für manche E-Fahrzeugfahrer eine (hohe) Partitionierung wahrnehmbar sein dürfte. Die Akteure des Lade-Ökosystems werden im Folgenden noch ausführlich dargestellt, da sie für den diskutierten Anwendungsfall von hoher Relevanz sind. Ersichtlich wird weiter, dass im Dezember 2018 eine Minderheit aller physisch verfügbaren Ladesäulen den Fahrern ein einheitliches und im besten Fall komfortables Ladeerlebnis[465] ermöglicht. Bei Auswahl anderer Anbieter stellen sich ähnliche Leistungsbilder dar. Zwar unterliegt das Feld der Elektromobilität, welches u. a. auch elektrifizierte Nutzfahrzeuge wie bspw. Busse und Lkw umfasst, einer hohen Dynamik. Dennoch ist die Bereitstellung einer anbieterübergreifenden, bedarfsgerecht dimensionierten Ladeinfrastruktur von hoher Relevanz[466]. Insbesondere stellt sich auf der ökonomischen Ebene die Frage, welche Möglichkeiten existieren, die Zugänglichkeit öffentlicher Ladeinfrastruktur zu erleichtern und einer Partitionierung entgegenzuwirken.

Im Folgenden konzentriert sich dieses Anwendungsfallbeispiel daher auf die Reduzierung der Partitionierung auf informatorischer und insbesondere ökonomischer Ebene, die aus den Subprozessen Authentifizierung, Autorisierung sowie Abrechnung und Werttransfer besteht. Dazu ist es insbesondere wichtig, einen Überblick über den aktuellen Stand der ökonomischen Ebene zu erhalten, welche umgangssprachlich vereinfachend häufig unter dem Begriff „Bezahlmöglichkeiten" zusammengefasst wird. So existieren aus Sicht eines Fahrers drei unterschiedliche Möglichkeiten, um für das Laden zu bezahlen:

[464] Verbreitet ist das Modell, dass Anbieter rein die Zugänglichkeit anbieten und Kunden eine einheitliche Monatsabrechnung bieten, allerdings den Preis der Ladesäule durchreichen und eine Gebühr zusätzlich für die Zugänglichmachung aufschlagen. Zwar entspricht dies dem Modell aus der auf Verbrennungsmotoren basierenden Mobilität, jedoch sind Tarifmodelle im elektrischen Laden meist heterogener und Preise variieren meist stärker (Zahlung pro Ladevorgang, pro Minute, pro Energieeinheit).

[465] Ladeerlebnis wird im Anwendungsfall als eine Erfahrung bzw. Erlebnis eines E-Fahrzeugfahrers in einer Ladesituation verstanden. Aus Sicht eines Ladeinfrastrukturbetreibers bspw. kann man so auch von Kundenerlebnis sprechen. Der Begriff Kundenerlebnis stammt aus dem Englischen („Customer Experience") und wird in der modernen Betriebswirtschaftslehre als bedeutsames Konzept verstanden, das die Beziehung zum Kunden definiert und damit den Erfolg einer Unternehmung mitbestimmt.

[466] *Anderson*, LADEN2020 Schlussbericht.

(1) *Ladeinfrastrukturbetreiber-individuelle Bezahlung:* Die Fahrer von E-Fahrzeugen können den Ladevorgang bspw. über eine App des Ladeinfrastrukturbetreibers auf ihren Smartphones starten. In der App wiederum sind die für die Zahlung notwendigen Zahlungsdetails, wie etwa Lastschriftverfahren, hinterlegt. Alternativ kann die Authentifizierung durch eine Near-Field-Communication (NFC)-fähige Ladekarte erfolgen.

(2) *Webbasiertes Direktbezahlverfahren:* Nach der Ladesäulenverordnung II müssen sämtliche neu errichteten Ladesäulen einen Ad-hoc-Bezahlvorgang über ein sogenanntes Web-basiertes Direktbezahlverfahren ermöglichen. Dieser Zugang muss diskriminierungsfrei und ohne die Notwendigkeit eines vorherigen Vertragsabschlusses mit dem Ladeinfrastrukturbetreiber ausgestaltet sein. Ein akzeptiertes Web-basiertes Bezahlverfahren ist die Kreditkarte.

(3) *Bezahlung über Drittanbieter:* Nutzern von E-Fahrzeugen kann der Zugang zu Ladeinfrastruktur auch ohne ein direktes Vertragsverhältnis zwischen dem Fahrer und dem Ladeinfrastrukturbetreiber ermöglicht werden. Zum Einsatz kommt in diesen Fällen ähnlich zu (1) eine Ladekarte oder ein Smartphone inklusive Lade-App. Jedoch stellt ein Drittanbieter, mit dem der E-Fahrzeugfahrer einen Vertrag abgeschlossen hat, die App bzw. die Ladekarte bereit. Der Fahrer des E-Fahrzeugs erhält die Rechnung in diesem Szenario vom Drittanbieter. Der Ladeinfrastrukturbetreiber wiederum verrechnet den geladenen Strom dann mit dem Drittanbieter.

Für den vorliegend untersuchten Anwendungsfall ist die Bezahlung über einen Drittanbieter von besonderem Interesse und Fokus der Betrachtung einer denkbaren DLT-basierten Lösung. Ziel dieser Bezahloption ist es, Fahrern von E-Fahrzeugen ein über alle Ladesituationen hinweg gewohntes und komfortables Ladeerlebnis zu offerieren und damit einen Beitrag zur Akzeptanz der Elektromobilität zu leisten.[467]

Peer-to-peer-Laden an der Wallbox anderer Hauseigentümer

Ein neuer Trend ist es, fremden E-Fahrzeugfahrern die Haussteckdose oder eine zugängliche Wallbox gegen Bezahlung anzubieten. Die Idee ist dabei, den Nutzungsgrad der eigenen Ladeinfrastruktur zu erhöhen und durch die Zahlungsrückflüsse die Investition gegenzufinanzieren. Gleichzeitig könnte so auch in ländlichen Räumen die Verfügbarkeit von Ladeinfrastruktur verbessert werden. Während dieser Spezialfall des Ladens am Zielort nicht vom aktuellen Anwendungsfallbeispiel abgedeckt ist, so ist doch sehr angezeigt, eine Erweiterung der Blockchain-basierten Realisierung zu überprüfen. Jedoch sind abrechnungsfähige Wallboxes dieser Art aktuell wenig weit verbreitet. Eine eingehendere Betrachtung des Themas des Datenschutzes wird so vermutlich relevant, da Wallboxes in der Regel einer kleinen Gruppe von Personen zuordenbar sind und somit Personenbezug erhalten dürften.

Um die entsprechenden Subprozesse zur Beladung zu vereinheitlichen und ein konsistent kundenorientiertes Laderlebnis zu unterstützen, wurde das sogenannte E-Roaming etabliert, welches die dritte Bezahloption realisiert. Das Roaming-Konzept ist bspw. auch aus der Mobilfunkbranche bekannt. So wird etwa während eines Aufenthalts im EU-Ausland in der Regel automatisch durch das Smartphone ein anderer Netzbetreiber gewählt, zu dem der Mobilfunkkartenanbieter des Smartphone-Benutzers einen Roaming-Vertrag unterhält. Ein weiteres Beispiel sind Geldautomaten, auch wenn hier seltener der Begriff

[467] *Grathwohl,* Kartellrechtliche Bewertung von Standardisierungsstrategien 2015, 221.

„Roaming“ verwendet wird. Im Netzwerk der Geldautomaten haben sich mehrere Banken zu Bankennetzwerken mit gleichen IT-System zusammengeschlossen und bieten – gegebenenfalls gegen ein Entgelt – „Roaming“, also die Möglichkeit, bei dem Automaten einer fremden Bank Geschäfte zu tätigen, an. Dieses Konzept existiert in ähnlicher Weise in der Elektromobilität, wo Roaming-Beziehungen auch im Inland zwischen unterschiedlichen Ladenetzwerken existieren. Während Roaming-Gebühren in der Mobilfunkbranche auf Ebene der Europäischen Union begrenzt sind, liegt im Bereich der Geldautomaten meist eine nationale Regulierung vor. Analog zielt das E-Roaming darauf ab, ein konsistentes und gutes Kundenerlebnis mit möglichst hoher Flächenabdeckung zu erzielen. Ein solches Kundenerlebnis ist durch viele differierende Leistungsmerkmale bestimmt. Den Kern des E-Roamings jedoch machen aus der Perspektive der E-Fahrzeugfahrer zwei entscheidende Leistungsmerkmale aus:

- Transparente, faire und möglichst einheitliche Tarif- und Preisgestaltung
- Einheitliche, einfache Authentifizierung und Autorisierung in jeder Ladesituation

Authentisierung, Authentifizierung und Autorisierung

Im Beispiel eines Computerprogrammes, welches Zugang zu einem gesicherten Bereich gewähren kann, behauptet der Benutzer zuerst seine Zugangsberechtigung, indem er einen Benutzernamen eingibt. Zusätzlich authentisiert er sich, indem er sein Passwort angibt. Das Programm identifiziert dann den Benutzer anhand dieser Angaben und führt anschließend die Authentifizierung durch, also die Verifizierung der erbrachten Behauptung über die Authentizität. Erst wenn diese Verifizierung erfolgreich ist, werden dem Benutzer die festgelegten Zugangsberechtigungen im Rahmen der Autorisierung üblicherweise für die Dauer einer Sitzung zugewiesen.

Damit dieses Leistungsversprechen bzw. -ziel ermöglicht wird, haben sich im Rahmen von E-Roaming neue Marktakteure bzw. -rollen etabliert. Diese werden im Folgenden skizziert. Zu beachten ist, dass ein Unternehmen bzw. allgemein eine juristische Person durchaus mehrere der im Folgenden sequenziell dargestellten Rollen wahrnehmen kann.

Ein Charging Point Operator (CPO) betreibt an einem oder mehreren Standorten eine gewisse Anzahl von Ladesäulen mit wiederum potenziell mehreren Anschlüssen und Steckern. CPOs können durchaus eine Schnittstelle zu Endkunden haben, im Allgemeinen ist dies aber nicht immer der Fall. Vielmehr lassen sich CPOs dadurch charakterisieren, dass ihre Ladestationen eine Authentifizierung mit der vom CPO bereitgestellten Ladekarte oder Lade-App ermöglichen. Infolgedessen werden diese Verbünde häufig auch als Ladenetzwerke bezeichnet. Die Gestaltung der Ladeinfrastruktur orientiert sich an den Erfordernissen der zuvor skizzierten Ladesituationen. Ladestationen für das Laden unterwegs (Fall (c)) werden häufig von CPOs errichtet und betrieben, deren Kerngeschäft dies ist. In diesem Fall sind Betreiber und Eigentümer der Infrastruktur typischerweise identisch. Gerade im Falle der Ladesituation „Laden am Zielort“ hingegen sind Eigentum und Betrieb manchmal getrennt. Hierzu lassen sich für das Anwendungsfallbeispiel relevante Szenarien unterscheiden. Grundsätzlich sind drei Betreibermodelle möglich, die sich an den unterschiedlichen Betreiberarten orientieren und deren individuelle Interessen adressieren:

1. *Eigenbetrieb:* In diesem Fall ist der Eigentümer gleichzeitig auch der Betreiber (CPO). Er betreibt die komplette Ladeinfrastruktur eigenständig. Die Schnittstellen zur Anbindung an die IT-Systeme sind in diesem Fall individuell zu implementieren und zu

warten. Diese Betriebsart ist typisch für Akteure mit einer großen Anzahl von Ladestationen, etwa große Unternehmen oder Stadtwerke.

2. *Fremdbetrieb:* In diesem Fall ist der Eigentümer nicht der Betreiber (CPO) der Ladeinfrastruktur, sondern überlässt den Betrieb einem Fremdbetreiber, bspw. einem lokalen Stadtwerk. In solchen Fällen spricht man von Integration in ein (CPO-)Ladenetzwerk. Während sich operative Aufwände so für den Eigentümer sehr stark reduzieren, geht ebenfalls die Kontrolle über die Ausgestaltung des operativen Betriebs, wie etwa der Tarifierung, in weiten Teilen an den Fremdbetreiber über. Zuweilen kaufen potenzielle Eigentümer von Ladeinfrastruktur Ladesäulen von großen CPOs ein, die wiederum die Ladesysteme als „White-Label"-Lösung von sogenannten Charge-Point-Manufacturern (CPM), d. h. Herstellern von Ladesystemen, einkaufen. Der Strom wird in diesen Fällen nicht selten zum Selbstkostenpreis oder sogar kostenlos an Fahrer von E-Fahrzeugen bereitgestellt, da die Eigentümer ihren Kunden (z. B. ein Hotel) einen besonderen differenzierbaren Service anbieten möchten. Wenn Ladestrom kostenfrei angeboten wird, ist E-Roaming folglich irrelevant.
3. *Teilfremdbetrieb:* Einige CPMs oder CPOs, die „White-Label"-Lösungen vertreiben, bieten darüber hinaus Zwischenlösungen an. So können etwa die Tarifierung oder Zugangsmöglichkeiten selbst im Detail festgelegt werden[468] und die Implementierung von Schnittstellen u. a. im Rahmen von Ladesteuerungs- und -abrechnungsprotokollen vom CPM übernommen werden. Der First-Level-Support[469] liegt in diesen Fällen ebenfalls häufig beim Eigentümer. Da CPMs normalerweise nicht auch gleichzeitig CPOs sind, unterhalten sie typischerweise keine E-Roaming-Beziehungen, sodass in diesen Fällen analog zum Eigenbetrieb eine Integration in E-Roaming-Netzwerke Seltenheit hat. Falls die Ladesäule in ein CPO-Ladenetzwerk integriert werden kann, ist eine Authentifizierung und Autorisierung darüber möglich. Darüber hinaus werden über gegebenenfalls existente E-Roaming-Beziehungen des CPO-Ladenetzwerks Zugänglichkeiten weiter verbessert.

Typische Eigentümer, die sich intensiv mit den drei zuvor beschriebenen Betriebsszenarien auseinandersetzen, sind vor allem Hoteliers, Parkraumbewirtschafter, Unternehmen und Vermieter. Diese Akteure haben ein Interesse an Ladediensten, da ihre Gäste/Kunden/Mitarbeiter/Mieter durch das Laden an diesen typischen Zielorten ihre Mobilitätsbedarfe für die Weiterreise decken können.

E-Mobility Service Provider (eMSP): Besonders zentral ist die Rolle des eMSP, der im deutschsprachigen Raum häufig auch als Fahrstromanbieter bezeichnet wird und die Realisierung des zuvor bereits skizzierten Leistungsversprechens für seine Kunden anstrebt. Ein eMSP ist letztlich der Betreiber einer Plattform, auf der Ladestationen und E-Fahrzeugfahrer zusammenkommen. Als Zugang zur Plattform werden Benutzerschnittstellen – engl. Human-Machine-Interfaces (HMI) – an der Ladeinfrastruktur, in In-Car-Entertainment-Systemen sowie in Mobile sowie gegebenenfalls Web-Apps eingesetzt. Konsumenten bzw. Nutzer der Plattform setzen Letztere ein, um etwa im Rahmen von Routenplanung geeignete Ladestandorte auszuwählen bzw. auswählen zu lassen. Dieses Rollen- und Akteursgefüge ist in Abbildung 27 dargestellt.

Nicht selten wird das grundlegende Leistungsversprechen im Sinne einer Plattformökonomie zusätzlich um Premium-Leistungskomponenten wie den Nachweis von Grünstromzertifikaten bzw. einen Carbon-Offset, Lokalstromnachweise, Reservierung von Ladeinfrastruktur (sofern von anderen involvierten Marktakteuren ermöglicht) oder

[468] Z. B. Zugang nur privat, öffentlich, öffentlich auf Anfrage etc.

[469] Bei der Bezeichnung First-Level-Support handelt es sich um die erste Anlaufstelle für alle eingehenden Supportanfragen.

Ausleihdiensten für Verbrennungsfahrzeuge für Langstrecken ergänzt. In diesem Anwendungsfallbeispiel fokussieren wir in einem grundlegenden ersten Schritt das Thema Zugänglichkeit von öffentlicher Ladeinfrastruktur und Komfort beim Laden. Beide bedingen das Kunden-Ladeerlebnis positiv und wirken dem Konzept der Reichweitenangst, einem der großen Hemmnisse der Elektromobilität[470], entgegen. eMSP sind nicht selten in der Realität auch CPOs. Gleichzeitig gibt es auch zahlreiche „reine" eMSPs, welche z. T. dezidiert für einzelne Kundengruppen wie etwa Firmenflotten Fahrstromangebote offerieren. Wichtig für eMSP sind die Flächenabdeckung bzw. die Anzahl und Verteilung zugänglicher Ladeinfrastruktur über die Plattformschnittstellen. Entsprechend der klassischen Theorie zur Plattformökonomie unterliegen sie Wirkungen von positiven Netzwerkeffekten und dem Konzept der kritischen Masse.

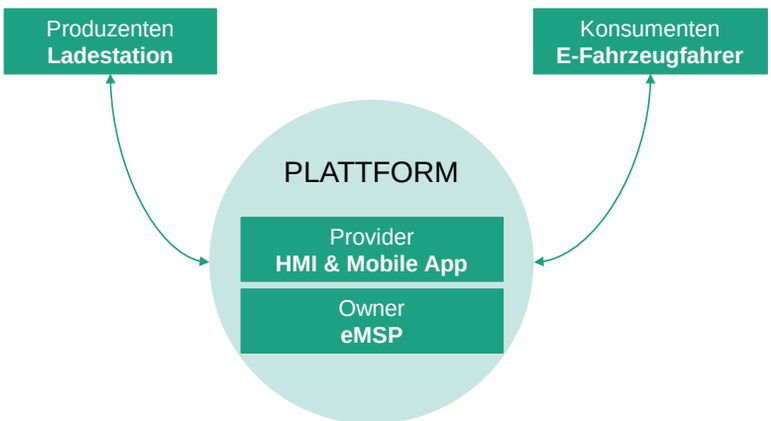


Abbildung 27: Repräsentation der Rollen und Akteure des elektrischen Ladens in Form der Platform Economy – in Anlehnung an van Alstyne et al. (2016)

Clearing & Roaming (C&R): Während große CPO-Ladenetzwerke theoretisch eigenständig eine eMSP-Plattform betreiben und dabei eine notwendige kritische Masse erreichen können, ist dies bspw. für reine eMSPs ohne Vernetzung und Zahlungsausgleich technisch nicht realisierbar. Gleiches gilt für kleinere und auch mittlere CPO-Ladenetzwerke. Um sowohl für Produzenten als auch Konsumenten einen gesteigerten Nutzen ihrer Plattformen zu realisieren, wurde das voranstehend eingeführte E-Roaming erforscht, entwickelt und eingeführt. In diesem Anwendungsfallbeispiel bezeichnen wir mit Clearing & Roaming (C&R) jene Rolle, welche das E-Roaming ausführt. Die Rollenbezeichnung umfasst im Namen die zwei wesentlichen Dienstleistungen, welche C&Rs ihren Teilnehmern anbieten können. So bezeichnet Clearing den (teil-)automatisierten Zahlungsausgleich, welcher zwischen eMSPs und CPOs plattformübergreifend realisiert wird. Dies setzt eine prinzipielle Roaming-Befähigung voraus. Zwar ist für das Roaming nicht zwingend erforderlich, dass ein Zahlungsausgleich (teil-)automatisiert ausgeführt wird. Jedoch bedeutet ein rein auf Roaming beschränkter Dienst manuellen Zahlungsausgleich und dementsprechende betriebswirtschaftliche Aufwände. Es ist anzumerken, dass ein solcher Akteur potenziell Daten von allen über ihn abgewickelten Ladevorgängen sammeln könnte. Diese Kenntnis kann einem solchen Akteur gegenüber einzelnen eMSPs und CPOs ein besseres Marktverständnis ermöglichen. In dieser Rolle stellen C&Rs eine Plattform für eMSPs dar, auf der diese untereinander vernetzt werden. Da eMSPs selbst Plattformen sind, bieten C&Rs eine Plattform für Plattformen. Eine solche Rolle wird auch als Superplattform bezeichnet.[471] Abbildung 28 visualisiert das zugehörige Beziehungsgefüge. Als Konsequenz konzentriert sich je nach Ausgestaltung der C&R-Rolle Marktmacht bei diesen Akteuren, sodass vorstellbar ist, dass andere Rollen Misstrauen in diese

[470] *Melliger/Vliet/Liimatainen,* Transportation Research Part D: Transport and Environment 2018a, 101.
[471] *Lang/Szczepanski/Wurzer*, The Emerging Art of Ecosystem Management.

Form der Intermediation hegen bzw. entwickeln könnten. Dies ist insofern bemerkenswert, als dass gerade die oben beschriebenen Subprozesse Vertrauen in die korrekte Vermittlung und Abrechnung durch die C&Rs voraussetzen.

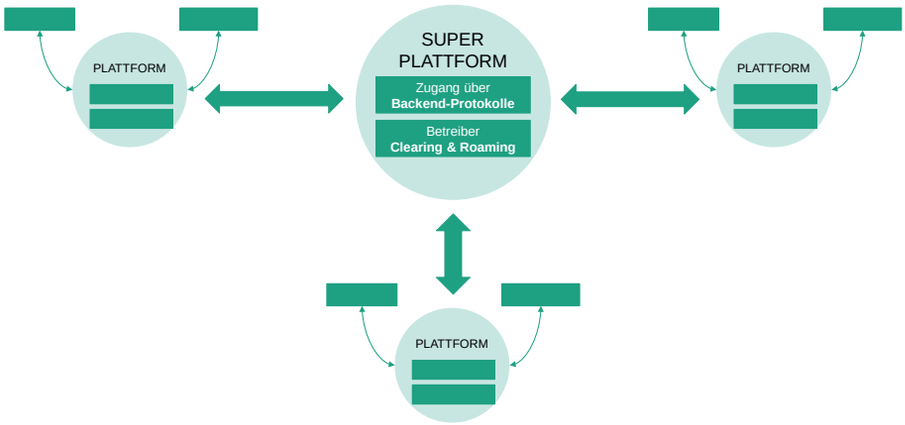


Abbildung 28: Superplattform Lang/Szczepanski/Wurzer 2019.: Eine Plattform aus Plattformen der eMSPs – schematische Darstellung eines reinen Hub-and-Spoke-Modells für Kooperationsmodelle im E-Roaming

In der Praxis haben sich mehrere solcher Intermediäre herausgebildet, die nicht selten selbst CPOs als Anteilseigner führen. Laut einer Studie[472] sind drei idealisierte Modelle der Kooperation innerhalb des E-Roamings unterscheidbar: (1) Das Meshed Network, (2) das Hub-and-Spoke-Network und (3) das Spoke-Model-Interroaming Network:

Das Meshed Network (1) realisiert E-Roaming über bilaterale Beziehungen, was die Implementierung von Schnittstellen mit proprietären Systemen erfordern würde und daher im Vergleich langsam und aufwendig in der Realisierung ist. Im Hub-and-Spoke-Network (2) existiert analog zu einer Superplattform ein zentraler C&R-Anbieter, zu dem alle CPOs und eMSPs Schnittstellen aufbauen. In Spoke-Model-Interroaming Network (3) koexistieren mehrere C&R-Anbieter, welche wiederum Schnittstellen zueinander implementiert haben. Es ist zu beachten, dass in der Praxis nicht alle C&Rs paarweise miteinander kooperieren und transitive Beziehungen nicht möglich sind. Derartige transitive Beziehungen würden ermöglichen, dass Kunden eines eMSP, welcher an einen C&R-Anbieter angebunden ist, welcher über einen "Mittels-C&R" eine Schnittstelle zu einem dritten C&R-Anbieter verfügt, an den ein CPO C angebunden ist, laden könnte. Abbildung 29 skizziert in idealisierter Form die drei prototypischen Kooperationsmodelle für das elektrische Laden. In Deutschland hat sich Modell (3) etabliert. Wünschenswert wäre im Sinne des Wettbewerbs allerdings Modell (1) und am wenigsten Modell (2), da jenes zur Marktkonzentration bei nur einem Akteur führte. Modell (3) stellt in diesem Sinne eine Zwischenlösung dar. Unklar bleibt, ob insbesondere die zuvor beschriebenen Netzwerkeffekte dazu führen, dass eine weitere Marktkonzentration stattfindet.

[472] *Begleit- und Wirkungsforschung Schaufenster Elektromobilität* (BuW), Good E-Roaming Practice: Praktischer Leitfaden zur Ladeinfrastruktur-Vernetzung in den Schaufenstern Elektromobilität.

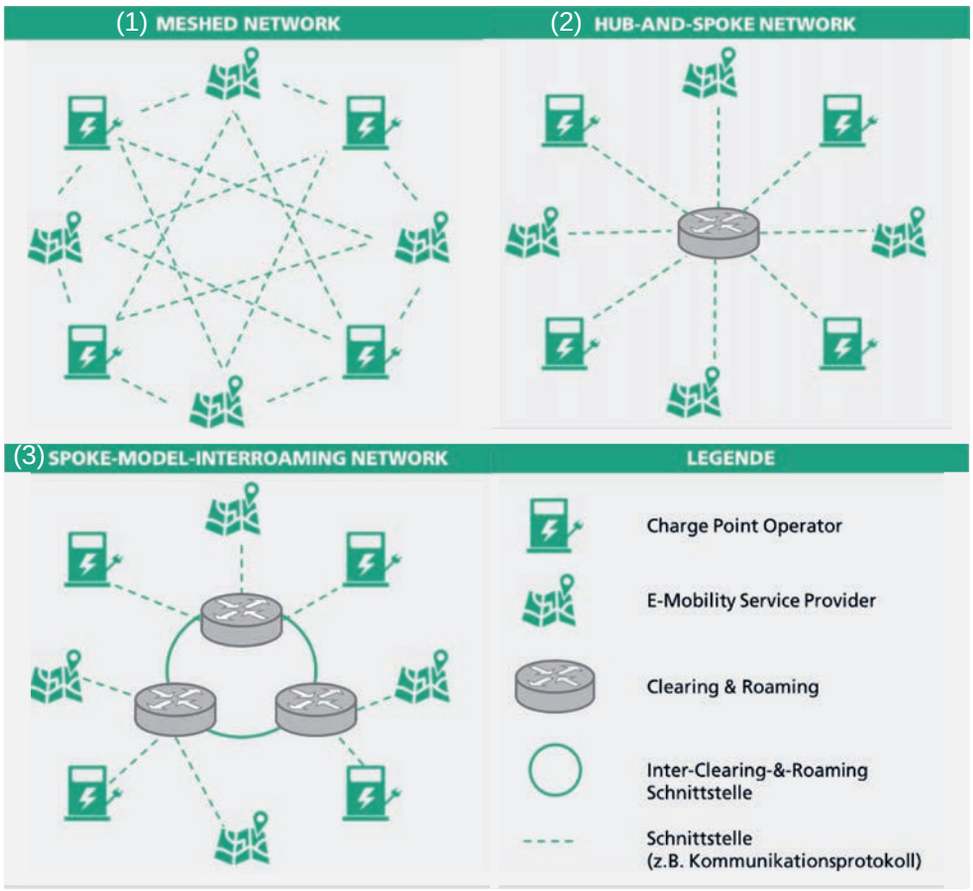


Abbildung 29: Kooperationsmodelle für E-Roaming in Anlehnung an Begleit- und Wirkungsforschung Schaufenster Elektromobilität (BuW) 2015.

Neben den drei Kooperationsmodellen unterscheiden sich wie oben angesprochen C&Rs nach ihrer Wertschöpfungstiefe bzw. in der Frage, ob diese neben Roaming auch Clearing anbieten. Dies gilt umso mehr für das Kooperationsmodell (3), in dem mehrere C&Rs diese Funktionalitäten implementiert haben sollten, um sie Ende zu Ende, d. h. von der Initiierung durch den E-Fahrzeugfahrer bis zum Abschluss der Beladung, realisieren zu können. In der Praxis werden bei Beziehungen dieser Art nicht immer pauschal alle Funktionalitäten angeboten. Während die für das Roaming notwendigen Prozesse umfassend abgebildet sein müssen, muss dies für das (teil-)automatisierte Clearing nicht der Fall sein. Auch ist zu beachten, dass z. B. aus ökonomischen Gründen bestimmte Funktionalitäten im Sinne eines Premiumdiensts optional sind. Diese müssen dann von den Nutzern eines C&Rs nicht zwingend eingesetzt werden.

Zunächst sollen die technisch-funktionalen Abläufe skizziert werden, bevor anschließend die vertraglichen Beziehungen grob beschrieben werden. Eine eingehende Beleuchtung findet dann im rechtlichen Teil statt.

Zur Realisierung des C&R-Diensts sind zwei Prozessgruppen zu unterscheiden.

(1) Authentifizierung, Autorisierung und Transaktionsdatenübermittlung (Roaming)

(2) Fakturierung[473] und Zahlungsausführung (Clearing)

Prozessgruppe (1) bezieht sich auf die Informationsbereitstellung zum Ladepunkt[474], die Legitimation eines Ladevorgangs, der von einem identifizierten E-Fahrzeugfahrer initiiert wird (Authentifizierung und Autorisierung), die energietechnische Abwicklung zwischen Fahrzeug und Ladesäule sowie die Messung der Leistungsfaktoren (z. B. Zeit, Energie, Ladeleistung, Anschlusszeit, Parkdauer etc.) im sogenannten Charge Detail Record (CDR).

Auf Basis dieser Prozesse ist eine bilaterale Abrechnung der bezogenen Ladeleistungen zwischen CPO und eMSP möglich. Einige Roaming-Anbieter ohne kombiniertes Clearing lassen ihren Dienst allein auf diesen Komponenten basieren. Der CPO ist in der Verantwortung, die entstandenen Kosten nachzuweisen. Zum Zeitpunkt der Gutachtenerstellung ist dies zum Teil mit erheblichem manuellem Aufwand verbunden, weshalb CPOs häufig in komplexere Backend-Lösungen zur Erhöhung des Automatisierungsgrads investieren.

Prozessgruppe (2) bezieht sich auf die Inrechnungstellung bzw. das Abrechnen und Gegenverrechnen von Ladeleistungen zwischen CPOs und eMSPs sowie auf die Ausführung von in Rechnung gestellten Ladeleistungen über Zahlungsdienste. Dazu werden monetäre Werte je nach Zahlungsverfahren zwischen dem eMSP und dem CPO transferiert. Dies geschieht mithilfe der Informationen aus dem CDR. Im Anschluss werden vereinbarte Tarife und Preise angewendet, um die Leistungen zu fakturieren. Dazu setzt die Prozessgruppe (2) das Funktionieren der Prozessgruppe (1) voraus.

Die IT-seitige Koordination dieser Vorgänge übernimmt eine Vielzahl an zumeist offenen Kommunikationsprotokollen. Während die Kommunikation zwischen dem E-Fahrzeug und der Ladesäule fast immer auf den Standard ISO bzw. IEC 15118 setzt und die Kommunikation zwischen der Ladesäule und dem CPO als Marktstandard das Open Charge Point Protocol (OCPP) verwendet, existiert eine große Anzahl unterschiedlicher Protokolle, die an dieser Stelle im Einsatz sind. In der Regel setzen konkurrierende C&Rs auf unterschiedliche Protokolle. So bauen der größte C&R intercharge auf das Open Intercharge Protocol und der C&R e-clearing.net auf das Open Clearing House Protocol. Bereits aus dem Namen ist ersichtlich, dass beide Protokolle von ihrem Anwender maßgeblich gestaltet wurden. Neuere und bisher weniger verbreitete Protokolle, die direkt zwischen eMSPs und CPOs vermitteln, befinden sich aktuell in der Entwicklungsphase. Allerdings erfordern auch diese das Vorhandensein zentraler Register, welche die Beziehungen zwischen den eMSPs und den CPOs statisch speichern und zur Abfrage vorhalten bzw. freigeben. In Deutschland übernimmt diese Aufgabe bspw. der Bundesverband der Energie- und Wasserwirtschaft (BDEW).

Zusammenfassend stellt sich die vertragliche Abbildung vereinfacht [475] wie folgt dar: Damit eMSPs über C&R mit CPOs zusammenarbeiten können, sind E-Roaming-Verträge zwischen eMSPs und C&Rs sowie zwischen C&Rs und CPOs notwendig, um die Leistungsbeziehung zu vereinbaren. Zudem müssen auch eMSPs Verträge direkt mit CPOs abschließen, um Abrechnungskonditionen zu spezifizieren. Gegeben N CPOs und M eMSPs, so müssen potenziell N x M viele Verträge zwischen den letztgenannten Akteuren geschlossen werden. Diese Verträge sind notwendig, weil ein C&R die technischen Voraussetzungen der Zusammenarbeit ermöglicht, nicht aber notwendigerweise die Leistungsverrechnung zwischen dem eMSP und CPO. Abschließend sei angemerkt, dass ein

[473] Fakturierung: Der Prozess der Rechnungserstellung mit dem Ergebnis der Faktura (Rechnung), welche den Fakturawert (Rechnungswert) und seine Rechnungsbestandteile enthält.

[474] Ladepunktinformationen wie Preis, maximale Ladegeschwindigkeit, Belegung etc.

[475] In der Realität existieren viele alternative Ausgestaltungen. Das hier dargestellte Vertragssetting stellt ein gängiges und weitverbreitetes Modell dar.

Unternehmen in der Praxis mehrere Rollen einnehmen kann. Insbesondere größere CPOs bieten häufig auch Fahrstromangebote an, die E-Roaming-fähig sind. So können Kunden auch bei anderen einem C&R angehörigen CPOs, mit denen Verträge bestehen, geladen werden.

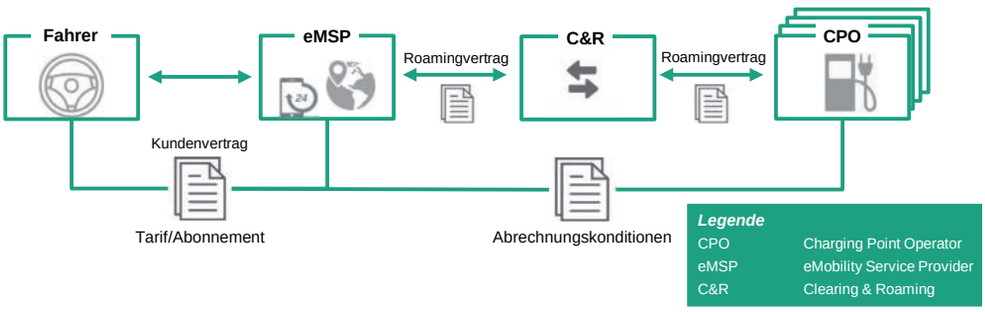


Abbildung 30: Marktrollen bzw. -akteure und vertragliche Beziehungen (vereinfachte, schematische Darstellung)

Zusammenfassend soll folgendes Beispiel, die Interaktion der Akteure aus E-Fahrzeugfahrersicht demonstrieren: Auf dem Parkplatz des Supermarkts „SuperPreis“ in Musterstadt ist eine Schnellladesäule installiert, an der es möglich ist, sich mittels der Ladekarte des Stadt-werks Musterstadt zu authentifizieren und einen von „SuperPreis“ festgelegten vergünstigen Ladetarif von 10 ct/min zu bezahlen. Da das Stadtwerk Musterstadt E-Roaming-Beziehungen unterhält, kann auch der Fahrer aus dem nahegelegenen Musterdorf, welcher über einen Flatrate-Tarif von Musterfahrstrom verfügt, aufgrund seiner Flatrate kostenlos laden.

8.1.2 Status quo und Herausforderungen

Da die Verfügbarkeit von bedarfsgerechter Ladeinfrastruktur ein wichtiges Hemmnis aufzeigt, sind die Analyse und das Verständnis über den Status quo der Zugänglichkeit öffentlicher Ladeinfrastruktur und dessen Probleme besonders wichtig. Im Folgenden werden daher zuerst die Herausforderungen aus Sicht der Fahrer bzw. der Nutzer der Elektromobilität zusammengefasst, bevor im Anschluss die Herausforderungen der CPOs und eMSPs erläutert werden.

Zum einen besteht das Wertversprechen von eMSPs insbesondere darin, Kunden eine konsistentes Ladeerlebnis zu bieten. Das bedeutet, dass die Kunden eines solchen Anbieters an möglichst vielen (schnellladefähigen) Ladesäulen Strom zu transparenten und für sie preiswerten Konditionen beziehen können und der dazugehörige Abrechnungsvorgang reibungslos und mit minimalem Einsatz des Fahrers erfolgt. Vor diesem Hintergrund stellt die Partitionierung der theoretisch verfügbaren Ladesäulen per se bereits eine unbefriedigende Situation dar. Zwar ist die direkte Bezahlung per Web-basiertem Direktbezahlverfahren, wie voranstehend beschrieben, aufgrund der Ladensäulenverordnung II auf allen seit 2017 verbauten Ladensäulen möglich. Jedoch bedeutet dies zwei Einschränkungen für den Fahrer:

- *Komfort:* Zum einen ist das Direktbezahlverfahren eine weniger komfortable Möglichkeit des Zahlens, da der Fahrer mit einer ihm im Allgemeinen unbekannten Benutzerschnittstelle zu z. T. ungünstigen Witterungsbedingungen direkt an der Ladesäule interagieren muss. Zum anderen ist das Preisgeben von persönlichen und vertraulichen Kreditkarteninformationen (sofern eine Kreditkarte im Besitz des Fahrers ist) vielen Anwendern unangenehm. In einigen Fällen werden Web-basierte Direktbezahlverfahren von E-Roaming-Anbietern angeboten. Diese setzen wiederum auf proprietäre mobile Apps oder separate Websites, welche der Nutzer per Browser

zunächst öffnen muss, um den Vorgang abzuschließen. Beide Varianten werden vielfach als wenig kundenfreundlich wahrgenommen[476]. Darüber hinaus erhalten die Nutzer ihre Abrechnungen, anders als über ihren eMSP, nicht in einer konsolidierten Endabrechnungsperiode, sondern auf Einzelladevorgangsbasis in separaten Dokumenten.

- *Abrechnungsmodalitäten:* Zum einen sind Tarif und Preise lediglich mit zusätzlichem Aufwand abfragbar. Beispielsweise sind Klauseln zu Angaben bezüglich möglicher Roaming-Gebühren nicht selten versteckt und damit schwer zu finden. Zum anderen tendieren Ad-hoc-Ladetarife aus Sicht eines Kunden eines eMSP dazu, ungünstig bzw. teuer zu sein. So ist es nachvollziehbar, dass sich ein Fahrer bzw. Besitzer eines nur vergleichsweise langsam beladbaren E-Fahrzeugs explizit für einen Mobilitätsdienstleister entscheidet, der nicht pro Zeit oder pro Ladevorgang abrechnet, sondern per Energieaufnahme (in kWh). Wenn die Ladesäule, an welcher der Fahrer laden möchte, hingegen lediglich einen zeitbasierten Tarif anbietet, würde er diese Ladesäule womöglich ungern nutzen oder wäre gegenüber Nutzern mit schnellladefähigen E-Fahrzeugen benachteiligt. Dies gilt analog für Ladesäulen mit gleichem Tarifschema, in dem ein höherer Preis pro Abrechnungseinheit beim Ad-hoc-Laden zu zahlen wäre, und insbesondere für solche Fahrstromangebote, in denen ein hoher fixer Sockelbetrag gezahlt wird, um niedrige variable Kosten zu tragen (im Extremfall keine – eine sogenannte „Flatrate").

Aus Sicht des CPOs ergeben sich im Status quo Herausforderungen, die im Folgenden zusammenfasst werden. Je nach Betreibermodell streben CPOs an, ihre Ladeinfrastruktur möglichst vielen potenziellen Fahrer von E-Fahrzeugen bereitzustellen. Dies geschieht insbesondere vor dem Hintergrund der Erwirtschaftung zusätzlicher Erträge. Aus heutiger Perspektive ist es dazu notwendig, mehrere unterschiedliche Kommunikationsprotokolle zu implementieren. Dies treibt die IT-Integrationskosten in die Höhe. Zusätzlich fallen für die Teilnahme an C&R-Diensten Kosten an. Diese bestehen zumeist aus monatlichen oder jährlichen Zahlungen im drei- bzw. vierstelligen Bereich. Diese werden manchmal ergänzt um einmalige Anschlussgebühren im mittleren vierstelligen Bereich. Eine Teilnahme an mehreren C&R-Diensten kann kleinere CPOs daher IT-seitig und/oder finanziell überfordern. Dass je nach C&R-Dienst eine z. T. manuelle Fakturierung zum Monatsende für jeden eMSP notwendig wird, erschwert die Situation zusätzlich. Zudem sind Verträge bei den etablierten C&R-Diensten weitestgehend bilateral ausgehandelt und statisch. Bei Fusionen bzw. Übernahmen von eMSPs oder der Entstehung neuer eMSPs müssen daher Beziehungen und Konditionen manuell festgelegt werden. Aufgrund erhöhter Aufwendungen fakturieren CPOs daher nicht selten Roaming-Gebühren.

Aus Sicht der eMSP stellen sich weitestgehend analoge Herausforderungen zu den CPOs. Da es noch erheblich mehr CPOs als eMSPs gibt, gestalten sich die Bestrebungen, Beziehungen zu CPOs zu halten bzw. neu aufzubauen und die Konditionen individuell zu gestalten, als sehr aufwendig. Zudem stellt die technische Komplexität auch für eMSPs eine Hürde dar. Schließlich ist es für eMSPs in hohem Maße herausfordernd, die nötige Kapazität aufzubringen, um die Korrektheit der Monatsabrechnungen von CPOs bei gegebener verzögerter Fakturierung sicherzustellen.

8.1.3 Mögliche Lösungsansätze und Rollen von DLT

Rolle

Im untersuchten Anwendungsfall könnte die DLT mindestens drei potenzielle Funktionen wahrnehmen, um die zuvor skizzierten Herausforderungen zu adressieren. Diese sind:

[476] *Dudenhausen/Hahn,* Herausforderung Utility 4.0 2017, 683.

1) Authentifizierung und Autorisierung über DLT-basierte selbstsouveräne Identitätslösungen

2) Manipulationssichere Dokumentation und Nachhaltung der Ladevorgänge

    - Zu diesen zählt vor allem die Eigenschaft der Evidenz und Überprüfbarkeit der Abrechnung des Ladevorgangs vom eMSP bis hin zum Sensor, um eichrechtskonforme Ladeergebnisse[477] unwiderruflich im CDR zu dokumentieren.

3) Zeitnahe Abrechnung und Werttransfer der Ladevorgänge durch Token

Durch Abbildung voranstehender drei Funktionen kann eine DLT-Lösung die Rolle eines zuvor dargestellten C&R-Anbieters einnehmen und damit die Kooperationsmodellvariante des Meshed Networks (3) umsetzen, welches durch Disintermediation die Risiken einer Konzentration von Marktmacht einzelner C&R-Akteure „by design" ausschließt. Natürlich würde eine auf DLT-basierte Lösung den CPOs und eMSPs zunächst eine (weitere) Alternative im Sinne einer neutralen Plattform[478] zur Verfügung stellen, welche mit bestehenden C&R-Akteuren koexistiert. Im Falle zu starker Konzentration der Marktmacht werden Akteure dann wohl zunehmend auf die neutrale Plattform wechseln.

Lösungsansatz
Die Verwendung einer auf einem öffentlichen DLT-System – bspw. Ethereum – basierenden Plattform kann erreichen, dass anders als bei existierenden C&R-Diensten neuen Teilnehmern schneller und vergleichsweise einfacher Zugang und Partizipation ermöglicht werden. Jeder CPO und jeder eMSP repräsentiert dazu idealerweise einen Node. Inwieweit sich IT-Integrationskosten reduzieren lassen, bedarf einer detaillierteren Betrachtung und ist stark abhängig von der konkreten Ausgestaltung der DLT-Lösung. Aufgrund der Tatsache, dass zumindest theoretisch keine Roaming-Kommunikationsprotokolle (mehr) implementiert werden müssten, beschränkt sich die Implementierung auf den Einsatz von etablierten Kommunikationsstandards zwischen Fahrzeug und Ladesäule, Ladesäule und CPO sowie CPO und der DLT-basierten Plattform. Dadurch, dass nicht jede Ladestation, sondern jeder CPO einen Node repräsentiert, sind keine Modifikationen an Bestandsladeinfrastruktur notwendig – zumal Internetkonnektivität für aktuelle C&R-Dienste ebenfalls schon existent sein muss[479]. Aus Sicht des E-Fahrzeugfahrers werden Ladekonditionen transparent, da diese Informationen als Teil der Smart-Contract-Spezifikation in die DLT-Schicht geschrieben werden und öffentlich wären. Zudem könnte es von Vorteil sein, dass der Fahrer bei der hier angedachten Rolle nicht selbst über ein Wallet und auch nicht über öffentlich bekannte Identifikation verfügen muss, sondern mit einem zeitlich begrenzten Pseudonym operieren kann, solange der eMSP ein Register über die Kombination von Pseudonym, Zeitstempel und Kunde pflegt. Aus Sicht des CPOs sind Ladevorgänge dann leicht autorisierbar und beim Schreiben eines CDRs in die DLT-Schicht nachhaltig dokumentiert, sodass die Smart-Contract-Ausführung einen Werttransfer vom eMSP zum CPO auslöst.

[477] Notwendige manipulationssichere Sensorik wird bspw. im Rahmen des Bundesministeriums für Wirtschaft und Energie geförderten Projekts SecMobil (weiter-)entwickelt.
[478] Vgl. Abschnitt 5.2.5.1.
[479] Vgl. Kapitel 8.1.1.

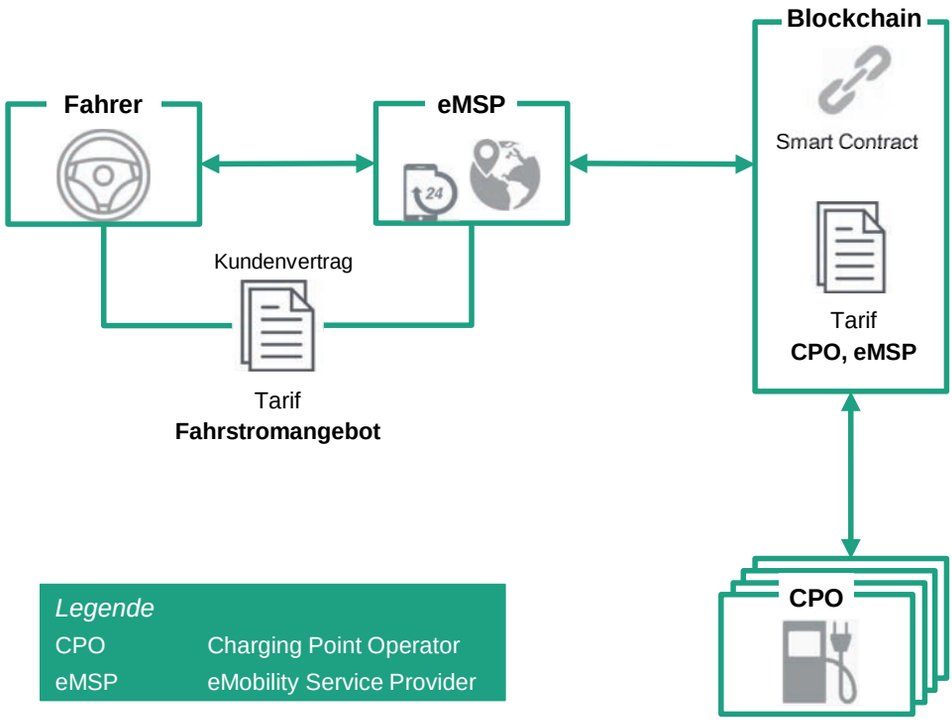


Abbildung 31: Das Zusammenspiel der Rollen mit DLT

8.1.4 Prozessbeschreibung

Authentifizierung und Autorisierung: Bereits im Vorfeld, z. B. bei der Routenplanung, hat der E-Fahrzeugfahrer sich über die Konditionen der Ladeinfrastruktur informiert bzw. etwa durch das In-Car-Entertainmentsystem informieren lassen und entsprechend eine Ladestation ausgewählt. Denkbar ist ebenfalls, dass es vor- oder benutzerdefinierte Profile im E-Fahrzeug gibt, das die Ladepräferenzen enthält. Nach Anschluss des E-Fahrzeugs an die Ladesäule erhält es die Ladesäulen-ID direkt vom CPO, z. B. über die durch das Plug & Charge[480]-Protokoll festgelegten Kommunikationsregeln[481]. Diese Kommunikation wird über einen direkten Kanal – also off-Chain – geführt, da Eigenschaften wie Geschwindigkeit im Vordergrund stehen und fehlendes Vertrauen bisher an dieser Stelle nicht als Hemmnis identifiziert worden ist. Mit den erhaltenen Informationen meldet sich das E-Fahrzeug bei seinem eMSP, welcher die Konditionen für die Kombination Fahrer und Ladesäule (und damit CPO) überprüft und im positiven Fall autorisiert. Damit können die Konditionen zum Starten des Ladevorgangs leicht nochmals überprüft und akzeptiert bzw. abgelehnt werden. Durch einen Knopfdruck auf einem Bildschirm des In-Car-Entertainmentsystems kann die entsprechende Anfrage initiiert bzw. eine Willenserklärung ausgedrückt werden.

Dokumentation und Nachhaltung: Im Rahmen der Dokumentation wird bereits vor dem eigentlichen Ladevorgang spezifiziert, welche Vereinbarungen getroffen wurden. Dazu zählen die Konditionen des bevorstehenden Ladevorgangs wie etwa Tarifstruktur sowie die Signaturen der Vertragsparteien. A posteriori werden dann die gemessenen Leis-

[480] Plug & Charge erlaubt, dass das E-Fahrzeug sich selbst authentisieren kann (ohne Lade-App oder Ladekarte an der Ladesäule).
[481] Etwa im Rahmen der ISO 15118.

tungsparameter des Ladevorgangs sowie abermals die Signaturen notiert. Es zu anzumerken, dass eine Aufteilung des Ladevorgangs in Abschnitte möglich ist, in denen sich dieses Prozedere wiederholt. Dies erhöht die Dokumentationskraft. In diesen Fällen ist es allerdings angezeigt, insbesondere Skalierbarkeit und Transaktionskosten in die Überlegungen einzubeziehen. So kann durch die manipulationssichere Ablage des CDR im DLT das notwendige Vertrauen zwischen zwei Parteien (CPO, MSP) erzielt werden, ohne dass dafür notwendigerweise ein C&R-Dienst zur Vertrauensinstanz avancieren müsste.

Abrechnung und Werttransfer: Zum Zwecke des Zahlungsausgleichs wird a priori eine Anzahlung[482] des eMSPs im Rahmen eines Treuhand-Smart-Contracts[483] ausgeführt, damit der CPO sicher sein kann, dass der eMSP über Token für die Bezahlung verfügt und diese danach initiiert. Die Token[484] beider Parteien werden als Teil des Transaktionsprozesses auf dem Treuhand-Smart-Contract gespeichert zurückgehalten, bis die Transaktion abgeschlossen ist. Der Energietransfer läuft nach üblichen Open-Charge-Point-Protocol (OCPP)-Spezifikationen ab. Im Anschluss schreibt der CPO das CDR, das idealerweise auf Daten manipulationssicherer Sensorik basiert, zusammen mit dem temporären Pseudonym des Fahrers und der eMSP-ID als Beleg in die DL. Dies quittierend werden die Token aus dem Treuhand-Smart-Contract an das CPO-Wallet transferiert. A posteriori wird das eigentliche Clearing vorgenommen, das den Zahlungsausgleich durchführt – d. h., die übrigen Token wieder an den eMSP zurückgibt. Analog zu den zentralen C&R-Diensten ist der (automatisierte) Zahlungsausgleich eine Zusatzdienstleistung.

Dem E-Fahrzeugfahrer, der eine Vertragsbeziehung im Allgemeinen nur zum eMSP unterhält, wird der Ladevorgang am Ende des Monats in Rechnung gestellt.

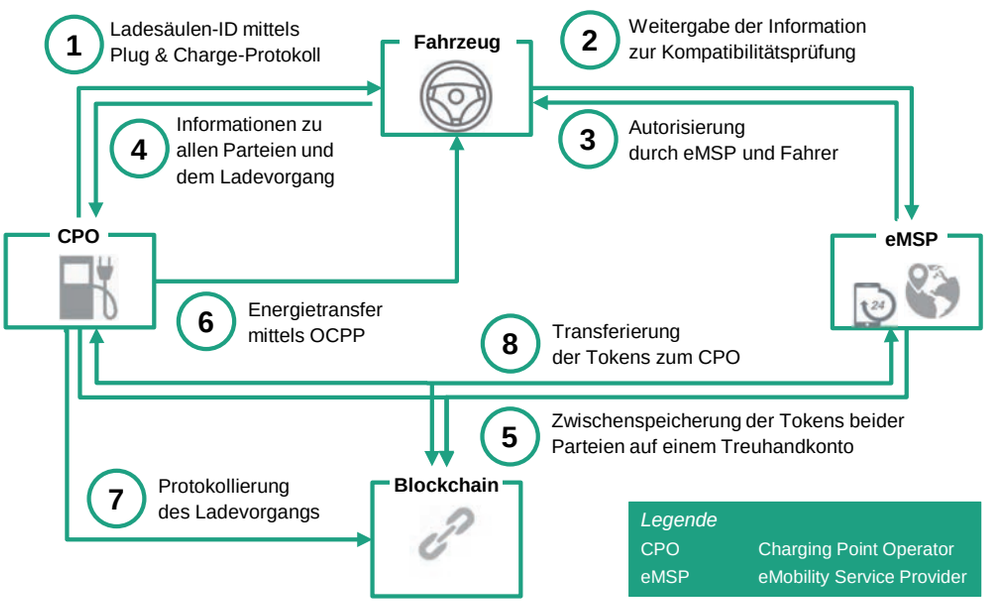


Abbildung 32: Schematische Ablaufbeschreibung einer DLT-basierten Realisierung

[482] Wir nehmen vereinfachend an, dass immer ein Maximalbetrag (z. B. 60 Euro wie bei chargeNow) angezahlt wird, sodass der eMSP nie am Ende des Ladevorgangs zusätzliche Token übermitteln muss.

[483] Siehe allgemeiner technischer Teil.

[484] Die konkrete Ausgestaltung der Tokenart (vgl. Kapitel 5.2.5.6) kann pauschal nicht getroffen werden bzw. ist für den Abstraktionsgrad, der für diesen Anwendungsfall getroffen worden ist, irrelevant.

8.1.5 Fazit und Handlungsempfehlungen

Die hier im Anwendungsfall untersuchte Verwendung von DLT stellt ein Einsatzszenario dar, in dem die DLT eine Disintermediation durchführt, nachdem heutige C&R-Anbieter eine typische Intermediärsfunktion im Sinne einer Superplattform im Elektromobilitäts-wertschöpfungsnetz wahrnehmen. Der Einsatz des hier skizzierten Vorgehens deutet darauf hin, dass technisch-konzeptionelle Lösungen möglich sind und dass dadurch entsprechend dem Anwendungsmuster der neutralen Plattform eine Machtkonzentration erschwert werden könnte. Es bleibt jedoch sehr fraglich, ob eine DLT-basierte Lösung, die ausschließlich die bestehenden Funktionalitäten nachbildet, signifikante Marktanteile erzielen kann, nachdem insbesondere in Deutschland bereits sehr etablierte Marktakteure den Markt weitestgehend definieren und CPOs zudem daran selbst mit Unternehmensanteilen beteiligt sind. Diese C&R-Dienste profitieren von Netzwerkeffekten bereits erheblich. Über Standardschnittstellen verfügen große CPOs über Zugang zu in der Regel allen relevanten C&R-Diensten gleichzeitig. Des Weiteren entwickeln sich die C&R-Dienste und deren Protokolle mit erheblichem Tempo weiter. Ob Preise für Roaming durch die DLT-basierte Lösung sinken können bzw. werden, ist offen. Für eine genaue Einschätzung dieses Effekts bedarf es einer detaillierteren Analyse, als dies im Rahmen dieses Anwendungsfallbeispiels möglich ist. Die hier skizzierte DLT-Lösung würde sich so in ein vergleichsweise kompetitives Umfeld einfügen. Versteht man die DLT-Lösung als Plattform, auf der Mehrwertdienste abgewickelt werden, zeichnet sich ein neues Bild. Denn dann agiert die DLT-Lösung auf einem noch nicht verteilten Markt und kann sich leichter als neutrale Plattform etablieren. Solche Mehrwertdienste können sein: Die erwähnten Grün- und Lokalstromzertifikate, das Aufteilen der Ladeleistung über mehrere E-Fahrzeuge im Rahmen von Smart Charging und/oder das Peer-to-Peer-Laden zu Hause.

Verbraucherschutzportale

Bürgern ist voraussichtlich aufgrund der komplexen Natur der DLT nicht zuzumuten, jedes Detail der Technologie zu verstehen. Dennoch ist ein weitreichendes Grundverständnis in der Bevölkerung wichtig, da die DLT als digitale Infrastrukturtechnologie potenziell - zumindest indirekt - zukünftig durch viele Bürger genutzt wird. Ein Verständnis der Implikationen (Manipulationssicherheit etc.) ist deshalb von hoher Wichtigkeit. Zudem kann ein gesellschaftliches Misstrauen bzw. eine grundsätzliche Skepsis gegenüber der DLT ein Hemmnis in der Innovationsdiffusion darstellen. Es ist eruieren, ob für DLT gemeinsam mit Verbraucherschutzportalen und Instanzen wie dem TÜV ein weitreichendes Technologieverständnis und -akzeptanz im privaten Bereich hergestellt werden kann.

8.2 Rechtlicher Teil

Die vorstehende umfangreiche ökonomisch-technische Analyse des Status quo in Kapitel 8.1.2 konnte aufzeigen, dass heutzutage elektrisches Laden nur unter Beteiligung vieler Akteure möglich ist. Nachfolgend gilt es die dafür erforderlichen Vertragsbeziehungen rechtlich einzuordnen und noch weiter zu konkretisieren. Der Einsatz von DLT könnte die Anzahl der Vertragsbeziehungen reduzieren, führt aber zu datenschutzrechtlichen Herausforderungen, weshalb auf diese ebenfalls nachfolgend eingegangen werden soll.

8.2.1 Vertragsbeziehungen

Aus § 4 der Ladesäulenverordnung (LSV) lässt sich ableiten, dass sich die Vertragsbeziehungen abhängig von der zu wählenden Bezahlmethode unterscheiden lassen (so auch

bereits 8.1.1). Die LSV des Bundeswirtschaftsministeriums[485] setzt die EU-Richtlinie 2014/94/EU über den Aufbau der Infrastruktur für alternative Kraftstoffe um, deren Zielsetzung der Ausbau der Ladeinfrastruktur ist.[486] Der Gesetzgeber setzte zunächst nur die technischen Vereinheitlichungsvorgaben der Richtlinie um (Ladesäulenverordnung I) und ergänzte diese später u. a. um die ebenfalls umzusetzenden Aspekte Authentifizierung und Bezahlung (Ladesäulenverordnung II).[487] Gewährt der Betreiber eines Ladepunkts den Nutzern ohne Authentifizierung gemäß § 4 Nr. 1 lit. a) LSV das Laden ohne Gegenleistung oder gemäß § 4 Nr. 1 lit. b) LSV gegen Barzahlung, so liegt im ersteren Falle meist eine Schenkung i. S. d. § 516 BGB und im letzteren Falle ein Kaufvertrag über elektrische Energie, §§ 453 Abs. 1, 433 BGB[488] vor. Letzteres gilt auch im Falle der kartenbasierten bzw. Web-basierten Bezahlung, die jeweils aber gemäß § 4 Nr. 2 LSV eine Authentifizierung erfordern.

Vorliegend interessiert statt des soeben geschilderten punktuellen Ladens[489] das sogenannte Roaming. Dieses soll das anbieterübergreifende Laden ermöglichen.[490] Wie im Bereich des Mobilfunks muss hierfür jeder Endkunde einen sogenannten „Fahrstromvertrag (Dauerschuldverhältnis)“[491] mit einem eMSP schließen (vgl. Abbildung 30). Der Fahrstromvertrag ähnelt klassischen Stromlieferverträgen, da es auf die Zweckbestimmung der Verwendung der geladenen elektrischen Energie, wie hier zu Zwecken der Mobilität, nicht ankommt.[492] Folglich ist er gemäß §§ 453 Abs. 1, 433 BGB im Kern ein Kaufvertrag über die Ware Strom, unterscheidet sich aber von klassischen Stromlieferverträgen durch die vermittelte Berechtigung zur Nutzung der Ladeinfrastruktur.[493] Um das anbieterübergreifende Laden zu ermöglichen, schließen die R&C bilaterale Roaming-Verträge mit einzelnen eMSPs und einzelnen CPOs (vgl. Abbildung 30). Gegenstand dieser bilateralen Roaming-Verträge ist insbesondere, dass mit ihrem Abschluss auch eigenständige multilaterale (Ladenetzwerk-)Verträge zwischen allen beteiligten eMSPs und CPOs zustande kommen (vgl. Abbildung 30).[494] Dies ist erforderlich, da zwischen einem Endkunden, der am Roaming teilnimmt, und einem CPO kein eigenständiger Vertrag zustande kommt.[495] Lädt der Endkunde sein Elektromobil, so stellt sich dies demnach vertragsrechtlich als Nutzungsvorgang des eMSP beim jeweilig dem Endkunden uneingeschränkten Zugang gewährenden CPO dar.[496]

Der eMSP sieht sich in der vorstehenden Konstellation dem Preisrisiko ausgesetzt. Mit seinem Kunden mag er etwa eine Flatrate vereinbart haben, gegenüber einem am Roaming teilnehmenden CPO muss er aber womöglich pro Kilowattstunde oder Ladevorgang abrechnen. Vergleichbar den herkömmlichen Tankvereinbarungen bei Flottenleasingfahrzeugen besteht daher ein Anreiz für eMSPs, Sondervereinbarungen mit CPOs zu schließen, um ihr Geschäft kalkulieren zu können.[497]

[485] § 49 Abs. 4 Ss. 1 Nr. 1 bis 4 des EnWG.
[486] Richtlinie 2014/94/EU, Erwg. 23.
[487] *Lehner,* RAW 2018, 17 (18).
[488] Graf von Westphalen/*Schöne*,37. EL. Okt. 2015, Stromlieferverträge Rn. 369.
[489] § 4 LSV.
[490] *Overkamp/Schings,* EnWZ 2019, 3.
[491] *Overkamp/Schings,* EnWZ 2019, 3 (7).
[492] Graf von Westphalen/*Schöne*, 37. EL. Okt. 2015, Stromlieferverträge Rn. 369.
[493] Graf von Westphalen/*Schöne*, 37. EL. Okt. 2015, Stromlieferverträge Rn. 368.
[494] *Hahn/Grün,* IR 2013, 293 (295).
[495] *Hahn/Grün,* IR 2013, 293 (294).
[496] *Hahn/Grün,* IR 2013, 293 (294).
[497] *Hahn/Grün,* IR 2013, 293 (295).

Die Organisation des Roamings erfordert heutzutage – wie aufgezeigt – eine Vielzahl an Verträgen. Perspektivisch könnte DLT durch die Reduktion der Beteiligten, insbesondere durch die Substitution von R&Cs, zu einer verringerten Komplexität beitragen. Mittelfristig können auf einer DLT-Plattform gespeicherte und in den Vergütungsvereinbarungen vereinbarte Smart Contracts aber bereits die Bezahlung von Ladezyklen mittels Token automatisieren.[498]

8.2.2 Datenschutz bei EV-Ladeinfrastrukturen über die Blockchain

Im Rahmen des Zahlungsvorgangs für die Nutzung der Ladeinfrastruktur können personenbezogene Daten der Nutzer des Systems verarbeitet werden. Die datenschutzrechtliche Relevanz der Datenverarbeitungen hängt davon ab, ob es sich bei der Information über Nutzer des Systems auch um Informationen über natürliche Personen handelt. Bei den Nutzern des Systems muss danach differenziert werden, ob es sich um ein E-Roaming-Verfahren oder ein Verfahren mit direkter Bezahlung zwischen Fahrer und CPO handelt. Beim E-Roaming ist weiter entscheidend, ob durch Kenntnis von eMSP und CPO auch Informationen über die dahinterstehenden natürlichen Personen bekannt werden.

8.2.2.1 Datenschutz beim E-Roaming, wenn keine Informationen über die hinter eMSP und CPO stehenden natürlichen Personen erlangt werden können

Im Falle des E-Roamings ist generell vorgesehen, die Transaktionen auf der Blockchain-Ebene allein durch eine B2B-Lösung zwischen dem eMSP und dem CPO abzuwickeln. Der Fahrer wird gegenüber dem CPO zur Einleitung des Ladevorgangs aktiv. Dabei kann auch eine Authentifizierung des Fahrers erfolgen. Die für die Zahlungsabwicklung zwischen eMSP und CPO notwendigen Transaktionen werden auf der Blockchain durchgeführt. Diese Transaktionen inkludieren jedoch keine Informationen über den einzelnen Fahrer. Eine datenschutzrechtliche Problematik entsteht lediglich, wenn es sich bei eMSP und CPO um Unternehmen handelt, bei denen die Kenntnis vom Unternehmen auch Informationen über die dahinterstehenden natürlichen Personen offenbart.[499] Ist dies nicht der Fall, so sind die On-Chain-Verarbeitungen datenschutzrechtlich nicht relevant.

8.2.2.2 Datenschutz bei direkter Bezahlmethode und beim E-Roaming, wenn Informationen über die hinter eMSP und CPO stehenden natürlichen Personen erlangt werden können

Soll der Endkunde in einem eigenen Bezahlverfahren unmittelbar mit dem CPO die Transaktion auf der Blockchain abwickeln, so ist de lege lata eine der im Grundlagenteil erläuterten Lösungsmodelle zu wählen. Einer solchen Lösung bedarf es auch dann, wenn die Blockchain allein zwischen eMSP und CPO geführt wird, es sich jedoch bei eMSP oder CPO um kleine Unternehmen handelt, bei denen die dahinterstehenden Personen erkennbar werden. Dies kann insbesondere für die CPOs zutreffen. Handelt es sich bei diesen bspw. um Einzelpersonen und ist der Schlüssel zwischen Nutzerkennung und CPO bekannt, so handelt es sich bei den mit der Nutzerkennung des betroffenen CPO verbundenen Informationen um personenbezogene Daten. Hier sind entsprechende Lösungsansätze zu wählen, um den Vorgaben des Datenschutzrechts zu genügen.

Eine „offene Lösung“[500] würde erfordern, dass alle am System Beteiligten an allen Informationen ein berechtigtes Interesse aufweisen. An den Zahlungsvorgängen beim Betrieb

[498] In der Praxis weist bereits heute der Ladesäulenbetreiber Ionity, ein Zusammenschluss von BMW, Daimler, Ford und VW auf seiner Webseite Token als Bezahlmöglichkeit aus: https://ionity.eu/de/wo-und-wie.html.
[499] Siehe hierzu bereits die Ausführungen unter 6.2.2.2.1.1.1.
[500] Siehe zur „offenen Lösung“ bereits unter 6.2.3.4.2.1.

einer EV-Ladeinfrastruktur haben jedoch stets nur die beteiligten Parteien des Ladevorgangs ein Interesse. Eine Einsicht aller Aktivitäten durch alle am System Beteiligten ist demgemäß nicht datenschutzkonform. Die „offene Lösung" ist folglich hier nicht umsetzbar.

Möglich erscheint aber hingegen grundsätzlich eine „zentrale Lösung"[501]. Bei dieser müsste durch eine Zentralstelle eine permissioned Blockchain betrieben werden. Über ein Rechte- und Rollen-System kann von der Zentralstelle gesteuert werden, welche Informationen für die einzelnen Teilnehmer sichtbar sind. Die Zentralstelle wäre somit datenschutzrechtlich Verantwortliche für die On-Chain-Verarbeitungen. Als Rechtsgrundlage für die Verarbeitung kommt dann ein zwischen den Teilnehmern und der Zentralstelle geschlossener Vertrag in Betracht.[502] Die Zentralstelle muss über geeignete Löschkonzepte verfügen. Diesbezüglich kommen eine „Redactable Blockchain"[503], bei der nachträglich durch die Zentralstelle Änderungen eingebracht werden können, oder Forks[504], bei denen die Nodes dazu verpflichtet werden, ungewünschte Daten aus der dezentralen Datenbank zu löschen, in Betracht.

Ist eine „zentrale Lösung" nicht möglich oder nicht gewünscht, kann ebenfalls eine „Anonymisierungslösung"[505] gewählt werden. Im Falle des E-Roamings ist hier grundsätzlich eine Off-Chain-Saldierung möglich.[506] Die beteiligten eMSP und CPO tragen nicht jede Transaktion in die Blockchain, sondern führen off-Chain ein jeweils separates Kontobuch. Die fälligen Ausgleichszahlungen werden dann zwischen den Beteiligten in regelmäßigen Zeitabständen on-Chain ausgeführt. Dabei sollten bei den Ausgleichszahlungen keine Muster erkennbar werden, die auf die Identität des hinter einer Nutzerkennung stehenden CPO oder eMSP schließen lassen.

In Betracht kommen daneben technische Anonymisierungslösungen, wie bspw. Zero-Knowledge-Proofs[507] oder Einsatz von Stealth-Adressen in Kombination mit Ring-Signaturen[508]. Bei einer Anonymisierung finden on-Chain keine datenschutzrechtlich relevanten Datenverarbeitungen mehr statt. Folglich ist hierfür auch keine Rechtsgrundlage erforderlich. Eine Löschung ist ebenfalls nicht nötig.

8.2.3 Fazit und Handlungsempfehlungen

Elektrisches Laden bietet insbesondere im Bereich des Roamings Einsatzraum für DLT. Ihr Einsatz kann mittelfristig zur Bezahlung von Ladezyklen mittels Token führen und langfristig möglicherweise zu einer Reduktion der Beteiligten, was auch die Vielzahl heutiger Verträge reduzieren dürfte. Perspektivisch gilt es im Blick zu behalten, dass es nicht nur elektrisches Laden, sondern auch Entladen gibt. Elektromobile eignen sich auch als Energiespeicher etwa in einem Microgrid. Insoweit stellen sich aus rechtlicher Perspektive weniger DLT-spezifische Fragen als vielmehr energierechtliche Hürden.[509] Letztere sind aber nicht Teil des hier zugrunde liegenden Begutachtungsauftrags.

[501] Siehe zur „zentralen Lösung" bereits die Ausführungen unter 6.2.3.4.1.
[502] Siehe zu den Rechtsgrundlagen bei Wahl der zentralen Lösung bereits unter 6.2.4.2.2.
[503] Siehe zur Redactable Blockchain bereits unter 6.2.5.2.1.
[504] Siehe zu Forks bereits unter 6.2.5.2.2 und 4.4.3.
[505] Siehe zur „Anonymisierungslösung" bereits unter 6.2.3.4.2.2.2.4.
[506] Zur Saldierung bereits allgemein unter 6.2.3.4.2.2.2.2.
[507] Zu Zero-Knowledge-Proofs siehe bereits unter 6.2.3.4.2.2.2.3 und 5.1.3.
[508] Zu Stealth-Adressen in Kombination mit Ring-Signaturen bereits unter 6.2.3.4.2.2.2.4.
[509] Einführend etwa: *Scholtka/Kneuper,* IR 2019, 17; *Overkamp/Schings,* EnWZ 2019, 3.

Wird ein E-Roaming-Verfahren über eine DLT-Plattform abgewickelt, so ist diese datenschutzrechtlich zulässig, soweit die natürlichen Personen hinter den beteiligten eMSPs und CPOs nicht identifizierbar werden. Anpassungsbedarf besteht hingegen dann, wenn es sich bei eMSP oder CPO um Unternehmen handelt, bei denen Informationen über Transaktionen dieser Unternehmen auch Informationen über die hinter den Unternehmen stehenden natürlichen Personen offenbaren. Gleiches gilt, wenn statt eines E-Roaming-Verfahrens ein Verfahren mit direkter Bezahlung zwischen Fahrer und CPO eingesetzt werden soll.

Umfang des elektrischen Ladens

Perspektivisch gilt es nicht nur das DLT-basierte Laden, sondern auch das Entladen, d.h. die Einbeziehung der Elektromobile in Stromnetze (bspw. Microgrids) zu fördern. Hierfür bedarf es zunächst der Lösung energierechtlicher Herausforderungen.

9 Ridesharing

9.1 Ökonomisch-technischer Teil

9.1.1 Definition und Beschreibung des Anwendungsbeispiels

Um mobil zu sein, greifen Verbraucher vermehrt auf gemeinsam genutzte Transportmittel zurück, anstatt diese allein zu nutzen. So können potenziell Kosten eingespart sowie Ressourcen und damit die Umwelt geschont werden. Während öffentliche Transportmittel, bspw. Busse, U-Bahnen oder Züge, festgelegte Fahrtrouten und Zeitpläne aufweisen, verspricht die geteilte Nutzung von Kraftfahrzeugen erhöhte Flexibilität. Diese geteilte Nutzung geht oft mit erhöhtem Komfort und kürzeren Reisezeiten einher. Dies gilt insbesondere für den ländlichen Raum, wo ein regelmäßiges und flächendeckendes Angebot an öffentlichen Verkehrsmitteln schwierig zu generieren ist.

Ridesharing selbst bezeichnet in diesem Kontext die geteilte Nutzung eines Fahrzeugs durch mehrere Personen mit ähnlichen Reiseanforderungen, wobei etwaige entstehende Kosten in der Regel aufgeteilt werden.[510] Für den Zweck dieses Gutachtens ist es unerheblich, ob die fahrende Person die Fahrt zum eigenen Transport (Peer-to-peer) oder zu Erwerbszwecken (kommerziell) durchführt.

In den Regionen Europa, USA und China wird das jährliche Wachstum des gesamten Markts für geteilte Mobilität bis 2030 auf 15 bis 28 Prozent geschätzt.[511] Während in den USA und in China monopolistische Anbieter jeweils mehr als 80 Prozent des dortigen Markts beherrschen, ist die Fragmentierung in Europa aktuell aufgrund regulatorischer Bestimmung höher[511]. Eine Expertenbefragung des Deutschen Zentrums für Luft- und Raumfahrt hat ergeben, dass Modelle zur geteilten Nutzung von Kraftfahrzeugen bislang in Deutschland wenig bekannt sind. Es wird jedoch erwartet, dass diese Mobilitätsformen in einigen bestimmten Kontexten, insbesondere nicht in Kernstädten und hauptsächlich bei jüngeren Personen, zukünftig an Bedeutung gewinnen.[512]

Die Verbreitung geteilter Mobilitätsangebote hängt eng mit der fortschreitenden Digitalisierung zusammen. Für die skalierbare Echtzeit-Koordination von Transportangeboten und -nachfrage sind digitale Plattformen notwendig, die erst mit der hohen Verfügbarkeit des Internets und moderner Informations- und Telekommunikationstechnologie umsetzbar geworden sind.[513] Generell sind digitale Plattformen als Unternehmungen in zwei- oder mehrseitigen Märkten anzusehen, die das Internet nutzen, um Interaktionen zwischen zwei oder mehr differierenden, aber dabei voneinander abhängigen Nutzergruppen zu ermöglichen.[514] Dabei soll für mindestens eine der Nutzergruppen Mehrwert geschaffen werden[514]. Konkret bedeutet das, dass digitale Mobilitätsplattformen Anbieter und Nachfrager von Mobilitätsangeboten dynamisch zusammenführen. Das Bundesministerium für Wirtschaft und Energie führt diesbezüglich aus, dass digitale Plattformen auch als Intermediäre bezeichnet werden können, die durch digitalisierte Informationen auf vernetzten Geräten Suchvorgänge vereinfachen und Vergleichskosten reduzieren[515].

[510] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28..
[511] *Grosse-Ophoff/Hausler/Heineke/Möller*, How shared mobility will change the automotive industry.
[512] *Heinrichs/Thomaier/Parzonka*, Arbeitsberichte zur Verkehrsforschung: Ko-Automobilität.
[513] *Cohen/Kietzmann,* Organization & Environment 2014, 279.
[514] *European Commission*, Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.
[515] *Bundesministerium für Wirtschaft und Energie* (BMWi), Grünbuch Digitale Plattformen.

Im Kontext des Ridesharings existieren sowohl digitale Plattformen, die als Unternehmen selbst Fahrten anbieten bzw. Fahrer unter Vertrag haben, als auch solche, die lediglich die Sammlung und Koordination von Angebot und Nachfrage übernehmen[516]. Bei beiden Typen gibt es in der Regel pro Fahrt immer einen Fahrtanbieter sowie einen bis mehrere Mitfahrer.

In der Praxis haben sich drei Modelle für Ridesharing-Plattformen durchgesetzt, die sich anhand zeitlicher Aspekte der gelisteten Angebote unterscheiden[517]. Die beiden zuerst genannten Formen sind dabei in Bezug auf den Aufbau der Plattform sehr ähnlich.

- *Mitfahrgelegenheits-Angebote*: An erster Stelle stehen Plattformen, auf denen ein Fahrtanbieter sein Angebot bereits mit großem zeitlichem Vorlauf auf der Plattform listet. In diesem Szenario können interessierte Mitfahrer das Angebot über die digitale Plattform buchen.
- *Regelmäßige Pendler-Angebote*: Zudem existieren Modelle, bei denen ein Fahrtanbieter ein wiederkehrendes Angebot, bspw. für regelmäßige Fahrten zu seiner Arbeitsstätte, listet. Dieses Angebot kann dann wiederum durch Mitfahrer gebucht werden, wobei in der Regel nur der Initialkontakt über die Ridesharing-Plattform hergestellt wird.
- *Ad-hoc-Ridesharing*: Darüber hinaus gibt es Plattformen, die dynamisches Ad-hoc-Ridesharing anbieten. Hierbei werden Fahrer und potenzielle Mitfahrer unmittelbar und spontan auf der digitalen Plattform zusammengebracht, wobei Letztere sich in der Regel über mobile Endgeräte mit Fahrtgesuchen an die digitale Plattform wenden. Insbesondere dieses Modell hat in den vergangenen Jahren vermehrt an Nutzern gewonnen und von der Verbreitung mobiler Endgeräte sowie mobiler Internetverbindungen profitiert. In der Praxis decken die meisten digitalen Plattformen für Ridesharing mehrere Modelle ab.[517]

9.1.2 Status quo und Herausforderungen

Die Personenbeförderungsbranche in Deutschland steht aktuell im Zwiespalt zwischen der traditionell stark regulierten und genossenschaftlich organisierten Taxibranche sowie neuen digitalen Mobilitätsplattformen, die Gelegenheiten zum Ridesharing anbieten. Durch höhere Auslastungen der Fahrzeuge und Fahrtangebote, die durch Privatpersonen günstig angeboten werden, erreichen Ridesharing-Anbieter teilweise niedrigere Preise als reguläre Taxianbieter. Durch die verstärkte Konkurrenzsituation auf dem Markt ergeben sich für Verbraucher laut einer Studie[518] zunächst monetäre Vorteile. Durch diese ökonomischen Anreize sowie wachsende / steigende Flexibilität bei der Auswahl des Transportmittels ergibt sich insgesamt eine hohe Nachfrage nach Ridesharing-Diensten. Darüber hinaus entstehen aus gesellschaftlicher Sicht möglicherweise weitere positive Externalitäten wie verringerte Emissionen und ein niedrigeres Gesamtverkehrsaufkommen.[519] Demgegenüber stehen jedoch einige Herausforderungen, die bislang noch ungelöst sind[520] und neue Denkansätze erfordern.

1. *Monopolbildung*
   Bei Ridesharing-Plattformen steigt der Nutzen aufgrund sogenannter Netzwerkeffekte für alle Beteiligten, je mehr Teilnehmer es sowohl auf der Anbieter- als

[516] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.
[517] *Andersson/Hjalmarsson/Avital,* The 34th International Conference on Information Systems. ICIS 2013, 1.
[518] *Haucap/Pavel/Aigner/Arnold* et al., List Forum für Wirtschafts- und Finanzpolitik 2017, 139.
[519] *Hahn/Metcalfe*, The Ridesharing Revolution: Economic Survey and Synthesis.
[520] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.

auch auf der Nachfragerseite gibt.[521] Somit entsteht die Gefahr der Monopolbildung, da sich die gesamte Marktkoordination auf natürliche Weise auf wenige Plattformanbieter konzentriert.[522] Während zunächst verschiedene Anbieter fragmentiert existieren, bildet sich ein Marktführer als marktbeherrschende Plattform heraus. In der Folge können konkurrierende Ridesharing-Anbieter durch die Monopolisten aufgrund ihrer Markmacht vom Zugang zu Kunden und folglich aus dem Markt ausgeschlossen werden.[521] Als Konsequenz können die monopolistischen Plattformen die Preise für Ridesharing-Angebote dann nahezu beliebig gestalten und beeinflussen. Zusätzlich entstehen seitens der Plattformanbieter durch den alleinigen Besitz der Nutzerdaten isolierte Datensilos. Diese erhöhen zusätzlich die Vormachtstellung der Anbieter und erschweren es neuen Wettbewerbern, in den Markt einzutreten.[522] Insgesamt bestehen langfristig also Gefahren für den freien Wettbewerb und daraus resultierende Nachteile für Endkunden.

2. *Identitätsmanagement und Schaffen von Vertrauen*

Auf der operativen Ebene bestehen beim Ridesharing zudem Probleme in Bezug auf das Identitätsmanagement und das Vermitteln von Vertrauen zwischen den involvierten Parteien. Eine zentrale Herausforderung ist es bspw., das für die Fahrt erforderliche Vertrauen zwischen den sich gegenseitig meist unbekannten Reisenden herzustellen. Mitreisende Fahrgäste sind bspw. daran interessiert, ob der Fahrer eine gültige Fahrerlaubnis besitzt oder die Leistung in der Regel ordnungsgemäß erbracht wird. Zu diesem Zweck müssen Plattformnutzer zumeist eine Vielzahl an Informationen gegenüber zentralen Parteien wie dem Plattformbetreiber oder Verifizierungsstellen offenlegen. Diese umfassen oft für den Vorgang unerhebliche Informationen, wie Angaben zum Wohnort oder über das Geburtsdatum.

Zudem muss gewährleistet werden, dass nur für tatsächlich und wie vereinbart stattgefundene Dienstleistungen bezahlt wird, um Betrug zu vermeiden.[523] Es muss also Vertrauen hinsichtlich der Zahlungsbereitschaft der einzelnen im Prozess beteiligten Parteien geschaffen werden. Häufig werden hierzu sogenannte Reputationssysteme genutzt, die jedoch diverse Schwachstellen aufweisen. Als kritischster Aspekt wird hierbei die Frage angesehen, wie man Nutzer dazu anreizt, Reputationsinformationen tatsächlich wahrheitsgemäß zu berichten.[524] Um die Zahlung für adäquat erhaltene Fahrdienstleistungen verlässlich zu gewährleisten, werden außerdem Treuhanddienstleistungen genutzt. Hierbei wird ein Geldbetrag für die Fahrtleistung von Drittanbietern eingefroren und erst nach Bestätigung des Erhalts der nachweislich angemessen erbrachten Dienstleistung

[521] *Alstyne/Eisenmann/Parker,* Harvard business review 2006, 92.

[522] *Bundesministerium für Wirtschaft und Energie* (BMWi), Grünbuch Digitale Plattformen..

[523] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.

[524] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.

ausgeschüttet.[525] Die Leistungen der Drittanbieter implizieren wiederum eine Informationsweitergabe an eine weitere Partei sowie zusätzlichen Prozessaufwand und gegebenenfalls Gebühren.
Durch die Notwendigkeit, für jeden verfügbaren Plattformdienst einen eigenen Account anlegen zu müssen, werden außerdem Anbieterwechsel und die Einbindung anderer, gegebenenfalls anbieterübergreifender Services, erschwert. Dieser Umstand verstärkt die zuvor erläuterte Monopolproblematik zusätzlich.

3. *Zahlungsabwicklungen*
Ein weiterer kritischer Aspekt aktueller Ridesharing-Plattformen betrifft die Zahlungsabwicklung für die erhaltenen Fahrtdienstleistungen. Dahingehend lassen sich in der Praxis zwei vorherrschende Alternativen unterscheiden: Einerseits direkte (Bar-)Zahlungen der Fahrgäste an den Fahrer und andererseits die Zahlungsabwicklung über eine dritte Partei, wie bspw. Online-Zahlungsdienstleister.[526] Bei bilateralen Barzahlungen bestehen die Risiken, dass Mitfahrer keinen passenden oder ausreichenden Geldbetrag bei sich haben oder die Fahrt insgesamt nicht antreten, während dem Fahrer nichtsdestotrotz Kosten entstehen.[527] Zudem kann in der Praxis im Falle eines Disputs nicht realistisch nachgeprüft werden, ob eine Barzahlung tatsächlich stattgefunden hat. Die Zahlungsabwicklung über Drittanbieter wiederum impliziert Transaktionskosten, welche die Gesamtkosten für Anbieter und Verbraucher erhöhen.[528] Zusätzlich werden so die Daten über die Transaktion nochmals an eine weitere involvierte Partei geleitet. Diese Zahlungsweise wird in der Regel bei Ad-hoc-Ridesharing-Plattformen verwendet.[529] Werden, wie unter Punkt 2 beschrieben, Treuhanddienstleistungen verwendet, entsteht ein zusätzlicher Prozessaufwand.

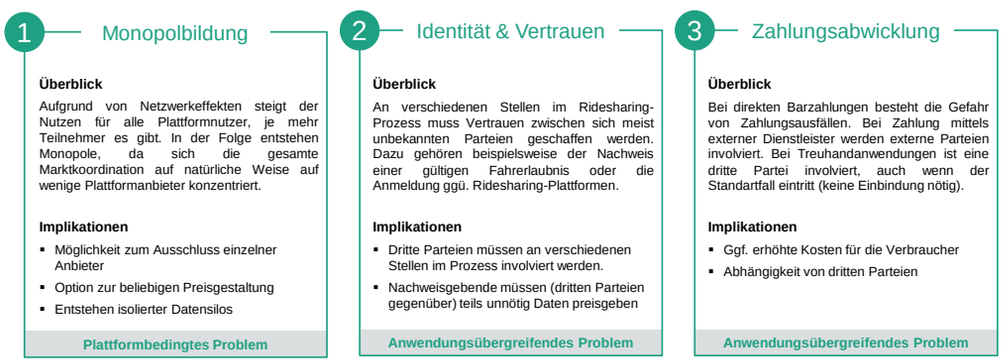


Abbildung 33: Zusammenfassung der Probleme des Status quo

Um die angedeuteten Herausforderungen zu adressieren, besteht zusammenfassend ein Bedarf an neuartigen Ansätzen zur Gestaltung von Ridesharing-Plattformen. Für die Lösung der Monopolproblematik scheint eine offene Plattformlösung erstrebenswert, die keine Anbieter und Nachfrager vom Markt ausschließt. Zudem besteht ein Bedarf an Alternativentwürfen zu aktuellen Mechanismen, um Sicherheit und Vertrauen zwischen den Reisenden zu schaffen. Dabei ist insbesondere ein anbieterübergreifendes Identitätsmanagement notwendig, das eine selektive Informationsweitergabe ermöglicht. Zuletzt

[525] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28
[526] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.
[527] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.
[528] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.
[529] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.

sollten alternative Möglichkeiten für die effiziente und sichere Zahlungsabwicklung zwischen Fahrtanbietern und Mitfahrern evaluiert werden.

9.1.3 Mögliche Lösungsansätze und Rolle von DLT

1. *Monopolbildung*

   Um Mehrwert für die Nutzer zu bieten, ist es für digitale Plattformen notwendig, hohe Netzwerkeffekte zu ermöglichen[530] – dies gilt auch im Markt für Ridesharing-Plattformen. Generell lässt sich jedoch beobachten, dass die über die Plattform generierten Profite im Allgemeinen nicht (fair) auf die Plattformteilnehmer aufgeteilt werden, sondern häufig in großem Maße von den Intermediären, welche die Plattform betreiben, einbehalten werden.[531] Um eine Marktkonzentration auf wenige Anbieter zu verhindern, scheint folglich die Schaffung einer offenen Plattform unabdingbar, die keine Anbieter und Kunden von der Teilnahme ausschließt und nicht durch eine einzelne Institution kontrolliert wird.

   Prinzipiell ist die DLT aufgrund ihrer dezentralen Natur und ihrer Möglichkeiten zur Automatisierung von Geschäftsprozessen mittels Smart Contracts gut geeignet, um einzelne Institutionen als Intermediäre für bilaterale Beziehungen obsolet zu machen.[532] Im konkreten Kontext von Ridesharing allerdings stellt sich die Frage der mehrwertschaffenden konzeptionellen und technischen Umsetzbarkeit.

   Eine Kernfunktionalität von Ridesharing-Plattformen ist die Koordination von Angebot und Nachfrage, also das sogenannte Matching von Fahrtanbietern und Mitfahrern.[533] Zu diesem Zweck müssen große Datenmengen kontinuierlich analysiert, aktualisiert und verarbeitet werden. Besonders bei dynamischem Ad-hoc-Ridesharing gestaltet sich dies als äußerst komplexer Vorgang, da hierbei diverse, sich häufig ändernde Parameter (wie bspw. GPS-Daten), verarbeitet werden.[534] Ein sinnvoller Einsatz der DLT ist deshalb zumindest bei dieser Form des Ridesharings im Hinblick auf den aktuellen Stand der Technik aus mehreren Gründen fraglich. Aufgrund der hohen (monetären) Kosten für die Durchführung von Rechenoperationen mittels Smart Contracts in aktuellen öffentlichen DLT-Systemen und der generellen Limitierungen von Smart Contracts hinsichtlich der Speicherung, Abfrage und Verarbeitung großer Datenmengen scheint die Implementierung entsprechender Algorithmen mittels Smart Contracts nicht sinnvoll. Zusätzliche limitierende Faktoren sind die hohen Latenzzeiten und der Datendurchsatz im Sinne von verarbeiteten Transaktionen pro Sekunde in aktuell verfügbaren öffentlichen DLT-Systemen[535]. Obwohl es mehrere Initiativen gibt, die Ad-hoc-Ridesharing-Plattformen mittels DLT umsetzen möchten, sind konkrete Angaben über deren technische Implementierung schwer einzuschätzen und verfügbar. Das Matching von Angebot und Nachfrage findet jedoch nach verfügbaren Informationen oftmals nicht direkt auf einem DLT-System statt[536]. Zusätzlich ist die Frage zu beantworten, inwiefern bspw. die manipulationssichere Speicherung aller abgegebenen Fahrtangebote und -gesuche einen Mehrwert schafft. Darauf bezugnehmend ergibt sich außerdem möglicherweise

[530] *Bundesministerium für Wirtschaft und Energie* (BMWi), Weißbuch Digitale Plattformen.
[531] *DeFilippi,* Harvard Business Review Digital Articles 2017, 2.
[532] *Schweizer/Schlatt/Urbach/Fridgen*, 38th International Conference on Information Systems (ICIS), 1.
[533] *Hahn/Metcalfe*, The Ridesharing Revolution: Economic Survey and Synthesis.
[534] *Mukherjee/Banerjee/Misra*, Proceedings of the 21st International Conference on World Wide Web, 579.
[535] Vgl. Kapitel 5.3.2.1.
[536] *Johnson*, Can La'Zooz Take Ridesharing to the Moon?.

eine Problematik hinsichtlich des Datenschutzes (vgl. Kapitel 6.2). Auch in diesem Kontext ist ein Einsatz der DLT vor dem Matching von Angebot und Nachfrage kritisch zu betrachten.

Im Falle von Ad-hoc-Ridesharing bedarf es voraussichtlich einer oder mehrerer, bspw. lokal orientierter, neutraler und zentraler Instanzen, welche die Sammlung und Koordination von Angebot und Nachfrage in Echtzeit übernehmen. Auf dieser Basisschicht können dann in der Folge verschiedene Ridesharing-Anbieter ihre Angebote veröffentlichen und die Endkundenschnittstellen weiterhin besetzen. Ein Ausschluss anderer Anbieter oder bestimmter Kunden ist dergestalt nicht mehr möglich. Mögliche Geschäftsmodelle umfassen in diesem Szenario die Nutzung der anonymisierten Nutzungsdaten oder die Bereitstellung von Endkundenschnittstellen, die gegebenenfalls in andere Systeme eingebunden werden können. Insgesamt ist also eine Kombination aus On- und Off-Chain-Prozessen in diesem Anwendungsfall wahrscheinlich. Aspekte, die über ein DLT-System abgewickelt werden können, werden nachfolgend ausführlicher dargelegt.

Ridesharing-Plattformen für regelmäßige Strecken (Pendler-Angebote) und für Angebote mit langer Vorlaufzeit (Mitfahrgelegenheits-Angebote) stellen hingegen verhältnismäßig statische Auflistungen von Fahrtangeboten und -gesuchen dar, die den Endnutzern entsprechend verwendeter Suchanfragen aufgezeigt werden. Eine Koordination in Echtzeit ist in diesen Anwendungsszenarien in der Regel nicht notwendig. Für diese Bereiche des Ridesharings können dezentrale Marktplätze auf Basis von DLT genutzt werden, um Angebote und Nachfrage zu koordinieren.[537] Hierbei werden in der Regel dezentrale und verteilte Speichersysteme, wie das Interplanetary File System[538] genutzt, um die Speicherlimitationen in DLT-Systemen zu umgehen. Über definierte Schnittstellen können somit verschiedene Anbieter Anwendungen für Ridesharing-Kunden umsetzen, die alle auf dieselbe offene Datenschicht und die darauf gespeicherten Fahrtangebote und -gesuche zugreifen. Ungeachtet verschiedener Endkundenschnittstellen kann somit eine offene und dezentrale Datenschicht geschaffen werden.

Um die Schaffung offener Ridesharing-Plattformen, die für verschiedene Anbieter zugänglich sind, zu ermöglichen, kann die DLT weitere unterstützende Rollen einnehmen. Zum Beispiel ist ein Einsatz der DLT als Anreizsystem für die Teilnahme an einer offenen Ridesharing-Plattform denkbar. Dabei soll eine kritische Masse an Plattformteilnehmern (und somit Netzwerkeffekte) erreicht werden, indem diese für aktive Mitwirkung auf der Plattform mittels Token, die einen Anteil an der offenen Plattform selbst repräsentieren, belohnt werden oder die Plattform mitgestalten können.[539,540] Die Implementierung der Matching-Algorithmen selbst ist wiederum aus voranstehend beschriebenen technischen Gründen nicht notwendigerweise auf einem DLT-System umzusetzen.[541] Es bestünde lediglich eine Schnittstelle, über die für jede Aktion auf der Plattform Token ausgeschüttet werden. Mit diesen Token könnte zudem für Dienstleistungen über die Plattform bezahlt werden. Überdies lässt sich über die Token die Abrechnung der Leistungen einzelner Anbieter auf einer offenen Plattform potenziell leichter

[537] *Origin Protocol*, ORIGIN - Decentralized marketplaces on the blockchain.
[538] *Protocol Labs*, IPFS is the Distributed Web.
[539] *Beck/Müller-Bloch* et al., Journal of the Associacion for Information Systems, 2018, S. 1020-1034.
[540] *DeFilippi,* Harvard Business Review Digital Articles 2017, 2.
[541] *Johnson*, Can La'Zooz Take Ridesharing to the Moon?.

durchführen und überprüfen. Dies ist insbesondere relevant, wenn z. B. fremde Nutzerschnittstellen für die Buchung von Leistungen verwendet werden.

2. *Identitätsmanagement und Schaffung von Vertrauen*
Eine in diesem Kontext nutzbare Anwendung der DLT ist bspw. die Möglichkeit der selektiven und die Privatsphäre erhaltenden Identifikation und Authentifizierung einzelner Parteien.[542] Diese Funktionalität lässt sich zum einen potenziell dazu verwenden, einzelne Nutzer gegenüber einer oder verschiedenen (offenen) Ridesharing-Plattformen zu authentifizieren und anzumelden, ohne verschiedene Accounts verwenden zu müssen. Dies würde auch einen Anbieterwechsel erleichtern. Zum anderen könnte die DLT in diesem Bereich Verwendung finden, um ein zuvor identifiziertes Vertrauensproblem[543] zwischen Fahrern und Fahrgästen zu beheben. Beispielsweise kann so ein Fahrer direkt seinen Mitfahrern oder einer Plattform gegenüber selektiv die verifizierte Information mitteilen, dass er eine gültige Fahrerlaubnis besitzt, ohne dabei bspw. das Geburtsdatum offenzulegen[544].

3. *Zahlungsdienstleistungen*
Eine weitere Anwendungsmöglichkeit der DLT im Bereich Ridesharing ist die Nutzung der Historisierungsfunktion für die Speicherung von Metadaten über die Geschäftsbeziehungen zwischen Fahrern und Fahrgästen. Somit lassen sich im Nachhinein die ursprünglich vereinbarten Konditionen der Fahrtdienstleistung nachweisen. Eine Verwendung in diesem Bereich ist ähnlich zu der Anwendung im Bereich des Platoonings denkbar.

Token sind aktuell ein integraler Bestandteil nahezu sämtlicher DLT-Systeme[545]. Solche Token, die einen Gegenwert in Fiat-Währungen haben, können z. B. als Alternative zu herkömmlichen Zahlungsmitteln dienen und in Ridesharing-Plattformen eingebunden werden. Kreditkartenzahlungen setzen einen bestehenden Vertrag mit entsprechenden Zahlungsdienstleistern (Drittanbietern) voraus. In der Praxis besitzen – zumindest global betrachtet – allerdings weniger Personen einen entsprechenden Vertrag als ein (für die Zahlung mit Kryptowährungen benötigtes) Smartphone[546], wodurch die Verbreitung von Ridesharing-Plattformen generell erhöht werden könnte. Eine umfangreiche Erklärung der Zahlungsfunktionalität von DLT-Systemen ist dem allgemeinen Teil dieses Gutachtens zu entnehmen. Zu beachten ist jedoch, dass dadurch mit dem aktuellen Stand der Technik oftmals noch höhere Transaktionskosten als durch Einbindung herkömmlicher Zahlungsdienstleister entstehen. An einer Reduktion der Transaktionskosten bei öffentlichen DLT-Systemen wird jedoch im Rahmen der Entwicklung alternativer Konsensmechanismen wie Proof of Stake intensiv geforscht.

Insbesondere die Nutzung von Smart Contracts zur Umsetzung sogenannter Treuhandverträge[547] erscheint zudem im Kontext der Zahlungsabwicklung beim Ridesharing vielversprechend. Bei herkömmlichen Plattformlösungen wird im Allgemeinen vor der Fahrtdienstleistung ein gewisser Geldbetrag an eine dritte

[542] *Dunphy/Petitcolas,* IEEE Security & Privacy 2018, 20.
[543] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.
[544] Siehe auch Kapitel 4.3.7 und 5.2.5.5.
[545] Vgl. Kapitel 5.2.5.6.
[546] *Hahn/Metcalfe*, The Ridesharing Revolution: Economic Survey and Synthesis.
[547] Vgl. Kapitel 5.2.3.2.

Partei gesendet. Nach Bestätigung des Erhalts der Dienstleistung wird dieser Betrag dann an den Fahrer ausgeschüttet.[548] Durch die DLT könnte dieser Prozess automatisiert ohne die notwendige Einbindung intermediärer Parteien durchgeführt werden. Im Standardfall[549] könnte somit der Ablauf über einen weiteren Intermediär verhindert werden, indem eine Ausschüttung des vereinbarten Geldbetrags nach der Signatur mit den privaten Schlüsseln der Fahrtteilnehmer automatisch stattfindet. Des Weiteren könnte die Auswahl verschiedener verifizierter Mediatoren über ein DLT-System (bspw. über deren öffentliche Schlüssel), die im Falle eines Disputs eingeschaltet werden[550], genutzt werden, um die Beilegung möglicher Dispute durch Mediatoren automatisiert auszulösen und den Prozess nachvollziehbar in einem DLT-System abzuspeichern.

9.1.4 Prozessbeschreibung

Der Prozessablauf unterscheidet sich für die unterschiedlichen Arten von Ridesharing im Wesentlichen lediglich in den Prozessschritten bis zum Matching von Angebot und Nachfrage. Auf Ridesharing-Plattformen, die Angebote mit zeitlichem Vorlauf koordinieren, laden Fahrtanbieter ihr Angebot für eine genau spezifizierte Fahrtstrecke zu einem bestimmten Zeitpunkt mittels einer (mobilen) Anwendung auf die Plattform. Dies umfasst die Formen Mitfahrgelegenheits- und Pendler-Angebote. Wiederum mittels einer (mobilen) Anwendung suchen potenzielle Mitfahrer im nächsten Schritt nach Ridesharing-Angeboten für genau spezifizierte Fahrtstrecken. Sofern sich (Teil-)Strecken überschneiden, werden die entsprechenden Angebote dem Suchenden angezeigt und dieser kann eines davon entsprechend auswählen. In der Folge kommt eine bilaterale Verbindung zwischen Fahrer und Mitfahrer zustande. Die genauen Fahrtmodalitäten, wie der Treffpunkt, können anschließend häufig über die jeweils genutzte Plattform diskutiert und direkt koordiniert werden.

Während die Schnittstellen zu den Endnutzern (i. S. v. (mobilen) Anwendungen) weiterhin über verschiedene, zentralisierte Anbieter angeboten werden können, lassen sich die Datenschicht zur Speicherung und die Protokolle zur Koordination von Angeboten dezentral mithilfe von DLT-Systemen umsetzen. Dabei entstehen aus Sicht des Endkunden zunächst allerdings keine Prozessveränderungen.

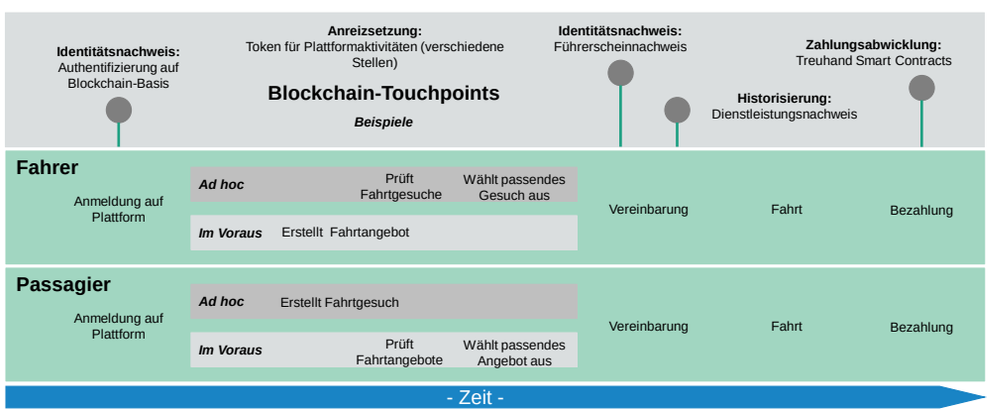


Abbildung 34: Die DLT unterstützt den Ridesharing-Prozess partiell.

[548] *Furuhata/Dessouky/Ordóñez/Brunet* et al., Transportation Research Part B: Methodological 2013, 28.
[549] D. h., wenn keine Schlichtung durch Einschaltung eines Intermediärs notwendig ist.
[550] *Goldfeder/Bonneau/Gennaro/Narayanan* in Kiayias, Financial Cryptography and Data Security, 321.

Im Falle von Ad-hoc-Ridesharing hingegen verwenden potenzielle Mitfahrer zunächst eine (meist mobile) Anwendung und geben ein Fahrtgesuch für eine bestimmte Fahrtstrecke auf. Ein Matching-Algorithmus, der aktuell zumeist auf einer IT-Infrastruktur des jeweiligen Plattformanbieters läuft, sucht anschließend für das jeweilige Fahrtgesuch passende Angebote. Dies können bspw. Fahrer sein, die in einem geeigneten geografischen Feld um den potenziellen Mitfahrer verfügbar sind. Diesen Fahrern wird (zumeist wiederum mittels einer mobilen Anwendung) die entsprechende Anfrage angezeigt. Sofern der Fahrer diese annimmt, kommt eine Vereinbarung zustande und der Fahrer holt den oder die Fahrgäste am jeweiligen über die Anwendung spezifizierten Abholpunkt ab. Auch in diesem Szenario ist es wiederum erstrebenswert, zumindest die Datenschicht und nach Möglichkeit auch den Matching-Algorithmus offen zu gestalten. Aufgrund der oben beschriebenen Performanzbedingungen ist in dieser Hinsicht jedoch ein Einsatz der DLT fragwürdig. Vielmehr bedarf es dazu einer neutralen Instanz, wobei die DLT die Umsetzung einer entsprechenden Plattform an mehreren Stellen potenziell unterstützen kann (vgl. mögliche Lösungsansätze und Rolle von DLT). Auch stellt sich die Frage nach der Notwendigkeit einer manipulationssicheren Speicherung (und der damit verbundenen Kosten) aller abgegebenen Angebote und Gesuche in einem DLT-System.

Bis zu diesem Punkt könnte die DLT wie im vorherigen Kapitel beschrieben möglicherweise bereits als digitale Infrastruktur zur Anmeldung der Nutzer der jeweiligen (mobilen) Ridesharing-Anwendungen verwendet werden. Es ist wichtig zu betonen, dass die verwendeten DLT-Systeme im Anwendungsszenario einer offenen Ridesharing-Plattform ebenfalls öffentliche Systeme sein sollten (vgl. Kapitel 4.3.1), da hierbei Interaktionen zwischen vielen Parteien (in der Praxis oftmals Privatpersonen), abgebildet werden. Ein Einsatz nach dem Matching von Angebot und Nachfrage ist wiederum für das selektive Identitätsmanagement denkbar. Der Fahrer kann seinen Mitfahrern gegenüber mittels seiner digitalen Identität beweisen, dass er eine gültige Fahrerlaubnis besitzt. Diese Behauptung wäre von der zuständigen Behörde bereits signiert und ein anonymisierter Verweis auf einer öffentlichen Blockchain gespeichert, ohne dabei Rückschlüsse auf die tatsächliche Person hinter der Fahrerlaubnis zu ermöglichen.

Nach dem Matching von Angebot und Nachfrage kann zudem ein Treuhand-Smart-Contract aufgesetzt werden. Dies bedeutet, dass ein standardisierter Smart Contract erstellt wird, der die Metadaten der Fahrt (z. B. Datum, Strecke, Preis und Anzahl der Fahrtteilnehmer) enthält. Sofern alle beteiligten Parteien einverstanden sind, können sie diesen mittels ihres privaten Schlüssels auf dem jeweiligen DLT-System signieren, woraufhin der Smart Contract auf das DLT-System geschrieben und damit dort ausführbar wird. Nach Erbringen der Fahrtdienstleistung müssen wiederum alle Parteien den jeweiligen Smart Contract durch eine von ihnen signierte Nachricht ansprechen, woraufhin der vereinbarte Betrag für die Fahrt entsprechend an den jeweiligen Fahrer ausgeschüttet werden kann. Verweigert eine Partei ihre Signatur, kann ein zuvor festgelegter und in dem Smart Contract definierter Mediator eingesetzt werden. Alternativ ist die Einbindung einer Schnittstelle zur Verwendung von DLT als Zahlungsinfrastruktur in (mobile) Anwendungen für Endkunden denkbar. In diesem Fall können Kryptowährungen als alternatives Zahlungsmittel genutzt werden. Die Verwendung für den Endnutzer ist dabei ähnlich den traditionellen Onlinezahlungsdienstleistungen gestaltet und würde in der Praxis vermutlich ergänzend zu herkömmlichen Methoden gestaltet. Für eine ausführlichere Diskussion der Vor- und Nachteile der Verwendung von Kryptowährungen als Zahlungsmittel ist auf Kapitel 5.2.5.6.2 zu verweisen.

Im Falle der Nutzung der DLT als Anreizsystem, das durch Anteils-Token an der Plattform implementiert wird, werden zudem für jede Aktion auf der Plattform (z. B. die Bereitschaft zum Fahren, die tatsächliche Fahrt und die Abgabe einer Bewertung mittels eines Reputationssystems) Token ausgeschüttet. Diese Token repräsentieren einen Anteil an der offenen Plattform und könnten bspw. wiederum zur Bezahlung bzw. zur Kompensation von Leistungen auf der offenen Plattform dienen.

9.1.5 Fazit und Handlungsempfehlungen

Um die Bildung von Monopolen und damit einhergehenden Datensilos zu verhindern, ist die Schaffung einer offenen und geteilten Ridesharing-Plattform notwendig, die keine Nachfrager und Anbieter von der Teilnahme ausschließt. Ein Abgleich der praktischen Anforderungen entsprechender Systeme mit den technischen Besonderheiten von öffentlichen Blockchains lässt einen Einsatz der DLT allein für diesen Zweck allerdings zumindest im Bereich des Ad-hoc-Ridesharing fragwürdig erscheinen. Für statische Angebote und Gesuche, wie im Falle von Mitfahrgelegenheits- oder Pendler-Angeboten, lassen sich Protokolle verwenden, die dezentrale Marktplätze auf Basis der DLT umsetzen. Die DLT eignet sich grundsätzlich gut, um direkte Beziehungen und Prozesse zwischen verschiedenen Parteien abzubilden, sowie um eine rückwirkend unveränderbare Historisierung von Ereignissen abzuspeichern. Diese bi- bzw. multilateralen Beziehungen bestehen jedoch erst nach dem Matching von Angebot und Nachfrage, wo sich auch Anwendungsfälle für die Historisierungsfunktion finden lassen. Dementsprechend kann die DLT als digitale Infrastruktur wichtige unterstützende Funktionen während des Ablaufs von Ridesharing-Aktivitäten übernehmen. Dies inkludiert bspw. ein erweitertes Identitätsmanagement an mehreren Stellen im Ablauf, die Bereitstellung Vertrauen schaffender Mechanismen sowie die Implementierung einer Anreiz- und Abrechnungsstruktur für die Nutzung offener Plattformsysteme.

Wird der Anwendungsfall erweitert, bspw. um die Integration von Anbietern unterschiedlicher Transportmittel zusätzlich zu Ridesharing-Angeboten[551] in einer offenen multimodalen Plattform, könnte die DLT überdies potenziell wiederum Mehrwert stiften. In diesem Szenario müssen bereits bestehende Beziehungen mehrerer Anbieter abgebildet werden, z. B. um die garantierte Abrechnung bereitgestellter Dienstleistungen im multimodalen Transport zu erleichtern. Beispielhafte Ansätze finden sich u. a. in der Initiative zur Schaffung eines offenen und dezentralen Mobilitätssystems OMOS[552] und der Forderung nach einem Deutschlandticket. Eine Integration in multimodale Angebote könnte überdies generell die Verbreitung von Ridesharing positiv beeinflussen.[553]

Erforschung multimodaler Mobilitätsplattformen

Die Umsetzungsmöglichkeiten und Implikationen offener und dezentraler Plattformen sollten untersucht werden, um die Entstehung monopolistischer Plattformanbieter zu vermeiden. Weil ein Einsatz der DLT an mehreren Stellen entlang etwaiger Prozesse auf einer Mobilitätsplattform denkbar ist und gleichzeitig verschiedene alternative Technologien zur Verfügung stehen, sollte zunächst eine technologieagnostische Untersuchung durchgeführt werden. Dabei sollten auch multimodale Plattformen untersucht werden, da hierbei Transaktionen und Interaktionen verschiedener Unternehmen abgebildet und koordiniert werden müssen. Hierfür ist die DLT perspektivisch sehr gut geeignet.

9.2 Rechtlicher Teil

Wie in der ökonomisch-technischen Analyse aufgezeigt, steht die Charakteristik heutiger DLT-Plattformen, d. h. insbesondere die Latenz der Datenverarbeitung und die energetischen Transaktionskosten, einem Ridesharing ohne Intermediär entgegen. Auch aus juristischer Perspektive ergeben sich Hindernisse, die zwar im Hinblick auf den Datenschutz

[551] *Deakin/Frick/Shively,* Transportation Research Record 2010, 131.
[552] *MotionWerk GmbH*, Open Mobility System (OMOS).
[553] *Heinrichs/Thomaier/Parzonka*, Arbeitsberichte zur Verkehrsforschung: Ko-Automobilität.

DLT-spezifisch sind, im Übrigen aber vor allem aus der Verkehrsform Ridesharing als solcher resultieren.

9.2.1 Personenbeförderungsrecht

Die entgeltliche und geschäftsmäßige Personenbeförderung mit Kraftfahrzeugen wird in Deutschland durch das Personenbeförderungsgesetz (§ 1 Abs. 1 S. 1 PBefG) geregelt. Diesem ist ein „numerus clausus der [genehmigungspflichtigen] Verkehrsarten- und formen"/„Typenzwang" ureigen, weshalb nur genehmigungsfähig ist, was das Gesetz als Verkehrstyp anerkennt.[554] Unter diesem Gesichtspunkt sind Ridesharing-Dienste, sofern sie nicht bereits aufgrund ihrer Unentgeltlichkeit oder Betriebskostendeckung schon gar nicht dem PBefG unterfallen (§ 1 Abs. 2 Nr. 1 PBefG) oder aufgrund ihrer Neuartigkeit zur Erprobung über die Öffnungsklausel (§ 2 Abs. 7 PBefG) befristet genehmigungsfähig sind, regelmäßig nur als Mietwagenverkehr gemäß § 49 Abs. 4 PBefG genehmigungsfähig.[555] Problematisch hieran ist, dass das PBefG in § 49 Abs. 4 S. 2 PBefG vorschreibt, dass Mietwagen nur Beförderungsaufträge ausführen dürfen, die am Betriebssitz oder in der Wohnung des Unternehmers eingegangen sind. Darüber hinaus schreibt § 49 Abs. 4 S. 3 PBefG vor, dass ein Mietwagen nach Ausführung des Beförderungsauftrags unverzüglich zum Betriebssitz zurückzukehren muss, sofern er nicht vor der Fahrt von seinem Betriebssitz oder der Wohnung oder während der Fahrt fernmündlich einen neuen Beförderungsauftrag erhalten hat. Beides widerspricht der Ridesharing-Praxis.[556] Dem Gedanken des Ridesharings, Fahrten zu bündeln (Pooling), wiederstrebt zudem § 49 Abs. 4 S. 1 PBefG, wonach Verkehr mit Mietwagen die Beförderung von Personen mit Personenkraftwagen ist, die nur im Ganzen zur Beförderung gemietet werden können. Eine Bündelung von Fahrten kann lediglich der Fahrgast veranlassen, dem gemäß § 49 Abs. 4 S. 1 PBefG die Bestimmung des Zwecks, des Ziels und des Ablaufs der Fahrt obliegt.

Aufgrund der vorgenannten Genehmigungsschwierigkeiten ist das derzeitige PBefG daher in die Kritik geraten.[557] Dies nahm die Koalition aus CDU, CSU und SPD im Koalitionsvertrag der 19. Legislaturperiode zum Anlass für die Bekundung einer Novellierungsabsicht.[558]

Die Novellierung des PBefG ist kein leichtes Unterfangen[559], denn der Gesetzgeber operiert an dieser Stelle im Spannungsfeld zwischen dem Öffentlichen Personennahverkehr (ÖPNV) und dem Taxigewerbe, die Teil der Daseinsvorsorge sind und im Übrigen den wirtschaftlichen Interessen neuer mitunter gewichtiger Mobilitätsanbieter wie etwa Uber. In Bezug auf den perspektivischen Einsatz von DLT im Bereich des Ridesharings gilt es dabei nicht außer Acht zu lassen, dass Intermediäre obsolet werden, sodass antizipiert etwaige Genehmigungsanforderungen nicht nur große Anbieter, sondern auch den Fahrer einschließen sollten. Letzterer könnte zukünftig Beförderungsverträge (§ 631 BGB) mit Smart-Contract-basierter Vergütungsabrede ohne Intermediär schließen.

9.2.2 Datenschutz

Eine Ridesharing-Lösung, die zentrale Intermediäre bei der Abwicklung der notwendigen Transaktionen überflüssig machen soll, wird regelmäßig eine direkte Interaktion von Fahrer und Gefahrenen auf der Blockchain erfordern. Bei diesen wird es sich sehr häufig um

[554] *Linke/Jürschik,* NZV 2018, 496 (498f.).
[555] *Linke/Jürschik,* NZV 2018, 496 (499).
[556] *Ludwigs,* NVwZ 2017, 1646 (1648).
[557] BT-Drs. 19/726.
[558] Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, Zeile 2140.
[559] Zu möglichen konkreten Ansatzpunkten einer Novellierung siehe *Linke/Jürschik,* NZV 2018, 496 (501 ff.).

natürliche Personen handeln, womit die Verarbeitung der Daten der Nutzer datenschutzrechtlich relevant wird. In der Folge erfordert die Abwicklung von Ridesharing-Transaktionen auf der Blockchain die Implementierung geeigneter Vorkehrungen. Hierbei sind grundsätzlich eine „zentrale Lösung“[560] als auch eine „Anonymisierungslösung“[561] denkbar. Aufgrund der Tatsache, dass eine DLT-Plattform für das Ridesharing derzeit keine vielversprechende Lösung darstellt, sollen nähere Ausführungen zur datenschutzkonformen Umsetzung an dieser Stelle unterbleiben.

9.2.3 Fazit und Handlungsempfehlungen

Derzeit erschwert das bestehende PBefG das Ridesharing. Eine Novellierung ist aber beabsichtigt. Diese sollte betreffend DLT antizipieren, dass Intermediäre wie Plattformbetreiber/Vermittler perspektivisch obsolet werden könnten, sodass etwaige Genehmigungserfordernisse auch den Fahrer einschließen sollten.

Auch aus datenschutzrechtlicher Perspektive ergeben sich beim Ridesharing Herausforderungen. Da zu den Teilnehmern auch natürliche Personen zählen, ist eine offene DLT-Lösung ohne Anpassung der Architektur nicht denkbar. Es müsste vielmehr eine verantwortliche Zentralstelle geschaffen werden oder die Verbindung zwischen den Nutzerkennungen und den Teilnehmern durch eine Anonymisierungslösung aufgehoben werden.

Novellierung des PBefG und Datenschutz

Bei der Novellierung des PBefG sollte antizipiert werden, dass DLT Intermediäre perspektivisch obsolet werden lassen kann, wenn derzeitig bestehende technologische Unzulänglichkeiten überwunden werden. Insoweit sollten Genehmigungserfordernisse auch den Fahrer einschließen. Da die Teilnehmer des Ridesharing insbesondere natürliche Personen sind, erfordert der Datenschutz eine Anpassung der DLT-Architektur. Hierzu wurden verschiedene Lösungsmöglichkeiten aufgezeigt.

[560] Siehe zur zentralen Lösung bereits allgemein unter 6.2.3.4.1, zu den Rechtsgrundlagen unter 6.2.4.2.2 und zur Umsetzung der Löschpflichten unter 6.2.5.2.

[561] Siehe zur Anonymisierungslösung bereits unter 6.2.3.4.2.2.2.

10 Platooning

10.1 Ökonomisch-technischer Teil

10.1.1 Definition und Beschreibung des Anwendungsbeispiels

Unter Platooning – im deutschsprachigen Raum gelegentlich auch als elektronische Deichsel bezeichnet – wird ein techno-ökonomisches System für den Straßenverkehr verstanden, in dessen Rahmen zwei oder mehrere Fahrzeuge in sehr geringem Abstand hintereinanderfahren. Dazu gehört ein Vergütungssystem zum Teilen der damit verbundenen Kosteneinsparungen. Ein sogenanntes Platoon ist demnach eine Kolonne aus zwei oder mehreren Fahrzeugen, die für einen im Allgemeinen nicht näher bestimmten Zeitraum gemeinsam über einen geteilten Abschnitt ihrer individuellen Routen[562] fahren. Voraussetzung für das Platooning sind zahlreiche Technologien, die typischerweise auch beim (voll-)automatisierten Fahren zum Einsatz kommen[563], etwa Abstandssensoren oder automatische Steuerungssysteme für Lenkrad, Gaspedal etc. Daneben setzt Platooning digitale Infrastrukturen voraus, um technische Abläufe zwischen den Fahrzeugen sowie den (monetären) Leistungsaustausch koordinieren und abwickeln zu können. Aktivitäten im Bereich des Platoonings befinden sich heute (noch) im vorwettbewerblichen Bereich. Eine wettbewerbliche Realisierung ist dabei technisch sowohl mithilfe einer zentralen Architektur[564], verbunden mit der Entstehung eines entsprechenden zentralen koordinativen Marktakteurs, als auch mithilfe einer intermediärfreien, DLT[565]-basierten Architektur denkbar.

Platooning wird unabhängig von der spezifischen zugrunde liegenden IT-Architektur als aussichtsreiches Konzept eingestuft[566], das für den zunehmenden Güterverkehr auf deutschen Straßen[567] maßgebliche Verbesserungspotenziale bieten könnte. Insbesondere beim Lkw-Platooning werden neben erheblichen Kosteneinsparungen auch Chancen darin gesehen, die Verkehrssicherheit[568] sowie die Verkehrseffizienz[569] zu fördern und Umweltbelastungen durch den Verkehr zu reduzieren.

Das ökonomische Rational, das dem Zusammenschluss zu einem Platoon zugrunde liegt, erklärt sich durch eine erwartete Kostenersparnis in den Kostenarten Treibstoff, Personal (Fahrer – insbesondere im gewerblichen Bereich) und Versicherung.

[562] Platooning ist generell geeignet für Fernstraßen. Autobahnen eignen sich dabei aufgrund guter Überholmöglichkeit am besten.

[563] *McKinsey & Company*, Lkw-Industrie: Jeder dritte Lastwagen bis 2025 teilautonom.

[564] Die Begriffe „Architektur" und „Plattform" werden im allgemeinen Teil beschrieben.

[565] DLT (Distributed-Ledger-Technologie) wird im allgemeinen Teil beschrieben.

[566] *Deutsches Zentrum für Luft- und Raumfahrt (*DLR), Automatisiertes und vernetztes Fahren im Güterverkehr - Auswirkungen auf die Logistikbranche.

[567] *Bundesministerium für Verkehr und digitale Infrastruktur (*BMVI), Verkehrsverflechtungsprognose 2030.; *Sutter/Maibach/Bertschmann/Ickert* et al., Finanzierung einer nachhaltigen Güterverkehrsinfrastruktur.

[568] Bis zu 90 Prozent aller Unfälle basieren auf menschlichen Fehlern (*Janssen/Zwijnenberg/Blankers/Kruijff*, Truck Platooning: Driving the Future of Transportation.

[569] Eine Verdoppelung der vorhandenen Straßeninfrastrukturkapazität wird als möglich gesehen (*Flämig,* Autonomes Fahren 2015, 377.

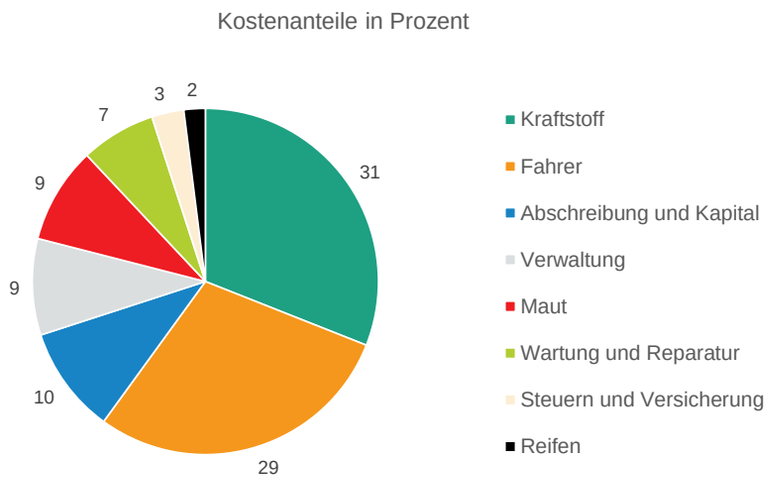


Abbildung 35: Prozentuale Kostenanteile bei Speditionen[570]

Vielversprechend, sowohl in der Größenordnung als auch in Bezug auf die Umsetzungsnähe, sind Ersparnisse in der Kostenart Treibstoff. Die Fahrzeuge, die dem Führungsfahrzeug im Platoon folgen, sparen aufgrund eines verringerten Luftwiderstands („Windschatten") Treibstoff. Überraschenderweise kann aber sogar das vorweg fahrende Fahrzeug aufgrund verminderter Turbulenzen seinen Spritverbrauch reduzieren, auch wenn dieser Strömungsabbruchseffekt im Allgemeinen deutlich geringer ausfällt als der Windschatteneffekt. Die genaue Treibstoffersparnis kann theoretisch nur näherungsweise bestimmt werden und hängt u. a. maßgeblich von dem Abstand der Fahrzeuge sowie der Geschwindigkeit des Platoons ab. Zusätzlich müssen weitere Parameter, wie etwa Straßen- und Umweltbedingungen (Belag, Temperatur, Steigungen, Höhenlage) für die Berechnung des individuellen Einsparpotenzials berücksichtigt werden. Je nach Expertenmeinung liegen die typischen Einsparungen bei etwa 5 Prozent für das führende Fahrzeug, etwa 10 Prozent für das letzte Fahrzeug eines Platoons und etwa 15 Prozent für alle Platooning-Teilnehmer dazwischen[571]. Versuche des Unternehmens Scania zeigen bspw., dass beim Lkw-Platooning Einsparpotenziale von bis zu 12 Prozent möglich sind.[572]

Dass Platooning aus ökonomischer (aber auch aus ökologischer Sicht) ein relevanter Anwendungsfall ist, zeigt folgende einfache Abschätzung für den Treibstoffverbrauch: Es werden pro Jahr in Deutschland etwa 35 Mrd. Kilometer von Lkw auf Mautstraßen gefahren[573]. Angenommen, alle Strecken werden in Zweier-Platoons gefahren (was einerseits die gefahrene Strecke in Platoons überschätzt, da etwa nachts auf wenig befahrenen Straßen kaum Platoons gebildet werden können, andererseits aber auch die Anzahl an führenden (und hinteren) Fahrzeugen überschätzt und damit die Treibstoffersparnis pro Fahrzeug unterschätzt), so scheint es eine sinnvolle Annahme zu sein, dass 50 Prozent der 35 Mrd. km bei einer Treibstoffersparnis von durchschnittlich 10 Prozent gefahren werden. Bei einem heute typischen Dieselpreis von etwa 1,30 Euro/Liter[574] und einem durchschnittlichen Verbrauch von 30l/100 km erhält man somit ein Treibstoffeinsparpotenzial in Deutschland in Höhe von

[570] *Schwertberger*, Cross Innovationen im KV: Platooning 2017.
[571] *Tsugawa*, Energy ITS: What We Learned and What We should Learn.
[572] *Scania*, Platooning saves up to 12 percent fuel.
[573] *Bundesamt für Güterverkehr (*BAG), Entwicklung der gefahrenen Mautkilometer in Deutschland von 2005 bis 2017 (in Milliarden Kilometer).
[574] https://de.statista.com/statistik/daten/studie/779/umfrage/durchschnittspreis-fuer-dieselkraftstoff-seit-dem-jahr-1950.

$$35\ \text{Mrd km} \times 50\% \times 10\% \times \frac{30\ \text{l}}{100\ \text{km}} \times\ 1{,}30\ \frac{€}{\text{l}} \approx 683\ \text{Mio €}.$$

Es bleibt allerdings abzuwarten, ob die erhofften Treibstoffeinsparungen auch so bedeutsam ausfallen, wie sie bisher von den Herstellern und Wissenschaftlern vorausgesagt worden sind. So hat bspw. Daimler Trucks auf der Technologiemesse CES in Las Vegas im Januar 2019 bekannt gegeben, dass bisherige Schätzungen zu den erwarteten Treibstoffeinsparungen nicht erfüllt werden[575] und will daher das Geschäftsmodell nicht weiterverfolgen. Zukünftig soll bei Daimler Trucks der Fokus auf der Weiterentwicklung autonom fahrender Lkw nach SAE-Level 4 liegen, um Zweier-Platoons zu ermöglichen und dem Fahrer des Folgefahrzeugs Ruhezeiten während der Fahrt zu ermöglichen.[576] Das soeben beschriebene Potenzial wird im übernächsten Absatz genauer erläutert.

Gleichzeitig führt die Einsparung von Treibstoff zu geringerem CO_2-Ausstoß.[577] Dies eröffnet ein weiteres wichtiges Nutzenpotenzial, da Lkw-basierte Emissionen für einen Großteil der im Straßenverkehr erzeugten Emissionen verantwortlich sind. In der EU resultieren etwa 6 Prozent der Gesamtemissionen sowie 25 Prozent der CO_2-Emissionen aus dem Straßenverkehr aus schweren Nutzfahrzeugen wie Lkw und Bussen.[578] Um eine Abschätzung der CO_2-Einsparungen durch Platooning in Deutschland zu erhalten, wird wie in der vorigen Rechnung angenommen, dass bei 50 Prozent der 35 Mrd. gefahrenen Kilometer durch Lkw auf Mautstraßen 10 Prozent Treibstoff eingespart wird. Darüber hinaus werden nach Angaben des Zentralverbands des Deutschen Kraftfahrzeuggewerbes pro Liter Diesel 2,65 kg CO_2 ausgestoßen[579], noch bevor eine Abgasreinigung durch etwa katalytische Verfahren stattfinden kann. Insgesamt können so bei einem durchschnittlichen Treibstoffverbrauch von 30l/100 km jährlich etwa 1,39 Mio. Tonnen CO_2-Emissionen vermieden werden.

$$35\ \text{Mrd km} \times 50\% \times 10\% \times \frac{30\ \text{l}}{100\ \text{km}} \times 2{,}65\ \frac{\text{kg}}{\text{l}} \approx 1{,}39\ \text{Mio t}\,.$$

Neben den Kosteneinsparungen für Treibstoff und dem positiven Einfluss auf CO_2-Emissionen wird häufig angemerkt, dass elektrisch betriebene Fahrzeuge durch die Reduktion der benötigten elektrischen Energie ihre Reichweite erhöhen könnten. Reichweite ist im Rahmen der Elektromobilität als eine der wichtigsten Markthürden identifiziert worden.[580]

Ersparnisse in der Kostenart Personal lassen sich realisieren, indem bereits nach heutigem Stand der Technik durch die beim Lkw-Platooning eingesetzten Assistenzsysteme ein solcher Autonomiegrad erreicht werden kann, dass ein Fahrer eines folgenden Lkw im Platoon die Fahrt anstatt als Lenkzeit theoretisch als Ruhezeit oder für andere Tätigkeiten verfügbare Zeit verwenden könnte. Diese Flexibilisierung der Arbeitszeit könnte dem Fahrer neue Möglichkeiten eröffnen, anstehende Aktivitäten zu planen. Denkbar sind u. a.

[575] Grund hierfür sind offenbar die benötigten zusätzlichen Beschleunigungs- bzw. Abbremsvorgänge, die ein Ein- bzw. Ausfädeln von Pkw zwischen die Platooning-Teilnehmer erlauben, etwa zum Auf- oder Abfahren auf bzw. von der Autobahn.

[576] *Hoffmann*, Paukenschlag aus Las Vegas.

[577] *Scora/Barth*, Comprehensive Modal Emissions Model (CMEM).

[578] *Europäische Kommission*, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung von CO2-Emissionsnormen für neue schwere Nutzfahrzeuge.

[579] *Deutsche Handwerkszeitung*, Kraftstoffverbrauch: So viel CO2 stößt Ihr Auto aus.

[580] *Melliger/Vliet/Liimatainen,* Transportation Research Part D: Transport and Environment 2018b, 101..

Planungsaktivitäten logistischer Natur, wie etwa das Arrangieren anstehender Entladevorgänge sowie der Rückladefahrt. Darüber hinaus könnte der Fahrer bei Planabweichungen mit der Speditionszentrale kommunizieren oder notwendige elektronische Dokumente für den Warenübergang vorbereiten.[581] Zum einen wird diese Kostenart als einer der wichtigsten Hebel für Kosteneinsparungen betrachtet. Zum anderen dürfte sie jedoch als diejenige gelten, welche am meisten Zeit zur Realisierung bedarf, da gewisse technische und rechtliche Rahmenbedingungen vorliegen müssen. Insbesondere könnten für den Fahrer des im Platoon folgenden Fahrzeugs nach geltendem deutschen Recht Lenkzeiten während des Platoonings nicht als Ruhezeiten gewertet werden.[582] Zudem gibt es Untersuchungen, ob der Fahrer nicht während des Platoons – etwa durch die kontinuierlich benötigte Bereitschaft zum Eingreifen oder Übernehmen – genauso konzentriert sein muss wie während des eigenständigen Fahrens. Es ist allerdings anzunehmen, dass bei einem gewissen Reifegrad der Entwicklung eine solche permanente Bereitschaft zum Eingreifen nicht mehr nötig sein wird.

Ein weiteres Potenzial von Platooning wird durch die erhöhte Verkehrssicherheit infolge der Nutzung von Assistenzsystemen sichtbar, die für den richtigen Abstand zwischen den Lkw im Platoon sorgen und das Tempo der Folge-Lkw regulieren. Assistenzsysteme können bei unvorhergesehenen Zwischenfällen im Allgemeinen früher eingreifen als ein Mensch und auf diese Weise etwa Auffahrunfälle vermeiden.[583] Die daraus resultierenden geringeren Zahlen von schweren Verkehrsunfällen könnten so langfristig nicht nur die Zahl an Toten und Verletzten durch Verkehrsunfälle reduzieren, sondern sich damit auch positiv auf die Versicherungsbeiträge auswirken. Bereits heutige Versicherungsmodelle, die Telemetriedaten mit in die Berechnung der Versicherungsprämien einbeziehen, deuten eine solche Entwicklung an[584]. Im Vergleich zu den anderen Potenzialen wird der monetäre Vorteil durch geringere Versicherungsbeiträge jedoch voraussichtlich geringer ausfallen, da weniger als ein Zehntel heutiger Speditionskosten auf die Kostenart Versicherung entfällt.[585]

10.1.2 Status quo und Herausforderungen

Im Rahmen der European Truck Platooning Challenge wurde bereits im Jahr 2016 die technologische Machbarkeit von Lkw-Platooning unter realen Bedingungen demonstriert.[586] Auf verschiedenen Strecken haben insgesamt sechs europäische Nutzfahrzeug-Hersteller – Daimler, MAN, DAF, IVECO, Scania sowie Volvo – Lkw-Platoons zusammengestellt und zum Hafen in Rotterdam fahren lassen. Die Platoons fuhren dabei größtenteils bei Tageslicht und unter normalen Verkehrsbedingungen. Auch in Deutschland wird aktuell in Forschungs- und Entwicklungsprojekten Lkw-Platooning unter realen Testbedingungen erprobt. Als Beispiel kann u. a. das vom Bundesministerium für Verkehr und Digitale Infrastruktur geförderte Projekt Elektronische Deichsel – Digitale Innovation EDDI[587] auf der Digitalen Teststrecke A9 zwischen München und Nürnberg in Kooperation mit MAN und DB Schenker dienen.

[581] *Reus*, Interview: Platooning wird Nerven und Kraft der Fahrer schonen.

[582] Siehe hierzu: rechtlicher Teil.

[583] *Alam/Besselink/Turri/Martensson* et al., jurisPR-BKR 2015, 34.

[584] Z. B. https://emil.de/, *EMIL Deutschland AG*, Wer wenig fährt, sollte wenig zahlen.

[585] *Schwertberger*, Cross Innovationen im KV: Platooning 2017.

[586] *Alkom/Vliet/Aarts/Eckhardt*, European Truck Platooning Challenge.

[587] *Bundesministerium für Verkehr und digitale Infrastruktur (*BMVI), Elektronische Deichsel – Digitale Innovation – EDDI.

Die angesprochenen Initiativen testen Platooning aktuell jedoch nur vorwettbewerblich. Für den wettbewerblichen Erfolg des Konzepts ist es von hoher Relevanz, dass Lastkraftwagen unabhängig vom Eigentümer (z. B. Spediteur) und Fahrzeughersteller befähigt werden, sogenannte „gemischte Platoons" zu bilden. Dahinter steckt die Überlegung, dass sich aus ökonomischer Sicht (Rentabilität der zusätzlichen Investitionen, etwa für Sensorik) nur dann häufig genug Platoons bilden, wenn sich die beteiligten Akteure auf eine Technologie bzw. einen Standard verständigen können, die es jedem Lkw ermöglicht, mit jedem anderen Lkw einen Platoon zu bilden bzw. jedem anderen Platoon beizutreten. Diese Eigenschaft wird von zahlreichen Pilot- bzw. Forschungs- und Entwicklungsprojekten als entscheidend angesehen, wenngleich sie bislang noch nicht realisiert werden konnte. In der EU-Strategie für die Mobilität der Zukunft wurde dieses Problem eingeräumt[588] und zur Förderung von gemischten Platoons das Projekt ENSEMBLE ins Leben gerufen. Dieses hat zum Ziel, die Standardisierung von Kommunikationsprotokollen für gemischtes Lkw-Platooning voranzutreiben.[589]

Beim Platooning kann die Kommunikation der Lkw bspw. über eine WLAN-Verbindung basierend auf dem IEEE 802.11p Standard stattfinden[590]. Hierbei werden zwischen den Assistenzsystemen der Lkw Sensordaten über Position und Geschwindigkeit der umliegenden Fahrzeuge ausgetauscht. Aus technischer Sicht sind für das teil-automatisierte Fahren im Platoon (Autonomisierung nach SAE-Level 4 für die Folgefahrzeuge) Kommunikationsprotokolle zwischen Lkw untereinander umliegender Straßeninfrastruktur notwendig. Diese müssen verschiedene Manöver einer Platooning-Fahrt abbilden können, wie etwa das Formen und Auflösen eines Platoons. Darüber hinaus müssen sie Mechanismen beinhalten, damit die Verkehrssicherheit für Lkw-Fahrer und andere Verkehrsteilnehmer zu jedem Zeitpunkt sichergestellt wird. Damit solche Kommunikationsprotokolle bei der gegebenen Vielfalt unterschiedlicher Lkw inklusive deren proprietärer „IT-Systeme" funktionieren, ist, wie auch die Zielsetzung des ENSEMBLE-Projekts lautet, eine Standardisierung der Kommunikationsprotokolle und Schnittstellen notwendig. Eine weitere technische Herausforderung sind für Assistenzsysteme nicht ausreichend lesbare Straßenmarkierungen sowie dichter Verkehr und Staus. Es besteht hierbei die Gefahr, dass durch Fehlinterpretation der Umwelt falsche Aktionsmuster abgeleitet werden, die dann einen Unfall verursachen können. Daher sind Weiterentwicklungen im Bereich des automatisierten Fahrens notwendig.

Damit Lkw-Platooning Realität werden kann, gilt es jedoch, abgesehen von den beschriebenen technischen Herausforderungen, noch weitere ökonomische Fragestellungen zu lösen. Aus ökonomischer Sicht besteht beim gemischten Platooning grundsätzlich kein Anreiz, die Führung des Platoons zu übernehmen: Die Ersparnisse durch geringeren Treibstoffverbrauch sind für die hinteren Fahrzeuge höher als für das führende Fahrzeug, und falls eines Tages auch eine Reduktion von Lenkzeiten im Platoon möglich sein sollte, betreffen damit verbundene Einsparungen ebenfalls nicht das führende Fahrzeug bzw. dessen zugehöriges Unternehmen. Fahren Fahrzeuge eines Unternehmens häufiger vorn, so ergibt dies einen Wettbewerbsnachteil gegenüber den im Platoon hinterherfahrenden und dadurch Kosten sparenden Konkurrenten. Ein regelmäßiges Abwechseln des Fahrens an der Spitze, wie es aus dem Radsport bekannt ist, scheint kompliziert und kann zudem die Treibstoffersparnisse reduzieren und insbesondere den Verkehrsfluss negativ beeinflussen. Ein monetäres Anreizsystem, das den führenden Lkw im Platoon für die ermöglichten Kosteneinsparungen während der Platoon-Fahrt vergütet, scheint die logische Konsequenz. Dafür ist ein geeignetes Abrechnungssystem nötig.

[588] *Europäische Kommission*, Künstliche Intelligenz: Kommission treibt Arbeit an Ethikleitlinien weiter voran.
[589] *Cordis*, ENSEMBLE: ENabling SafE Multi-Brand pLatooning for Europe.
[590] *Bergenhem/Hedin/Skarin,* Procedia - Social and Behavioral Sciences 2012, 1222.

In einem derartigen Szenario bietet sich zunächst eine zentrale Plattform, die als Intermediär zwischen den einzelnen Speditionen fungiert, als Lösung an. Ähnlich wie bei anderen digitalen Plattformen, etwa Airbnb, regelt dieser Intermediär das Zusammenspiel zwischen den unabhängigen, konkurrierenden Akteuren. Der Intermediär stellt somit sicher, dass sich alle Teilnehmer an ein festgesetztes Regelwerk halten (Berechnung der Kompensationszahlung, Sicherstellung der Bezahlung), das idealerweise allen Nutzergruppen Mehrwert stiftet. Das Geschäftsmodell der Plattform selbst basiert darauf, Nutzungsentgelte, in der Regel in Form von Transaktionsgebühren, von den Teilnehmern für die im Netzwerk stattfindenden Interaktionen zu verlangen.

Es besteht die Möglichkeit, dass sich kurzfristig unterschiedliche Insellösungen entwickeln, die eine solche Plattformrolle einnehmen. Langfristig ist jedoch zu erwarten, dass sich wenige bis eine einzige technologisch überlegene (oder marktbeherrschende) Lösung durchsetzt. Der Grund dafür besteht darin, dass der Nutzen einer Plattform ganz maßgeblich von sogenannten Netzwerkeffekten abhängt. Das bedeutet, dass in diesem Anwendungsfall die zu erwartenden Gesamteinsparungen für einen Teilnehmer gerade zu Beginn überproportional mit jedem zusätzlichen Teilnehmer zunehmen, da mit jedem zusätzlichen Teilnehmer ebenso die Wahrscheinlichkeit für eine Platoon-Bildung auf den Straßen erhöht wird.

Das Problem einer derartigen Entwicklung besteht darin, dass sich einzelne Plattformen langfristig zu einem Monopolanbieter entwickeln und erfahrungsgemäß ihre Vormachtstellung nutzen, um Markteintrittsbarrieren für neue Mitbewerber zu schaffen oder die Nutzungsentgelte für die Plattform so zu erhöhen, dass sie gesamtwirtschaftlich nicht die Wohlfahrt für die teilnehmenden Akteure maximieren (vgl. 5.2.3 oder Ridesharing).

Insbesondere im B2B-Bereich werden Hersteller und/oder Spediteure eine Welt fürchten, in der ein Plattformbetreiber, an dem möglicherweise auch direkte Konkurrenten (erhebliche) Unternehmensanteile besitzen, den Markt dominiert. Analysen von Beratungshäusern[591] skizzieren im Einklang mit den Beobachtungen aus den gesellschaftlich-ökonomischen Grundlagen die Erwartung, dass sich sowohl Fahrzeughersteller als auch Technologiekonzerne um die zentrale Rolle des Plattformbetreibers bemühen werden.

10.1.3 Mögliche Lösungsansätze und Rolle von DLT

Wie bereits expliziert, stellt eine zentrale Plattform potenziell eine Lösung für das grundlegende Problem der Zahlungsabwicklung zwischen den sich gegenseitig misstrauenden Akteuren beim Lkw-Platooning dar. Um die bereits im allgemeinen Fall diskutierte Gefahr einer Monopolbildung zu verhindern, bietet sich dafür auch der Einsatz von DLT an.[592] Um eine detaillierte Betrachtung der Einsatzmöglichkeiten vorzunehmen, wird an dieser Stelle zwischen zwei differierenden Varianten des Platoonings unterschieden: das geplante Platooning und das spontane Platooning.[593] Diese unterscheiden sich hinsichtlich des Grades an Spontaneität sowie des Maßes an Vertrauen, das die DLT schaffen kann. Das geplante Platooning zeichnet sich dadurch aus, dass der Zusammenschluss verschiedener Fahrzeuge zum Platoon schon vor der tatsächlichen Platoon-Fahrt geplant wird[594]. Bei dieser Form von Platooning besteht im Vergleich zum spontanen Platooning ein geringeres Vertrauensbedürfnis zwischen den einzelnen Parteien, da diese sich im Voraus schon kennen und gegebenenfalls die Art und Weise der Verteilung von Kosten und Einsparungen bereits vor der Platoon-Fahrt aushandeln und gegebenenfalls sogar in einem Smart Contract / Offline Payment Channel festhalten können. Beim spontanen Pla-

[591] *Nowak/Viereckl/Kauschke/Starke*, The era of digitized trucking.
[592] Vgl. auch Anwendungsmuster „Neutrale Plattform".
[593] *Bhoopalam/Agatz/Zuidwijk,* Transportation Research Part B: Methodological 2018, 212.
[594] *Bhoopalam/Agatz/Zuidwijk,* Transportation Research Part B: Methodological 2018, 212.

tooning hingegen geschieht die Platoon-Bildung ad hoc und ohne vorhergehende Planung. Das spontane Platooning weist somit ein größeres Vertrauensbedürfnis auf, da die Art und Weise der Verteilung von Kosten und Einsparungen ohne vorherige Absprache ablaufen muss.

Die DLT kann für das Platooning insbesondere für die Verrechnung der gegenseitigen Kompensationen der Platooning-Teilnehmer von Nutzen sein. Sie bietet dabei neben der Monopolvermeidung die Vorteile, dass die Real-time-Verrechnung von Mikrotransaktionen automatisiert möglich ist und durch ihre Peer-to-peer-Struktur kein nachträgliches Clearing notwendig wird.

Prinzipiell ist für die Real-time-Verrechnung ein kontinuierlicher Internetzugriff notwendig. Es können jedoch auf deutschen Straßen auch Situationen auftreten, in denen dieser für längere Zeit nicht gewährleistet ist. Dies eröffnet theoretisch die Möglichkeit, dass sich in Offlinephasen Platoons bilden und die hinteren Fahrzeuge anschließend (wenn wieder Internetzugriff besteht) keine Zahlung ausführen. Während der Offlinephase kann gegebenenfalls nicht verifiziert werden, ob das hintere Fahrzeug solvent ist. Es ist jedoch zu erwähnen, dass es sich bei diesem Betrugsszenario wohl eher um ein theoretisches Konstrukt handelt, da es zum einen sehr aufwendig und zum anderen bei Kleinstbeträgen nicht lohnend erscheint. Zudem gibt es verschiedene Ansätze, dieses Problem auch technisch zu umgehen.

Breitbandausbau

Ein durchdachter Ausbau des Internets bzw. dessen Zugänglichkeit ist für die Realisierung der Chancen von DLT höchst förderlich, um verschiedene (wirtschaftliche) Anwendungsfallbeispiele zu ermöglichen. Am Anwendungsfall „Platooning“ zeigt sich der Vorteil eines flächendeckenden und schnellen Internetzugangs besonders deutlich, da so die Platooningvorgänge durchgängig und effizient abgewickelt werden können. Blockchain als Ausprägung von DLT basiert wiederum selbst auf dem Internet, welches seinerseits auf Kommunikationsnetze angewiesen ist. Erfolgversprechende DLT-Projekte sind besonders in bereits hochdigitalisierten Bereichen zu erwarten. Die Erwartungshaltung bei gezielter Förderung von Projekten sollte dieser Erkenntnis Rechnung tragen. Förderungsschwerpunkt sollten im Falle der DLT bereits digitalisierte Bereiche (oder leicht zu digitalisierende Bereiche) sein, damit die Hürde für die Einführung möglichst niedrig und die realisierten Potenziale möglichst hoch sind.

Das geplante Platooning kann dieses Problem bspw. mithilfe sogenannter Offline-Channels umgehen: Wird der Platoon bereits ausreichend früh geplant, so kann noch vor Beginn des Platoons und bei bestehender Internetverbindung ein Smart Contract in die DLT geschrieben werden. Dieser beinhaltet das Einfrieren eines gewissen Betrags („Treuhänder“). Sendet man an die Adresse dieses Smart Contracts nun eine Transaktion, die von beiden Platooning-Teilnehmern digital signiert (unterschrieben) wurde, wird automatisch der entsprechende Teil von Token/der Kryptowährung an den betreffenden Teilnehmer überwiesen. So kann das Führungsfahrzeug, durch regelmäßiges Unterschreiben des hinteren Platooning-Teilnehmers von Platooning-Daten oder entsprechenden Transaktionsansprüchen auch offline eine Garantie für die faire Kompensation erhalten. Bei einer derartigen technischen Umsetzung ist entsprechend der großen Anzahl von Lkw (größer als 100 000) auf deutschen Straßen auf die Skalierbarkeit zu achten. Dieser Ansatz offenbart überdies den Nachteil, dass gerade im Straßenverkehr häufig unerwartete Verzögerungen auftreten, sodass das geplante Platooning, also eine Verabredung mit hinreichend viel Vorlaufzeit, im Allgemeinen eher unpraktisch zu organisieren ist. Insgesamt

ist dieser Ansatz somit zwar technisch interessant, in der Praxis aber wohl eher weniger relevant.

Das spontane Platooning dagegen soll diese Schwäche beheben und ohne Vorlaufzeit („in Echtzeit") das Bilden von Platoons ermöglichen, indem es den Teilnehmern garantiert, auch Ad-hoc-Kompensationszahlungen zu erhalten. Aus diesem Grund beschränkt sich die folgende Untersuchung auf den Fall des spontanen Platoonings. Auch beim spontanen Platooning bietet sich theoretisch die Möglichkeit des o.g. Betrugsszenarios. Es gibt allerdings verschiedene Möglichkeiten, dieses auszuschließen. Beispielsweise könnte jeder Teilnehmer eine Mindestdeckung seines Kontos vorhalten müssen oder Reputationsmechanismen implementiert werden. Aufgrund der geringen ökonomischen Relevanz soll an dieser Stelle aber nicht weiter auf dieses Szenario eingegangen werden. Unter den Gesichtspunkten Spontanität, Skalierbarkeit und Transaktionskosten bietet sich für diesen Anwendungsfall eine DLT an, die kostenfreie Mikrotransaktionen und eine hohe Skalierbarkeit erlaubt. Die IOTA Foundation mit Sitz in Berlin[595] forscht z. B. an solch einem Protokoll. Mit einer solchen Technologie könnte die Verrechnung beim spontanen Platooning grundsätzlich ermöglicht werden.

Eine sinnvolle Größenordnung für die Anzahl an gefahrenen Kilometern, sowohl in einem langfristig geplanten als auch in einem spontanen Zweier-Platoon, rangiert im Bereich von ca. 100 km. Für die gesamte Strecke ergeben sich dabei (bei fairer Aufteilung der Erlöse aus dem Platooning, d. h., beide Teilnehmer erhalten 50 Prozent der Ersparnisse des hinteren Fahrzeugs) schätzungsweise Transaktionen in Höhe von

$$100\ \text{km} * 10\% * 30\ \frac{l}{100\ \text{km}} * 1{,}30\ \frac{€}{\text{l}} * 0{,}5 = 1{,}95€.$$

Für längere Platoons, etwa einen Platoon bestehend aus fünf Fahrzeugen, wird die typische Strecke in unveränderter Konstellation (zumindest bei spontanen Platoons) kürzer (etwa um den Faktor 5). Gleichzeitig muss jedes Folgefahrzeug nur einen Bruchteil der Gesamtkompensation für das führende Fahrzeug (1/4 der jeweiligen Einsparung) bezahlen. Die Größenordnung der Transaktion liegt dann mit ca. 10 Cent deutlich unter dem obigen Wert. Insbesondere müssen die Transaktionskosten hinreichend niedrig sein, damit sich eine solche Transaktion lohnt.

10.1.4 Prozessbeschreibung

Im Folgenden werden die notwendigen Grundlagen für das Verständnis der zentralen Phasen des spontanen Platoonings mit Zahlungsabwicklung über eine DLT-Infrastruktur kurz dargestellt. Die Beschreibung beschränkt sich der Verständlichkeit halber auf Erläuterungen anhand eines Zweier-Platoons, heuristisch folgt daraus aber auch eine Beschreibung für längere Platoons, indem man diese iterativ aufbaut und den jeweils bereits bestehenden Platoon als eine Einheit betrachtet.

1. *Platoon-Suche und Vertragsschluss:* Hier kann ein Fahrzeug bzw. dessen Fahrer vollautomatisiert bzw. mittels einer App entweder ein Angebot zum Platooning erstellen, indem er sich als führendes oder folgendes Fahrzeug anbietet. Hierbei sind sowohl invitationes ad offerendum oder bereits verbindliche Angebote denkbar. Alternativ können Angebote zum Platoonen von sich in der Reichweite des eigenen lokalen WLANs befindlichen Lkw analysiert werden. Danach muss eine Identifikation im Sinne einer Verknüpfung von Spedition bzw. Lkw und auf der DLT zugeordneter Adresse stattfinden. Weiter muss eine Einigung über die

[595] *IOTA Foundation*, IOTA.

Berechnung der Kompensationszahlung erfolgen, bspw. über das bilaterale Verhandeln von Parametern, die in die Berechnung aus Geschwindigkeit, Abstand etc. einfließen, oder Festsetzen einer Pauschale (x Euro/km). Hier werden Analogien zum Thema Ridesharing deutlich, denn es handelt sich hierbei in gewisser Weise um einen lokalen, freien „Marktplatz" zum Platzieren von Angeboten, auf dem ein Ökosystem aus Apps miteinander verhandeln und formale Verträge abschließen könnte. Für proprietäre Systeme der Fahrzeughersteller wurde bisher konstatiert, dass „[d]ie Berechnung und Fakturierung des Mehrwertes eines Platoons […] u. a. intransparent und für die Nutzer nicht konkret nachvollziehbar" ist.[596] Dieses Problem muss bei DLT-basierter Realisierung nicht eintreten.

2. *Koppeln:* Dabei entsteht die „elektronische Deichsel": Die beiden Lkw ordnen sich hintereinander an und beginnen, Sensorikdaten auszutauschen, die für das Platooning und/oder die vereinbarte Berechnung der Kompensation wesentlich sind, etwa Geschwindigkeitsdaten oder Abstand. Die Fahrzeuge fahren hintereinander und nähern sich allmählich auf den geplanten Zielabstand an.
3. *Mitfahren* (Führend, folgend): Es findet weiterhin ein kontinuierlicher Austausch von Sensorikdaten statt, der die Verkehrssicherheit des Platoons gewährleistet. Durch Signieren der Sensorikdaten vor dem Absenden und lokale Zwischenspeicherung könnte Transparenz und Nachweisbarkeit im Falle eines späteren Disputs gewährleistet werden. Eine Speicherung (auch in Form von Hashwerten) in der DLT ist vermutlich hier nicht sinnvoll, da im Falle eines Unfalls der Disput nur über die kürzlich ausgetauschten Daten bestehen würde. Für die Kompensation unterzeichnet in bestimmten, vertraglich spezifizierten Intervallen (möglicherweise auch erst am Ende der Platooning-Phase) das System des hinten fahrenden Fahrzeugs Transaktionen an das vorne fahrende Fahrzeug und schickt sie diesem zu. Diese können sofort (bei Internetkonnektivität) oder später (offline) an die DLT gesendet und – sofern das entsprechende Konto gedeckt ist – ausgeführt werden. Möglicherweise muss zwischenzeitlich der Abstand vergrößert werden, etwa um Autos einfädeln zu lassen oder der aktuellen Wettersituation Rechnung zu tragen.
4. *Entkoppeln:* Ist der Platoon am geplanten Ort angekommen, will sich ein anderes Fahrzeug dem Platoon anschließen oder soll das Platoon vorzeitig beendet werden – etwa weil der vorne Fahrende die Erwartungen des Folgenden nicht erfüllt oder das hinten fahrende Fahrzeug seine Versprechungen nicht erfüllt (i. S. v. keine Signierung von Transaktionen) –, muss der Platoon enden. Durch Steuerung wie in (1) oder automatisch wird der Befehl zum Entkoppeln gegeben und der Abstand zwischen den Lkw wieder vergrößert, bis der normale, in der Straßenverkehrsordnung vorgeschriebene Mindestabstand wieder erreicht ist. Sollte der Fahrer des hinten fahrenden Fahrzeugs während des Platoonings anderen Aktivitäten nachgegangen sein (sofern gesetzlich zulässig), muss das System prüfen, ob der Fahrer nun wieder die volle Kontrolle über sein Fahrzeug übernommen hat.

Nach Phase 4 findet möglicherweise noch eine Endabrechnung statt bzw. bei der nächsten Internetverbindung werden die angesammelten Transaktionen in die DLT geladen. Ansonsten sind beide Fahrzeuge nun in der Lage, neue Platoons einzugehen oder von der Autobahn abzufahren. Sollte ein Fahrer die Vertragsbedingungen verletzt haben (keine Zahlung), so können im Nachgang anhand des Kennzeichens Rechtsmittel eingelegt werden.

[596] *Sänn/Richter/Fraunholz,* Wirtschaftsinformatik & Management 2017, 60.

10.1.5 Fazit und Handlungsempfehlungen

Wie bereits angedeutet, sind das physische Bilden von Platoons sowie die Kommunikation zwischen den beteiligten Fahrzeugen aktuell bereits unabhängig von der DLT Gegenstand von Tests. Für die Abwicklung der Kompensationszahlung kann eine DLT-Lösung ermöglichen, dass sich gegenseitig nicht bekannte Marktteilnehmer vollautomatisch und ohne zentrale Rolle einer dritten Partei faire Kompensationszahlungen für das Platooning leisten können und dabei hinreichend vor Betrug geschützt sind. Weiter könnten eine Dokumentation bei Fahrfehlern oder technischen Fehlern eines der am Platoon beteiligten Fahrzeuge eine Nachweisbarkeit in der Schuldfrage gewährleisten. DLT können somit das nötige Vertrauen generieren, damit das im Platoon führende Fahrzeug sicher sein kann, auch eine faire Kompensation für die Leistung zu erhalten, auch wenn es mit direkten Konkurrenten (d. h. anderen Spediteuren) ein Platoon bildet. Letzteres dürfte für einen Durchbruch des Platoonings entscheidend sein. Ein solcher könnte etwa in Form einer Beschleunigung des Standardisierungsprozesses bei der Car2X-Kommunikation und der Entwicklung hochautomatisierter Fahrzeuge die technologische Entwicklung fördern und gleichzeitig die anfangs beschriebenen ökonomischen Potenziale, insbesondere in Form von Einsparungen bei Kraftstoff, Lenkzeiten (in Zukunft) sowie Versicherungsbeiträgen heben.

In der Praxis werden die Kompensationszahlungen für Platooning im Bereich von einigen Cent bis einigen Euro liegen, zudem werden pro Sekunde deutschlandweit Transaktionen in einem hohen dreistelligen bis niedrigen vierstelligen Bereich liegen. Wegen der großen Anzahl an Speditionen (~15 000 allein in Deutschland[597]) würde eine DLT-Lösung hinsichtlich ihrer Performanz und Effizienz eher die Charakteristiken einer öffentlichen Blockchain aufweisen. Demnach sind weitere Anstrengungen bei der technischen Entwicklung einer DLT erforderlich, welche die entsprechende Skalierbarkeit für eine fünfstellige Anzahl an Nodes bei gleichzeitig sehr niedrigen Transaktionskosten ermöglicht. Zudem bestehen nicht nur juristische Fragestellungen hinsichtlich der DLT, sondern auch allgemeiner Art. Auf diese soll im folgenden rechtlichen Teil eingegangen werden.

Vorantreiben internationaler Standardisierung

Ein Einsatz für die internationale Standardisierung und zur Förderung der Akzeptanz elektronischer Dokumente ist notwendig, insbesondere in Bezug auf eine Nutzung der DLT im Bereich der Frachtpapiere. Moderne Lieferketten und Logistikoperationen involvieren in der Regel eine Vielzahl verschiedener Staaten, weshalb Deutschland hier seine Rolle als Exportnation nutzen und Vorreiter bei nötigen Anpassungen sein sollte.

10.2 Rechtlicher Teil

Platooning als solches und im Kontext von DLT berührt viele Rechtsbereiche, wenngleich sich das Straßenverkehrsrecht, das Vertragsrecht und der Datenschutz aufgrund ihrer direkten Praxisrelevanz in den Fokus drängen. Auf sie soll daher nachfolgend näher eingegangen werden.

[597] *Statistisches Bundesamt*, Anzahl der Speditionen in Deutschland in den Jahren von 2009 bis 2016.

10.2.1 Straßenverkehrsrecht

Bisher müssen Lastkraftwagen über 3,5 t, die über 50 km/h fahren, gemäß § 4 Abs. 3 StVO zu vorausfahrenden Fahrzeugen einen Mindestabstand von 50 m einhalten. Ohne Ausnahmegenehmigung (§ 46 StVO) ist es daher auf deutschen Straßen aktuell noch nicht möglich im Windschatten eines vorausfahrenden Lastkraftwagens eine Ersparnis an Treibstoff oder Lenkzeit zu generieren. Vor der Anpassung der Abstandsregelung müsste zudem erst geklärt werden, wie es bei ordnungsbehördlichen Abstandskontrollen für diese zweifelsfrei ersichtlich wird, ob ein Lastkraftwagen im Platoon fährt oder nicht. Abhilfe könnten hier die nach § 63a Abs. 1 StVG zu speichernden Orts- und Zeitangaben schaffen, wenn Fahrer im Platoon die Fahrzeugführung dem Fahrzeug übergeben. Zwar erlaubt § 63a Abs. 2 S. 1 StVG die Übermittlung dieser Daten an die nach Landesrecht für die Ahndung von Verkehrsverstößen zuständigen Behörden, allerdings sind bisher u. a. der Adressat der Herausgabepflicht[598] und der Speicherort der Daten[599] unklar.

Unter dem Gesichtspunkt der Verkehrssicherheit ist weitergehend zu hinterfragen, ob es vertretbar ist, das Fahren in einem Platoon als Fahrtunterbrechung i. S. d. Art. 7 Abs. 1, Art. 4 lit. d) VO (EG) Nr. 561/2006 anzusehen, muss der Fahrer eines Fahrzeugs mit hoch- oder vollautomatisierter Fahrfunktion nach § 1b Abs. 1 i. V. m. Abs. 2 StVG doch jederzeit derart wahrnehmungsbereit bleiben, dass er die Fahrzeugsteuerung unverzüglich wieder übernehmen kann, was die gemäß Art. 4 lit. d) VO (EG) Nr. 561/2006 erforderliche Erholung ausschließen könnte.[600] Die Anerkennung als Fahrtunterbrechung ist aber unter Berücksichtigung von Art. 8 Abs. 8 der VO (EG) Nr. 561/2006 nicht ausgeschlossen, da nur dieser ausdrücklich vorschreibt, dass das Fahrzeug nicht fährt.[601]

10.2.2 Vertragsrecht

Für den finanziellen Ausgleich der Effizienzgewinne der Fahrzeuge im Platoon durch die Einsparung von Treibstoff und Lenkzeiten kommen Smart Contracts in Betracht. Dabei handelt es sich um (Zahlungs-)Software, die dezentral auf einer Vielzahl von Computern in einem P2P-Netzwerk (DLT-Plattform/Blockchain) gespeichert ist.[602] Die für die Berechnung des Ausgleichsbetrags erforderlichen Eingangswerte, wie bspw. der Treibstoffverbrauch, GPS-Daten etc., werden aus Gründen des Datenschutzes off-Chain (d. h. im Platoon) verarbeitet.[603] On-Chain (d. h. auf der DLT-Plattform) wird lediglich eine (Mikro-)Transaktion in Höhe des errechneten Ausgleichsbetrags vorgenommen.[604] Im Folgenden gilt es die vertragliche Grundlage, auf der diese Transaktionen abgewickelt werden, zu konkretisieren:

10.2.2.1 Vertragsschluss

Basis eines jeden Platoons muss eine vertragliche Beziehung sein, die den Ausgleich zwischen den Beteiligten interessengerecht regelt. So muss z. B. von vornherein eindeutig sein, wer das Führungsfahrzeug bildet und die Folgefahrzeuge mit Fahrdaten versorgt, damit diese sich automatisiert fahrend in den Windschatten des Führungsfahrzeugs ein-

[598] *Wagner/Goeble,* ZD 2017, 263 (268).
[599] *Brockmeyer,* ZD 2018, 258.
[600] Siehe Fn. 2 in *Ylinen,* RdTW 2018, 121.
[601] Siehe Fn. 2 in *Ylinen,* RdTW 2018, 121.
[602] Siehe allgemein zu Smart Contracts 4.2.1 und 6.1.1.
[603] Siehe zum Datenschutz 5.3.2.3.
[604] Siehe hierzu Abschnitt 10.1.3.

reihen können. Zudem muss vorab geklärt sein, wie der Ausgleich, den die Folgefahrzeuge für ihre Treibstoffersparnis an das Führungsfahrzeug leisten, bemessen werden soll.

Fraglich ist, wie und wann diese Vereinbarungen erfolgen. Jeder Vertrag kommt durch mindestens zwei übereinstimmende Willenserklärungen, Angebot und Annahme, zustande. Eine Willenserklärung ist eine Äußerung eines auf eine Rechtsfolge gerichteten Willens, der die Begründung, inhaltliche Änderung oder Beendigung eines Rechtsgeschäfts zum Gegenstand hat. Zu ermitteln ist also, in welchem Verhalten der Teilnehmer des Platoons entsprechende, rechtlich relevante Willensäußerungen zu sehen sind. Welche Erklärungen zu welchem Zeitpunkt abgegeben werden, hängt zunächst von den Umständen des Zusammenschlusses zum Platoon im jeweiligen Einzelfall ab. Zunächst kann eine vorherige Absprache zwischen den beteiligten Spediteuren bzw. Fahrern stattfinden (geplanter Platoon). Dann werden die relevanten Willenserklärungen in der Regel bereits im Rahmen dieser Absprache abgegeben. Sollen zudem spontane Zusammenschlüsse (spontaner Platoon) möglich sein, zeigt sich das Problem, dass auf der gefahrenen Strecke nicht immer eine Verbindung zum Internet und damit zur DLT-Plattform besteht.[605] Die Möglichkeit, Zahlungen durch ein vorheriges „Einfrieren" eines bestimmten Betrags zu garantieren, steht dann nicht zur Verfügung. Gleichwohl kann ein Interesse daran bestehen, einen Smart Contract zur Zahlungsabwicklung einzusetzen. Die Parteien können dann eine Vereinbarung treffen, die sowohl eine Zahlungsverpflichtung zum Inhalt hat als auch die Pflicht, bei bestehender Internetverbindung eine Ausgleichszahlung durch Übermittlung signierter Transaktionen an den Smart Contract auszulösen. Bei solchen spontanen Zusammenschlüssen kann zunächst das Signal eines zur Konvoi-Führung bereiten Fahrzeugs ein Angebot an einen unbestimmten Personenkreis darstellen, welches durch die Fahrer der teilnehmenden Fahrzeuge angenommen wird.[606] Möglich erscheint auch das Szenario, dass ein potenzielles Führungsfahrzeug eine invitatio ad offerendum für einen Platoon aussendet, womit es zunächst nur seine Bereitschaft signalisiert, den Platoon anzuführen und ein entsprechendes vertragliches Verhältnis einzugehen. Interessierte Folgefahrzeuge können hierauf mit einem Angebot antworten und das Führungsfahrzeug dieses jeweils bestätigen (= Annahme). Selbstredend fungieren die jeweiligen Fahrer als Vertreter i. S. d. §§ 164 ff. BGB ihrer Arbeitgeber. Das vertragliche Verhältnis entsteht somit nicht zwischen den Fahrern persönlich, sondern zwischen den dahinterstehenden Logistikunternehmen.

Der Vertragsschluss ist dem Einsatz des Smart Contracts zum Zahlungsausgleich vorgelagert. Rechtlich maßgeblich für Inhalt und Wirksamkeit des Vertrags ist damit diese Vereinbarung und nicht etwa der Programm-Code des Smart Contracts.[607]

10.2.2.2 Vertragsart

Nicht uneingeschränkt eindeutig gestaltet sich die Frage nach der dem Platooning zugrunde liegenden Vertragsart. In Betracht kommen zum einen Dienstvertrag und Werkvertrag, naheliegender dürfte aber eine BGB-Innengesellschaft sein.

10.2.2.2.1 Abgrenzung zum Dienstvertrag, §§ 611 ff. BGB

[605] Zur Reaktion auf die nicht ununterbrochene Netzabdeckung siehe 10.1.2.

[606] Diese Möglichkeit dürfte eine Grenze im technischen (Rechenleistung) und rechtlichen (Länge eines Platoons) Maximum eines Platoons finden.

[607] Siehe allgemein zu Smart Contracts 4.2.1 und 6.1.1.

Ein Dienstvertrag erfordert den Austausch einer Dienstleistung im Gegenzug für eine Vergütung. Hier könnte dies dahingehend festzumachen sein, dass der Fahrer des Leitfahrzeugs die Folgefahrzeuge in seinen Windschatten aufnimmt, kontinuierlich mit Fahrdaten versorgt und hierfür exemplarisch eine Kilometerpauschale bekommt. Der Fokus beim Platooning ist jedoch vorrangig auf das gemeinsame Ziel aller Teilnehmer, den Kraftstoffverbrauch[608] und zukünftig auch die Lenkzeiten zu reduzieren, ausgerichtet. Diesem gemeinsamen Ziel lässt sich über das Gesellschaftsrecht Rechnung tragen.

10.2.2.2.2 Abgrenzung zum Werkvertrag, §§ 631 ff. BGB

Aufgrund der vorstehenden Zielsetzung der Teilnehmer eines Platoons scheidet neben dem Dienstvertrag auch der erfolgsorientierte Werkvertrag aus, denn die erfolgreiche Güterbeförderung bildet nicht den Gegenstand einer Vereinbarung über die Bildung eines Platoons.

10.2.2.2.3 Gesellschaftsvertrag, §§ 705 ff. BGB

Der Gesellschaftsvertrag ist auf die Erreichung eines gemeinsamen Zwecks gerichtet und verpflichtet die Gesellschafter gegenseitig zur Förderung dieses Zwecks. Er bedarf keiner bestimmten Form und kann daher auch konkludent geschlossen werden.[609] Zugleich kommt es nicht auf das Bewusstsein der Beteiligten an, dass sie sich zu einer Gesellschaft entsprechend dem bürgerlichen Gesellschaftsrecht zusammenschließen, ihr Wille, sich überhaupt rechtlich verbindlich zu binden, genügt.[610]

10.2.2.2.3.1 Gemeinsamer Zweck

Das Ziel der Beteiligten, durch Zusammenwirken im Platoon Kraftstoff und Lenkzeiten zu sparen, ist ein erlaubter dauerhafter eigennütziger Zweck, da es auf die Förderung der Interessen aller Gesellschafter, d. h. der hinter den Fahrern stehenden Unternehmen, gerichtet ist.[611]

10.2.2.2.3.2 Zweckförderungspflicht, Beiträge

Um die Ersparnis zu generieren, nimmt der Fahrer des Leitfahrzeugs wie bereits verdeutlicht Folgefahrzeuge in den Windschatten seines Fahrzeugs auf, lässt sein Fahrzeug via WLAN kontinuierlich Fahrdaten zu u. a. Geschwindigkeit, Bremse, GPS-Position und Beschleunigung aussenden und wacht im Übrigen über den Platoon. Da eine Dienstleistung gemäß § 706 Abs. 3 BGB beitragsfähig ist, erbringt er so den zentralen Beitrag für einen Platoon. Zusätzlich tragen alle weiteren Fahrer der Folgefahrzeuge dadurch, dass sie ihre Fahrzeuge in den Windschatten einlenken und so den Platoon vervollständigen, zur Ersparnis bei. Zudem entrichten sie den finanziellen Ausgleich an das Leitfahrzeug.

10.2.2.2.4 Stellung der Gesellschaft nach außen

Das alleinige nach innen gerichtete Ziel der Ersparnis lässt annehmen, dass kein weitergehendes Interesse der Gesellschafter besteht, dass eine Platooning-GbR (Gesellschaft

[608] Hinweis: Auch das Leitfahrzeug eines Platoons erzielt aufgrund reduzierter Verwirbelungen hinter dem Fahrzeug eine wenn auch geringere Treibstoffersparnis als die im Windschatten fahrenden Folgefahrzuge, sodass im Ergebnis sämtliche Teilnehmer eines Platoons eine Treibstoffersparnis erzielen.

[609] Staudinger/*Habermeier*, § 705 Rn. 4.

[610] BeckOGK/*Geibel*, Stand: 1.1.2019, BGB § 705 Rn. 17.

[611] Staudinger/*Habermeier*, 705 Rn. 17 f.

bürgerlichen Rechts) nach außen am Rechtsverkehr teilnimmt.[612] Folglich dürfte die technisch bedingte Geschäftsführungsbefugnis des Fahrers des Leitfahrzeugs keine Vertretungsmacht gegenüber Dritten außerhalb des Platoons umfassen, § 714 BGB im Gesellschaftsvertrag mithin abbedungen werden.[613] Mangels Außenwirkung wäre eine Platooning-GbR demnach eine reine Innengesellschaft ohne Rechtsfähigkeit.[614] Die Beziehung zwischen den Beteiligten beschränkt sich somit auf ein reines Schuldverhältnis ohne übergeordnete Organisation.[615]

Im Weiteren liegt einer Innengesellschaft für gewöhnlich kein Gesamthandsvermögen zugrunde.[616] Wenn der finanzielle Ausgleich zwischen den Teilnehmern eines Platoons durch einen DLT-basierten Smart Contract erfolgt, wickelt dieser bei übereinstimmenden Ausgleichsanweisungen der Platoon-Fahrzeuge die Zahlungen vollautomatisch ab. Die diesem Vorgang zugrunde liegenden Token dürften dabei nach dem Willen der Gesellschafter kein Gesellschaftsvermögen begründen, da der Smart Contract als Treuhänder eines jeden Platooning-Teilnehmers fungieren sollte.

Für ein Gesellschaftsvermögen und damit für eine GbR mit Außenwirkung könnte die Übermittlung der übereinstimmenden Ausgleichsanweisungen aus den Fahrzeugen an die DLT-Plattform sprechen, da hier der Platoon nach außen ersichtlich ist. Um an dieser Stelle Haftungsrisiken zu vermeiden, wäre der zeitliche Zusammenfall der Übermittlung des Zahlungsausgleichs an den Smart Contract und die Auflösung des Platoons (direkte Liquidation der GbR) vorteilhaft. Alternativ können die Platooning-Beteiligten im Innenverhältnis schuldrechtlich ein gemeinsames Vermögen vereinbaren, das dinglich bspw. vom Führungsfahrzeug gehalten wird, das dann nach außen im eigenen Namen auftritt.[617] Dies wäre auch vorteilhaft für die Abrechnung im Falle des vorzeitigen Ausscheidens eines Teilnehmers aus einem aus mehreren Fahrzeugen bestehenden Platoons. Gegen Gesellschaftsvermögen und damit eine Außen-GbR spricht im Übrigen, dass die Fahrzeuge bilateral mit dem Führungsfahrzeug abrechnen. Aus Gründen der Haftung ist hiernach die Innen-GbR vorzugswürdig, denn diese nimmt wie zuvor bereits beschrieben nicht am Rechtsverkehr teil, weshalb sie auch nicht als Zurechnungssubjekt für gesetzliche Handlungs- oder Unterlassungspflichten in Betracht kommt und damit als Haftungsschuldner ausscheidet.[618]

In Hinblick auf die Haftung der Gesellschafter[619] im Innenverhältnis ist der Grundsatz der Vertragsfreiheit maßgeblich.[620] Danach können die Teilnehmer eines Platoons interne Haftungsbeschränkungsabreden oder Haftungsausschlussabreden z. B. bezüglich der Ausgleichpflichten treffen.

10.2.2.2.5 Ausscheiden eines Gesellschafters

Abhängig vom Lade- oder Abladeort kann ein Platoon bereits an der nächsten Autobahnausfahrt ein oder mehrere Folgefahrzeuge verlieren. Das Ausscheiden aus dem Platoon könnte dabei klassisch eine Kündigung i. S. d. § 723 Abs. 1 BGB darstellen. Unter

[612] MüKoBGB/*Schäfer*, § 714 Rn. 8.
[613] Staudinger/*Habermeier*, § 714 Rn. 7.
[614] Palandt/*Sprau*, § 705 Rn. 33; MüKoBGB/*Schäfer*, § 705 Rn. 279.
[615] BeckOK BGB/*Schöne*, 47. Ed. 01.08.2018, § 705 Rn. 159.
[616] In MüKoBGB/*Schäfer*, § 705 Rn. 277 wird dies sogar als Voraussetzung einer Innengesellschaft angesehen, wenngleich es umstritten ist, ob eine Innengesellschaft nicht auch ein Gesamthandsvermögen haben kann, s. MüKoBGB/*Schäfer*, § 705 Rn. 280 ff.
[617] MüKoBGB/*Schäfer*, § 705 Rn. 280.
[618] MüKoBGB/*Schäfer*, § 714 Rn. 8.
[619] Für unfallbedingte Schäden haftet entsprechend den Regelungen des StVG der Fahrer oder der Halter, selbst im Falle eines Folgefahrzeugs, das im Platoon hochautomatisiert fährt, § 1b Abs. 4 StVG.
[620] MüKoBGB/*Schäfer*, § 705 Rn. 133.

der Annahme, dass eine Platooning-GbR im Regelfall auf bestimmte Zeit, also bspw. für die Zeit, die es für eine Transportfahrt von München nach Nürnberg braucht, geschlossen wird, fordert § 723 Abs. 1 S. 2 BGB das Vorliegen eines wichtigen Kündigungsgrunds. Muss ein Teilnehmer auf halber Strecke, d. h. in Ingolstadt, laden oder abladen, ist es praxisfremd und ineffektiv, wenn er um des Fortbestands des Platoons willen erst bis nach Nürnberg weiterfahren müsste, um von dort aus wieder nach Ingolstadt zurückzufahren. Im Falle einer Fortsetzungsklausel im Gesellschaftsvertrag, § 736 BGB, wäre dieser Teilnehmer nachvollziehbar aus dem Platoon ausgeschieden. Bei der Möglichkeit ein Fahrziel auf unterschiedlichen Wegen bei fast vergleichbarer Fahrzeit zu erreichen, dürfte ein Teilnehmer aber nicht selten wohl eine andere erfahrungsbedingte (Anzahl der Baustellen, Stau, Unfallhäufigkeit, Landschaft etc.) Präferenz haben, als diejenige, die der Fahrer des Leitfahrzeugs hat. Bei rein objektiver Betrachtung liegt ein wichtiger Kündigungsgrund in diesem Fall dann fern. Gleichwohl muss es aber allein aufgrund wirtschaftlicher Erwägungen möglich sein, flexibel aus einem Platoon ausscheiden zu können, um bspw. auf einen vom Disponenten kurzfristig zusätzlich anberaumten Ladetermin an anderer Stelle reagieren zu können. Um diese Flexibilität gewährleisten zu können, ist es erforderlich, dass im Gesellschaftsvertrag das Ausscheiden aus dem Platoon und die Fortsetzung dessen im Falle des Ausscheidens mit den Verbliebenen geregelt werden.[621] Verbleibt nach dem Ausscheiden eines Teilnehmers aus dem Platoon nur noch ein Gesellschafter, so ist die Gesellschaft mangels eigenständigen Gesellschaftsvermögens ohne Liquidation beendet. Denn der Smart Contract wickelt mit dem Ausscheiden des letzten Folgefahrzeugs automatisch den finanziellen Ausgleich ab. Letzteres liegt nahe am Rechtsgedanken des § 721 Abs. 1 BGB, der den Rechnungsabschluss nach Auflösung der Gesellschaft beschreibt. Soll bereits dauernd kilometermäßig abgerechnet werden, was nicht praxisgerecht erscheint, wäre diese Regelung abzubedingen, was der Privatautonomie obliegt.[622]

10.2.2.2.6 Eintritt eines neuen Gesellschafters

Aus der Vertragsfreiheit und dem Hinweis in § 727 Abs. 1 BGB, dass die Auflösung einer Gesellschaft bei entsprechender Bestimmung der Rechtsnachfolge im Gesellschaftsvertrag im Erbfall nicht erfolgt, ergibt sich, dass sich jederzeit ein weiteres Folgefahrzeug einem bestehenden Platoon anschließen kann, wenn es mit den bisherigen Teilnehmern einen Aufnahmevertrag schließt.[623] Bereits im Gesellschaftsvertrag können sich die Platooning-Teilnehmer zur Aufnahme weiterer Folgefahrzeuge verpflichten und einen Gesellschafter, d. h. in der Praxis den Fahrer des Leitfahrzeugs, bevollmächtigen etwaige Aufnahmeverträge abzuschließen.

10.2.2.2.7 Wechsel eines Gesellschafters

Auch der Wechsel von Teilnehmern in einem Platoon ist möglich. Entweder gestaltet sich dieser durch einen Doppelvertrag, d. h., Eintretender und Ausscheidender schließen jeweils eigene Verträge mit den übrigen Gesellschaftern, d. h., es gibt keine Rechtsbeziehung zwischen eintretendem und ausscheidendem Gesellschafter oder der Gesellschafterwechsel erfolgt durch Abtretung des Gesellschaftsanteils gemäß §§ 398, 413 BGB. Letzteres erscheint aus Gründen der Interaktion mit dem Smart Contract und der durch ihn realisierten Abrechnung als eher fernliegend.

10.2.2.2.8 Liquidation

[621] Staudinger/*Habermeier*, § 736 Rn. 5.
[622] Staudinger/*Habermeier* § 721 Rn. 3.
[623] Jauernig/*Stürner*, § 737 Rn. 10.

Im Fall einer Platooning-Innen-GbR ohne Gesamthandsvermögen ist kein Raum für eine Abwicklung nach §§ 730 ff. BGB.[624] Mit alleinigem Verbleib des Führungsfahrzeugs im Platoon löst sich die Innengesellschaft auf, was einhergeht mit ihrer Vollbeendigung.[625] Für den internen Ausgleich bedarf es keines Fortbestands der Innengesellschaft. Vielmehr sind die Beteiligten im Rahmen der nachvertraglichen Pflichten untereinander zur Herbeiführung des Ausgleichs verpflichtet.[626] Dieser erfolgt bereits durch den Smart Contract.

10.2.2.3 Leistungsstörungen und Rückabwicklung von Transaktionen

Der hier betrachtete Einsatz von Smart Contracts betrifft lediglich den Ausgleich von Vorteilen, welche die Teilnehmer des Platoons durch dessen Nutzung haben. Bei einem einwandfreien Funktionieren der Software, die den Ausgleichsbetrag berechnet, wird die Vergütung allein für tatsächlich entstandene Einsparungen gewährt. Schlechtleistungen als solche, etwa in Form einer unzureichenden Teilnahme am Platoon, sind daher nicht denkbar.[627] Möglich ist allerdings, dass im Falle technischer Probleme oder einer Lücke zwischen dem vereinbarten und dem programmierten Inhalt eine zu geringe oder zu hohe Zahlung erfolgt. Dann muss die restliche Vergütung gewährt werden (mangels Erfüllung fortbestehender Primäranspruch) oder eine Rückerstattung des überzahlten Betrags nach Bereicherungsrecht stattfinden. Fragen der Rückabwicklung stellen sich auch im Fall einer Nichtigkeit des geschlossenen Vertrags, bspw. in Folge einer Anfechtung. Zu Fragen der Rückabwicklung siehe im Übrigen den Allgemeinen Teil zu Smart Contracts (Kapitel 6.1.1).

10.2.3 Datenschutz

Der Einsatz einer DLT-Plattform zur Abwicklung von Transaktionen im Rahmen des Platoonings erfordert datenschutzrechtliche Aufmerksamkeit. Als datenschutzrechtlich betroffene Personen kommen in erster Linie die Nutzer der Blockchain-Anwendung in Betracht. Im Falle des Platoonings wird die Anwendung von Speditionsunternehmern genutzt. Es muss danach differenziert werden, ob durch Kenntnis des Speditionsunternehmens auch Informationen über hinter dem Unternehmen stehende natürliche Personen bekannt werden. Ist dies nicht der Fall, so sind die Verarbeitungen der Daten der Nutzer datenschutzrechtlich nicht relevant. Es kann dann eine DLT-Plattform zur Abwicklung der Transaktionen im Rahmen des Platoonings eingesetzt werden.

Problematischer wird es allerdings, wenn die Informationen über das Speditionsunternehmen gleichfalls Informationen über dahinterstehende natürliche Personen offenbaren. In Betracht kommen dabei neben den Geschäftsführern oder Inhabern kleinerer Speditionsunternehmen auch die Fahrer von größeren Speditionsunternehmen, soweit sich allein aus der Aktivität einer Nutzerkennung auf diese schließen lässt. Ist nicht ausgeschlossen, dass auch Speditionsunternehmen teilnehmen, die diese Voraussetzungen erfüllen, so findet durch die Verarbeitung der Nutzerkennung auf der Blockchain eine datenschutzrechtlich relevante Datenverarbeitung statt. In diesem Fall bedarf der Einsatz der Blockchain einer Anpassung zur Einhaltung der datenschutzrechtlichen Vorgaben. Es muss dabei zwischen dem Austausch der Fahrdaten zur Ermittlung der fälligen Ausgleichszahlungen und dem Datenaustausch zur Durchführung der Ausgleichszahlungen unterschieden werden.

[624] MüKoBGB/*Schäfer*, § 730 Rn. 12.
[625] BeckOGK/*Koch*, § 730 Rn. 50.
[626] MüKoBGB/*Schäfer*, § 730 Rn. 2.
[627] Die Haftung für technische Fehlfunktionen der Fahrzeuge etc. ist nicht Blockchain-spezifisch und daher nicht Gegenstand dieser Untersuchung.

10.2.3.1 Datenaustausch der Fahrdaten

Für den Austausch der Daten zur Ermittlung der fälligen Ausgleichszahlungen zwischen den Teilnehmern des Platoons kann der Datenaustausch lokal zwischen den beteiligten Lkw stattfinden. Dabei können die Daten ebenfalls durch Smart Contracts ausgewertet und die fälligen Ausgleichszahlungen berechnet werden. Soll hierfür eine temporäre Blockchain gebildet werden, so kann diese als „offene Lösung“[628] zwischen den Teilnehmern des Platoons geführt werden. Damit sind alle Teilnehmer des Platoons für die bei ihnen stattfindenden Datenverarbeitungen verantwortlich. Die Datenverarbeitungen sind zeitlich auf das Bestehen des konkreten Platoons beschränkt. Nur wenn die Speicherung der Daten über das Bestehen des Platoons hinaus zu Beweiszwecken weiterhin nötig ist, werden die Daten entsprechend länger gespeichert. Alle Teilnehmer des Platoons löschen die Daten soweit diese für die Zwecke der Abrechnung nicht mehr erforderlich sind.

10.2.3.2 Datenaustausch zur Durchführung der Ausgleichszahlungen

Die fälligen Ausgleichszahlungen können dagegen nicht auf der lokalen Blockchain vorgenommen werden. Sollen diese ebenfalls DLT-basiert ausgeführt werden, muss die dafür eingesetzte Technologie, soweit bei den teilnehmenden Speditionsunternehmen Rückschlüsse auf die dahinterstehenden natürlichen Personen möglich sind, eine Lösung zur datenschutzkonformen Umsetzung vorsehen. Eine offene Lösung kommt hierbei nicht in Betracht, da nicht alle Teilnehmer des Zahlungssystems an allen Transaktionsdaten ein Interesse haben.
Möglich erscheint aber dagegen grundsätzlich eine „zentrale Lösung“[629]. Bei dieser müsste durch eine Zentralstelle eine permissioned Blockchain betrieben werden. Über ein Rechte- und Rollen-System kann von der Zentralstelle gesteuert werden, welche Informationen für die einzelnen Teilnehmer sichtbar sind. Die Zentralstelle wäre dann datenschutzrechtlich Verantwortlicher für die On-Chain-Verarbeitungen. Als Rechtsgrundlage für die Verarbeitung kommt ein zwischen den Teilnehmern und der Zentralstelle geschlossener Vertrag in Betracht.[630] Die Zentralstelle muss über geeignete Löschkonzepte verfügen. Hier sind bspw. eine „Redactable Blockchain“[631], bei der nachträglich durch die Zentralstelle Änderungen eingebracht werden können, oder Forks[632], bei denen die Nodes dazu verpflichtet werden, ungewünschte Daten aus der dezentralen Datenbank zu löschen, möglich.

Ist eine „zentrale Lösung“ nicht möglich oder nicht gewünscht, kann auch eine „Anonymisierungslösung“[633] gewählt werden. Dabei ließe sich grundsätzlich eine Off-Chain-Saldierung umsetzen.[634] Die beteiligten Speditionsunternehmen tragen hier nicht jede Transaktion in die Blockchain, sondern führen off-Chain ein jeweils separates Kontobuch. Die fälligen Ausgleichszahlungen werden dann zwischen den Beteiligten in regelmäßigen Zeitabständen on-Chain ausgeführt. Dabei sollten bei den Ausgleichszahlungen keine Muster erkennbar werden, die auf die Identität des hinter einer Nutzerkennung

[628] Siehe zur offenen Lösung bereits unter 6.2.3.4.2.1.
[629] Siehe zur „zentralen Lösung“ bereits die Ausführungen unter 6.2.3.4.2.1.
[630] Siehe zu den Rechtsgrundlagen bei Wahl der zentralen Lösung bereits unter 6.2.4.2.2.
[631] Siehe zur Redactable Blockchain bereits unter 6.2.5.2.1.
[632] Siehe zu Forks bereits unter 6.2.5.2.2 und 4.4.3.
[633] Siehe zur „Anonymisierungslösung“ bereits unter 6.2.3.4.2.2.
[634] Zur Saldierung bereits allgemein unter 6.2.3.4.2.2.2.2.

stehenden Speditionsunternehmens bzw. der damit verbundenen Personen schließen lassen. Hierfür sollten die Nutzerkennung für jede Interaktion von den Speditionsunternehmen einmalig genutzt werden. In Betracht kommen daneben technische Anonymisierungslösungen, wie bspw. Zero-Knowledge-Proofs[635] oder der Einsatz von Stealth-Adressen in Kombination mit Ring-Signaturen[636]. Gelingt auf diese Weise eine Anonymisierung, finden on-Chain keine datenschutzrechtlich relevanten Datenverarbeitungen mehr statt. Folglich ist hierfür auch keine Rechtsgrundlage erforderlich. Eine Löschung ist ebenfalls nicht nötig.

10.2.4 Fazit & Handlungsempfehlungen

Das flächendeckende Rollout des Platoonings erfordert eine Anpassung der Abstandsregelung des § 4 Abs. 3 StVO. Zuvor sollte eine Möglichkeit für die Ordnungsbehörden gefunden werden, wie diese zuverlässig erkennen können, ob ein geringer Abstand aus einem Platoon herrührt oder nicht. Naheliegend erscheint es hierfür auf die nach § 63a Abs. 1 StVG zu speichernden Orts- und Zeitangaben, die einen Rückschluss auf den Fahrmodus (manuell/automatisiert) ermöglichen, zurückzugreifen. Obwohl es über § 63a Abs. 2 S. 1 StVG möglich ist diese Daten Ordnungsbehörden zu übermitteln, bietet diese Lösung nur bei weiterer normativer Konkretisierung insbesondere des Adressaten und des Datenspeicherorts eine konkrete Alternative. Insoweit wäre der Gebrauch der Ermächtigungsgrundlage des § 63b StVG angezeigt.

Die Einstufung von Platooning als Lenkzeitunterbrechung i. S. d. Art. 7 Abs. 1, Art. 4 lit. d) VO (EG) Nr. 561/2006 erscheint rechtlich nicht gänzlich ausgeschlossen. Jedoch ist bisher wohl noch nicht abschließend erforscht, ob die Verpflichtung des Fahrers aus § 1b Abs. 1 i. V. m. Abs. 2 StVG wahrnehmungs- und übernahmebereit für die Fahraufgabe zu sein, eine vertretbare Erholung zulässt. Insoweit bestünde daher weiterer Forschungsbedarf. Im Weiteren gründet Platooning mit DLT-basierter Zahlungsabwicklung auf einer BGB-Innengesellschaft.

Datenschutzrechtlich ergeben sich ebenfalls Herausforderungen. Oftmals werden als Nutzer der Platooning-Plattform Unternehmen auftreten, bei denen die Kenntnis des Unternehmens auch Kenntnis über dahinterstehende natürliche Personen (Unternehmensinhaber, Fahrer etc.) beinhaltet. Werden diese mit einer Nutzerkennung auf einer öffentlichen DLT-Plattform aktiv, so können datenschutzrechtlich relevante Verarbeitungsvorgänge vorliegen. Es bedarf in diesem Fall einer Anpassung der Architektur. Diese kann durch Implementierung einer Zentralstelle, welche Einfluss auf die Datenverarbeitungen nehmen kann („zentrale Lösung"), geschaffen werden. Alternativ könnten Techniken angewandt werden, um die Verbindung zwischen Nutzerkennung und Identität der Teilnehmer aufzuheben („Anonymisierungslösung").

Für den Fall, dass es sich bei den Teilnehmern ausschließlich um Unternehmen handelt, bei denen Rückschlüsse auf die hinter den Unternehmen stehenden natürlichen Personen nicht möglich sind, genügt es, auf die Speicherung personenbezogener Daten auf dem DLT-Layer zu verzichten. Die Informationen sind off-Chain zu speichern und mittels eines Hashwerts auf der DLT-Plattform zu verlinken. Eine derartige Lösung erfordert jedoch eine vorherige Prüfung der Teilnehmer darauf, ob diese die obenstehenden Herausforderungen erfüllen. Insbesondere kleinere Unternehmen könnten dann wohl nicht am System teilnehmen.

[635] Zu Zero-Knowledge-Proofs siehe bereits unter 6.2.3.4.2.2.2.3 und 5.1.3.
[636] Zu Stealth-Adressen in Kombination mit Ring-Signaturen bereits unter 6.2.3.4.2.2.2.4.

Straßenverkehrsrecht und Datenschutz

Die flächendeckende Einführung von Platooning erfordert in Deutschland vereinzelte Anpassungen im Straßenverkehrsrecht (insbesondere §§ 4 Abs. 3 StVO, 63a, 63b StVG). Um neben der Einsparung von Treibstoff weitere Einsparungen über die Lenkzeit zu generieren, ist zu erforschen, ob trotz der Verpflichtung des automatisiert im Platoon fahrenden Fahrers zur Übernahme der Fahraufgabe eine Erholung möglich ist. Im Hinblick auf den Datenschutz kann im Falle der Verarbeitung personenbezogener Daten eine Anpassung der DLT-Architektur erforderlich werden. Hierzu wurden verschiedene Lösungsmöglichkeiten aufgezeigt.

11 Schlussbetrachtung

Die Distributed-Ledger-Technologie ist eine noch vergleichsweise junge Technologie, die sich nach Überschreiten des Peaks im Hype Cycle im Jahr 2017/18 auf dem Weg zur Marktreife befindet. Aktuell befasst sich – bedingt durch die vielfältigen Anwendungsmöglichkeiten der Technologie sowohl im öffentlichen als auch im wirtschaftlichen Bereich – eine Vielzahl von Institutionen in der öffentlichen Verwaltung (z. B. das European Blockchain Observatory and Forum, Bundesamt für Migration und Flüchtlinge und Bundesministerium für Verkehr und digitale Infrastruktur), Unternehmen (z. B. IBM, Maersk und BMW), Stiftungen (z. B. IOTA, Sovrin und Share&Charge) und Forschungseinrichtungen (z. B. Hochschulen und Fraunhofer Gesellschaft) mit der Weiterentwicklung, der Anwendung oder der Bewertung der Technologie aus differierenden Perspektiven . Dabei ist die DLT keine Technologie, die bei geeigneter Förderung einen „European Champion" – also einen Monopolisten mit DLT-Geschäftsmodell – hervorbringen kann, sondern vielmehr eine digitale Infrastruktur. DLT-Lösungen können im Zusammenspiel mit weiteren Schüsseltechnologien wie Künstlicher Intelligenz oder IoT sowohl aus technologischer Sicht und auch aus ökonomischer Sicht eine Grundlage für eine Reihe von Anwendungen bieten. Es ist hervorzuheben, dass die Gründe für die Verwendung einer DLT-Lösung im Regelfall nicht rein technologischer Natur sind – ein zentrales System ist in der Regel effizienter als ein dezentrales System. Vielmehr kann DLT Prozesse digital unterstützen und Effizienz heben, für die sich bislang aus unterschiedlichen Gründen keine zentrale Plattform etablieren konnte, bspw. aufgrund der Gefahr von Monopolbildungen oder im Sinne der Aufrechterhaltung föderaler Organisationsprinzipien. Besonders in fragmentierten Märkten, wie der mittelständisch-geprägten deutschen Industrie und in der deutschen und europäischen Verwaltung weisen DLT entsprechend hohes Potenzial auf, das nicht nur einzelnen Marktakteuren zugute kommt, sondern die Effizienz und damit Wettbewerbsfähigkeit einer gesamten Branche heben kann. Sie stellt damit möglicherweise einen freiheitlichen Gegenpol zu anderen, rein kapitalistischen Gesellschaftsformen mit wenigen Großkonzernen, staatlich kontrollierten Wirtschaftsmodellen oder digitalen Zentralstaaten dar. Diese Besonderheit bedarf jedoch gleichzeitig einer speziellen Förderung: Da die Initialkosten zum Aufbau von DLT-Systemen oftmals hoch sind und der Nutzen nicht nur dem Initiator einen Wettbewerbsvorteil ermöglicht, sondern vielmehr allen Teilnehmern zugutekommt, ist es nötig deren Initiierung zu fördern. Deshalb werden gezielte Hilfestellungen und Anschubfinanzierungen des Staats benötigt, damit die typischerweise erst ab einer bestimmten kritischen Masse realisierbaren Vorteile zugunsten gesellschaftlich-ökonomischer Aspekte überhaupt realisiert werden können. Viele Vorteile der DLT wie die Vermeidung von Monopolstrukturen, aber auch gesellschaftliche Aspekte wie die Verankerung europäischer Wertvorstellungen in der digitalen Infrastruktur sind letztlich Aufgabe des Staats.

Die DLT ist daher als digitale Infrastruktur zu verstehen und nicht als ein disruptives Geschäftsmodell an sich: Sie kann erst im Zusammenspiel mit weiteren Technologien und als Grundlage für darauf aufbauende Geschäftsmodelle ihre Potenziale entfalten, um branchenweit und branchenübergreifend Effizienz zu heben.

Die besonderen Eigenschaften der DLT werfen jedoch etliche grundlegende Fragen auf: Von technischer Seite ist insbesondere das Thema der Skalierbarkeit noch unbeantwortet. Hier befinden sich Aspekte rund um die Rolle von Ansätzen zur Vergrößerung der Skalierbarkeit bzw. Konzepte, die eine geringere Skalierbarkeit erfordern (Sharding, Pruning, On-/Off-Chain-Konzepte, Hierarchien und entsprechend Interoperabilität von DLT) noch im Bereich der Grundlagenforschung. Im Rahmen des infrastrukturellen Charakters und der hohen Komplexität stellt sich zudem die Frage, ob eine Bewertung oder Zertifizierung von DLT notwendig ist.

Auch auf rechtlicher Seite sind zahlreiche Hürden vorhanden. Einerseits lässt sich zwar festhalten, dass der Einsatz von Smart Contracts zivilrechtlich gut fassbar ist. Insbesondere grundlegende Bedenken, die Fragen der Rückabwicklung betreffen, lassen sich ausräumen, da DLT-Transaktionen nicht mit den zugrunde liegenden Rechtsgeschäften gleichzusetzen sind. Bei Verträgen, die den Einsatz von Smart Contracts beinhalten, bestehen auch insofern keine Besonderheiten, als dass die Parteien das geltende Recht einhalten müssen. Grenzen sind den vertraglichen Einsatzmöglichkeiten im Ergebnis vielmehr durch den aktuellen Stand der Technik gesetzt.

Unabhängig von vertragsrechtlichen Fragestellungen ist in der weiterführenden Diskussion eine stärkere Fokussierung auf die rechtliche Qualifikation von Token zu erwarten. Es ist insbesondere zu klären, welche Rechte an Token bestehen, inwieweit diese zivilrechtlichen Schutz genießen und ob hier gesetzgeberischer Handlungsbedarf bestehen könnte.

Beachtenswert sind andererseits die datenschutzrechtlichen Herausforderungen beim Einsatz von DLT. Die europäische Datenschutz-Grundverordnung geht vom Prinzip eines zentral Verantwortlichen aus, während DLT auf eine verteilte Speicherung der Daten bei einer Vielzahl von Nodes setzt. Dieser Widerspruch lässt sich teilweise durch entsprechende Gestaltung der Architektur auflösen. Es zeigt sich jedoch, dass hierbei nicht gänzlich auf den Einsatz von Intermediären verzichtet werden kann. Koordinierende Zentralstellen können Anspruchsgegner für den von der Datenverarbeitung Betroffenen darstellen. Der offene Austausch von Daten ohne eine derartige Zentralstelle kann jedoch lediglich dann datenschutzkonform gestaltet werden, wenn auf dem DLT-Layer auf personenbezogene Daten gänzlich verzichtet wird. Eine solche Umsetzung bringt beachtliche Herausforderungen mit sich. Während Daten von Dritten off-chain gespeichert und mittels Hashwerten verlinkt werden können, befinden sich, in Gestalt des öffentlichen Schlüssels, zumindest dann personenbeziehbare Informationen der unmittelbaren Nutzer auf dem DLT-Layer, wenn die DLT-Applikation von natürlichen Personen genutzt wird oder von Unternehmen, bei denen auf die hinter den Unternehmen stehenden natürlichen Personen geschlossen werden kann. Hier bedarf es einer Anonymisierung der Nutzerkennungen, was durch deren einmalige Vergabe und gegebenenfalls durch technische Maßnahmen, wie z. B. Zero-Knowledge-Proofs, umgesetzt werden müsste. Die Umsetzung müsste zudem in der Praxis gegen Missbrauch abgesichert werden. Beachtenswert ist bei Anwendung einer Anonymisierungslösung die Abwägung mit widerstreitenden Interessen. Eine DLT-Applikation, die vollständige Anonymität der Teilnehmer sicherstellt, eröffnet Chancen zum Missbrauch für illegale Aktivitäten. Das staatliche Interesse z. B. an der Überwachung der Zahlungsströme muss daher bei der Wahl der Umsetzungsalternativen Beachtung finden und kann im Zweifel gegen die Implementierung einer Anonymisierungslösung sprechen.

Der darüber hinaus bestehende Konflikt zwischen der Immutabilität der DLT und der Durchsetzung der Betroffenenrechte auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten, muss ebenfalls aufgelöst werden. Während in gewöhnlichen Datenbanken der Verantwortliche nachträgliche Änderungen vornehmen kann, ist dies bei einer DLT-Plattform grundsätzlich weder möglich noch gewünscht. Als Lösungsansätze kommen die Implementierung technischer Vorkehrungen zur Ermöglichung einer nachträglichen Berichtigung durch einen Berechtigten oder abermals der Verzicht auf die Speicherung personenbezogener Daten auf dem DLT-Layer in Betracht, welcher eine nachträgliche Veränderung verhindern würden.

Bei der Analyse der vier Use Cases im speziellen Teil stellt sich heraus, dass diese hinsichtlich der Potenziale der DLT ein großes Spektrum aufweisen. Beim elektrischen Laden, Ridesharing und Platooning kann eine praktische Anwendung der DLT Effizienz heben und Prozesse optimieren. Allerdings sind in diesen Use Cases die Einsparungen überschaubar oder schwer quantifizierbar. Im Gegensatz dazu handelt es sich besonders beim

Anwendungsfall „Bill of Lading“ um ein Beispiel, bei dem mithilfe der DLT enorme Verbesserungen bzw. Einsparungen möglich sind.

Insgesamt ist davon auszugehen, dass die Distributed-Ledger-Technologie kurzfristig viele der hohen Erwartungen nicht erfüllen wird, die auch im Rahmen des Hypes um Kryptowährungen entstanden sind. Langfristig jedoch werden viele technologische Hürden überwunden und rechtliche Probleme von technologischer oder gesetzgeberischer Seite gelöst werden. Entsprechend ist bei der Förderung ein interdisziplinärer Rahmen nötig, der über einen langen Atem verfügt und die Bildung von unternehmensübergreifenden Konsortien fördert. Der Staat sollte sich als Profiteur der Vorteile der Distributed-Ledger-Technologie begreifen und für den Wirtschaftsstandort und für die Gesellschaft alle nötigen Maßnahmen ergreifen, um die Verwendung der Technologie zu fördern. Andernfalls wird die Weiterentwicklung der Technologie in andere Länder abwandern. In Deutschland sind sowohl von der gesellschaftlichen als auch von der technologisch-kreativen Seite beste Voraussetzungen geschaffen, um die Entwicklung der DLT zu prägen und ihre Vorteile zu nutzen. Verpasst Deutschland bzw. Europa diese Chance, so ist zu befürchten, dass die Entwicklung der DLT sich in andere Länder und Gesellschaften verlagert, dann letztlich aber dennoch in Europa adaptiert wird. Dies hätte entsprechende negative Konsequenzen, da die Regulierung neuer Technologien immer mehr Zeit benötigt, als die technologische Weiterentwicklung. Regulierung geschieht typischerweise erst dann, wenn die Nachfrage nach Regulierung vorhanden ist und Rechtssicherheit für die kreativen Köpfe in unserer Gesellschaft geschaffen werden soll. Dies kann durch Sandboxes, Reallabore und das Vorhandensein kompetenter Ansprechpartner in öffentlichen Einrichtungen bzw. Ministerien erreicht werden. Erst dann kann gezielte Förderung einen fruchtbaren Boden für Entwicklungen schaffen.

Literaturverzeichnis

Acs, Blockchain Innovation 2018, abrufbar unter: https://www.ipaustralia.gov.au/sites/default/files/reports_publications/acs-blockchain-report_0.pdf.

Alam/Besselink/Turri/Martensson/Johansson, Heavy-Duty Vehicle Platooning for Sustainable Freight Transportation: A Cooperative Method to Enhance Safety and Efficiency, jurisPR-BKR 2015, 34-56.

Ali/Awad, Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes, Sensors (Basel, Switzerland) 2018, 1-17.

Alkom/Vliet/Aarts/Eckhardt 2016 European Truck Platooning Challenge (European Truck Platooning, Hrsg.), abrufbar unter: https://eutruckplatooning.com/PageByID.aspx?sectionID=131542&contentPageID=529927.

Alstyne/Eisenmann/Parker, Strategies for two-sided markets, Harvard business review 2006, 92-104.

Ammann, Bitcoin als Zahlungsmittel im Internet, Rechtliche Fragestellungen und Lösungsansätze, CR 2018, 379-386.

Anderson, LADEN2020 Schlussbericht 2016, abrufbar unter: https://elib.dlr.de/111054/2/LADEN2020_Schlussbericht.pdf.

Andersson/Hjalmarsson/Avital, Peer-to-Peer Service Sharing Platforms: Driving Share and Share Alike on a Mass-Scale, The 34th International Conference on Information Systems. ICIS 2013, 1-15.

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE 2007, abrufbar unter: https://www.lda.bayern.de/media/wp136_de.pdf.

Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 00264/10/DE 2010.

Ateniese/Magri/Venturi/Andrade, Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. in: 2017 IEEE European Symposium on Security and Privacy (EuroS&P) 2017, 111.

Auer-Reinsdorff/Conrad Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Baird/Mance/Madsen 2018 Hedera: A Governing Council & Public Hashgraph Network, abrufbar unter: https://s3. amazonaws. com/hedera-hashgraph/hh-whitepaper-v1. 0-180313. pdf.

Bajpai, IBM and Blockchain: What It Did In 2018, And Where It's Going In 2019 2019, abrufbar unter: https://www.nasdaq.com/article/ibm-and-blockchain-what-it-did-in-2018-and-where-its-going-in-2019-cm1100102.

Baliga/Subhod/Kamat/Chatterjee 2018 Performance evaluation of the quorum blockchain platform, abrufbar unter: https://arxiv.org/abs/1809.03421.

Bamberger/Roth/Hau/Poseck Beck'scher Online Kommentar BGB, 48. Aufl., München 2018.

Bambrough, A Gold Standard Of ICOs Is Needed -- But It Won't Be Easy 2018, abrufbar unter: https://www.forbes.com/sites/billybambrough/2018/07/04/a-gold-standard-of-icos-is-needed-but-it-wont-be-easy/#7d652a5b4600.

Bechtolf/Vogt, Datenschutz in der Blockchain – Eine Frage der Technik, Technologische Hürden und konzeptionelle Chancen, ZD 2018, 66-71.

Beck 2011 Die Finanzkrise ist auch eine Vertrauenskrise (Max-Planck-Institut für Gesellschaftsforschung (MPIfG), Hrsg.), abrufbar unter: http://www.mpifg.de/pu/ueber_mpifg/mpifg_jb/JB1112/MPIfG_11-12_06_Beckert_Vertrauen.pdf.

Beck/König, Bitcoin: Der Versuch einer vertragstypologischen Einordnung von kryptographischem Geld, JZ 2015, 130-138.

Beck/König, Bitcoins als Gegenstand von sekundären Leistungspflichten, Erfassung dem Grunde und der Höhe nach, AcP 215 (2015), 655-682.

Beck/Müller-Bloch/King, Governance in the blockchain economy: A framework and research agenda, Journal of the Association for Information Systems 2018, 1020-1034.

Beecher, Can the Electronic Bill of Lading Go Paperless?, The International Lawyer 2006, 627-647.

Begleit- und Wirkungsforschung Schaufenster Elektromobilität, Good E-Roaming Practice: Praktischer Leitfaden zur Ladeinfrastruktur-Vernetzung in den Schaufenstern Elektromobilität 2015, abrufbar unter: https://schaufenster-elektromobilitaet.org/media/media/documents/dokumente_der_begleit__und_wirkungsforschung/Ergebnispapier_Nr_5_Good_E-Roaming_Practice.pdf.

Bergenhem/Hedin/Skarin, Vehicle-to-Vehicle Communication for a Platooning System, Procedia - Social and Behavioral Sciences 2012, 1222-1233.

*Bernstein/*Buchmann, J. (Hrsg.), Dahmen E., Introduction to post-quantum cryptography, Post-Quantum Cryptography 2009, 1-14.

Bernstorff, Das "reine Konnossement" im Seefrachtverkehr und die Ersatzmöglichkeit durch das elektronische "Bolero - bill of lading", RIW 2001, 504-512.

Bertram, Smart Contracts, Praxisrelevante Fragen zu Vertragsabschluss, Leistungsstörungen und Auslegung, MDR 2018, 1416-1421.

Beyerer/Müller-Quade/Reussner, Karlsruher Thesen zur Digitalen Souveränität Europas, DuD 2018, 277-280.

Bhoopalam/Agatz/Zuidwijk, Planning of truck platoons: A literature review and directions for future research, Transportation Research Part B: Methodological 2018, 212-228.

Binns/Lyngs/Kleek/Zhao/Libert/Shadbolt, Third Party Tracking in the Mobile Ecosystem, Proceedings of the 10th ACM Conference on Web Science 2018, 23-81.

Bitkom, Blockchain und Datenschutz – Faktenpapier Bitkom 2017, abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf.

Bitkom, Künstliche Intelligenz 2017.

Blockchain Bundesverband, Blockchain, data protection and the GDPR 2018, abrufbar unter: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf.

Blockchain Bundesverband Finance Working Group 2018 Statement on Token Regulation with a Focus on Token Sales, abrufbar unter: http://bundesblock.de/wp-content/uploads/2019/01/180209_Statement-Token-Regulation_blockchain-bundesverband.pdf.

BMVI, Ethik-Kommission: Automatisiertes und Vernetztes Fahren 2017.

BMW Group. 13.02.2019 Blockchain: Developing standards for universal application in the mobility sector, München, abrufbar unter: https://www.press.bmwgroup.com/global/article/detail/T0291855EN/blockchain:-developing-standards-for-universal-application-in-the-mobility-sector?language=en.

BMWi, Energiekonzept für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung BMWi, BMU 2010.

*Böhm (*2019, 21. Januar), Google soll 50 Millionen Euro Strafe zahlen, DSGVO in Frankreich, Spiegel Online, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/dsgvo-50-millionen-euro-strafe-fuer-google-in-frankreich-a-1249171.html.

Boom, Certain legal aspects of electronic bills of lading, European Transport Law (ETL) 1997, 9-24.

Borgia, The Internet of Things vision: Key features, applications and open issues, Computer Communications 2014, 1-31.

Brandt, Neue Kryptoprojekte bald so effizient wie Visa 2018.

Brink/Wolff Beck'scher Online-Kommentar Datenschutzrecht, 26. Aufl., München 2018.

Brockmeyer, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, Erwägungen zur ausstehenden Regulierung des Speicherorts für die Daten nach § 63a Abs. 1 StVG, ZD 2018, 258-263.

Bruckner, Organisationales Vertrauen initiieren, Wiesbaden 2015.

BTC-Echo, Der deutsche Blockchain Index 2018, abrufbar unter: https://www.btc-echo.de/blockchain-studie-oekosystem-deutschland-2018/.

Bundesamt für Güterverkehr, Entwicklung der gefahrenen Mautkilometer in Deutschland von 2005 bis 2017 (in Milliarden Kilometer) 2019, abrufbar unter: https://de.statista.com/statistik/daten/studie/202642/umfrage/entwicklung-der-gefahrenen-mautkilometer-in-deutschland/#0.

Bundesanstalt für Finanzdienstleistungsaufsicht, Merkblatt Finanzinstrumente vom 20.12.2011, geändert am 26.07.2018 2011, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html.

Bundesanstalt für Finanzdienstleistungsaufsicht, Virtuelle Währungen/Virtual Currency (VC) 2016, abrufbar unter: https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_artikel.html.

Bundesanstalt für Finanzdienstleistungsaufsicht, Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs) 2017, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html?nn=11056122.

Bundesanstalt für Finanzdienstleistungsaufsicht, Hinweisschreiben vom 20.02.2018, GZ: WA 11-QB 4100-2017/0010 2018.

Bundesministerium für Verkehr und digitale Infrastruktur, Verkehrsverflechtungsprognose 2030 2014, abrufbar unter: https://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/verkehrsverflechtungsprognose-2030-zusammenfassung-los-3.pdf?__blob=publicationFile.

Bundesministerium für Verkehr und digitale Infrastruktur, Elektronische Deichsel – Digitale Innovation – EDDI Bundesministerium für Verkehr und digitale Infrastruktur 2019, abrufbar unter: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/AVF-projekte/eddi.html.

Bundesministerium für Wirtschaft und Energie, Grünbuch Digitale Plattformen 2016, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/gruenbuch-digitale-plattformen.pdf?__blob=publicationFile&v=20.

Bundesministerium für Wirtschaft und Energie, Weißbuch Digitale Plattformen 2017, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v=24.

Buterin 2018 Ethereum White Paper, abrufbar unter: https://github.com/ethereum/wiki/wiki/White-Paper.

Christine Lagarde (2018, November), Winds of Change: The Case for New Digital Currency, Singapore Fintech Festival.

Christopher/Lee, Mitigating supply chain risk through improved confidence Emerald Group Publishing Limited 2013, abrufbar unter: https://www.emeraldinsight.com/doi/full/10.1108/09600030410545436.

Cohen/Kietzmann, Ride on! Mobility business models for the sharing economy, Organization & Environment 2014, 279-296.

CoinMarketCap, Historical Snapshots 2019, abrufbar unter: https://coinmarketcap.com/historical/.

Cong/He, Blockchain disruption and Smart Contracts 2018, abrufbar unter: https://www.nber.org/papers/w24399.pdf.

Cordis 2018 ENSEMBLE: ENabling SafE Multi-Brand pLatooning for Europe, abrufbar unter: https://cordis.europa.eu/project/rcn/216001/factsheet/en.

Customs, Saudi Customs Pilot Sees the Integration of Customs Tracking Feature with IBM and Maersk TradeLens Blockchain Solution 2018, abrufbar unter: https://www.customs.gov.sa/en/node/1022.

Danwerth, The Regulation of Bitcoin and Other Virtual Currencies under Japanese Law in Comparative Perspective, ZVglRWiss 2018, 117-155.

Dauner-Lieb/Langen Bürgerliches Gesetzbuch - BGB, 3. Aufl., Baden-Baden 2016.

Dead Coins, Curated List of cryptocurrencies forgotten by this world…and more 2019, abrufbar unter: https://deadcoins.com/#.

Deakin/Frick/Shively, Markets for Dynamic Ridesharing?, Transportation Research Record 2010, 131-137.

DeFilippi, What blockchain means for the sharing economy, Harvard Business Review Digital Articles 2017, 2-5.

Deutsche Handwerkszeitung, Kraftstoffverbrauch: So viel CO2 stößt Ihr Auto aus 2018, abrufbar unter: https://www.deutsche-handwerks-zeitung.de/kraftstoff-verbrauch-in-co2-ausstoss-umrechnen/150/3097/57956.

Deutsches Zentrum für Luft- und Raumfahrt, Automatisiertes und vernetztes Fahren im Güterverkehr - Auswirkungen auf die Logistikbranche 2017, abrufbar unter: https://www.dlr.de/dlr/presse/desktopdefault.aspx/tabid-10172/213_read-25203/#/gallery/29204.

Diepenbrock/Sachweh, Ein konzeptionelles Rahmenwerk für die Integration Digitaler Souveränität in Softwarearchitekturen, DuD 2018, 281-285.

*Dittmer (*2017, 29. November), Gigantischer Schwund: Millionen Bitcoins sind für immer verloren, n-tv, abrufbar unter: https://www.n-tv.de/wirtschaft/Millionen-Bitcoins-sind-fuer-immer-verloren-article20158230.html.

Djazayeri, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 2016, Anm. 1.

Dudenhausen/Hahn, Ganzheitliche Digitalisierungsansätze im Stadtwerk: Von der Strategie bis zur Umsetzung, Herausforderung Utility 4.0 2017, 683-700.

Dunphy/Petitcolas, A First Look at Identity Management Schemes on the Blockchain, IEEE Security & Privacy 2018, 20-29.

DuPont, Experiments in algorithmic governance, A history and ethnography of “The DAO,” a failed decentralized autonomous organization, Bitcoin and Beyond 2017, 157-177.

Ehmann/Selmayr DS-GVO, Beck'sche Kurz-Kommentare, 2. Aufl., München 2018.

EMIL Deutschland AG, Wer wenig fährt, sollte wenig zahlen EMIL Deutschland AG 2019, abrufbar unter: https://emil.de/.

Engelhardt/Klein, Bitcoins – Geschäfte mit Geld, das keines ist, Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355-360.

Ernst & Young, Initial Coin Offerings (ICOs): The Class of 2017 – one year later 2018.

Etherscan, www.etherscan.io Etherscan 2019, abrufbar unter: https://etherscan.io/address/0xbb9bc244d798123fde783fcc1c72d3bb8c189413#.

EU Blockchain Observatory and Forum, About the European Union Blockchain Observatory and Forum 2019, abrufbar unter: https://www.eublockchain-forum.eu/about.

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

Europäische Kommission, COM(2018) 109 final 2018.

Europäische Kommission 2018 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung von CO2-Emissionsnormen für neue schwere Nutzfahrzeuge, abrufbar unter: https://eur-lex.europa.eu/resource.html?uri=cellar:93c5b96c-7ed6-11e8-ac6a-01aa75ed71a1.0009.02/DOC_1&format=PDF.

Europäische Kommission 2019 Künstliche Intelligenz: Kommission treibt Arbeit an Ethikleitlinien weiter voran (Europäische Kommission, Hrsg.). : Europäische Kommission.

European Commission, Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy 2015, abrufbar unter: https://ec.europa.eu/digital-single-market/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud.

European Commission, European countries join Blockchain Partnership 2018, abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership.

European Securities and Markets Authority, ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements 2017, abrufbar unter: unter https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.

European Securities and Markets Authority, Own Initiative Report on Initial Coin Offerings and Crypto-Assets 2018, abrufbar unter: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.

European Securities and Markets Authority, Advice Initial Coin Offerings and Crypto-Assets 2019, abrufbar unter: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

Falkon, The Story of the DAO — Its History and Consequences Medium 2017, abrufbar unter: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.

Filippi/Hassan, Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code, First Monday 2016, 1-23.

Finck, Blockchains and Data Protection in the European Union, EDPL 2018, 17-35.

FINMA, Faktenblatt Virtuelle Währungen, Stand 30.08.2018, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaetter/faktenblatt-virtuelle-waehrungen.pdf?la=de.

FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16.02.2018, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de&hash=6518A4B3067554A0E22600E167601EF59AA20542.

Flämig, Autonome Fahrzeuge und autonomes Fahren im Bereich des Gütertransportes, Autonomes Fahren 2015, 377-398.

Frantz/Nowostawski, From institutions to code: Towards automated generation of smart contracts, IEEE 1st International Workshops on Foundations and Applications on Self* Systems 2016, 210-215.

Fridgen/Guggenmos/Lockl/Rieger/Urbach 2018 Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain: Eine Machbarkeitsstudie des Bundesamtes für Migration und Flüchtlinge, Nürnberg: Bundesamt für Migration und Flüchtlinge, Bundesamt für Migration und Flüchtlinge (S. 1-32), abrufbar unter: https://eref.uni-bayreuth.de/46480/.

Froitzheim, Code is Law, isn't it? in: *Taeger (Hg.)* Rechtsfragen digitaler Transformationen. Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, 311.

Furuhata/Dessouky/Ordóñez/Brunet/Wang/Koenig, Ridesharing: The state-of-the-art and future directions, Transportation Research Part B: Methodological 2013, 28-46.

Fußwinkel/Kreiterling, Blockchain-Technologie – Gedanken zur Regulierung 2018, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel.html?nn=11056122#U33.

Glatz, What are Smart Contracts? In search of a consensus. 2014, abrufbar unter: https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad.

Global Agenda Council on the Future of Software & Society 2015 Deep Shift: World Economic Forum, abrufbar unter: www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

Goldby, Electronic bills of lading and central registries: what is holding back progress? Routledge 2008, abrufbar unter: https://www.tandfonline.com/doi/abs/10.1080/13600830802239381.

Goldfeder/Bonneau/Gennaro/Narayanan, Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. in: *Kiayias (Hg.)* Financial Cryptography and Data Security, Cham 2017, 321.

Grassi, Letter of Credit Transactions: the Banks' Position in Determiningg Documentary Compliance. A Comparative Evaluation Under U.S., Swiss and German Law, 7 Pace Int'l Rev. 1995, 81-128.

Grathwohl, Die Rolle einer Roaming- und Clearing-Stelle für Elektrofahrzeuge im System der Elektromobilität, Kartellrechtliche Bewertung von Standardisierungsstrategien 2015, 221-271.

Gratzke/Schatsky/Piscini, Banding together for blockchain 2017, abrufbar unter: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/emergence-of-blockchain-consortia.html#endnote-sup-2.

Grembergen/Haes, Introduction to the Minitrack on IT Governance and its Mechanisms. in: *Bui (Hg.)* Proceedings of the 51st Hawaii International Conference on System Sciences 2018, 4877.

Grosse-Ophoff/Hausler/Heineke/Möller, How shared mobility will change the automotive industry 2017, abrufbar unter: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/how-shared-mobility-will-change-the-automotive-industry.

Gsell/Krüger/Lorenz/Reyman beck-online GROSSKOMMENTAR, München.

Gtreview, New blockchain shipping consortium to rival Maersk and IBM's TradeLens 2018, abrufbar unter: https://www.gtreview.com/news/fintech/new-blockchain-shipping-consortium-to-rival-maersk-and-ibms-tradelens/.

Habersack Münchener Kommentar zum Bürgerliches Gesetzbuch, 7. Aufl., München 2017.

Hahn/Grün, Modell eines eRoaming-Systems für die Elektromobilität, IR 2013, 293-296.

Hahn/Metcalfe, The Ridesharing Revolution: Economic Survey and Synthesis 2017, abrufbar unter: https://www.brookings.edu/wp-content/uploads/2017/01/ridesharing-oup-1117-v6-brookings1.pdf.

Hahn/Wons, Initial Coin Offering (ICO), Wiesbaden 2018.

Haucap/Pavel/Aigner/Arnold/Hottenrott/Kehder, Chancen der Digitalisierung auf Märkten für urbane Mobilität: Das Beispiel Uber, List Forum für Wirtschafts- und Finanzpolitik 2017, 139-183.

Hazard/Haapio, Wise contracts: smart contracts that work for people and machines, Proceedings of the 20th International Legal Informatics Symposium IRIS 2017, 425-432.

Heinrichs/Thomaier/Parzonka, Arbeitsberichte zur Verkehrsforschung: Ko-Automobilität 2017, abrufbar unter: https://elib.dlr.de/112759/1/Autoteilen-Abschlussbericht%20%28final%29%20_2017_08_22.pdf.

Henssler/Strohn Gesellschaftsrecht, 4. Aufl., München 2019.

Herber Münchener Kommentar zum Handelsgesetzbuch, 3. Aufl., München 2014.

Hochhold/Rudolph, Principal-Agent-Theorie, Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende 2011, 131-145.

Hoeren/Sieber/Holznagel Handbuch Multimedia-Recht, 47. Aufl., München 2019.

Hofert, Regulierung der Blockchains, Tübingen 2018.

Hoffmann, Paukenschlag aus Las Vegas 2019, abrufbar unter: https://www.eurotransport.de/artikel/paukenschlag-aus-las-vegas-daimler-kehrt-sich-von-platooning-ab-10644852.html.

Hopt/Kumpan/Merkt/Roth Handelsgesetzbuch, 38. Aufl., München 2018.

Hyland-Wood/Khatchadourian, A Future History of International Blockchain Standards, The JBBA 2018, 3724.

ICOdata.io, ICO Status 2019, abrufbar unter: https://www.icodata.io/ICO.

International Chamber of Shipping, Shipping and World Trade Shipping and World Trade, abrufbar unter: http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

International Organization for Standardization, Standards catalogue ISO/TC 307 2019, abrufbar unter: https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0.

IOTA Foundation, IOTA 2019, abrufbar unter: https://www.iota.org/.

Janssen/Zwijnenberg/Blankers/Kruijff, Truck Platooning: Driving the Future of Transportation 2015, abrufbar unter: https://www.tno.nl/en/about-tno/news/2015/3/truck-platooning-driving-the-future-of-transportation-tno-whitepaper/.

Jentzsch 2016 Decentralized autonomous organization to automate governance. White paper, November., abrufbar unter: https://download.slock.it/public/DAO/WhitePaper.pdf.

Joblift, Nach Start-ups entdecken auch Konzerne die Blockchain: über 1.500 Stellen rund um die innovative Technologie in Deutschland 2018, abrufbar unter: https://joblift.de/Presse/blockchain-jobs.

Johnson, Can La'Zooz Take Ridesharing to the Moon? 2015, abrufbar unter: https://cointelegraph.com/news/can-lazooz-take-ridesharing-to-the-moon.

Joos/Karlstetter, Blockchain-as-a-Service im Unternehmen nutzen 2018, abrufbar unter: https://www.cloudcomputing-insider.de/blockchain-as-a-service-im-unternehmen-nutzen-a-763985/.

Kaulartz, Die Blockchain-Technologie, CR 2016, 474-480.

Kaulartz, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, Taeger (Hg.) 2016 – Smart world 2016, 1023-1037.

Kaulartz/Heckmann, Smart Contracts - Anwendungen der Blockchain-Technologie, CR 2016, 618-624.

Kaulartz/Matzke, Die Tokenisierung des Rechts, NJW 2018, 3278-3283.

Keding, Die aufsichtsrechtliche Behandlung von Machine-to-Machine-Zahlungen unter Rückgriff auf Peer-to-Peer-Netzwerke, WM 2018, 64-72.

Klein/Kottbauer, Strategien erfolgreich entwickeln und umsetzen, München 2017.

Klein/Prinz/Gräther, A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities, Reports of the European Society for Socially Embedded Technologies 2018, 1-10.

Kling, Sprachrisiken im Privatrechtsverkehr, Tübingen 2008.

Kraftfahrt-Bundesamt, Pressemitteilung Nr. 06/2018 - Der Fahrzeugbestand am 1. Januar 2018 Kraftfahrt-Bundesamt 2018, abrufbar unter: https://www.kba.de/DE/Service/Nachrichten/2018/PM/PM_Nr_06_2018_Bestand_2018.html.

Kshetri/Voas, Blockchain-Enabled E-Voting 2018, abrufbar unter: https://www.researchgate.net/publication/326239528_Blockchain-Enabled_E-Voting.

Kühling/Buchner Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Kütük/Sorge, Bitcoin im deutschen Vollstreckungsrecht, Von der "Tulpenmanie" zur "Bitcoinmanie", MMR 2014, 643-646.

Lamberti/Gatteschi/Demartini/Pranteda/Santamaria, Blockchain or not blockchain, that is the question of the insurance and other sectors, IT Professional (Early Access) 2017, 1-13.

Lang/Szczepanski/Wurzer, The Emerging Art of Ecosystem Management 2019, abrufbar unter: https://www.bcg.com/publications/2019/emerging-art-ecosystem-management.aspx?utm_medium=Email&utm_source=201902&utm_campaign=201902_NoVal_EALERT_NONE_GLOBAL&utm_usertoken=6f68b280d06f3c5d6d5badb9dfafb98414c9fa6e&redir=true.

Layne/Lee, Developing fully functional E-government: A four stage model, Government information quarterly 2001, 122-136.

Lehner, Der rechtliche Rahmen der Elektromobilität, Eine Betrachtung der Ladesäulenverordnung und des Messstellenbetriebsgesetzes unter Berücksichtigung der Blockchain-Technologie, RAW 2018, 17-21.

Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau 2017 Blockchain und Smart Contracts: vbw Die Bayerische Wirtschaft.

Leupold/Glossner Münchener Anwaltshandbuch IT-Recht, München 2008.

Lin/Liao, A Survey of Blockchain Security Issues and Challenges, International Journal of Network Securtiy 2017, 653-659.

Linke/Jürschik, Analog trifft digital - Neuigkeiten bei den rechtlichen Rahmenbedingungen zum Ridesharing, NZV 2018, 496-506.

Ludwigs, Rechtsfragen der Sharing Economy am Beispiel der Modelle Uber und Airbnb, NVwZ 2017, 1646-1653.

Lyons/Courcelas/Timsit, Blockchain for Government and Public Services 2018, abrufbar unter: https://www.eublockchainforum.eu/reports.

MaaS Alliance, Guidelines & recommendations to create the foundations for a thriving MaaS Ecosystem 2017.

Macaulay/Buckalew/Chung 2015 Internet of Things in Logistics: DHL Trend Research, Cisco Consulting Services, abrufbar unter: http://www.dpdhl.com/content/dam/dpdhl/presse/pdf/2015/DHLTrendReport_Internet_of_things.pdf.

MarketsandMarkets, Blockchain Market by Provider, Application (Payments, Exchanges, Smart Contracts, Documentation, Digital Identity, Supply Chain Management, and GRC Management), Organization Size, Industry Vertical, and Region - Global Forecast to 2023 2018, abrufbar unter: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html.

Markl, Eine nationale Daten- und Analyseinfrastruktur als Grundlage digitaler Souveränität, Informatik Spektrum 2018, 433-439.

Marnau, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung. in: *Eibl & Gaedke (Hg.)* INFORMATIK 2017, Bonn 2017, 1025.

Marquette, Crypto-based funds crawl toward mom and pop 2019, abrufbar unter: https://www.rollcall.com/news/congress/the-future-holds-cryptocurrency-based-funds-says-secs-jackson.

Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, 1251-1259.

*Martin-Jung (*2019, 4. Februar), Passwort für 190 Millionen Dollar fehlt, Süddeutsche Zeitung, abrufbar unter: https://www.sueddeutsche.de/digital/krypto-waehrung-passwort-tod-bitcoin-blockchain-1.4315793.

Mattila/Seppälä 2016 Digital trust, platforms, and policy. (no. 42). : ETLA Brief.

Mattila/Seppälä, Distributed Governance in Multi-sided Platforms: A Conceptual Framework from Case: Bitcoin, Collaborative Value Co-Creation in the Platform Economy 2018, 183-205.

McKinsey & Company, Lkw-Industrie: Jeder dritte Lastwagen bis 2025 teilautonom McKinsey & Company 2016, abrufbar unter: https://www.mckinsey.com/de/news/presse/lkw-industrie-jeder-dritte-lastwagen-bis-2025-teilautonom.

Melliger/Vliet/Liimatainen, Anxiety vs reality – Sufficiency of battery electric vehicle range in Switzerland and Finland, Transportation Research Part D: Transport and Environment 2018a, 101-115.

Melliger/Vliet/Liimatainen, Anxiety vs reality-Sufficiency of battery electric vehicle range in Switzerland and Finland, Transportation Research Part D: Transport and Environment 2018b, 101-115.

MotionWerk GmbH, Open Mobility System (OMOS) 2019, abrufbar unter: https://www.omos.io/.

Mühle/Grüner/Gayvoronskaya/Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review 2018, 80-86.

Mukherjee/Banerjee/Misra, Ad-hoc ride sharing application using continuous sparql queries. in: Proceedings of the 21st International Conference on World Wide Web 2012, 579.

Müller, Studie über internationalen Arbeitsmarkt 2018, abrufbar unter: https://www.datacenter-insider.de/deutschland-stark-bei-bitcoin-blockchain-und-dlt-a-782634/.

Mulligan/Scott/Warren/Rangaswami 2018 Blockchain Beyond the Hype (World Economic Forum, Hrsg.), abrufbar unter: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf.

Nærland/Müller-Bloch/Beck/Palmund, Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments. in: 38th International Conference on Information Systems (ICIS) 2017, 1.

Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2008, abrufbar unter: https://bitcoin.org/bitcoin.pdf.

Narayanan/Bonneau/Felten/Miller/Goldfeder, Bitcoin and cryptocurrency technologies: A comprehensive introduction, Princeton 2016.

Natoli/Gramoli, The blockchain anomaly, 2016 IEEE 15th International Symposium 2016, 310-317.

Nowak/Viereckl/Kauschke/Starke, The era of digitized trucking 2018, abrufbar unter: https://www.strategyand.pwc.com/media/file/The-era-of-digitized-trucking-charting-your-transformation.pdf.

Oberländer/Röglinger/Rosemann/Kees, Conceptualizing business-to-thing interactions – A sociomaterial perspective on the Internet of Things, European Journal of Information Systems 2018, 486-502.

Oliveira/Zavolokina/Bauer/Schwabe, To Token or not to Token: Tools for Understanding Blockchain Tokens 2018, abrufbar unter: https://www.zora.uzh.ch/id/eprint/157908/.

Origin Protocol, ORIGIN - Decentralized marketplaces on the blockchain 2019, abrufbar unter: https://www.originprotocol.com/en.

Osterland/Rose, Engineering sustainable blockchain applications, Proceedings of 1st ERCIM Blockchain 2018, 1-8.

Otte, Die Finanzmärkte und die ökonomische Selbstbehauptung Europas, Wiesbaden 2019.

Overkamp/Schings, Blockchain im Strom- und Verkehrssektor, Potenziale und rechtliche Herausforderungen, EnWZ 2019, 3-8.

Paal/Pauly Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Beck'sche Kompakt-Kommentare, 2. Aufl., München 2018.

Palandt Bürgerliches Gesetzbuch, 78. Aufl., München 2019.

Panetta, Gartner Top 10 Strategic Technology Trends for 2019 2018, abrufbar unter: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/.

Parhofer/Klöhn/Resas, Initial Con Offerings (ICOs), ZBB 2018, 89-106.

Paulus, C./Matzke, Digitalisierung und private Rechtsdurchsetzung, Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?, CR 2017, 769-778.

Paulus, D./Matzke, Smart Contracts und das BGB - Viel Lärm um nichts?, ZfPW 2018, 431-466.

Pike/Capobianco/Gomes 2018 Blockchain Technology and Competition Policy - Issues paper by the Secretariat (Organisation for Economic Co-operation and Development, Hrsg.), abrufbar unter: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf.

Popov 2018 The tangle, abrufbar unter: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

Port of Rotterdam, ABN AMRO, Samsung SDS and the Port of Rotterdam Authority are launching a container logistics blockchain pilot 2018, abrufbar unter: https://www.portofrotterdam.com/en/news-and-press-releases/abn-amro-samsung-sds-and-the-port-of-rotterdam-authority-are-launching-a.

Porter/Heppelmann, How Smart, Connected Products Are Transforming Competition, Harvard business review 2014, 1-23.

Prinz 2018 Blockchain and CSCW – Shall we care? (European Society for Socially Embedded Technologies (EUSSET), Hrsg.), Proceedings of 16th European Conference on Computer-Supported Cooperative Work - Exploratory Papers, abrufbar unter: https://hdl.handle.net/20.500.12015/3124.

Protocol Labs, IPFS is the Distributed Web 2019, abrufbar unter: https://ipfs.io/.

Rabe/Bahnsen Seehandelsrecht, 5. Aufl., München 2018.

Ramming, Die Sperrwirkung von Ladeschein und Konnossement, RdTW 2018, 45-58.

Rauh/Franke/Krems, Understanding the impact of electric vehicle driving experience on range anxiety, Human factors 2015, 177-187.

Redeker, IT-Recht, 6. Auflage, München 2017.

Reiff, Bitcoin ETFs Explained 2018, abrufbar unter: https://www.investopedia.com/investing/bitcoin-etfs-explained/.

Reiter/Methner, Bitcoin und Blockchain-Technologie: Rechtliche Aspekte für Verbraucher und Anbieter beim anonymen Bezahlen. in: *Taeger (Hg.)* Rechtsfragen digitaler Transformationen. Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, 359.

Reus, Interview: Platooning wird Nerven und Kraft der Fahrer schonen 2017, abrufbar unter: https://logistik-aktuell.com/2017/02/23/interview-platooning/.

Reuters, Barclays says conducts first blockchain-based trade-finance deal 2016, abrufbar unter: https://www.reuters.com/article/us-banks-barclays-blockchain/barclays-says-conducts-first-blockchain-based-trade-finance-deal-idUSKCN11D23B.

Römer/Tscheulin, Die Bedeutung von Vertrauen in risikoreichen Kooperationsentscheidungen — Analyse der theoretischen Grundlagen und empirische Überprüfung, Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 2008, 434-458.

Rowan/Clear/Gerla/Huggard/Goldrick 2017 Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels, abrufbar unter: http://arxiv.org/pdf/1704.02553v1.

Saberhagen, CryptoNote v 2.0 2013, abrufbar unter: https://cryptonote.org/whitepaper.pdf.

Sächsische Energieagentur – SAENA GmbH, Kompetenzatlas Elektromobilität Sachsen 2016, abrufbar unter: http://www.saena.de/download/Broschueren/BE-Mob_Kompetenzatlas.pdf.

Säcker/Rixecker/Oetker/Limperg *et al.* Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7. Aufl., München 2018.

Saive, Blockchain in der Transportwirtschaft, RdTW 2018, 85-89.

Saive, Das Blockchain-Traditionspapier, Die transportrechtlichen Traditionspapiere vor dem Hintergrund neuer Technologien, TranspR 2018, 234-238.

Saive, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764-767.

Sänn/Richter/Fraunholz, Car-to-X als Basis organisationaler Transformation und neuer Mobilitätsleistungen, Wirtschaftsinformatik & Management 2017, 60-71.

Sasson/Chiesa/Garman/Green/Miers/Tromer et al., Zerocash: Decentralized Anonymous Payments from Bitcoin. in: The Institute of Electrical and Electronics Engineers (Hg.) IEEE Symposium on Security and Privacy 2014, 459.

Scania, Platooning saves up to 12 percent fuel 2015, abrufbar unter: https://www.scania.com/group/en/platooning-saves-up-to-12-percent-fuel/.

Schneier, Applied Cryptography, Indianapolis 2015.

Scholtka/Kneuper, Lokale Energiemärkte auf Basis der Blockchain-Technologie, IR 2019, 17-21.

Schrey/Thalhofer, Rechtliche Aspekte der Blockchain, NJW 2017, 1431-1436.

Schulze, 'We are about to see massive disruptions': IMF's Lagarde says it's time to get serious about digital currency CNBC 2017, abrufbar unter: https://www.cnbc.com/2017/10/13/bitcoin-get-serious-about-digital-currency-imf-christine-lagarde-says.html.

Schulze Bürgerliches Gesetzbuch, 10. Aufl., Baden-Baden 2019.

Schütte/Fridgen/Prinz/Rose/Urbach 2017 Blockchain und Smart Contracts (Wolfgang Prinz, Axel T. Schulte, Hrsg.). : Fraunhofer, abrufbar unter: https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf.

Schweizer/Schlatt/Urbach/Fridgen, Unchaining Social Businesses: Blockchain as the Basic Technology of a Crowdlending Platform. in: 38th International Conference on Information Systems (ICIS) 2017, 1.

Schweizer Bundesrat, Bericht Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, abrufbar unter: https://www.mme.ch/fileadmin/files/documents/Publikationen/2018/181207_Bericht_Bundesrat_Blockchain.pdf.

Schweizer Bundesrat, Medienmitteilung vom 18.01.2018, abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69539.html.

Scora/Barth 2006 Comprehensive Modal Emissions Model (CMEM), University of California, USA.

Securities and Exchange Commission, Statement on Digital Asset Securities Issuance and Trading 2018, abrufbar unter: https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading.

Securities Exchange Comission 2017 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO: Securities and Exchange Commission, abrufbar unter: https://www.sec.gov/litigation/investreport/34-81207.pdf.

Seitz, Distributed Ledger Technology - Die Revolution hat begonnen und das Recht muss folgen. in: *Taeger (Hg.)* Recht 4.0. Innovationen aus den rechtswissenschaftlichen Laboren, Edewecht 2017, 777.

Shah, Global Blockchain Market Could Reach $60 Billion by 2024, Shows Report 2018, abrufbar unter: https://blokt.com/news/global-blockchain-market-could-reach-60-billion-by-2024-shows-report.

Shen/Pena-Mora, Blockchain for Cities—A Systematic Literature Review, IEEE Access 2018, 76787-76819.

Shermin, Disrupting Governance with Blockchains and Smart Contracts, Strategic Change 2017, 499-509.

Shmatenko/Möllenkamp, Digitale Zahlungsmittel in einer analog geprägten Rechtsordnung, A bit(coin) out of control - Rechtsnatur und schuldrechtliche Behandlung von Kryptowährungen, MMR 2018, 495-501.

Simmchen, Blockchain (R)Evolution, Verwendungsmöglichkeiten und Risiken, MMR 2017, 162-165.

Simpson/Cooke, Blockchain: competition issues in nascent markets 2016, abrufbar unter: https://www.nortonrosefulbright.com/en/knowledge/publications/81f70b38/blockchain-competition-issues-in-nascent-markets.

Sovrin Foundation 2018 A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, abrufbar unter: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.

Spiegel Online, Merkel und Steinbrück im Wortlaut 2008, abrufbar unter: http://www.spiegel.de/wirtschaft/merkel-und-steinbrueck-im-wortlaut-die-spareinlagen-sind-sicher-a-582305.html.

Spindler/Bille, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357-1369.

Spindler/Schuster Recht der elektronischen Medien, 3. Aufl., München 2015.

Statista, Blockchain 2018, abrufbar unter: https://www.statista.com/study/39859/blockchain-statista-dossier/.

Statista, Trends in global export volume of trade in goods from 1950 to 2017 2018, abrufbar unter: https://www.statista.com/statistics/264682/worldwide-export-volume-in-the-trade-since-1950/.

Statistisches Bundesamt, Anzahl der Speditionen in Deutschland in den Jahren von 2009 bis 2016 statista 2019, abrufbar unter: https://de.statista.com/statistik/daten/studie/422098/umfrage/anzahl-der-speditionen/.

Staudinger J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch. Buch 2: Recht der Schuldverhältnisse: §§ 705 - 740 (Gesellschaftsrecht), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Berlin 2003.

Staudinger J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Neubearb. 2013, Berlin 2013.

Staudinger J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Neubearb. 2017, Berlin 2017.

Stürner Bürgerliches Gesetzbuch, 17. Aufl., München 2018.

Sun/Yamamoto/Morikawa, Fast-charging station choice behavior among battery electric vehicle users, Transportation Research Part D: Transport and Environment 2016, 26-39.

Sutter/Maibach/Bertschmann/Ickert/Peter/Doll et al., Finanzierung einer nachhaltigen Güterverkehrsinfrastruktur 2016, abrufbar unter: https://www.umweltbundesamt.de/sites/default/files/medien/376/publikationen/texte_53_2016_finanzierung_einer_nachhaltigen_gueterverkehrsinfrastruktur_aktualisiert.pdf.

Sydow Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018.

Tamm/Tonner/Bergmann Verbraucherrecht, 2. Aufl., Baden-Baden 2016.

The Linux Foundation 2017 Hyperledger Architecture, Volume 1, abrufbar unter: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf.

Thomas Halleck, Facebook: One Out Of Every Five People On Earth Have An Active Account 2015, abrufbar unter: https://www.ibtimes.com/facebook-one-out-every-five-people-earth-have-active-account-1801240.

Thüsing/Westphalen Vertragsrecht und AGB-Klauselwerke, 41. Aufl., München 2018.

Tobin/Reed, The Inevitable Rise of Self-Sovereign Identity Sovrin Foundation 2016.

Todd, Dematerialisation of shipping documents, Journal of International Banking Law 2000, 410-418.

TOOP Project, Once-Only 2019, abrufbar unter: http://www.toop.eu/once-only.

Tractica, Enterprise Blockchain Revenue to Surpass $20 Billion by 2025 2018, abrufbar unter: https://www.tractica.com/newsroom/press-releases/enterprise-blockchain-revenue-to-surpass-20-billion-by-2025/.

Tradelens, The Power of the Ecosystem 2019, abrufbar unter: https://www.tradelens.com/ecosystem/.

Tsugawa, Energy ITS: What We Learned and What We should Learn TRB Road Vehicle Automation Workshop 2012, abrufbar unter: http://onlinepubs.trb.org/onlinepubs/conferences/2012/Automation/presentations/Tsugawa.pdf.

Tual, Vitalik Buterin, Gavin Wood, Alex van De Sande, Vlad Zamfir announced amongst exceptional DAO Curators Medium 2016, abrufbar unter: https://blog.slock.it/vitalik-buterin-gavin-wood-alex-van-de-sande-vlad-zamfir-announced-amongst-stellar-dao-curators-44be4d12dd6e.

Tulpule, Enforcement and Compliance in a Blockchain(ed) World, CPI Antitrust Chronicle 2017, 45.

Ulmer/Brandner/Hensen AGB-Recht, 12. Aufl., Saarbrücken 2016.

UN News, World Book Day: new UN report spotlights potential of mobile technology to advance literacy 2014, abrufbar unter: Grundsätzlich abzugleichen_ https://www.acatech.de/wp-content/uploads/2018/10/acatech-HORIZONTE_Blockchain.pdf.

Underwood, Blockchain beyond bitcoin, Communications of the ACM 2016, 15-17.

V2G Clarity, IEC 63110 – Standardizing the Management of Electric Vehicle (Dis-)Charging Infrastructures 2017.

Valenta/Sandner 2017 Comparison of Ethereum, Hyperledger Fabric and Corda (Frankfurt School Blockchain Center, Hrsg.) (FSBC Working Paper).

Virmani, 18 blockchain consortia you should know about 2019, abrufbar unter: https://medium.com/blockchain-blog/18-blockchain-consortia-you-should-know-about-6262b6a30ba9.

Vukolic, Rethinking Permissioned Blockchains, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts 2017, 3-7.

Wagner/Goeble, Freie Fahrt für das Auto der Zukunft, Kritische Analyse des Gesetzentwurfs zum hoch- und vollautomatisierten Fahren, ZD 2017, 263-269.

Werbach, Trust, But Verify: Why the Blockchain Needs the Law, Berkeley Tech. L.J. 2018, 491-552.

Wieske, Transportrecht, 3. Auflage, Berlin 2012.

Yermack, Corporate Governance and Blockchains 2016, abrufbar unter: https://www.nber.org/papers/w21802.pdf.

Ylinen, Zusammenarbeit beim Platooning zu Lande und zur See – kartellrechtliche Gesichtspunkte, RdTW 2018, 121-125.

YouGov, Umfrage zur Bekanntheit von Einsatzmöglichkeiten einer Blockchain im Mittelstand 2017 2017, abrufbar unter: https://de.statista.com/statistik/daten/studie/683657/umfrage/umfrage-zur-bekanntheit-von-blockchain-einsatzmoeglichkeiten-im-mittelstand-in-deutschland/.

Zare-Garizy/Fridgen/Wederhake, A Privacy Preserving Approach to Collaborative Systemic Risk Identification: The Use-Case of Supply Chain Networks, Security and Communication Networks 2018, 1-18.

Impressum

Herausgeber
Bundesministerium für Verkehr und digitale Infrastruktur
Invalidenstraße 44
10115 Berlin

Stand
Mai 2019

Druck
Bundesministerium für Verkehr und digitale Infrastruktur
Referat Z 32, Hausdruckerei

Bildnachweis
Titelbild: © logicbomb - stock.adobe.com
Fraunhofer-Institut für Angewandte Informationstechnik FIT

Text
Fraunhofer-Institut für Angewandte Informationstechnik FIT

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der Bundesregierung.
Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.bmvi.de