PLATTFORM INDUSTRIE 4.0

ERGEBNISPAPIER

Blockchain und Recht im Kontext von Industrie 4.0

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung
PRpetuum GmbH, München

Stand
Februar 2019

Druck
MKL Druck GmbH und Co. KG, 48346 Ostbevern

Bildnachweis
Iaremenko – iStockphoto (Titel),
Alengo – Getty Images (S. 3),
simpson33 – iStockphoto (S. 6),
mattjeacock – iStockphoto (S. 10),
ilkercelik – iStockphoto (S. 11),
Yuichiro Chino – Getty Images (S. 15),
NicoElNino – iStockphoto (S. 18),
Juhari Muhade – Getty Images (S. 19),
maxkabakov – iStockphoto (S. 21),
Erik Isakson – Getty Images (S. 24),
Cecilie_Arcurs – iStockphoto (S. 26)

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Einführung

Blockchain

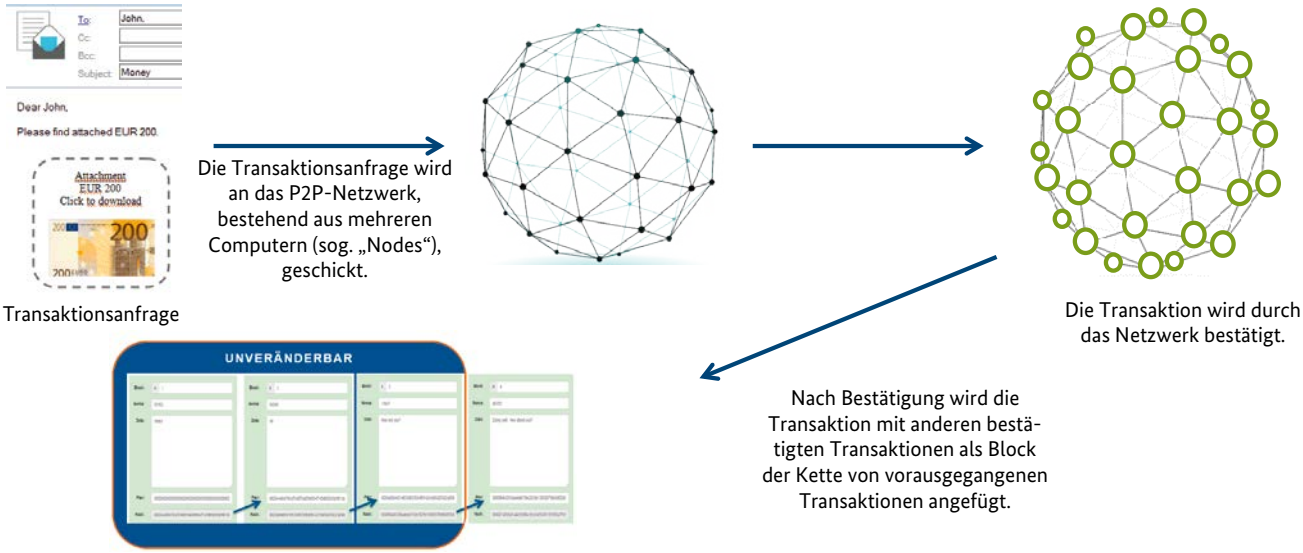
Blockchain selbst ist keine Anwendungssoftware oder ein Programm, sondern bezeichnet eine bestimmte, nicht-manipulierbare Art des Speicherns und des Austausches von Daten. Eine Blockchain funktioniert ähnlich wie ein Register, in dem bestimmte Abläufe und aufeinanderfolgende Vorgänge dokumentiert werden, wie z. B. das Handelsregister oder das Grundbuch. Im Unterschied zu einem herkömmlichen Register erfolgt die Verwaltung jedoch nicht zentral durch eine Stelle (sog. Single Ledger), sondern dezentral durch alle dem Register angeschlossenen Parteien (sog. Distributed Ledger). Jeder Teilnehmer (sog. Node) hat eine Kopie der das Register darstellenden Datenbank auf seinem Computer. Durch diese Distributed-Ledger-Technologie (DLT) sollen die bei einem Single Ledger mit dem Betrieb der Datenbank durch eine Stelle verbundenen Risiken, wie z. B. Manipulation oder Verlust von Daten, vermieden werden.

Technisch gesehen basiert DLT im Kern auf chronologisch aufgebauten, dezentralisierten und kryptographisch gesicherten Datenbanken. DLT kombiniert Kryptographie, Peer-to-Peer-Netzwerke (P2P), Konsens-Algorithmen und Smart Contracts (siehe nachstehend) und ermöglicht es einer Vielzahl von Parteien, Daten zu teilen und zu verarbeiten, ohne dabei auf ein zentrales Verwaltungssystem zurückzugreifen. Mit Hilfe einer Blockchain können Daten gespeichert und ausgetauscht werden. Dies geschieht entweder innerhalb eines offenen (für jeden etwa durch den freien Download der entsprechenden Software zugänglichen) oder eines geschlossenen Peer-to-Peer-Netzwerks. Man spricht dann von einer Public bzw. einer Private Blockchain.[1]

Der Zugang zur Datenbank und den einem Teilnehmer zugeordneten Daten, z. B. der Inhaberschaft von Bitcoins, erfolgt über eine sog. Wallet, bestehend aus einem Public Key und einem Private Key. Beide sind für die Initiierung einer Transaktion erforderlich. Der Public Key entspricht der Adresse der Wallet (vergleichbar einer Kontonummer) und wird dem Transaktionspartner (außerhalb der Blockchain) mitgeteilt. Der Private Key entspricht der PIN beim Konto und ist für die Initialisierung einer Transaktion erforderlich. Ein Wirtschaftsgut, Vermögenswert oder Vermögensgegenstand (wie z. B. auch Kryptowährungen wie Bitcoin) wird auf einer Blockchain durch einen sog. „Token“ repräsentiert.

Wenn eine Transaktion in der Blockchain-Datenbank registriert werden soll, muss diese durch den Inhaber des privaten Schlüssels ausgelöst werden. Außerdem muss diese Transaktion von allen (oder zumindest einer vorab festgelegten Mehrheit von) Teilnehmern bestätigt, d. h. validiert werden.

1 Diese Publikation stützt sich auf die Begrifflichkeiten der DIN SPEC 3103 „Smart Contracts und Sensoren in Blockchains für Industrie 4.0-Anwendungen“, die voraussichtlich in der zweiten Jahreshälfte 2019 veröffentlicht wird und die der AG „Rechtliche Rahmenbedingungen“ im derzeitigen Entwurfsstand dankenswerterweise vorliegt. Auch die DIN SPEC 3104 („Blockchain-basierte Validierung von Dokumenten“) ist herangezogen worden.



Die Kette von Blöcken

Quelle: Arbeitsgruppe 4 „Rechtliche Rahmenbedingungen“ der Plattform Industrie 4.0

Zum Zwecke der Bestätigung werden Transaktionen in einem Block zusammengefasst. Alle Teilnehmer stimmen in Zyklen ab (sog. Consensus), wann der Block mit welchen Transaktionen in welcher Reihenfolge geschlossen wird. Jeder geschlossene Block ist mit einem Code (Hash) versehen und trägt zudem den Hashwert des Vorgängerblocks. Auf diese Art werden die Transaktionsblöcke über die Hashs zu einer „Kette“ verbunden (daher der Begriff „Blockchain“); über die Kette der Transaktionen lassen sich Änderungen bis zum Ursprung nachverfolgen und z. B. im Fall von Bitcoin Kontostände zu jedem Zeitpunkt errechnen. Die Tatsache, dass jeder Node eine Kopie aller Transaktionsdaten hat und mit dieser Datenhistorie die Validität einer neuen Transaktion prüft, bevor er seine Zustimmung erteilt, macht eine Manipulation der Blockchain sehr schwer.

Ähnlich wie bei Computern gibt es verschiedene „Betriebssysteme“ für eine Blockchain. Die bekanntesten sind Bitcoin, R3 Corda, Hyperledger und Ethereum. Je nach System können die Zugangsvoraussetzungen für Teilnehmer, der Umfang der Daten, den die Teilnehmer sehen, die Berechtigungen zur Initiierung einer Transaktion und die Validierungserfordernisse für eine Transaktion unterschiedlich ausgestaltet werden. Das macht die Blockchain vielseitig und für nahezu alle Anwendungsbereiche der Industrie individuell einsetzbar.

Ein Beispiel für einen Praxiseinsatz von Blockchain-basierten Systemen im Mobilitätsbereich ist die Hinterlegung von Fahrzeugdaten, die eine manipulationssichere Fahrzeughistorie gewährleisten. Eine solche Fahrzeughistorie könnte beispielsweise verhindern, dass ein Fahrzeug mit einem manipulierten Kilometerstand veräußert wird. Über die in der Blockchain hinterlegte und unabänderbare Historie kann ein potenzieller Käufer sich Gewissheit verschaffen, dass die Angaben des Verkäufers zutreffend sind.

Die (weitestgehende) Unmanipulierbarkeit der Blockchain und die faktische Ausführungsgarantie von Smart Contracts bieten zahlreiche industrielle Anwendungsmöglichkeiten zur Prozessoptimierung, Kostenersparnis und Entwicklung neuer Geschäftsmodelle. Besonders deutlich wird dies z. B. im Bereich Logistik, wo es zahlreiche Blockchain-basierte Anwendungen gibt, um die aufwendige Dokumentation und Abwicklung von Supply-Chain-Prozessen zu vereinfachen.

Beispiel

Eine gemeinsam von Technologie-Provider X und Transportunternehmen Y für weltweiten Handel zugeschnittene Blockchain-Plattform bietet eine Informationsplattform für Versanddaten, Dokumente, Zollanmeldungen und IoT-Daten. Verlader, Reedereien, Spediteure, Hafen- und Terminalbetreiber sowie Binnenverkehrs- und Zollbehörden können mittels der Plattform in Echtzeit auf diese in der Blockchain gespeicherten Informationen – je nach Rolle und Berechtigung – zugreifen. Anstelle des jeweils bilateralen Austauschs der Dokumente haben die Beteiligten Zugriff auf die Informationen in Form eines einheitlichen, unmanipulierbaren Datensatzes und können damit sicher, effizient und vertrauensvoll zusammenarbeiten. Sie sind außerdem in der Lage, IoT- und Sensordaten zu nutzen, etwa zur Temperaturkontrolle oder beim Containergewicht. Mittels Smart Contracts können Gebühren und Zusatzkosten automatisch validiert werden.

Smart Contracts

Smart Contracts sind Computerprogramme (und nicht unmittelbar Verträge im zivilrechtlichen Sinne), die aus Wenn-dann-Befehlen aufgebaut sind. Diese Art von Befehlen ist nicht neu. Das Neue ist die Tatsache, dass Smart Contracts auf der Blockchain verteilt auf vielen Nodes gleichzeitig laufen und das Ergebnis nach automatisierter Validierung „in die Blockchain geschrieben“ wird. Das automatisierte, parallele Betreiben der Smart-Contract-Programme und das parallele Abspeichern der Daten in Blockchain-Nodes machen die individuellen Programme in der Praxis unmanipulierbar.

Anders als bei Single-Ledger-Datenbanken kann daher deren Durchführung auch nicht von einer einzelnen Partei verhindert werden: Die Umsetzung ist also faktisch garantiert. So kann etwa die Lieferung von Waren gegen Zahlung des Kaufpreises automatisiert mit Abwicklungsgarantie binnen Sekunden ohne Counterparty-Risiko abgewickelt werden, sobald die in der Blockchain vordefinierten Voraussetzungen (sog. „Trigger“), wie z. B. Bestätigung der Mangelfreiheit der Ware und ausreichende Deckung des Käuferkontos, erfüllt sind.

Ein Beispiel für den potenziellen Einsatz von Smart Contracts könnte wie folgt aussehen: Ein Provider X bietet ein System zur Steuerung des sog. Platooning an. Unter Platooning wird verstanden, dass sich mehrere LKWs auf einer Autobahn in eine Reihe hintereinander begeben. Die Besonderheit des Platooning-Systems liegt darin, dass die Abstände zwischen den im Platoon eingereihten Fahrzeugen jederzeit berechnet werden und durch das System vorausgesagt und auch gesteuert werden kann, wie die Abstände optimal zu gestalten sind, damit der ansonsten auftretende „Ziehharmonikaeffekt“ (das heißt, ein Fahrzeug bremst leicht ab, die nachfolgenden Fahrzeuge bremsen immer etwas stärker, dasselbe umgekehrt im Falle der Beschleunigung des führenden Fahrzeuges) möglichst vermieden werden kann. Durch diese voraussehende Fahrweise sind erhebliche Dieseleinsparungen möglich. Das Blockchain- und Smart-Contract-basierte System kommt dann zum Einsatz, wenn es um die Abrechnung der Platooning-Leistung geht. Ein solches System würde es ermöglichen, dass ab dem Einreihen in das Platoon ein Zähler läuft und in dem Moment, in dem ein Fahrzeug aus dem Platoon ausschert, über den in der Blockchain hinterlegten Smart Contract automatisiert und sekundengenau berechnet wird, welche Leistung der Betreiber des LKWs erhalten hat und welche Vergütung dafür zu entrichten ist (denkbar wäre beispielsweise ein bestimmter Prozentsatz der prognostizierten Diesel-Einsparung).

Allgemein kann man sagen, dass Smart-Contract-basierte Abrechnungen insbesondere dort lohnend sein können, wo es um sehr viele Transaktionen mit geringem Volumen geht. Bei solchen sogenannten „Mikrotransaktionen“ macht es sich am stärksten bemerkbar, dass der manuelle Aufwand für die Durchführung und Prüfung einer Transaktion über den Smart Contract automatisiert abgebildet wird.

Mit den nachfolgend ausgewählten Überlegungen sollen einige wesentliche Rechtsfragen aufgezeigt werden. Vieles ist dazu noch im Fluss. Aber die Möglichkeiten zur Gestaltung sind da und sollten genutzt werden.

Zivilrechtliche Aspekte

Code is Law – Recht für Smart Contracts und Anwendungen auf der Blockchain. Anwendbare Rechtsordnungen für Blockchain und Übertragung von Sachen und Rechten im internationalen Kontext

A: Steckbrief

Worum geht es bei dem Thema?

Die dezentrale Blockchain-Technologie ist prädestiniert für den internationalen Einsatz, gerade auch in der Industrie 4.0. Die geltenden Rechtsordnungen sind national strukturiert und gelten nur im jeweiligen Staatsgebiet. Eine internationale Vereinheitlichung ist bislang kaum umgesetzt, wie etwa teilweise in der Europäischen Union.

Für die Teilnahme an und Aktivitäten im Rahmen einer Blockchain ist daher zu klären, welche nationalen Rechtsnormen für die Gültigkeit und Wirksamkeit von Aktivitäten sowie deren Auswirkungen gelten.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Welche Rechtsnormen gelten für die Teilnahme an einer Blockchain im internationalen Kontext?
- Welche Rechtsnormen gelten für die Aktivitäten auf einer Blockchain und deren rechtliche Auswirkungen im internationalen Kontext?
- Welche Rechtsordnungen gelten für die Übertragung von Sachen und Rechten im internationalen Kontext?

B: Juristische Einschätzung

Nationale Rechtsnormen bestimmen, ob und inwieweit die nationale Rechtsordnung eigene Geltung im internationalen Kontext beansprucht. Solche Regelungen nationaler Rechtsordnungen können auch zu unterschiedlichen Ergebnissen führen, da diese nur in Teilbereichen harmonisiert sind.

Für die Frage, welches nationale Recht jeweils gilt, sind zwei Themenbereiche zu unterscheiden: Einerseits bestehen Regelungen für die Entstehung und die Durchführung von rechtlichen Verpflichtungen, insbesondere für Verträge. Andererseits bestehen Regelungen für Rechte an Gegenständen und geistigem Eigentum sowie deren Einräumung und Übertragung.

Die Geltung einer bestimmten nationalen Rechtsordnung für rechtliche Verpflichtungen und Verträge kann von Vertragspartnern in weiten Bereichen vereinbart werden. In der EU ist dies in Art. 3 Rom I VO ausdrücklich geregelt. Solche Rechtswahlvereinbarungen sind in der Praxis seit Langem üblich. Deren Wirksamkeit und Inhalt ist grundsätzlich nach dem jeweils gewählten Recht zu prüfen. Nur wenn ein nationales Recht als anwendbar gewählt wird, das keinerlei Bezug zu den beteiligten Parteien und deren Aktivitäten im Kontext der Blockchain hat, wird dies teilweise kritisch beurteilt.

Im Gegensatz dazu haben die Parteien grundsätzlich keine Wahlmöglichkeit, welche nationalen Regelungen für Rechte an Gegenständen und geistigem Eigentum sowie deren Einräumung und Übertragung gelten sollen. Es gilt jeweils die nationale Rechtsordnung an dem Ort, an dem sich das Rechtsobjekt aktuell befindet. Wenn dieses Rechtsobjekt von einem Staat in einen anderen Staat verlagert wird, führt das auch zu einem Wechsel der geltenden nationalen Rechtsvorschriften. Allerdings bestehen für einige Bereiche des geistigen Eigentums, insbesondere für das Urheberrecht, internationale Abkommen, durch die ausländische Rechtsinhaber in einer nationalen Rechtsordnung wie Inländer geschützt werden.

Im Ergebnis kann daher für eine Vereinbarung der Übertragung von Rechten oder Sachen auf der Blockchain ein nationales Recht gelten, etwa aufgrund einer getroffenen Rechtswahl. Für die rechtliche Situation des Übertragungsgegenstands und seinen rechtlichen Schutz gilt gleichwohl das nationale Recht des Orts, an dem sich dieser Übertragungsgegenstand aktuell befindet.

C: Handlungsoptionen und Handlungsempfehlungen

- Die Beteiligten einer Blockchain sollten vereinbaren, welche nationale Rechtsordnung für die Entstehung und Durchführung rechtlicher Verpflichtungen gelten soll. Dies ist grundsätzlich in weiten Grenzen möglich, solange das gewählte Recht einen Bezug zur Blockchain oder den Transaktionen auf der Blockchain aufweist.
- Für Rechte an Gegenständen und geistigem Eigentum gilt grundsätzlich die Rechtsordnung des Orts, an dem sich das Rechtsobjekt befindet. Damit müssen die Beteiligten sinnvoll umgehen.

Wie sind Smart Contracts rechtlich einzuordnen?

A: Steckbrief

Worum geht es bei dem Thema?

Die Blockchain-Technologie ermöglicht die Implementierung von automatisch ausführbaren Regeln für Transaktionen. Ein Beispiel ist die Erklärung der Übertragung von Rechten, die bei Eintritt einer Bedingung (etwa Zahlung) automatisch erfolgt. Die Möglichkeiten für solche automatisch ausgeführten Regeln sind vielfältig und gleichzeitig zunächst auf die Blockchain selbst beschränkt. Solche automatischen Regeln werden oft als „Smart Contract“ bezeichnet, wenn sie rechtlich relevante Auswirkungen erzeugen sollen.

Für solche Smart Contracts ist zu klären, welche Wirkungen solche Mechanismen nach deutschem Recht auslösen.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Welche Voraussetzungen gelten für rechtliche Wirkungen von Smart Contracts nach deutschem Recht?
- Wie erfolgt typischerweise der Vertragsschluss unter Nutzung von Smart Contracts im Bereich Industrie 4.0?
- Können Smart Contracts die bestehenden Rechtsnormen für Verträge ersetzen?
- Wie ist mit den Formvorschriften für bestimmte Rechtsgeschäfte umzugehen?

B: Juristische Einschätzung

Aufgrund der Vertragsfreiheit kann jedes Rechtssubjekt grundsätzlich frei entscheiden, ob und welche Willenserklärung es abgeben und welche Verträge es abschließen will oder nicht. Willenserklärungen und Vertragsabschlüsse sind in jeder beliebigen Form möglich, soweit nicht spezielle gesetzliche Formanforderungen bestehen (etwa die notarielle Form für Grundstücksgeschäfte).

Außerhalb solcher spezifischen Einschränkungen können durch Transaktionen auf der Blockchain sowohl rechtsverbindliche Willenserklärungen abgegeben als auch Verträge abgeschlossen werden. Dafür ist grundsätzlich die Identifizierbarkeit der natürlichen oder juristischen Person notwendig, für und gegen die eine Willenserklärung oder ein Vertrag wirkt.

Ein denkbarer Fall im Bereich Industrie 4.0 liegt in der konsortialen Nutzung einer Private Blockchain. Dabei verständigen sich die Teilnehmer – außerhalb der Blockchain – ganz herkömmlich im Wege allgemeiner Geschäftsbedingungen über die Voraussetzungen des Vertragsschlusses (einschließlich qualifizierender Merkmale, wer als Vertragspartner zugelassen wird), den Inhalt der wechselseitigen Verpflichtungen (Hauptleistung und Gegenleistung) und ggf. die Abwicklung von Teilaspekten der Transaktion (Nachweis von Orderpapieren, Zahlung etc.) durch den automatisierten Mechanismus der Smart Contracts.

Es bestehen darüber hinaus auch Überlegungen, die Wirkung von Willenserklärungen sowie den Abschluss und die Abwicklung von Verträgen soweit möglich vollständig durch automatisch ausführbare Regeln auf der jeweiligen Blockchain abzubilden. Auch solche Regeln können im Rahmen der Vertragsfreiheit grundsätzlich wirksam vereinbart werden. Allerdings gelten für Willenserklärungen und Verträge jeweils die gesetzlichen Vorschriften (einschließlich solcher zum Verbraucherschutz). Die Blockchain ist kein „rechtsfreier Raum“.

C: Handlungsoptionen und Handlungsempfehlungen

- Es empfiehlt sich eine gesetzliche Klarstellung, dass bestehende Regelungen für Willenserklärungen und Verträge auch dann anzuwenden sind, wenn diese unter Verwendung von Maschinen oder automatisch erfolgen.
- Die derzeit absehbaren Use Cases werden typischerweise aufgrund von Vertragsbedingungen realisiert, die die Parteien (ggf. auch konsortial) durch herkömmliche allgemeine Geschäftsbedingungen vorab für die Nutzer einer Private Blockchain vereinbaren.
- Für die bestehenden Rechtsvorschriften für Verträge und deren Abwicklung auf der Blockchain besteht insoweit kein Handlungsbedarf. Die gesetzlichen Vorschriften gelten stets für Aktivitäten auf einer Blockchain.

Blockchain und Recht der Allgemeinen Geschäftsbedingungen

A: Steckbrief

Worum geht es bei dem Thema?

Die bestehenden Rechtsvorschriften sind nicht auf die Blockchain-Technologie ausgerichtet. Umso weniger bestehen gesetzliche Vorschriften für spezifische Regelungsbedürfnisse im Zusammenhang einer konkreten Blockchain und deren Umsetzung. Mögliche Einsatzgebiete und Umsetzungen von Blockchains entwickeln sich genauso dynamisch weiter wie die Blockchain-Technologie selbst.

Umso größer ist der Bedarf, spezifische Regelungen für eine konkrete Blockchain mit und gegenüber den Beteiligten zu vereinbaren. Soweit Transaktionen im Bereich Industrie 4.0 mit Hilfe konkreter Blockchains durchgeführt werden sollten, müssen die dafür geltenden Regelungen notwendigerweise für alle Beteiligten gleichförmig gelten, also quasi standardisierte Inhalte für diese Blockchain enthalten. Mit solchen vorformulierten Vertragsbedingungen stellt das deutsche Recht der Allgemeinen Geschäftsbedingungen die Nutzer vor erhebliche Herausforderungen angesichts der Vielzahl an Beschränkungen der Vertragsfreiheit, die sich im unternehmerischen Verkehr auch durch die zum Teil immer strenger interpretierte Rechtsprechung ergibt. Diese Beschränkungen sind im internationalen Vergleich besonders weitgehend und können aus mehreren Gründen innovationshemmend wirken.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Wirkt das deutsche Recht der Allgemeinen Geschäftsbedingungen im Verhältnis zu beteiligten Unternehmern innovationshemmend?
- Wie könnten negative Auswirkungen des Rechts der Allgemeinen Geschäftsbedingungen im Verhältnis zu Unternehmern vermieden werden, ohne den Schutz von Verbrauchern einzuschränken?

B: Juristische Einschätzung

Es besteht erheblicher Bedarf für die identische Vereinbarung spezifischer Regelungen für eine konkrete Blockchain mit allen Beteiligten im Wege vorformulierter Vertragsbedingungen, also „Allgemeiner Geschäftsbedingungen“ (AGB) gemäß § 305 BGB.

Das deutsche AGB-Recht schränkt den Gestaltungsspielraum im Verhältnis zwischen Unternehmern erheblich ein. Dies gilt auch im Vergleich zu anderen Rechtsordnungen innerhalb und außerhalb der EU. Ein zu weites Abweichen von den gesetzlichen Regelungen, etwa für vordefinierte Vertragstypen (Kauf, Miete etc.), führt zur Unwirksamkeit der Regelung. Die Rechtsprechung interpretiert diese Einschränkungen zudem laufend strenger. Auf den Schutz von Verbrauchern ausgerichtete Regelungen werden immer weiter auch im Verhältnis zwischen Unternehmen nahezu unverändert angewendet. Diese Gestaltungsrestriktionen sind für deutsche Unternehmen innovationshemmend gegenüber den Möglichkeiten von Unternehmen im Ausland. So können etwa die vordefinierten Vertragstypen des BGB von 1900 die Bedürfnisse innovativer Geschäftsmodelle des 21. Jahrhunderts im Kontext der Blockchain nicht „proaktiv“ abdecken oder auch nur berücksichtigen. Zudem bestehen erhebliche Unsicherheiten, ob die zukünftige Rechtsprechung die bislang als wirksam angesehene AGB-Regelung für unwirksam erklären wird.

C: Handlungsoptionen und Handlungsempfehlungen

- Die immer strenger interpretierten Einschränkungen des deutschen AGB-Rechts im Verhältnis zwischen Unternehmern sind zu flexibilisieren. Dazu besteht keine Handlungsalternative, um Innovations- und Wettbewerbsnachteile gegenüber anderen Ländern nicht weiter ansteigen zu lassen.
- Die ständige und immer restriktivere Anwendung von Verbraucherschutzregelungen des AGB-Rechts auch im Verhältnis zwischen Unternehmen engt den Handlungsspielraum gerade für innovative Geschäftsmodelle immer weiter ein.
- Die Auswirkungen dieser Restriktionen treffen besonders auch kleinere und mittelständische Unternehmen, was auch für angemessene Regelungen für Gewährleistungs- und Haftungsthemen gilt.

- Diese Nachteile des deutschen Rechts im internationalen Kontext zwischen Unternehmen sollten beseitigt oder zumindest erheblich verringert werden. Sonst werden gerade innovative Unternehmen zur Verlagerung in das Ausland genötigt, um neue Geschäftsmodelle rechtlich umzusetzen.
- Der Schutz von Verbrauchern soll unberührt bleiben.

Verwendung von Nutzungsbedingungen im Kontext von Blockchain: Umgang mit Wirksamkeitshindernissen, Leistungsstörungen und Möglichkeiten der Rückabwicklung

A: Steckbrief

Worum geht es bei dem Thema?

Um dieselben Regelungen für alle Beteiligten an einer bestimmten Blockchain zu schaffen, bietet sich die Vereinbarung spezifischer Nutzungsbedingungen an. Hierbei stellt sich eine Reihe von Fragen, die den Vertragsschluss, die Durchführbarkeit und Fehlerhaftigkeit einer intendierten Transaktion auf der Blockchain betreffen.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Wie können spezifische Nutzungsbedingungen für eine bestimmte Blockchain zwischen den Beteiligten wirksam vereinbart werden?
- Wie können Nutzungsbedingungen für eine bestimmte Blockchain mit den Beteiligten vereinbart werden?
- Wie ist mit Wirksamkeitshindernissen und Leistungsstörungen auf der Blockchain sowie rechtlichen Anforderungen an die Rückabwicklung umzugehen?

B: Juristische Einschätzung

Grundsätzlich können durch Nutzungsbedingungen spezifische Regelungen für eine bestimmte Blockchain geschaffen werden. Dies gilt sowohl für die Frage der Teilnahme an dieser Blockchain als auch für die von den Teilnehmern auf dieser Blockchain ausgelösten Transaktionen. Aufgrund der Vertragsfreiheit besteht dafür jeweils Gestaltungspielraum, soweit keine zwingenden gesetzlichen Einschränkungen (etwa nach dem deutschen AGB-Recht im unternehmerischen Verkehr bzw. auch gegenüber Verbrauchern) bestehen.

Um Nutzungsbedingungen für eine spezifische Blockchain mit dem jeweiligen Beteiligten wirksam zu vereinbaren, muss der Beteiligte diese Nutzungsbedingungen zur Kenntnis nehmen können und diesen zustimmen. Diese Zustimmung unterliegt keinen formalen Anforderungen, soweit nicht ausnahmsweise besondere gesetzliche Formerfordernisse bestehen. Sofern der Vertragsschluss – also die sich entsprechende Abgabe korrespondierender Willenserklärungen bzw. die Annahme der Nutzungsbedingungen – innerhalb der Blockchain selbst erfolgen soll, ist die eindeutige Zuordnung zu einem Rechtssubjekt und Nachvollziehbarkeit (einschließlich der Möglichkeiten realer Rechtsdurchsetzung, s. u.) unverzichtbare Voraussetzung.

Die Unveränderbarkeit der in einem Block abgelegten Daten bzw. Information ist wesentliches Merkmal der Blockchain. Das schließt aber keineswegs aus, dass das zugrunde liegende Rechtsgeschäft (Kausalgeschäft) fehlerbehaftet ist, etwa weil es von vorneherein nichtig ist (also von Rechts wegen nie hätte ausgeführt werden dürfen), es nachträglich angefochten wird oder eine Partei aufgrund Rücktritts (aus Schlechtleistung oder anderen Gründen der Leistungsstörung) einen Anspruch auf Rückabwicklung hat.

Denkbare Fälle der Nichtigkeit sind z. B., dass das zugrundeliegende Rechtsgeschäft als illegales Geldwäsche-Geschäft (im Bereich Finanztransaktionen) oder wegen Verstoßes gegen ein sonstiges gesetzliches Verbot von vornherein nichtig ist oder es wegen arglistiger Täuschung erfolgreich angefochten wird.

Zwar ist die Transaktion in der Blockchain automatisch und unveränderlich vollzogen – aber nach deutschem Recht darf die Transaktion keine Rechtswirkung entfalten bzw. ist diese Rechtswirkung von Anfang an („ex tunc“) nicht vorhanden bzw. rückwirkend zu beseitigen. Wenn es also nicht möglich ist, eine erfolgte Transaktion aus der Blockchain zu „löschen“, müsste sie ggf. im Wege einer „reverse transaction“ – durch Erstellung eines neuen Blocks „unter umgekehrten Vorzeichen“ – rückabgewickelt werden. Damit könnten die wirtschaftlichen Folgen der Transaktion beseitigt werden, auch wenn die Transaktionshistorie naturgemäß weiterhin transparent bleibt.

Soweit es darum geht, im Nachhinein Sekundäransprüche durchzusetzen (z. B. Minderung der Vergütung wegen Schlechtleistung), ließen sich entsprechende Rückgewährmöglichkeiten vorher im Code eines Smart Contract festschreiben. Soweit es dazu aber auf die Auslegung unbestimmter Rechtsbegriffe und auf Wertungsspielräume ankommt (z. B. Nichterfüllung aufgrund wesentlicher Mängel – im Gegensatz zu unwesentlichen Abweichungen von der versprochenen Leistung), stößt der Automatismus einer vorprogrammierten Rückabwicklung an natürliche Grenzen.

Noch schwieriger wird es, wenn der Initiator der Transaktion – insbesondere in der Public Blockchain – nicht persönlich erkennbar ist und/oder wenn die Nichtigkeit des Vertrages bereits an einer deutlich früheren Stelle in der Blockchain ansetzt. Denn dann wären sämtliche Folgetransaktionen, die auf der nichtigen Transaktion aufbauen,

ohne Grundlage und es käme zu einer systemwidrigen Rückabwicklung durch die ganze Kette. Möglicherweise könnte dazu ein direkt im Block integrierter, automatisierter Streiterledigungsmechanismus helfen.

Im Ergebnis folgt daraus (einstweilen), dass Smart Contracts in Private Blockchains und Permissioned Blockchains bei Zugrundlegung von – ggf. außerhalb der Blockchain vereinbarten – AGB bzw. Teilnahmebedingungen als gut realisierbar erscheinen, wenn die rechtliche Handhabe von Nichtigkeits- und Rückabwicklungsansprüchen einschließlich Maßnahmen der Rechtsdurchsetzung bzw. Streiterledigung in transparenter Form unter namentlich bekannten bzw. identifzierbaren Teilnehmern geregelt ist. Dabei ist klar, dass in diesem Themenkomplex noch viel Neuland, sowohl rechtlich als auch in der technischen Umsetzung, zu erkunden ist.

C: Handlungsoptionen und Handlungsempfehlungen

- Für das Zustandekommen einer Vereinbarung von Nutzungsbedingungen besteht kein gesetzlicher Handlungsbedarf. Die Anforderungen einer möglichen Kenntnisnahme von Nutzungsbedingungen und der Zustimmung durch Beteiligte lassen sich durch entsprechende technische Gestaltungen – außerhalb und innerhalb der Blockchain – umsetzen.

- Die Abwicklung von Wirksamkeitshemmnissen (Nichtigkeit „ex tunc“) stellt ein erhebliches juristisches Problem dar, da eine bereits erfolgte Transaktion definitionsgemäß in der Blockchain dauerhaft sichtbar bleibt. Hier besteht weitergehender Klärungsbedarf, ob das Problem etwa im Rahmen einer Private Blockchain bereits über Nutzungsbedingungen zufriedenstellend gelöst werden kann oder es auch einer gesetzgeberischen Klarstellung bedarf, dass die Nichtigkeitsfolgen im Wege einer (oder mehrerer) „reverse transactions“ in zulässiger Weise abgebildet werden können.

Rechteübertragung in der Blockchain

A: Steckbrief

Worum geht es bei dem Thema?

Rechte an Sachen und Rechten können grundsätzlich auch über die Blockchain übertragen werden, soweit dies nach dem jeweils anwendbaren nationalen Recht und den zugrundeliegenden Formvorschriften und sonstigen Anforderungen zulässig ist (siehe oben zu Fragen des anwendbaren Rechts). Für Anwendungen der Industrie 4.0 stellt sich die Frage, ob die Blockchain hierzu Erleichterungen bieten kann, um z. B. den Eigentumserwerb an Sachen für jedermann transparent und nachvollziehbar zu dokumentieren oder den Risiken des gutgläubigen Erwerbs von Sacheigentum aufgrund von Rechtsscheinerwerb vorzubeugen.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Wie können Rechte und Sachen mittels Blockchain übertragen werden?

- Wie kann ein physischer Gegenstand nachvollziehbar und eindeutig einer in der Blockchain abgelegten Kodierung zugeordnet werden, damit ein etwaiger Eigentumserwerb auch zweifelsfrei an dem betreffenden Gegenstand erfolgt?

B: Juristische Einschätzung

Soweit es sich bei den Übertragungsgegenständen um Rechte an immateriellen Gütern bzw. Daten als solche handelt – wie beispielsweise bei einem vertraglich vereinbarten Austausch von Maschinendaten –, ist eine selbst ausführende Transaktion in der Blockchain einfach zu bewerkstelligen: Der Datenaustausch im Wege eines Zugriffs oder Downloads wird automatisch gestartet in Abhängigkeit von einer ggf. automatisch angewiesenen Zahlung oder einem anderen Freigabebefehl.

Aber auch bei beweglichen Sachen ist eine Eigentums- bzw. Rechteübertragung mittels Smart Contract möglich. Denkbar ist etwa, dass außerhalb der Blockchain die tatsächliche Übergabe einer Sache vorgenommen wird oder auch ein Besitzkonstitut vereinbart wird (i. S. d. § 929 S. 1, 930 BGB) und im Smart Contract der Austausch der Willenserklärungen für die Eigentumsübertragung (dingliche Einigung) an die Bedingung eines wiederum digital überprüfbaren Zahlungseingangs programmiertechnisch geknüpft ist. Die eindeutige Zuordnung beweglicher Sachen zu ihren jeweiligen Rechteinhabern kann innerhalb der Blockchain über entsprechende digitale Identitäten („digital twin") bewerkstelligt werden.

C: Handlungsoptionen und Handlungsempfehlungen

- Die Blockchain und Smart Contracts bieten sich als taugliches Mittel zur Abbildung von Rechteübertragungen an Sachen und digitalen Gütern an. Dabei bedarf es einer eindeutigen Zuordnung des physischen Gegenstands zu seinem in der Blockchain abgelegten Ebenbild.

Haftung für Fehler in der Programmierung

A: Steckbrief

Worum geht es bei dem Thema?

Wenn der derzeit absehbare Einsatz von Blockchains im Bereich Industrie 4.0 in Private Blockchains aufgrund vorgegebener Nutzungsbedingungen erfolgt, stellt sich die Frage, ob die Funktion der Blockchain oder eines Smart Contracts fehlerhaft programmiert ist und – möglicherweise – dadurch bedingt auch fehlerbehaftete Transaktionen ausführt.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Welche Haftungsszenarien könnten eintreten und wer haftet für eine Fehlfunktion der Blockchain oder des Smart Contracts?

B: Juristische Einschätzung

Bei der Frage nach etwaigen „Fehlern" in Smart Contracts ist es wichtig, die technischen und rechtlichen Aspekte klar zu unterscheiden. Ein einzelner Block der Kette ist genau dann fehlerfrei erstellt, wenn er erfolgreich mit den anderen Blöcken der Blockchain verknüpft werden kann. Die Realisierung einer Smart-Contract-Transaktion kann technisch in diesem Sinne nicht falsch ablaufen – entweder sie wird technisch erfolgreich abgewickelt oder eben nicht. Ob die Transaktion aber in den Augen der Beteiligten auch rechtlich dem zugrundeliegenden Vertrag bzw. dem von den Parteien intendierten Kausalgeschäft entspricht, ist eine andere Frage. Der Smart Contract lässt keine Auslegung zu, diese greift nur mit Blick auf das außerhalb des Smart Contracts Gewollten, um ggf. den Parteien zur Realisierung des gemeinsam gewünschten Erfolges zu verhelfen.

Für die Authentizität bzw. inhaltliche Richtigkeit der einer Transaktion zugrundeliegenden Daten und hinter der Transaktion stehenden wirtschaftlichen Motivation in einem Block ist in erster Linie das Unternehmen verantwortlich, das diese Daten in der Blockchain abgelegt hat. Ein juristisch noch näher zu beleuchtendes Problem ergibt sich daraus, wenn sich eine inhaltlich fehlerhafte Dateneingabe über mehrere Blöcke fortsetzt, nachfolgende Blöcke von anderer Seite veranlasst werden und Dritte auf die inhaltliche Richtigkeit der Daten vertrauen. Hier könnte man die Frage stellen, ob dies – bei Erkennbarkeit der Fehlerhaftigkeit – zu einer Haftung mehrerer bzw. einer gesamtschuldnerischen Haftung über mehrere Teilnehmer führt.

C: Handlungsoptionen und Handlungsempfehlungen

- Bei vollständiger Transparenz vorausgehender Transaktionen und der zugrundeliegenden vertraglichen Annahmen und Datenbestände kann die Frage eines Zueigenmachens in der Folgetransaktion und – bei Datenfehlern – einer etwaigen Kumulierung oder Vergemeinschaftung der Haftung „über die Kette" aufkommen. Nutzungsbedingungen sollten eine solche Wirkung zur Sicherung der Verkehrsfähigkeit von Blockchain-basierten Transaktionen bestmöglich ausschließen.

Durchsetzung von Ansprüchen auf bzw. außerhalb einer Public bzw. Private Blockchain

A: Steckbrief

Worum geht es bei dem Thema?

Wenn es bei Smart Contracts oder anderen mittels Blockchain durchgeführten Transaktionen zu Leistungsstörungen kommt, ist die Durchsetzung der zivilrechtlichen Ansprüche von entscheidender Bedeutung, um die Nutzung der Blockchain verlässlich abzusichern.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Wie können Ansprüche auf bzw. außerhalb einer Public bzw. Private Blockchain durchgesetzt werden?

B: Juristische Einschätzung

Der Smart Contract beruht als selbstausführende Transaktion auf einem typischerweise außerhalb (aber denkbar auch innerhalb) der Blockchain zuvor geschlossenen Vertrag bzw. entsprechender Nutzungsbedingungen (AGB). Während die binäre Funktion eines Smart Contracts – im Sinne der Wenn-dann-Logik – für die automatische Auslösung von Zahlungen leicht an einen vordefinierten, messbaren Eintritt der Hauptleistung zu knüpfen ist (und damit das Problem adressiert „Wer sagt mir, dass mein Kunde zahlt?“), wird es komplizierter, wenn es um Sekundäransprüche (Gewährleistung, Schadensersatz etc.) geht. Damit auch diese reibungslos durchgesetzt werden können, müssten sie im Programmcode bereits von Anfang an berücksichtigt werden („einprogrammiertes Gesetz“). Das ist aber wegen der Komplexität und Auslegungsbandbreite ebenso wie der Relevanz unbestimmter Rechtsbegriffe (z. B. „wesentliche Abweichung von der vertraglich vereinbarten Beschaffenheit“) für mögliche Sekundäransprüche erheblich schwieriger.

Für alle Sekundäransprüche, die sich nicht im Smart Contract wiederfinden bzw. beim Schreiben des Smart-Contract-Codes nicht bedacht werden können, muss die Durchsetzung auf „herkömmlichem Weg“ erfolgen, also in der „realen Welt“, etwa aufgrund zugrundeliegender AGBs in einer Private Blockchain, deren Teilnehmer – jedenfalls typischerweise – im Gegensatz zur Public Blockchain aufgrund entsprechender Signaturen namentlich identifizierbar wären. Welche Ansprüche konkret bestehen und unter welchen Voraussetzungen diese durchgesetzt werden können, richtet sich nach dem der Transaktion zugrundeliegenden Vertrag (sog. „Kausalgeschäft“). Bei der Durchsetzung dieser Ansprüche könnte aber der Smart Contract helfen, wenn eine verpflichtende Schiedsstelle, die Einschaltung eines Ombudsmanns oder eine Justizschnittstelle (sog. „Oracle“) in den Code mit aufgenommen wird und damit vorab das passende Streiterledigungsverfahren festgelegt ist. Kann nicht auf eine einprogrammierte Möglichkeit der Streiterledigung zurückgegriffen werden, ist eine Durchsetzung von Ansprüchen gegen den Vertragspartner nur möglich, wenn er auch (außerhalb der Blockchain) identifiziert werden kann. Insofern ist die Nutzung einer Private/Permissioned Blockchain eindeutig vorzugswürdig.

C: Handlungsoptionen und Handlungsempfehlungen

- Effektive Rechtsdurchsetzung ist bei der Nutzung der Blockchain ein entscheidender, vertrauensbildender Faktor.

- Beim Einsatz der Private Blockchain – also innerhalb der derzeit absehbaren Use Cases – sind Streiterledigungsmechanismen auf herkömmlichem Wege im Rahmen der Nutzungsbedingungen das übliche Mittel der Wahl.

- Bei der Public Blockchain bestehen erhebliche Schwierigkeiten, Streiterledigung zwischen Teilnehmern – auch wenn diese durch digitale Identitäten verifizierbar sind – innerhalb der Blockchain zu erledigen. Hier ist noch verstärkt über automatisierte Streiterledigungsmechanismen für einfache, binäre Entscheidungslagen nachzudenken.

- Für komplexe Streiterledigung, insbesondere solche, die auf die Auslegung unbestimmter Rechtsbegriffe angewiesen ist, dürfte eine automatisierte Streiterledigung innerhalb der Blockchain faktisch in der näheren bis mittleren Zukunft ausgeschlossen sein und mit Blick auf das Rechtsstaatsprinzip insgesamt problematisch bleiben.

Blockchain und Datenschutz

A: Steckbrief

Worum geht es bei dem Thema?

Blockchain-Technologie verspricht ein großes Potenzial im Rahmen der Digitalisierung der Industrie. IoT-Dienste, Logistik oder Smart Contracts: Die Bereiche, in denen die dezentrale Architektur der Blockchain der Vernetzung vieler Beteiligter in der Industrie 4.0 entgegenkommt, sind vielfältig.

Der Einsatz von Blockchain-Technologie bringt einige datenschutzrechtliche Fragestellungen mit sich. Die im Mai 2018 in Kraft getretene DSGVO fußt auf zentraler Serverarchitektur und datenbasierten Geschäftsmodellen einzelner Datenverarbeiter. Die entsprechenden Regelungen erscheinen daher in Hinblick auf neue, dezentrale Technologien schon teilweise veraltet.

Insbesondere das Merkmal der Unveränderlichkeit (immutability) der Blockchain und deren u. U. vielzählige und unbekannte Teilnehmer stehen hierbei im Fokus der rechtlichen Diskussion. Das nachträgliche Löschen von Daten oder deren Änderung ist der Blockchain prinzipiell wesensfremd – gerade eine kontinuierliche Fortschreibung sorgt für das Vertrauen, das mit dieser Technologie einhergeht.

Permissioned/Private-Blockchains, die im Bereich der Industrie 4.0 vorzugsweise zum Einsatz kommen, weisen hier weniger Konfliktpotenzial auf als Lösungen, die für jedermann zugänglich und „permissionless" sind.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Können personenbezogene Daten auf der Blockchain gespeichert werden?
- Wer ist als Blockchain-Teilnehmer Verantwortlicher, wer Auftragsverarbeiter, wer Betroffener?
- Welche Lösungen gibt es für Unternehmen, um den Rechten der Nutzer (Betroffenen) Genüge zu tun?
- Wo muss der Gesetzgeber nachbessern, damit Blockchain-Technologie im Industrie-4.0-Umfeld ihr volles Potenzial entfalten kann?

B: Juristische Einschätzung

Das potenzielle Konfliktfeld Blockchain und Privacy ist ein Paradebeispiel für die mitunter negativen Auswirkungen eines zu starren Datenschutzrechtsrahmens. Dies betrifft nicht nur Wirtschaft und Innovation, die unter einem gewissen Maß an Unwägbarkeit in Bezug auf den Blockchain-Einsatz leiden. Auch Blockchain als „Privacy Enhancement Technology", also ein Mittel, das Nutzern Kontrolle und Souveränität hinsichtlich ihrer Datenverwendung verleiht, ist hiervon betroffen.

Dieses Spannungsverhältnis ist bereits auf politischer Ebene zur Kenntnis genommen worden. Es ist Gegenstand eines Reports des EU Blockchain Observatory („Blockchain and the GDPR"), von Leitfäden (Bitkom, „Blockchain und Datenschutz – Faktenpapier"), Positionspapieren (Blockchain Bundesverband, „Blockchain, data protection, and the GDPR") und wissenschaftlicher Betrachtungen (Finck, Blockchain and Data Protection in the European Union, Max Planck Institute for Innovation & Competition Research Paper No. 18-01.). Auch die französische Datenschutzbehörde CNIL hat sich als erste Aufsichtsbehörde zum Thema Blockchain und Datenschutz geäußert (Premiers éléments d'analyse de la CNIL: Blockchain, September 2018).

Alle Betrachtungen heben den Umstand hervor, dass private Blockchains, in denen die Teilnehmer bekannt und ggf. weitere Vereinbarungen zur Nutzung getroffen werden, juristisch leichter zu handhaben sind als öffentliche Blockchains. Dies kommt dem Einsatz im Rahmen der Industrie 4.0 zupass.

Zudem darf auch in tatsächlicher Hinsicht nicht vergessen werden, dass Blockchain eine sehr junge Technologie ist. Sie wird kontinuierlich auch in technischer Hinsicht weiterentwickelt, auch um datenschutzrechtlichen Herausforderungen besser begegnen zu können.

Anwendung der DSGVO – Personenbezogene Daten auf der Blockchain

Um in den Anwendungsbereich der DSGVO zu fallen, müssen Daten, die auf einer Blockchain verarbeitet werden, einen Personenbezug aufweisen. Es geht also um Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person (die „betroffene Person") beziehen (Art. 4 Abs. 1 DSGVO). Pseudonymisierte Daten, die mittels Zusatzinformationen wieder einer natürlichen Person zugeordnet werden können, sind im Sinne der DSGVO noch immer

solche mit Personenbezug. Lediglich anonymisierte Daten fallen nicht in den Anwendungsbereich der DSGVO (siehe Erwägungsgrund 26). Die Anforderungen an eine wirksame Anonymisierung werden jedoch seitens der Aufsichtsbehörden mitunter streng gehandhabt. Insbesondere gelten verschlüsselte Daten regelmäßig lediglich als pseudonymisiert, nicht als anonymisiert.

Fraglich ist, welche typischen Daten, die im Blockchain-Kontext genutzt werden, einen Personenbezug aufweisen können:

Public Keys: Ein regelmäßig öffentlich sichtbarer Public Key ist vielen Blockchains immanent. Sobald dieser einer natürlichen Person zugeordnet werden kann, handelt es sich um ein personenbezogenes Datum im Sinne der DSGVO.

On-Chain Data: Prinzipiell können Daten jeglicher Art in die Blockchain geschrieben werden, so bspw. Namen natürlicher Personen und andere, die aufgrund ihrer Personenbeziehbarkeit in den Anwendungsbereich der DSGVO fallen.

Hashwerte: Hash-Daten lassen sich als kurze Zeichenketten beschreiben, die einen eindeutigen und einzigartigen Finderabdruck einer (in der Regel größeren) Datenmenge darstellen. Hierdurch lassen sich Daten, Dateien, Dokumente etc. eindeutig zuordnen. Es lässt sich zudem überprüfen, ob eine Datei oder ein Dokument im Nachhinein verändert wurde (da bei dem erneuten Bilden des Hashwerts nach Veränderung einer Information auch ein anderer Hashwert entstehen würde). Ob es sich bei diesem „Fingerabdruck“ überhaupt um ein personenbezogenes Datum handelt, ist fraglich.

Die Zuordnung des Hash zu einer bestimmten Information setzt deren Verfügbarkeit und den Abgleich zwischen Hash und Originaldokument bei der verantwortlichen Stelle voraus. Diese Zuordnung ist für viele Beteiligte der Blockchain schlicht nicht möglich. Dies gilt insbesondere dann, wenn die Originaldaten, auf die sich der Hashwert bezieht (z. B. Lieferdaten einer natürlichen Person), außerhalb der Blockchain gespeichert und später gelöscht werden. Der in der Blockchain gespeicherte Hashwert würde somit „ins Leere“ laufen und nicht mehr zu einer identifizierbaren Person (bzw. zu den entsprechenden Daten) führen. Die Article 29 Data Protection Working Group hielt Hashwerte hingegen für pseudonymisierte personenbezogene Daten (siehe WP216, Opinion 05/2014 on Anonymisation Techniques, S. 20). Vollständige Rechtssicherheit in Bezug auf die Verwendung von Hashes in der Blockchain kann hier jedoch nur eine entsprechende Klarstellung durch den Europäischen Datenschutzausschuss und letztendlich durch die Rechtsprechung erfolgen.

Wen trifft welche datenschutzrechtliche Rolle im Blockchain-Kontext?

Ein weiteres Feld offener Fragen ist das der Beteiligten einer Blockchain und deren datenschutzrechtliche Einordnung. Die Zuordnung zur Rolle einer betroffenen Person (Art. 4 Abs. 1 DSGVO), eines Verantwortlichen (Art. 4 Abs. 7 DSGVO), eines Auftragsverarbeiters (Art. 4 Abs. 8 DSGVO) oder gar eines gemeinsam Verantwortlichen (Art. 26 DSGVO) bestimmt die damit korrespondierenden datenschutzrechtlichen Pflichten und Rechte.

In privaten/permissioned Blockchains liegt in der Regel eine (vertragliche) Übereinkunft vor, die festlegt, wer verantwortet, welche Daten wo verarbeitet werden. Dies ist ein Vorteil gegenüber einer öffentlichen/permissionless Blockchain-Architektur. Hier ist dem Einzelnen nicht bekannt, welche anderen Beteiligten in welchem Teil der Welt Blockchain-Daten verarbeiten. Hierdurch können keine Regelungen, z. B. zur Auftragsdatenverarbeitung oder im Rahmen der gemeinsamen Verantwortlichkeit nach Art. 26, getroffen werden. Im industriellen Bereich stehen zumeist die Bedingungen der Blockchain-Nutzung fest. Hiernach kann im Einzelfall beurteilt werden, ob es sich bei den Beteiligten um Verantwortliche, Auftragsverarbeiter oder gemeinsam Verantwortliche handelt.

Rechteausübung

Die Ausübung der Betroffenenrechte, bspw. auf Löschung (bzw. auf Vergessenwerden, Art. 17 DSGVO) oder Berichtigung von Daten (Art. 16 DSGVO), kann eine Herausforderung in einer Blockchain-Umgebung darstellen. Ein Löschen von Daten in einzelnen Blöcken der Blockchain ist schließlich vom Grundsatz her nicht vorgesehen (aber in einer entsprechend gestalteten Architektur auch nicht unmöglich).

Insbesondere in einer öffentlichen/permissionless Blockchain-Umgebung ist oftmals gar nicht klar, gegen welche Datenverarbeiter so ein Anspruch zu richten wäre. In einer solchen Konstellation wäre schon die datenschutzrechtliche Einwilligung nur sehr umständlich zu konstruieren und als Basis der Verarbeitung verfügbar. Dieses Problem ist in

einer industriellen, privaten Blockchain-Lösung wesentlich einfacher zu lösen.

Das Recht auf Löschung bzw. auf Vergessenwerden ist in einer Blockchain-Umgebung schwer, aber ebenfalls nicht unmöglich umzusetzen. Hashwerte, moderne Verschlüsselungsverfahren bei Zerstörung der entsprechenden Schlüssel können hier Lösungen bieten (so auch die französische Aufsichtsbehörde CNIL, Premiers éléments d'analyse de la CNIL: Blockchain, September 2018).

Insgesamt besteht hier, auch in einer privaten Blockchain-Umgebung im Rahmen der Industrie 4.0, Bedarf an weiteren technischen Lösungen und einer praktikablen Auslegung und Anwendung der DSGVO durch die Aufsichtsbehörden.

C: Handlungsoptionen und Handlungsempfehlungen

- Nach Möglichkeit sollte im Einsatzgebiet Industrie 4.0 auf private/permissioned Blockchain-Lösungen zurückgegriffen werden. Hierdurch lassen sich datenschutzrechtliche Risiken minimieren. In der Regel sind hier die Teilnehmer der Blockchain bekannt. Es lässt sich festlegen, wo die Daten verarbeitet werden. Auch lassen sich bei Verarbeitung außerhalb der EU die datenschutzrechtlichen Instrumente des Drittstaatentransfers einsetzen.

- Personenbezogene Daten sollten (auch) nicht (verschlüsselt) in der Blockchain selbst gespeichert werden, sondern in gesonderten Datenbanken „off-chain". Hashwerte sind hier das geeignete Mittel, um den Bezug zur Blockchain herzustellen.

- Um die datenschutzrechtlichen Verantwortlichkeiten zwischen den Beteiligten festzulegen, sollten verbindliche (vertragliche) Absprachen getroffen werden. In einer privaten Blockchain lassen sich hierdurch Rollen und Pflichten der (gemeinsamen Auftrags-)Datenverarbeitung festschreiben.

- Datenschutz-Aufsichtsbehörden und der Europäische Datenschutzausschuss müssen Leitlinien erarbeiten, die einen angemessenen Ausgleich zwischen den Möglichkeiten, die die Blockchain eröffnet, und dem Datenschutz anstreben.

- Das Recht auf Datenschutz ist nicht absolut gewährt. Datenschutz muss immer im Kontext gesellschaftlicher Entwicklung und im Ausgleich mit anderen grundrechtlich geschützten Positionen gesehen werden.

- Vor diesem Hintergrund ist im Rahmen der Überprüfung der DSGVO durch die Europäische Kommission zu erwägen, ob eine Flexibilisierung des Datenschutzrechtsrahmens in Hinblick auf innovative Technologien wie Blockchain erfolgen sollte.

- Hier geht es konkret um die Möglichkeit der rechtmäßigen Verwendung von Public Keys sowie Einschränkungen des Löschungsrechts in Fällen, in denen dieses aus technischen Gründen nicht durchgesetzt, aber bspw. durch ein Sperren der Daten substituiert werden könnte.

IP- und patentrechtliche Aspekte bei der Verwendung von Blockchain-Protokollen

A: Steckbrief

Worum geht es bei dem Thema?

Auch aufgrund der Präsenz in der öffentlichen Berichterstattung wird in vielen Unternehmen geprüft, welche Blockchain-Anwendungen für die Verbesserung interner und externer Abläufe in Betracht kommen.

Die unternehmerische Beteiligung an einem Blockchain-Start-up, aber auch die Einrichtung einer unternehmenseigenen Taskforce mit der Aufgabe, eine Eigenentwicklung auf Blockchain-Basis zu erstellen, sind die üblichen ersten Schritte in die Blockchain-Welt. Eigenentwicklungen werden dadurch vereinfacht, dass die Blockchain-„Community" sog. Blockchain-Frameworks/Blockchain-Protokolle zur Verfügung stellt, die wie ein Betriebssystem als Grundlage für die neuen Blockchain-Anwendungen genutzt werden können.

Bei diesen Protokollen handelt es sich um Software, so dass die typischen Software-Themen zu beachten sind, d. h. zu prüfen ist, welche Urheberrechte bzw. Lizenzen zu beachten sind. Blockchain-Protokolle werden in der Regel unter sog. Open-Source-Software-Lizenzen zur Verfügung gestellt. Aber auch proprietäre Lizenzen spielen eine Rolle, weil für eine unternehmerische Anwendung nicht immer die öffentlich verfügbare Open-Source-Basisversion des Protokolls ausreicht, sondern die lizenzpflichtige „Profiversion" erforderlich wird. Zu beachten ist außerdem, dass die Blockchain-Anwendungen regelmäßig zur Lösung technischer Verfahren eingesetzt werden und damit eine Patentierbarkeit denkbar ist.

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Was muss bei der Nutzung von Open-Source-Blockchain-Protokollen beachtet werden?
- Welche Fallstricke sind bei der Verwendung von lizenzpflichtigen Blockchain-Protokollen zu beachten, um etwaige Abhängigkeiten von Anbietern von Blockchain-Protokollen zu vermeiden?
- Wann ist eine Blockchain-Anwendung patentierbar?
- Welche Konsequenzen ergeben sich aus der möglichen Patentierbarkeit?

B: Juristische Einschätzung

Was muss bei der Nutzung von Open-Source-Blockchain-Protokollen beachtet werden?

Open-Source-Blockchain-Protokolle werden, ähnlich wie bisher ein Betriebssystem, häufig als Grundlage für die Programmierung eigener neuer Blockchain-Anwendungen, sog. Decentralized Applications, kurz DApps, genutzt. Bekannte Beispiele für derartige Open-Source-Blockchain-Protokolle sind „Ethereum", „Hyperledger Fabrics" oder auch „R3 Corda". Diese Protokolle sind weit verbreitet und öffentlich verfügbar und bieten sich daher als Grundlage für die Entwicklung einer Blockchain-basierten Softwarelösung an. Es lassen sich schnell und einfach DApps entwickeln und testen.

Gemeinsam ist diesen Blockchain-Protokollen, dass sie unter sog. Open-Source-Lizenzen zur Nutzung bereitgestellt werden. D. h. sie stehen im sog. Source Code zur Verfügung und können, ohne dass eine Lizenzgebühr erhoben wird, von Entwicklern ergänzt, verbessert oder in sonstiger Weise bearbeitet oder verwendet werden. Jedoch ist Open-Source-Software keine urheberrechtsfreie Software. Jeder, der Open-Source-Software verwendet, unterliegt den Verpflichtungen der jeweils gültigen Open-Source-Software-Lizenz. Besonders relevant sind die in den Software-Lizenzen häufig enthaltenen sog. „Copyleft"-Verpflichtungen. Diese regeln, dass der Verwender der Open-Source-Software die von ihm erstellten „Bearbeitungen" der Open-Source-Software unter derselben Open-Source-Lizenz vertreiben muss. Zwar ist die Reichweite des Begriffs der „Bearbeitung" je nach Open-Source-Software-Lizenz unterschiedlich. „Bearbeitung" in diesem Sinne kann aber unter Umständen die gesamte selbst entwickelte Software sein, z. B. auch schon dann, wenn die neu entwickelte Software „nur" auf die Open-Source-Software zugreift. Die Konsequenz ist, dass der Verwender einer Open-Source-Software, für die ein strenges Copyleft gilt, verpflichtet wäre, die für eine DApp neu entwickelte Software als Open Source zur Verfügung zu stellen.

Eine proprietäre Anwendung der DApp würde ausscheiden, was das geplante Geschäftsmodell ggf. unattraktiv machen könnte.

Von den eingangs genannten Blockchain-Protokollen werden Hyperledger Fabrics und R3 Corda unter der Apache 2.0-Lizenz als Open Source zur Nutzung bereitgestellt. Die Apache 2.0-Lizenz ist eine sog. „Permissive Licence".[2] Das heißt, sie enthält kein Copyleft, also keine Verpflichtung des Lizenznehmers, unter Verwendung der lizenzierten Software erstellte Software unter der Apache 2.0-Lizenz zu veröffentlichen. Einer Nutzung dieser Blockchain-Protokolle zur Erstellung proprietärer Anwendungen steht die Apache 2.0-Lizenz daher nicht entgegen. Für Ethereum, eines der am häufigsten verwendeten Protokolle, ist unklar, welche Open-Source-Lizenz Anwendung findet. Die verschiedenen Bestandteile von Ethereum wurden unter unterschiedlichen Open-Source-Lizenzen veröffentlicht; unter anderem auch der sog. GPLv3. Also unter jener Lizenz, die unter Open-Source-Compliance-Richtlinien dann die Alarmglocken auslöst, wenn es um die Entwicklung von proprietärem Software-Code zur kommerziellen Nutzung geht. Für weitere Blockchain-Protokolle gelten wieder andere Open-Source-Lizenzen.

Daher muss sowohl bei der Auswahl eines Blockchain-Protokolls für eine eigene Entwicklung als auch beim Erwerb einer Beteiligung an einem Blockchain-Start-up sehr genau geprüft werden, welche Lizenzregelungen für die verwendete Software gelten und inwieweit dadurch der eigene, proprietäre Softwarecode „infiziert" werden kann. Wird das unterlassen, steht die kommerzielle Nutzung der betreffenden Blockchain-Anwendung im Risiko.

Welche Abhängigkeiten von Anbietern von Blockchain-Protokollen sind zu vermeiden?

Es gelten die gleichen Grundsätze wie bei jeder Software, die für wesentliche Unternehmensfunktionen erforderlich ist. Die langfristige Verfügbarkeit der Software bei hinreichender Kostenkontrolle ist sicherzustellen.

2 Zum Begriff siehe Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, Teil B. Immaterialgüterrecht § 9 Open Source und Open Content Rn. 50.

Sofern allein auf der Basis von Open-Source-Lizenzen gearbeitet wird und die betreffende Software vom Anwender auf eigenen Systemen betrieben werden kann, bestehen insoweit keine wesentlichen Risiken. Allerdings gibt es im Blockchain-Bereich vereinzelt Open-Source-Angebote, die nur zur Erstellung von Testanwendungen ausreichend sind. Soll dann die Testanwendung in den Regelbetrieb übernommen werden, fehlen insbesondere in Bezug auf die IT-Sicherheit wesentliche Funktionen, die nur in einer entgeltpflichtigen „Enterprise-Version" zur Verfügung gestellt werden. Diese „Enterprise-Versionen" werden dann nur gegen Zahlung einer Lizenzgebühr und unter bisweilen recht einseitigen Lizenzbedingungen zur Verfügung gestellt. Damit entsteht eine Abhängigkeit vom Anbieter der Software, da eine Umstellung auf ein anderes Blockchain-Protokoll wegen der bislang fehlenden Kompatibilität der verschiedenen Blockchain-Protokolle bedeutet, dass die Anwendung für das andere Protokoll neu entwickelt werden müsste.

Wann ist eine Blockchain-Anwendung patentierbar?

Auch im Hinblick auf die Patentierbarkeit gelten die für Software entwickelten Grundsätze. Gemäß den Regelungen des Europäischen Patentübereinkommens (EPÜ), das die rechtliche Grundlage für die Erteilung von Patenten durch das Europäische Patentamt (EPA) bildet, ist Software grundsätzlich vom Patentschutz ausgeschlossen.

Diese Regelung ist jedoch nach ständiger Rechtsprechung und der Prüfungspraxis des EPA eng auszulegen. Der Ausschluss der Patentierbarkeit gilt nur für Software an sich. Mit anderen Worten, es wird kein Patent auf den Source-Code an sich erteilt. Dieser Schutz ist dem Urheberrecht bzw. Copyright vorbehalten. Allerdings ist die der Software zugrundeliegende abstrakte technische Lehre durchaus dem Patentschutz zugänglich, man spricht dann von computerimplementierten Erfindungen (CIE).

Für CIE hat das EPA ein zweistufiges Prüfungsschema entwickelt. In einem ersten Schritt wird geprüft, ob es sich bei dem beanspruchten Gegenstand um Software an sich handelt. Diese Prüfung führt grundsätzlich bereits dann zu einem positiven Ergebnis, wenn in den Patentanspruch das technische System „Computer" einbezogen wird. Im zweiten Schritt des für CIE entwickelten Prüfungsschemas muss die beanspruchte CIE, insbesondere Blockchain-Anwendung, ferner neu und erfinderisch sein.

Dabei werden nur solche neuen Merkmale in Betracht gezogen, die zum technischen Charakter des beanspruchten Gegenstands beitragen. Für einen solchen technischen Charakter ist eine „weitere technische Wirkung" notwendig, die über die „normale" physikalische Wechselwirkung zwischen dem Programm und dem das Programm ausführenden Computer hinausgeht.

Die Richtlinien für die Prüfung im Europäischen Patentamt[3] führen in Teil G – Kapitel II-16; 3.6. Beispiele für eine derartige weitere technische Wirkung auf. Ferner werden unter Teil G – Kapitel VII-8, 5.4.2. praktische Beispiele für erfinderische und nicht erfinderische CIE erläutert.

In der jüngsten Vergangenheit wurden durch das Europäische Patentamt bereits einige auf Blockchain-Anwendungen gerichtete Patente erteilt. Beispielsweise wurden folgende Anwendungen als patentfähig, also insbesondere als neu und erfinderisch, angesehen:

- In einem Verfahren zur Überwachung eines Smart Contracts wurde die Verwendung eines ungenutzten Ausgangs (UTXO) zu einem Datensatz als erfinderisch angesehen, wenn dieser UTXO zur Interpretation eingesetzt wird, ob der Vertrag als offen oder gültig anzusehen ist.

- Für computerimplementierte Verfahren zur Feststellung, ob eine Software lizenziert und damit zulässig verwendet wird, wurde als erfinderisch angesehen, dass spezielle öffentliche Benutzerschlüssel unter Verwendung eines in dem Ledger gespeicherten Transaktionsdatensatzes verglichen werden.

Diese Beispiele zeigen, dass das EPA dem Schutz von Blockchain-Anwendungen offen gegenübersteht. Allerdings bleibt abzuwarten, ob die bisher erteilten Patente in möglichen Einspruchsverfahren oder nationalen Löschungsverfahren als wirksam bestätigt werden.

3 http://documents.epo.org/projects/babylon/eponet.nsf/0/2A358516CE34385CC125833700498332/$File/guidelines_for_examination_2018_hyperlinked_de.pdf

Welche Konsequenzen ergeben sich aus der möglichen Patentierbarkeit?

Aus der Patentierbarkeit ergeben sich große Chancen für innovative Firmen. Während der übliche Schutz von Software lediglich die konkrete Umsetzung, nicht aber die Idee schützt, können die den Blockchain-Anwendungen zugrundeliegenden abstrakten Ideen durch Patente geschützt werden. Dadurch kann die Marktposition gegenüber Wettbewerbern gestärkt und nicht zuletzt durch Lizenzierung der Technologie auch der Umsatz durch Lizenzeinnahmen erhöht werden. Hier scheint jedoch Eile geboten, da bereits eine Mehrzahl von grundlegenden Anwendungen angemeldet oder sogar bereits geschützt sind, insbesondere in anderen Ländern, wie den USA oder auch der Volksrepublik China.

Andererseits sollte bei Entwicklung einer Blockchain-Anwendung auch überwacht werden, ob es angemeldete oder erteilte Patente im relevanten Bereich gibt, um Risiken zu minimieren.

Einige Beobachter[4] sehen den Blockchain-Bereich als künftiges „Schlachtfeld“ für Patentstreitigkeiten an.

C: Handlungsoptionen und Handlungsempfehlungen

- Bereits bei der Auswahl eines Blockchain-Protokolls im Hinblick auf eine Testanwendung ist sehr genau zu prüfen, ob das gewählte Blockchain-Protokoll den Anforderungen eines späteren Regelbetriebs der Testanwendung genügen würde. Hierzu gehören nicht nur die technischen Anforderungen, sondern insbesondere auch die urheberrechtlichen Anforderungen.

- Bei der Verwendung von Open-Source-Protokollen, die einem Copyleft unterliegen, ist unbedingt zu prüfen, ob die eigene Entwicklung „infiziert“ wird. Das ist nicht immer der Fall, kann aber passieren.

- Bei der Entwicklung von Blockchain-Anwendungen sollte frühzeitig deren Patentierbarkeit geprüft werden, insbesondere vor einer Weitergabe von Details.

- Patentveröffentlichungen im Bereich der Blockchain sollten durch einen Serviceanbieter überwacht werden. Hierdurch kann frühzeitig erkannt werden, ob die eigene Entwicklung in den Schutzbereich von beantragten oder bereits erteilten Schutzrechten eingreift. Damit können frühzeitig Gegenmaßnahmen, wie die Erarbeitung von Umgehungslösungen, die Geltendmachung von Einwendungen gegen eine Patenterteilung oder der Angriff des Rechtsbestands des Patentes durch einen Einspruch, eingeleitet werden.

4 https://cointelegraph.com/news/is-blockchain-about-to-become-a-patent-war-battleground

Relevanz von IT-Sicherheit im Bereich Blockchain

A: Steckbrief

Worum geht es bei dem Thema?

Einer der meist erwähnten Vorteile der Blockchain und der derzeit noch im Vordergrund stehenden Anwendungen der Kryptowährungen ist die Sicherheit der Blockchain-Technologie. Dennoch berichtete die Wirtschaftswoche am 20. Juni 2018, dass bislang „insgesamt knapp eine Million Bitcoin gestohlen [wurden] – zum aktuellen (20. Juni 2018) Kurs ist das eine Beute von 6,6 Milliarden Dollar". Wie passen diese beiden Aussagen zusammen und welche Relevanz hat das Thema für die rechtliche Betrachtung im Rahmen von Industrie 4.0? Gibt es weitere Blockchain-typische IT-Sicherheitsrisiken?

Welche Fragen/Herausforderungen ergeben sich für Industrie 4.0?

- Etwaige IT-Sicherheitsrisiken müssen bekannt sein, damit sie in der Risikoanalyse berücksichtigt werden und auch im Rahmen einer Vertragsgestaltung zwischen den beteiligten Vertragspartnern adäquat zugeordnet werden können. Das gilt bspw. im Rahmen einer Finanzierung an einem oder auch bei einer Akquisition in Bezug auf ein Blockchain-Start-up. Das gilt aber auch für die erforderliche – aber häufig vernachlässigte – juristische Begleitung der Entwicklung von Applikationen auf der Blockchain.

B: Juristische Einschätzung

IT-Sicherheit: Blockchain-typische Risiken

Datenvertraulichkeit

Die Schutzziele der IT-Sicherheit sind die Datenintegrität (= keine unbefugte bzw. nicht nachvollziehbare Änderung von Daten), die Datenverfügbarkeit (= der Zugriff auf die Daten ist möglich) und die Datenvertraulichkeit (= nur berechtigte Personen können auf die Daten zugreifen). Zusammenfassend kann man sagen, dass die Blockchain-Technologie aufgrund der verteilten Datenbankstruktur und der Unveränderbarkeit der über den Konsensmechanismus anerkannten Transaktionsblöcke in Sachen Datenintegrität und Datenverfügbarkeit eine bisher nicht bekannte IT-Sicherheit ermöglicht. Die Korruption oder Blockade von Daten an einem Node des Systems ist nicht relevant, da die Daten auf den anderen Nodes noch verfügbar sind und das Blockchain-Protokoll dafür sorgt, dass die korrumpierten Daten auf dem von einem Sicherheitsvorfall betroffenen Node wieder korrigiert werden.

In Sachen Datenvertraulichkeit ist die Blockchain-Technologie aber weniger sicher. Die Blockchain-Technologie basiert darauf, dass jedem Betreiber eines Nodes die gesamten Datenblöcke des betreffenden Blockchain-Protokolls zur Verfügung stehen. Soweit Teilnehmer- oder Transaktionsdaten vertraulich bleiben sollen, wird allein auf Verschlüsselungstechnologie gesetzt.

Nach derzeitigem Stand ist die eingesetzte Verschlüsselungstechnologie sicher; das wird aber nicht so bleiben. Der Fortschritt der Entwicklung im Bereich der „Quantencomputer" stellt insoweit eine wesentliche Bedrohung dar. Quantencomputer werden komplizierte Berechnungen um ein Vielfaches schneller als heutige Computer durchführen können. Ist diese Technologie erst einmal einsatzbereit, muss man damit rechnen, dass die heutigen Verschlüsselungen keine Sicherheit mehr bieten.

Wenn also heute in einem Unternehmen Blockchain-Entwicklungen gestartet werden, muss bei der Risikoanalyse berücksichtigt werden, dass die betreffenden Daten in einigen Jahren entschlüsselt und einsehbar werden könnten. Müssen die Daten vertraulich bleiben, ist die Blockchain-Anwendung so zu gestalten, dass neue und dann wieder sichere Verschlüsselungssysteme auch auf die vorhandenen, historischen Transaktionsblöcke nachträglich angewandt werden können. Weiterhin bedeutet das, dass den Teilnehmern an einer Blockchain-Anwendung klare vertragliche Verpflichtungen auferlegt werden müssen, damit das dargestellte Risiko durch gemeinsame Handlungspflichten kontrolliert werden kann. Derartige einklagbare vertragliche Verpflichtungen sind aber nur im Bereich einer sog. privaten Blockchain denkbar. Hier sind regelmäßig, abweichend vom typischen Fall der öffentlichen Blockchain, die einzelnen Teilnehmer bekannt. Zwischen diesen Teilnehmern müssen die Implementierung und die Verwendung einer privaten Blockchain vertraglich im Detail geregelt werden.

Datenauthentizität

Die mit Blockchain-basierten Anwendungen einhergehende Datenverfügbarkeit und Datenintegrität ist allerdings nicht damit gleichzusetzen, dass die auf der Blockchain abgespeicherten Daten auch richtig sind. Datenverfügbarkeit und Datenintegrität bedeuten lediglich, dass die Daten, die in der Blockchain abgespeichert werden, auch verfügbar sind und nicht verändert werden können. Werden „unwahre" Daten in die Blockchain aufgenommen, bleiben diese „unwahr". Diese Feststellung mag zunächst banal klingen, ist aber sehr relevant. Gerade im Industriebereich lebt eine Blockchain-Anwendung davon, dass die Daten auch „wahr" sind. Geht es bspw. darum, zu verfolgen, ob ein Medikament tatsächlich vom Hersteller stammt, muss die Sicherheit bestehen, dass die in den Datenblöcken gespeicherten Transaktionsdaten von einer vertrauenswürdigen Stelle bestätigt worden sind. Das sind zunächst die Transaktionsdaten, die bspw. vom Hersteller eines Produktes selber in die Blockchain aufgenommen werden. Das sind aber auch die Daten, die von externen Quellen, einem sog. Oracle (wie z. B. einem Datenprovider außerhalb der Blockchain oder auch Sensoren), in die Blockchain übertragen werden. Geht es bspw. um den Nachweis, dass die Kühlkette eines Produktes dauerhaft eingehalten worden ist, muss sichergestellt werden, dass die Sensoren, die die Temperatur in die Blockchain speisen, nicht korrumpiert werden.

Das ist bei der vertraglichen Gestaltung zu berücksichtigen und darf nicht aufgrund einer (Fehl-)Vorstellung von uneingeschränkter Informationssicherheit ignoriert werden.

IT-Sicherheit: Bekannte Risiken, die unverändert bestehen

Die in Unternehmen üblichen Sicherheitsmechanismen der IT-Compliance sind im Blockchain-Bereich unverändert anzuwenden. Deren Nichtbeachtung (und nicht die mangelnde „Sicherheit der Blockchain") war in der Vergangenheit regelmäßig der Grund für IT-Sicherheitslücken und der Grund, warum in einem so erheblichen Umfang Kryptowährungen gestohlen werden können. Werden vom Betreiber einer Handelsplattform für Kryptowährungen die (klassischen) IT-Sicherheitsanforderungen nicht beachtet, ist es (trotz der per se sicheren Blockchain) einfach, ein digitales Asset wie eine Kryptowährung zu entwenden.

Dementsprechend gelten die klassischen IT-Sicherheitsrisiken für Software unverändert auch im Bereich der Blockchain. Da eine Blockchain-Anwendung nichts anderes als Software ist, die zur Lösung einer technischen Aufgabe eingesetzt wird, können Fehler in der Programmierung der Software ausgenutzt werden, um in Systeme einzudringen.

Des Weiteren sind die Grundsätze über den sicheren Umgang mit Zugangsdaten zu beachten. Um Transaktionen über eine Blockchain-Anwendung auszuführen, benötigen die Teilnehmer einen sog. „privaten Schlüssel", mit dem sie sich identifizieren. Der private Schlüssel ist im Endeffekt nichts anderes als ein Passwort in der bisherigen IT-Welt. Wird der private Schlüssel Dritten zugänglich, können diese anstelle des Berechtigten Transaktionen durchführen.

C: Handlungsoptionen und Handlungsempfehlungen

- IT-Sicherheitsrisiken müssen bekannt sein, damit man sie sowohl im Rahmen der Vertragsgestaltung allokieren als auch durch das Design der Blockchain-Anwendung minimieren kann.

- Bisherige Fragen der IT-Sicherheit stellen sich auch im Blockchain-Bereich, das gilt aber nicht für die Dateninteg rität und die Datenverfügbarkeit.

AUTOREN

RA Dr. Duisberg (Bird & Bird) | RA Dr. Philipp Haas (Robert Bosch GmbH) | Dr. Nils Hullen (IBM Deutschland GmbH) | Thomas Kriesel (Bitkom e.V.) | RA Ted Kroke (Jones Day) | RA Martin Schweinoch (SKW Schwarz Rechtsanwälte) | RA Dr. Nick Wittek (Jones Day)

Diese Publikation ist ein Debattenbeitrag der Plattform Industrie 4.0.
Sie basiert auf den Ergebnissen der AG 4 „Rechtliche Rahmenbedingungen“.

www.plattform-i40.de