weizenbaum
institut

Online-Konsultation zur Blockchain-Strategie der Bundesregierung: Stellungnahme Weizenbaum-Institut

Das Weizenbaum-Institut beteiligt sich an der Online-Konsultation zur Blockchain-Strategie der Bundesregierung:

https://www.blockchain-strategie.de/

Im Folgenden veröffentlichen wir unsere Antworten.

Die Stellungnahme wurde zusammengetragen und formuliert durch die Forschungsgruppe 17 „Vertrauen in verteilten Umgebungen“, mit Unterstützung durch die Forschungsgruppen 18, 11 und 9. Sie wird darüber hinaus getragen von den Bereichen „Governance und Normsetzung“ und „Vertrag und Verantwortung auf digitalen Märkten“.

Kontext und Hinweise

Als Kontext zu den Fragen dient das offizielle Konsultations-Dokument, verfügbar unter:

https://www.blockchain-strategie.de/BC/Redaktion/DE/Downloads/online-konsultation-zur-erarbeitung-der-blockchain-strategie.pdf

Es wurde ausdrücklich darauf hingewiesen, dass nicht alle Fragen beantwortet werden müssen, und dass man sich auf die Themen fokussieren kann, die aus Sicht der Stellung nehmenden Organisation besonders wichtig erscheinen. Des Weiteren wurde erbeten, Stellungnahmen bevorzugt in Form von Stichpunkten und Aufzählungen statt reinem Fließtext abzugeben. Alle Eingabefelder hatten eine Größenbeschränkung, die in den meisten Fällen bei 2500 Zeichen lag.

I. Relevanz der Blockchain-Technologie

Möglichkeit zur Stellungnahme bezüglich der Relevanz der Blockchain-Technologie.

- Es besteht z.Z. ein Hype um das Thema „Blockchain“ - oft werden Potential und technischen Möglichkeiten der Technologie übertrieben dargestellt.
- Sichere verteilte, und sogar dezentrale, Systeme werden seit sehr langer Zeit angewendet und erforscht, lange bevor Bitcoin ins Leben gerufen wurde oder „Blockchain“ ein Begriff wurde.
- Es ist wichtig, bei der Digitalisierung problemorientiert vorzugehen und technische Lösungen abhängig von konkreten Anforderungen und gesellschaftlichen Zielen auszuwählen.
- Wir sehen die Gefahr, dass vielversprechende Lösungen ohne „Blockchain“-Bezug nicht ausreichend diskutiert und gefördert werden könnten. Für viele der in dieser Konsultation angeführten Anwendungsgebiete könnten nachhaltigere und problemorientiertere Maßnahmen beispielsweise sein:
  - Förderung offener Standards und nichtkommerzieller Alternativen zu etablierten Internet-Plattformen und Software-Herstellern.
  - Umsetzung moderner Privacy-Enhancing-Technologies und IT-Security-Standards.
  - Nachhaltige Förderung von unabhängiger Forschung und Lehre.

- Auf der anderen Seite wird „Blockchain“ oft nicht im Sinne einer konkreten Technologie diskutiert, sondern als Symbolbild für Digitalisierung im Kontext verteilter Systeme. In diesem Sinne begrüßen wir die Diskussion, da eine Vielzahl von gesellschaftlichen und wirtschaftlichen Bereichen von der problemorientierten Anwendung gut erforschter digitaler Technologien profitieren können.

II. Blockchain-Technologie – Funktionsweise, Anwendungen, Potenziale

1. Was ist eine „Blockchain“?

Möglichkeit zur Stellungnahme bezüglich der Funktionsweise der Blockchain-Technologie.

- Ob ein Einsatz von Blockchain-Technologie tatsächlich zu „erheblichen Effizienzgewinnen“ führen kann, ist sehr stark anwendungsabhängig. Nach rein technischen Maßstäben haben Blockchain-basierte-Systeme eine niedrigere Effizienz als z.B. klassische verteilte Datenbanken.

- Aus technischer Sicht ist eine vollständige Dezentralisierung, selbst mit Blockchain, z.Z. nur in sehr wenigen Anwendungsfeldern sicher möglich.

- Datenredundanz wird selbstverständlich auch bei modernen Datenbank und Cloud-Lösungen gewährleistet, z.B. durch Verteilung von Daten auf mehrere Server oder Rechenzentren. Eine redundante Speicherung auf Computern mehrerer Stakeholder implementieren z.B. auch klassische Peer-to-Peer-Netze und Open-Source-Projekte wie Tahoe-LAFS. Redundanz als Alleinstellungsmerkmal von Blockchain zu betrachten ist absolut falsch.

- Sowohl Süßigkeitenautomaten als auch die quasi-vollautomatisierten Bestellsysteme großer Online-Händler erfüllen dieselben Funktionen wie die hier beschriebenen „Smart Contracts“ (automatisierter Vertragsabschluss und Vertragsdurchsetzung). Ob ausreichende Vorteile dadurch entstehen, dass Smart-Contract-Logik redundant auf allen Rechnern eines Blockchain-Netzes ausgeführt und geprüft wird, muss im Einzelfall geprüft werden.

- Proof-of-Stake ist keine fertige Lösung, die direkt mit Proof-of-Work vergleichbar ist. Obwohl das ressourcenintensive Mining dabei entfällt, bringt sie inhärente sicherheitstechnische und ökonomische Probleme mit sich (anfällig für Long-Range/Costless-Simulation-Angriffe, Gefahr von unüberwindbaren Oligopolen). Es ist u.a. deswegen unwahrscheinlich, dass etablierte Netze wie Bitcoin auf Proof-of-Stake umschwenken werden.

2. Anwendungsfelder

Möglichkeit zur Stellungnahme bezüglich der Anwendungsfelder.

Bei Existenz einer vertrauenswürdigen Stelle sollte bei einer langsamen, ineffizienten oder teuren zentralisierten Lösung zunächst geprüft werden, ob mit dem aktuellen Stand der Technik nicht die Implementierung einer verbesserten zentralisierten Lösung möglich ist. Blockchain-Technologie kann unter gewissen Umständen Vertrauensdefizite überbrücken, schneidet bei den anderen genannten Faktoren jedoch oft schlechter ab als Alternativlösungen.

Fehlen aus Ihrer Sicht Anwendungsfelder? Bitte benennen und begründen Sie dieses:

a) Finanzsektor

ICOs

Gibt es – außerhalb der Spekulation – nachhaltige Anwendungsmöglichkeiten für Kryptowährungen?

- Kryptowährungen sind nach aktuellem Stand der Technik notwendig für den Betrieb sicherer permissionless Blockchains. Sie dienen dort als Kompensationsmittel für Sicherung und Konsensbildung, sowie, da sie das Erheben von Gebühren ermöglichen, als Mittel gegen Spam.
- Schon heute werden Kryptowährungen wie Bitcoin zur Einsparung von Transaktionskosten bei internationalen Überweisungen genutzt.
- Fraglich ist, ob heutige Kryptowährungen hinreichend nutzerfreundlich sind, um auch außerhalb technikaffiner Bevölkerungsgruppen sicher nutzbar zu sein.
- Kryptowährungen mit dezentraler Emission (Bitcoin, Ethereum, u.a.):
  - Grundstein der Spekulation ist hier Folge von Erwartungen steigender Nachfrage durch großflächige Nutzung der Kryptowährung als Geld-Substitut.
  - Kryptowährungen mit dezentraler Ausschüttung sind derzeit noch nicht als „Geld“ oder „Währungen“ anzusehen, da sie grundlegende Geldfunktionen nicht erfüllen (speziell den Nutzen als Wertaufbewahrungsmittel und Rechnungseinheit).
  - Die Geldfunktion, ein Tauschmedium mit geringen Transaktionskosten zu sein, erfüllen Kryptowährungen allerdings heute schon zu einem gewissen Grad.
  - In Bezug auf Transaktionskosten, Nutzerfreundlichkeit, Wertstabilität und Transaktionsdauer ist es unwahrscheinlich, dass Kryptowährungen öffentlicher Blockchains mit zentralisierten Bezahldiensten (z.B. Paypal, Transferwise, Swift) konkurrieren können.
  - Die Existenz einer nur schwer kontrollierbaren und weitreichend anonym nutzbaren Währung kann im Kontext der Verhinderung und Verfolgung von Straftaten und der Terrorismusbekämpfung als problematisch angesehen werden.
  - Andererseits hätte eine solche Alternativwährung die Vorteile (1) bei Inflation der heimischen Währung als Ersatzwährung dienen zu können (ähnlich dem Dollar oder Euro), (2) durch potentielle Konkurrenz zum etablierten Finanzsystem die Anreize für nachhaltige staatliche Geldpolitik zu verstärken, (3) die Unterdrückung zivilen Ungehorsams durch Abschneidung von Finanzsystemen zu erschweren.
- Kryptowährungen und Tokens mit zentralisierter Emission und Steuerung (Ripple XRP, Tether, u.a.):
  - Zentralisierte Emission und Steuerung vereinfacht die Lösung ökonomischer Probleme und die Durchsetzung von staatlicher Regulierung.
  - Der Unterschied zu zentralisierten Bezahlsystemen beschränkt sich hier darauf, dass man für die Durchführung von Transaktionen nicht auf eine zentralisiert betriebene Plattform (wie bspw. Paypal) angewiesen ist.

Ist die Token-Emission eine zukunftsfähige Form der Unternehmens- und Projektfinanzierung bzw. unter welchen Rahmenbedingungen könnte sie sich dazu entwickeln?

- ICOs konkurrieren derzeit mit Beteiligungsfinanzierung, Venture Capital und Crowdfunding um die Eigenkapitalfinanzierung von jungen Unternehmen.

  - Vorteile von ICOs ergeben sich durch die hohe Liquidität von abgebildeten Anteilen durch ihr Potential für die Bildung informativer Marktbewertungen für insbesondere junge Unternehmen.
  - Nachteilig ist die stärkere Trennung zwischen Anleger und Management in Bezug auf Aufsicht und Kontrolle (und damit einhergehende Principal-Agent-Konflikte).

- Tokenisiertes Eigenkapital wurde bisher vor allem als Anschubfinanzierung für Startups gesehen, bietet Aktien gegenüber allerdings nur wenig grundsätzliche Neuerung.
  - Aktienemission ist für Startups ungünstig, da sich die Beratungskosten für die Erfüllung gesetzlicher Mindestvorschriften nur für hohe Ausgabevolumen rechnen
  - ICOs ignorierten bisher potentiell geltende Kapitalmarktregelungen und sparten diese Kosten ein.
  - Ein weiterer Grund, der gegen Dispersion kleiner Eigenkapitalanteile von Startups an Kleinanleger spricht ist, dass Eigenkapitalgeber zu wenig Mitwirkungsmöglichkeiten bei den ersten Schritten des Unternehmens haben um das hohe Risiko zu rechtfertigen.
  - Venture Capital Funds und Angel-Investoren bieten nicht nur Kapital, sondern auch Beratung, Kontrolle, Zugang zu ihrem Netzwerk sowie Reputation für spätere Fremdkapitalaufnahme.
- Als mögliche Neuerung kann die Ausgabe von Utility Tokens gesehen werden.
  - Utility Tokens sind ähnlich zu Rechten aus Vorverkäufen der Produkte eines Startups beim Crowdfunding, könnten jedoch liquide gehandelt werden.
  - Da Utility Tokens nur bei dem Emittenten gegen Produkte eingelöst werden kann, wird schon bei Emission eine bestimmte Kundenbindung erreicht.
  - Allerdings können Utility Tokens zur Anschubfinanzierung eingesetzt werden, ohne sich fremder Kontrolle unterwerfen zu müssen, was erneut zu einem Principal-Agent-Konflikt führt.
- Eine grundsätzliche Fragestellung ist, inwieweit der großflächige Einsatz von Utility Tokens wirklich praktikabel ist. Die Nutzung von Geld als effizientes Tauschmittel zwischen Gütern entsteht auch durch dessen Fungibilität. Warum halten Konsumenten nicht schon heute einen Teil Ihres Vermögens in Wertmarken?

Welcher Mehrwert und welche Hindernisse bestehen bei der Tokenisierung klassischer Wertpapiere?

Teilen Sie die Einschätzung, dass sich ICOs mit Utility-Token und Kryptowährungen primär zur Finanzierung dezentralisierter Blockchainprojekte eignen? Welche weiteren sinnvollen Finanzierungsbereiche sehen Sie?

Welche Tokenarten werden den Markt der ICOs in den nächsten 5 Jahren dominieren?

Welche Missbrauchsrisiken bestehen? Welche Risiken bestehen für Kleinanleger?

- Risiken für Kleinanleger:
  - Es bestehen Parallelen zu der Motivation hinter dem deutschen Kleinanlegerschutzgesetz.

  - Zusätzlich ist die Einschätzung von Blockchain-Projekten oft gleichermaßen technisch, juristisch und ökonomisch anspruchsvoll - Kleinanleger dürften oftmals nicht über die nötigen Fachkenntnisse zur Bewertung der Projekte verfügen.
  - Die Streuung von Eigenkapitalanteilen auf viele Kleinanleger verstärkt Principal-Agent-Konflikte.
  - Technische Fehler in der Programmierung können, je nach Ausgestaltung, zu unwiderruflichen Schäden führen (siehe z.B. den „DAO-Hack“).

- Missbrauchsrisiken:
  - Es besteht die Gefahr, dass öffentliche, dezentrale Kryptowährungen gesellschaftlich unerwünschte Transaktionen vereinfachen (z.B. Geldwäsche, Steuerhinterziehung, Terrorfinanzierung, Umgehung von Sanktionen).

Sollte die Emission von Utility-Token und Kryptowährungen reguliert werden? Sollte diese Regulierung auf europäischer oder auf nationaler Ebene erfolgen?

Da Risiken für Kleinanleger bestehen, erscheint eine Regulierung sinnvoll.

Welche inhaltlichen Aspekte (zum Beispiel Anlegerschutz, Marktintegrität (insbes. bzgl. Insiderhandel und Kurs-manipulation), Handelstransparenz, Erlaubnispflichten für bestimmte Dienstleistungen) sollte eine etwaige Regulierung von Kryptowährungen und Token adressieren?

Es sollten dieselben Grundsätze zur Geltung kommen, die auch bei der Regulierung konventioneller Finanzgeschäfte und -produkte angewandt werden.

Wie werden Potenziale von Kryptowährungen, die an Realwährungen gekoppelt sind, also sogenannte stable coins, bewertet?

- Wie in vorherigen Antworten beschrieben, sind Wertschwankungen ein Hauptgrund für fehlende Nutzbarkeit von Kryptowährungen als Alternativwährung.
- Allerdings ist die sichere Durchsetzung von tatsächlicher Wertstabilität ein bisher ungelöstes Problem:
  - Kryptowährungen und Tokens mit zentralisierter Emission und Steuerung (Ripple XRP, Tether, u.a.):
    - Wechselkursrisiken zu Währungen wie dem Dollar können hier recht simpel gelöst werden (durch Pfandbesicherung in der jeweiligen Währung).
    - Allerdings besteht hier ein hohes Gegenparteirisiko: Die Emittenten derartiger Tokens arbeiten oft ohne Banklizenz und sind oft intransparent in Bezug auf die verwalteten Vermögenswerte.
    - Zusätzlich ist fraglich, inwieweit alternative Zahlungsdienstleister wie Paypal oder Transferwise nicht bereits einen vergleichbaren Dienst anbieten, allerdings bei geringerer Unsicherheit.
- Kryptowährungen ohne zentrale Steuerung (Bitcoin, Ethereum, u.a.):
  - Wie in vorherigen Antworten beschrieben, kann eine stabile dezentrale Kryptowährungen neuartige gesellschaftliche Vorteile bieten.

- In Frage kommende Stabilisierungsmechanismen sind jedoch unzureichend erforscht.
- Erste empirische Erfahrungen mit dezentralen Stablecoins sind negativ (Bitshares-BitUSD, Nubits).
- Eine endgültige Einschätzung des Potentials ist aufgrund der hohen aktuellen Dynamik der Entwicklungen in diesem Feld z.Z. nicht möglich. Vielversprechende Ansätze könnten sich ergeben, sind aber bei weitem noch nicht gut genug durchdrungen, um einen praktischen Einsatz zeitnah denkbar erscheinen zu lassen; das Gebiet befindet sich im Statium der Grundlagenforschung.

Finanzwirtschaft

In welchen Anwendungsbereichen im Finanzsektor sind Blockchain-Anwendungen bereits im produktiven Einsatz bzw. wo werden sie in absehbarer Zeit zum Einsatz kommen?

Zu welchen Erkenntnissen hat die Erprobung geführt mit Blick auf den zukünftigen Einsatz der Blockchain als Alternative zu bestehenden Systemen?

Wie ist die deutsche Finanzwirtschaft im Vergleich zur Finanzwirtschaft in Europa, USA und Asien im Bereich Blockchain-Technologie positioniert?

b) Energie

Stromhandel

Welche besonders relevanten/geeigneten Anwendungsfälle werden im Energiebereich gesehen?

Handel mit Emissionszertifikaten / CO2-Bilanzierung

Welche Erfahrungen konnten mit Blockchain-basierten Anwendungen im Handel von Strom und Gas gewonnen werden?

Welche regulatorischen Anpassungen sind notwendig, um solche Pilotprojekte in die Praxis umzusetzen? Stehen diese in einem vertretbaren Verhältnis zu dem erwarteten Nutzen wie evtl. höherer Systemstabilität und -effizienz?

Welche Regulierungsanforderungen bestehen an die Ausgestaltung der Blockchain-Technologie für einen Einsatz im Strommarkt?

Mit welchen Maßnahmen könnte und sollte der Energiesektor auf die Dezentralisierung von Wirtschaftsbeziehungen ausgerichtet werden?

Können energiewirtschaftliche Regulierungspflichten wie die Bilanzkreisverantwortung implementiert werden?

Ist der Anbieterwechsel ein geeigneter Anwendungsfall für Blockchain? Gibt es Hindernisse? Gibt es weitere Anwendungsfälle?

Welche Schätzungen gibt es zur Energie- und Klimabilanz des Einsatzes von Blockchain-Technologie im Energiesektor (auch im Vergleich mit alternativen Maßnahmen)?

- Ein zwangsläufig höherer Energiebedarf entsteht bei Einsatz von Blockchain-Technologie dadurch, dass bei zunehmendem Grad der Verteilung ein erhöhter Datenaustausch zwischen Teilnehmern nötig wird (u.a. für die Konsensfindung, die bei einer autoritativen zentralen Stelle hinfällig ist).

- Im Energiesektor ist der Einsatz von energieeffizienten Konsensmechanismen denkbar. Somit wäre die Energiebilanz zwar immer noch höher einzuschätzen als bei einem gut umgesetzten (technisch) zentralisiertem System, allerdings ist dies in einem weit geringeren Umfang der Fall als bei dem Einsatz von Proof-Of-Work (dem Konsensalgorithmus von Bitcoin).
- Nachhaltig sichere energieeffiziente Konsensmechanismen basieren z.B. auf klassischen Verfahren der Konsensbildung wie PBFT (Castro und Liskov, 1999) und werden oft in „permissioned" Blockchain-Systemen eingesetzt.
- Es ist an einem konkreten Szenario zu prüfen, ob ein permissioned Einsatz möglich ist. Dies ist insbesondere dann der Fall, wenn ein Kreis von vertrauenswürdigen Stakeholdern eingegrenzt werden kann (bspw. eine Mischung aus behördlichen und wirtschaftsnahen Organisationen).
- Ist eine Einigung auf einen Kreis von allgemein als vertrauenswürdig eingestuften Stakeholdern schwierig, kommen eventuell technisch fundierte föderierte Ansätze in Frage. Siehe z.B. (Mazières, 2015), bzw. das „Stellar"-Projekt.

Castro, Miguel, und Barbara Liskov. „Practical Byzantine fault tolerance." USENIX OSDI 1999.

Mazières, David. „The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus." Stellar Development Foundation (2015).

Stromnetze

Möglichkeit zur Stellungnahme bezüglich des Themengebietes Stromnetze.

- Es ist unklar, welchen entscheidenden Vorteil der Einsatz von Blockchain-Technologie im Kontext von Stromnetzen bieten kann.
- Die beschriebenen Anforderungen können auch durch einen deutlich weniger komplexen Systemaufbau mit zentraler Koordination erfüllt werden.

Ergeben sich Risiken für kritische Netzinfrastrukturen durch dezentralen Stromhandel?

Welche Auswirkungen werden durch den Einsatz von Blockchain auf die Bepreisung von Strom sowie die Finanzierung und die Regulierung der Netze gesehen?

Welche Auswirkungen werden durch den Einsatz von Blockchain auf die Versorgungssicherheit und die Integration von erneuerbaren Energien gesehen?

Welcher zusätzliche nationale Stromverbrauch ergäbe sich durch eine ausgeweitete Nutzung der Blockchain-Technologie? Wären Netzkapazitäten hierfür ausreichend ausgelegt?

Können dezentrale Kleinspeicher mittels Blockchain zu einem virtuellen Großspeicher zusammengeschaltet werden?

- Dies ist sehr wahrscheinlich möglich.
- Ist es mittels Blockchain möglich, ist es sehr wahrscheinlich auch mit einem klassischeren Systemaufbau möglich, bei deutlich geringerer Komplexität und höherer Effizienz.

Kann eine lokale just-in-time Vermarktung von Strom zur Stabilität des Stromnetzes beitragen?

c) Gesundheit/Pflege

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Gesundheit/Pflege.

- Es ist unklar, welchen entscheidenden Vorteil der Einsatz von Blockchain-Technologie im Kontext von Gesundheit/Pflege bieten kann.
- Es ist schwierig, aktuelle Datenschutz-Standards mit den Prinzipien von Blockchain-Technologie in Einklang zu bringen. Die Eignung von Blockchain-Technologie für die Verarbeitung und Speicherung sensibler personenbezogener Daten sollte daher besonders hinterfragt werden.
- Es existieren zahlreiche Technologien neben „Blockchain“, die sich u.U. besser für Innovationen in Gesundheit und Pflege eignen. Dazu gehören sowohl etablierte Praktiken - wie das Bereitstellen von Schnittstellen für den sicheren Datenaustausch oder das Ausstellen digital signierter Dokumente - als auch neuere Technologien mit speziellem Fokus auf den Schutz personenbezogener Daten. Techniken wie „Secure Multi-Party-Computation“ ermöglichen es einer Gruppe von Stakeholdern beispielsweise, Berechnungen über die Sammlung all ihrer Datenbestände durchzuführen, wobei keiner der Stakeholder seine Datenbestände offenlegen muss (personenbezogene Daten also nicht weitergegeben werden).

Welche Anwendungsfälle gibt es im Bereich Gesundheit/Pflege?

- Eine Verwendung für das Erstellen von Zeitstempeln für Dokumente erscheint praktikabel. Diese Funktionalität kann allerdings auch ohne die Verwendung von Blockchain-Technologie realisiert werden - digitale Zeitstempel werden schon seit langem von vertrauenswürdigen Drittparteien angeboten (bspw. auch von der Deutschen Telekom/T-Systems und der Bundesdruckerei/D-Trust).
- Viele vorstellbare Anwendungsmöglichkeiten scheitern in der Praxis an den hohen Datenschutz-Anforderungen bei der Verarbeitung von Gesundheitsdaten. Dieser Datenschutzstandard sollte keinesfalls reduziert werden, nur um Systeme auf einer bestimmten technologischen Basis (Blockchains) aufbauen zu können, wenn auch andere Grundlagentechnologien mindestens ebenso gut geeignet erscheinen.

Zeigt die Blockchain-Technologie für diese Anwendungsfälle einen Mehrwert gegenüber herkömmlichen Technologien?

Für das Erstellen von Zeitstempeln existiert ein Mehrwert nur insoweit, falls es nicht praktikabel ist, eine oder mehrere vertrauenswürdige Stellen zu benennen und mit der Erfüllung dieser Aufgabe zu beauftragen. Im Gesundheitsbereich existieren ohnehin vielfältige zentrale Akteure, denen ein Mindestmaß an Vertrauen entgegengebracht werden muss, sodass die Voraussetzungen, die einen Einsatz von Blockchains sinnvoll erscheinen lassen könnten, nicht gegeben sind.

Welche rechtlichen und organisatorischen Herausforderungen gibt es beim Einsatz in diesen Bereichen?

Wie könnten datenschutzrechtskonforme Lösungen zur Anwendung von Blockchain aussehen, vor dem Hintergrund der besonderen Anforderungen im Umgang mit Gesundheitsdaten?

- Blockchain-Technologie ist eine Offenlegung und Verteilung von Daten immanent. Datenschutzrechtkonforme Anwendungen von Blockchain-Technologie sind somit solche, bei denen keine personenbezogenen Daten verarbeitet und auf der Blockchain gespeichert werden.

- Bei dem Erstellen von Zeitstempeln wird bspw. nur ein kryptographischer Hash verarbeitet - je nach konkreter technischer Ausgestaltung können somit datenschutzrechtliche Bedenken umschifft werden.

- Zusatztechnologien wie Verschlüsselung oder Zero-Knowledge-Proofs, die zu einer erhöhten Vertraulichkeit von auf der Blockchain gespeicherten Daten führen können, führen i.d.R. zu starken Einbußen bei der Dienstgüte, einer stark erhöhten Systemkomplexität und zu einem nicht zu vernachlässigendem Restrisiko durch potentiell fehlerhafte praktische Umsetzung.

- Da auf der Blockchain abgelegte Daten allen Systemteilnehmer zugänglich sind und von diesen dauerhaft gespeichert werden können bzw. sogar sollen, ist im Falle der zukünftigen Entdeckung von Schwachstellen in kryptographischen Verfahren auch dann ein Restrisiko nicht ausgeschlossen, wenn die Blockchain ausschließlich Hashwerte oder verschlüsselte Daten enthält. Ein nachträgliches Entfernen oder „Zurückrufen“ von Daten, deren Verschlüsselung sich später als unzureichend herausstellt, ist inhärent unmöglich.

Gibt es ethische Bedenken, die sich aus einer Ansammlung von Gesundheitsdaten in einer Blockchain ergeben?

Ethische Bedenken ergeben sich insbesondere dann, wenn sensible Gesundheitsdaten einem Risiko der Kompromittierung ausgesetzt werden, ohne dass dabei ein nennenswerter und konkreter Mehrwert für die Allgemeinheit zu erwarten ist (bspw. im Vergleich zur Verwendung alternativer und deutlich einfacherer technologischer Mittel).

d) Mobilität

Welche Anwendungsfälle im Bereich der Mobilität zeichnen sich ab (zum Beispiel im Bereich des automatisierten und vernetzten Fahrens, der Erhebung von Straßenbenutzungsgebühren, der intermodalen Transporte (Personen und Güter))?

- Es ist unklar, welchen entscheidenden Vorteil der Einsatz von Blockchain-Technologie im Kontext von Mobilität bieten kann.

- Denkbar ist der Einsatz von Blockchain-Technologie für die Verwaltung von Eigentums- bzw. Nutzungsrechten, bspw. an (autonomen) Fahrzeugen. Allerdings ist am konkreten Anwendungsfall und den dadurch implizierten Vertrauensbeziehungen zu prüfen, ob ein Einsatz von Blockchain-Technologie wirklich notwendig ist, bzw. einen tatsächlichen Mehrwert bringt.

- Blockchain-Technologie kann auch als Grundlage für Kryptowährungen für den Mobilitäts-Sektor relevant werden.

Wird gesetzlicher Handlungsbedarf im Bereich der Mobilität gesehen, um Blockchain-basierte Mobilitäts-lösungen massenmarktfähig einzusetzen?

Nein.

Inwiefern sollten Blockchain-basierte Mobilitätslösungen auf staatlichen Infrastrukturen aufsetzen? Welche Rolle könnte der geplanten europäischen Blockchain-Services-Infrastruktur dabei zukommen?

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

- Blockchain-Technologie ist eine Offenlegung und Verteilung von Daten immanent. Datenschutzrechtkonforme Anwendungen von Blockchain-Technologie sind somit solche, bei denen keine personenbezogenen Daten verarbeitet und auf der Blockchain gespeichert werden.

- Es existieren zahlreiche technische Vorschläge, um die Eigenschaften von Blockchain-basierten Systemen in Bezug auf den Schutz der Privatheit zu verbessern. Da sie teils zu starken Einbußen bei der Dienstgüte führen, ist ihre Eignung im Einzelfall zu prüfen.

- Selbst bei einem hochwertigen Entwurf einer technischen Maßnahme zur Verbesserung der Privatheit bleibt ein nicht zu vernachlässigendes Restrisiko durch die potentiell fehlerhafte praktische Umsetzung. Dies ist insbesondere bei komplexen technischen Lösungen der Fall. Bei Blockchain-basierten Systemen kommt dabei erschwerend hinzu, dass auf einer Blockchain gespeicherte Daten für alle Teilnehmer einsehbar sind, womit unkenntlich gemachte Daten bei Bekanntwerden einer Schwachstelle durch jedermann angreifbar und potentiell dechiffrierbar werden.

Mess- und Sensordaten werden vermutlich ohne Eichung oder Kalibrierung der Messgeräte oder Sensoren genutzt. Ist dieser Aspekt zukünftig in der Mess- und Eichverordnung zu berücksichtigen?

e) Lieferketten/Logistik

Welche Anwendungsfälle bzw. auch Projekte im Regeleinsatz gibt es für die Logistik?

Welche Anreize und Hindernisse bestehen bei der Etablierung einer Blockchain im Lieferketten-Bereich sowohl national als auch international?

Gibt es – wenn ja, welche – insbesondere rechtliche und organisatorische Herausforderungen beim Einsatz in diesem Bereich?

Ist die Abwicklung von Liefer- und Bezahlvorgängen über öffentliche und offene Blockchains (public permissionless) denkbar oder ist eine Moderation und Supervision innerhalb der Blockchain (private permissioned) auf Basis der bisherigen Praxiserfahrungen erforderlich?

Welche Schnittstellen oder sonstigen technischen und rechtlichen Voraussetzungen werden benötigt, um anbieterübergreifende Bezahlvorgänge zu ermöglichen?

f) Internet der Dinge

Welche Technologien haben ähnliche Funktionalitäten wie die Blockchain, um im Bereich IoT eingesetzt zu werden?

- Zentralisierte / „Cloud“-basierte Lösungen, ggf. ebenfalls mit Einsatz von moderner Kryptografie und Hashketten.

- Klassische Peer-to-Peer-Systeme, beispielsweise aufbauend auf verteilten Hashtabellen (distributed hash tables).

Welche rechtlichen und technologischen Hindernisse gibt es beim Einsatz von Blockchains im Bereich IoT?

- Rechtlich ist im Kontext von Smart-Contracts im IoT u.a. auf die Dash-Button Entscheidung des OLG München vom 10.01.2019 (Az.: 29 U 1091/18) zu verweisen.

    – Bei sogenannten Dash-Buttons von Amazon handelt es sich um aufklebbare Knöpfe, welche lediglich das Logo eines bestimmten Herstellers tragen, die vernetzt sind, und über welche per einfachem

Knopfdruck ein bestimmtes Produkt bestellt werden kann, wobei Amazon sich in den AGB offen hielt, Details hinsichtlich der Ware und dem Preis zu ändern.

  - Die Entscheidung betont, dass auch bei dem Einsatz neuer Technologien und Geschäftsmodelle die gesetzlichen Regeln zum Verbraucherschutz Beachtung finden müssen.
  - In dem konkreten Fall bemängelte das OLG, dass der Kunde bei Auslösung der Bestellung die konkrete Ware und den Preis nicht sehe und nicht durch eine Aufschrift auf dem Knopf oder ähnlich darüber informiert wird, dass durch den Knopfdruck eine zahlungspflichtige Bestellung ausgelöst wird.
  - Dieselbe Problematik kann sich auch bei einer durch einen Smart Contract selbständig erbrachten Leistung ergeben.
  - Zudem ist hinsichtlich weiterer verbraucherschützender Regeln über Verträge im elektronischen Geschäftsverkehr (§§ 312i, 312j BGB) fragwürdig, ob und wie diese bei dem Einsatz der Blockchain-Technologie und von darauf basierenden Smart Contracts in der oben geschilderten Form („selbständig entgeltliche Leistungen erbringen“) gewährleistet werden können.

- Technisch kann gegen einen Einsatz von Blockchain-Technologie sprechen:
  - Blockchain-basierten Systeme stellen hohe Anforderungen an Endgeräte in Bezug auf Leistung und Energieverbrauch. Insbesondere müssen zahlreiche aufwändige kryptografische Operationen durchgeführt werden und deutlich mehr Daten empfangen, versendet und verarbeitet werden als Systemen mit zentraler Koordination und Kontrolle.
  - Blockchains sind nicht für die Speicherung und Verarbeitung großer Datenmengen geeignet.
  - Blockchains sind nicht für hochfrequente Datenverarbeitung oder geringe Latenzen geeignet (was z.B. Industrieumfeld notwendig sein kann).

Welche Herausforderungen bestehen hinsichtlich der Interoperabilität?

Sind Blockchains auf die großen Datenmengen im IoT-Bereich skalierbar? Falls ja, welche Varianten sind hierfür besonders geeignet?

- Eine Blockchain, die von mehreren Systemen gepflegt und vorgehalten wird, eignet sich kaum für die Speicherung großer Datenmengen, bspw. von Sensormesswerten im IoT.
- Varianten von Blockchain, die angeblich für die Verarbeitung von großen Datenmengen ausgelegt sind, sind dies bei genauem Hinschauen entweder nicht wirklich (kaum vergleichbar zu Cloud-Lösungen nach dem aktuellen Stand der Technik, z.B.), oder können aufgrund ihres Vertrauensmodells und unzureichender Sicherheit kaum als „Blockchain“ bezeichnet werden.
- Im Kontext von IoT erscheint einzig eine Speicherung von Daten-Aggregaten und -Zeitstempeln praktikabel. Bei letzterem werden kryptografische Hashfunktionen auf Datenbestände angewandt, so dass statt eines großen Datenbestands nur ein einziger Hashwert gespeichert werden muss. Dieser Hashwert reicht aus, um nachträglich beweisen zu können, dass ein bestimmtes Datum zu dem Zeitpunkt der Speicherung auf der Blockchain bereits in genau dieser Form existierte (s.a. „Merkle-Baum“ und https://opentimestamps.org).

Wie kann sichergestellt werden, dass der Übertrag von nicht automatisch digitalisierten IoT-Daten auf die Blockchain und in Smart Contracts fehlerfrei erfolgt?

- Fehlerfreiheit kann nur unter bestimmten Annahmen garantiert werden.
- Nach aktuellem Stand der Technik ist es für nahezu alle Arten von Daten eine notwendige Annahme, dass eine vertrauenswürdige Partei (bzw. vertrauenswürdige Hardware) den Übertrag übernimmt.
- Bei Existenz so einer Partei ist allerdings zu prüfen, ob diese nicht auch weitere Funktionen im System übernehmen kann, womit die Notwendigkeit der zusätzlichen Komplexität durch Einsatz von Blockchain entfallen könnte. Es wäre zu untersuchen, ob der Einsatz von Blockchain Angriffe beziehungsweise Fehlerfälle ausschließen kann, die bei geeigneter Umsetzung mit weniger ressourcenintensiven Basistechnologien nicht ebenfalls ausgeschlossen werden könnten.

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

- Blockchain-Technologie ist eine Offenlegung und Verteilung von Daten immanent. Datenschutzrechtkonforme Anwendungen von Blockchain-Technologie sind somit solche, bei denen keine personenbezogenen Daten verarbeitet und auf der Blockchain gespeichert werden.
- Es existieren zahlreiche technische Vorschläge, um die Eigenschaften von Blockchain-basierten Systemen in Bezug auf den Schutz der Privatheit zu verbessern. Da sie teils zu starken Einbußen bei der Dienstgüte führen, ist ihre Eignung im Einzelfall zu prüfen.
- Selbst bei einem hochwertigen Entwurf einer technischen Maßnahme zur Verbesserung der Privatheit bleibt ein nicht zu vernachlässigendes Restrisiko durch die potentiell fehlerhafte praktische Umsetzung. Dies ist insbesondere bei komplexen technischen Lösungen der Fall. Bei Blockchain-basierten Systemen kommt dabei erschwerend hinzu, dass auf einer Blockchain gespeicherte Daten für alle Teilnehmer einsehbar sind, womit unkenntlich gemachte Daten bei Bekanntwerden einer Schwachstelle durch jedermann angreifbar und potentiell dechiffrierbar werden.

g) Identitäten-/Rechtemanagement

Digitale Identitäten

Welche Aufgaben kann bzw. sollte der Staat bei der Bereitstellung rechtssicherer digitaler Identitäten übernehmen?

- Dem Staat sollte in erster Linie die ursprüngliche Kreierung eines digitalen Identitäts-Abbilds obliegen. Er sollte somit als zentraler Vertrauensanker dienen.
- Der Staat sollte darüber hinaus die Möglichkeit haben, von ihm zertifizierte digitale Identitäten zu widerrufen, z.B. bei Diebstahl, und auf Antrag neu auszustellen.

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

- Blockchain-Technologie ist eine Offenlegung und Verteilung von Daten immanent. Datenschutzrechtkonforme Anwendungen von Blockchain-Technologie sind somit solche, bei denen keine personenbezogenen Daten verarbeitet und auf der Blockchain gespeichert werden.
- Es existieren zahlreiche technische Vorschläge, um die Eigenschaften von Blockchain-basierten Systemen in Bezug auf den Schutz der Privatheit zu verbessern. Da sie teils zu starken Einbußen bei der Dienstgüte führen, ist ihre Eignung im Einzelfall zu prüfen.
- Bei dem Anwendungsfeld der digitalen Identitäten gibt es mehrere grundsätzliche Vorschläge, bspw. basierend auf Zero-Knowledge-Proofs (Garman, 2014) oder Mixing (Florian et al., 2015). Allerdings ist auch hier eine Eignungsprüfung anhand konkreter Systemanforderungen notwendig.
- U.U. wird lediglich eine Zeitstempel-Funktionalität benötigt. Bei dem Erstellen von Zeitstempeln mithilfe eines Blockchain-Systems wird nur ein kryptographischer Hash verarbeitet - je nach konkreter technischer Ausgestaltung können somit datenschutzrechtliche Bedenken umschifft werden (s.a. https://opentimestamps.org).
- U.U. wird lediglich die Funktionalität benötigt, den Widerruf eines Identitäts-Zertifikats öffentlich bekannt zu machen. Auch hierbei reicht die Veröffentlichung eines kryptografischen Hashes aus (ob auf einer Blockchain oder über ein anderes Medium).
- Selbst bei einem hochwertigen Entwurf einer technischen Maßnahme zur Verbesserung der Privatheit bleibt ein nicht zu vernachlässigendes Restrisiko durch die potentiell fehlerhafte praktische Umsetzung. Dies ist insbesondere bei komplexen technischen Lösungen der Fall. Bei Blockchain-basierten Systemen kommt dabei erschwerend hinzu, dass auf einer Blockchain gespeicherte Daten für alle Teilnehmer einsehbar sind, womit unkenntlich gemachte Daten bei Bekanntwerden einer Schwachstelle durch jedermann angreifbar und potentiell dechiffrierbar werden.

Garman, Christina, Matthew Green, and Ian Miers. „Decentralized Anonymous Credentials.“ NDSS 2014.

Florian, Martin, Johannes Walter, and Ingmar Baumgart. „Sybil-Resistant Pseudonymization and Pseudonym Change without Trusted Third Parties.“ WPES@CCS 2015.

Welche Akzeptanzkriterien sind bei dezentralem Identitätsmanagement durch Bürgerinnen, Bürger und Unternehmen zu berücksichtigen?

Wie kann ein eindeutiger, rechtssicherer Identitätsnachweis erfolgen und Missbrauch verhindert werden?

Urheberrecht

Gibt es konkrete Blockchain-basierte Lösungen im Bereich Urheberrecht?

Sind diese Lösungen den herkömmlichen Lösungen überlegen?

welche Geschäftsmodelle stehen hinter den Lösungen?

Könnte die Blockchain-Technologie zu einer Neudefinition der Rolle der Urheberrechtsintermediäre führen?

h) Verwaltung

Welchen Mehrwert und welche Nachteile bietet eine verteilte Datenbank bei öffentlichen Registern?

- Ausschlaggebend ist, in welcher Form die Datenbank verteilt ist.
- Im Weiteren wird eine Realisierung der Datenbank als Blockchain angenommen, respektive als öffentlich einsehbare Datenbank mit „Blockchain-Kern“ für die Integritätssicherung.
- Potentielle Mehrwerte bei so einem Aufbau beinhalten: gesteigerte Transparenz (und somit Schutz vor Missbrauch), Schutz vor nachträglichen Manipulationen, Redundanz, Zensurresistenz
- Potentielle Nachteile beinhalten: höhere Komplexität (bspw. im Vergleich zu einem klassischen zentralisierten System), geringere Flexibilität (insbesondere in Bezug auf das Entfernen oder Verändern von Inhalten, beispielsweise wenn diese mit legitimem Grund nicht länger öffentlich einsehbar sein sollen)

Welchen Grad an Zentralisierung braucht eine von der öffentlichen Verwaltung eingesetzte Datenbank?

Für welche Anwendungen (Kommunikation mit den Bürgern, Dokumente/Ausweise, interne Behördenpro-zesse) bestehen die größten Potenziale?

Bei den genannten Anwendungen sind auch mit etablierten Technologien signifikante Verbesserungen möglich. Der Einsatz von Blockchain erscheint für deren Realisierung nicht zwingend, aufgrund der höheren Systemkomplexität möglicherweise sogar hinderlich.

Welche Restriktionen ergeben sich bei der Anwendung von Smart Contracts im Hinblick auf die automatisierte Entscheidung rechtsverbindlicher Verwaltungsakte?

- Zunächst ist bei der Entscheidung rechtsverbindlicher Verwaltungsakte an Art. 22 der DSGVO zu denken.
  - Bei einer Entscheidung über Verwaltungsakte durch Smart Contracts ist davon auszugehen, dass in der Regel auch personenbezogene Daten auf die Blockchain gelangen und verarbeitet werden.
  - Nach Art. 22 DSGVO hat jede Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
  - Hierzu formuliert Abs. 2 zwar Ausnahmen, doch z.B. hinsichtlich der Ausnahme der Einwilligung kann, wenn überhaupt, nur bei einer permissioned Blockchain eingewilligt werden, wenn es eine juristische (oder natürliche) Person gibt, die als Betreiber der Blockchain angesehen werden kann. Bei einer permissionless Blockchain ist unklar, wer „Verantwortlicher“ im Sinne der DSGVO ist.
- Zudem stellen sich weitere datenschutzrechtliche Fragen, wie bspw. zur Löschbarkeit personenbezogener Daten.
- Auch kann über Fälle, in denen ein Ermessensspielraum besteht, nicht automatisiert entschieden werden.

Schließt der Rechtsrahmen einen Einsatz in bestimmten Anwendungsbereichen derzeit aus?

Siehe obige Antwort.

Ergeben sich neue strategische Überlegungen bei der IT-Konsolidierung öffentlicher Netze?

Welche Governance-Aspekte sind bei internationalen Blockchain-Anwendungen mit öffentlicher Beteiligung zu beachten?

i) Plattformökonomie

Möglichkeit zur Stellungnahme bezüglich des Anwendungsfeldes Plattformökonomie.

- Dezentrale Lösungen führen in den meisten Anwendungskontexten der Plattformökonomie zu Effizienzeinbußen im Vergleich zu zentralisierten Lösungen, bei allerdings höherer technischer Komplexität.
- Es ist daher davon auszugehen, dass zentralisierte Lösungen weiterhin eine bessere Nutzererfahrung bereitstellen und somit ihre aktuelle Marktstellung weitgehend behalten werden.
- Allerdings könnten etablierte Plattformen durch die Konkurrenz mit potentiellen neuen dezentralen Plattformen dazu bewegt werden, ihre Gebührenordnung und ihre Geschäftspraktiken im Sinne von Konsumenten und Kleinunternehmern anzupassen.
- Dezentrale Plattformen können somit indirekt zu positiven Entwicklungen beitragen, auch wenn sie selbst nur kleinere Nutzerzahlen aufweisen.
- Es ist nicht ersichtlich, dass Blockchain-basierte Systeme einen entscheidenden Beitrag zur Datensouverenität bieten können. Angesichts der technischen Gegebenheiten von Blockchain-Systemen sind aktuelle Datenschutzstandards kaum oder nur bei hohem Komplexitätszuwachs realisierbar, während Anforderungen wie Datensparsamkeit, Anonymisierung und Daten-Portabilität sehr gut auch in einem zentralisierten Kontext umgesetzt werden können und werden. (Siehe auch Antworten zu „Identitäten-/Rechtemanagement“.)

Welche Anreizstrukturen bestehen, um eine Blockchain-basierte Plattformlösung aufzubauen? Kommt mit Blick auf die erforderliche Dezentralität und Datensouveränität letztlich nur eine öffentliche Blockchain in Frage oder sind auch private Blockchains denkbar?

Können diesbezügliche Blockchain-Lösungen kompatibel mit den rechtlichen Anforderungen zum Schutz personenbezogener Daten und zum Privatsphärenschutz ausgestaltet werden? Wenn ja, wie?

Welches Geschäfts- bzw. Betreibermodell sollte hinter einer Blockchain-basierten Plattformlösung stehen?

Welche Rolle spielt Blockchain für den Aufbau von digitalen Genossenschaften („platform cooperatives“)?

III. Zentrale Fragestellungen der Blockchain-Technologie

1. Technologische Herausforderungen

Freitextfeld zu technologischen Herausforderungen

- Als Mittelweg zwischen „permissionless“ und „permissioned“ ist hier außerdem der föderierte Ansatz zu nennen, besser bekannt als „Federated Byzantine Agreement“ (FBA). FBA bietet dezentral verwaltete Mitgestaltungsrechte bei geringem Ressourcenverbrauch und höherer Effizienz als permissionless Blockchains.
- Der Ansatz ist konzeptionell mit einem Web-Of-Trust vergleichbar: jeder Systemteilnehmer entscheidet lokal, welche weitere Teilnehmer er in welchem Umfang als „vertrauenswürdig“ einstuft.
- Aus diesen individuellen Entscheidungen bildet sich in dezentraler und organischer Art eine Struktur von Vertrauensbeziehungen heraus, innerhalb welcher mit vergleichbaren Konsensalgorithmen gearbeitet werden kann wie in „permissioned“ Systemen.
- Siehe hierzu insbesondere (Mazières, 2015) und das Projekt „Stellar“.

Mazières, David. „The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus.“ Stellar Development Foundation (2015).

a) Skalierbarkeit

Welche Lösungsansätze für das Skalierbarkeitsproblem von (öffentlichen) Blockchains sind erfolgversprechend?

- Skalierbarkeitsprobleme entstehen aufgrund der fundamentalen Eigenschaft von (öffentlichen) Blockchains: Jede Transaktion wird von allen Knoten verarbeitet und gespeichert. Die Verteilung und Speicherung sind dabei die hauptsächlichen limitierenden Faktoren.
- Die Speicherung wird innerhalb der Antworten zu „Ineffizienz durch Redundanz“ näher beleuchtet.
- Die Verteilung der Daten an jeden Knoten, und damit die Konsensfindung, kann aufgrund von physikalischen Beschränkungen nur begrenzt beschleunigt werden. Lösungsansätze weichen daher die fundamentale Eigenschaft, Transaktionen auf jedem Knoten zu speichern, auf.
  - Payment-/State Channel Networks, z.B., Lightning/Raiden, haben das Ziel den Großteil der Transaktionen off-chain durchzuführen und nur bestimmte, seltene Transaktionen in die Blockchain zu schreiben. Auch pegged sidechains, z.B., Liquid Bitcoin, verringern die Anzahl der Transaktionen in der ursprünglichen Blockchain – stellenweise auf Kosten der Dezentralität. Diese Ansätze sind erfolgversprechend, insbesondere da sie aktiv erforscht werden und wurden und teilweise produktiv verwendet werden.
  - Alternative Ansätze wie Sharding (z.B. geplant in Ethereum) brechen die Annahme auf, dass jeder Knoten die gleichen Daten speichert. Stattdessen sollen von unterschiedlichen Knoten unterschiedliche Teile der Blockchain gespeichert werden; Transaktionen müssen somit nur noch die für sie relevanten Knoten erreichen. Damit zielt diese Technik auch darauf ab, den notwendigen Speicherplatz zu reduzieren, da nicht mehr die gesamte Blockchain gespeichert werden muss. Sharding wird konzeptuell häufig in zentralisierten Datenbanksystemen verwendet. Die Sicherheitsannahmen in Blockchain-Systemen sind allerdings fundamental anders, daher lässt sich das Konzept nicht ohne weiteres übertragen. Der Einsatz von Sharding in Blockchain-Systemen öffnet neue Angriffsvektoren deren Mitigation zum Teil nur schwerlich, oder nur unter Verwendung von aufwändigen Verfahren, möglich ist. Wie erfolgversprechend und sicher Sharding in der Realität ist lässt sich momentan schwer abschätzen, dazu bleibt die weitere Entwicklung in diesem Bereich (z.B. die Implementierung in Ethereum 2.0) abzuwarten.

Inwiefern kann den Herausforderungen der Skalierbarkeit durch Interoperabilität von Blockchains begegnet werden?

Wie in der vorherigen Antwort ausgeführt, kann Interoperabilität im Sinne von Sidechains die Skalierbarkeit verbessern. Es ist allerdings zu beachten, dass die Sidechain, wenn sie auch eine permissionless Blockchain ist, ähnliche Skalierungsprobleme haben wird wie ihre ursprüngliche Haupt-Blockchain. Die Skalierungsproblematik kann daher nur gelöst werden, wenn die Sidechain fundamental andere Eigenschaften besitzt als die Haupt-Blockchain. In genau diese Richtung gehen Implementierungen wie Liquid Bitcoin: Statt einer weiteren Blockchain besteht diese Sidechain aus einem Konsortium an Knoten welches den Konsens herstellt – effektiv ein permissioned System. Auf Kosten der Dezentralität wird somit die Performanz des Systems erhöht, wobei die Benutzer selbst entscheiden können ob sie eine Transaktion lieber auf der Bitcoin-Blockchain oder der schnelleren, aber dafür weniger dezentralen Liquid Sidechain durchführen möchten.

Welche Hindernisse (technisch und verfahrensrechtlich) müssen zur Skalierung von bestehenden bzw. potenziellen Pilotprojekten überwunden werden?

b) Ineffizienz durch Redundanz

In welchem Maße konkurriert die Blockchain mit anderen Datenbanklösungen?

- Die Antwort hängt stark vom jeweiligen Anwendungsfall und der Art der Blockchain ab.
- Eine public & permissionless Blockchain sollte nicht als Konkurrenz zu Datenbanken verstanden werden, da sie nicht darauf ausgelegt ist, große Datenmengen zu speichern. Des Weiteren ist eine Speicherung von personenbezogenen Daten problematisch, da gespeicherte Daten öffentlich einsehbar und nicht ohne weiteres löschbar sind.
- Bei permissioned und private Blockchains ist die Bandbreite an möglichen Technologien zu groß, um eine pauschale Antwort über die Konkurrenz zu Datenbanksystemen zu geben.
- Stattdessen plädieren wir, wie oben ausgeführt, für eine technologieoffene Analyse von Problemen: Der Anwendungsfall sollte die zu verwendende Technologie bestimmen und nicht die Technologie als Selbstzweck gesehen werden.

In welchen Szenarien überwiegen die Vorteile der redundanten Datenspeicherung die Nachteile?

Redundanz ist eine technische Eigenschaft, die die Blockchain mit vielen anderen traditionellen Speicheransätzen gemein hat. Ein Blockchain-spezifischer Vorteil ist nicht ersichtlich.

Welche Lösungsansätze für das Redundanzproblem von Blockchains sind erfolgversprechend?

- Redundanz ist eines der Kernmerkmale von (öffentlichen) Blockchains und notwendige Voraussetzung für deren Sicherheit. Die Redundanz von Blockchains sollte daher nicht als „Problem“ gesehen werden, welches gelöst werden muss. Stattdessen sollte die Frage gestellt werden, ob eine Blockchain die passende Technologie für ein Szenario darstellt, wenn Redundanz als Problem gesehen wird. Des Weiteren muss zwischen öffentlichen und privaten/zugangsbeschränkten Blockchains unterschieden werden.
- Bei privaten/zugangsbeschränkten Blockchains ist eine redundante Speicherung, abhängig vom Anwendungsfall, u.U. nicht notwendig.
- Es existieren verschiedene Verfahren, um auch innerhalb von öffentlichen Blockchain-Netzen Speicherplatz zu sparen:
  - Simple Payment Verification (SPV). Bei Simple Payment Verification werden nur die Header der Blockchain anstatt der Blöcke gespeichert. Bei Bedarf werden Transaktionen und Blöcke von Nachbarknoten angefragt. SPV birgt daher Manipulations- und Betrugsrisiken und stellt einen Trade-Off zwischen Performanz/Speicherplatz und Sicherheit dar.
  - Pruning. Beim Pruning wird zunächst die vollständige Blockchain heruntergeladen, um den aktuellen Zustand des System zu Berechnen. Anschließend werden alle bis auf die aktuellsten (in Bitcoin 2 Tage) Blöcke gelöscht. Die Sicherheit wird dadurch nicht beeinträchtigt, Transaktionen können genauso verifiziert werden wie zuvor. Allerdings kann der Knoten nicht mehr in der Weiterleitung alter Blöcke partizipieren (notwendig für das Bootstrapping neuer Knoten).

- Siehe auch die Antworten zu „Skalierbarkeit“ (bspw. zu Sharding).

c) Technische Anforderungen

Welche Anforderungen bestehen, um die Integration von Blockchain-Lösungen in die Unternehmenstätigkeit, v.a. vor dem Hintergrund bestehender zentralisierter Systeme, zu ermöglichen?

Sollte es ein Zertifizierungsverfahren für Blockchain-Technologien im Hinblick auf die versprochenen Funktionalitäten geben?

d) Interoperabilität

Welche Lösungen bzw. Lösungsansätze gibt es, um die Interoperabilität von Blockchains herzustellen? Wie „marktfähig“ sind derartige Lösungsansätze?

Bringen bestimmte Mindeststandards einen „Mehrwert“ für alle Teilnehmer? Welche „Standards“ könnten das sein?

e) Irreversibilität

Reicht es zur Erfüllung von Löschansprüchen oder -pflichten aus, Daten, zum Beispiel illegale Inhalte, im übertragenen Sinne „zu schwärzen“ – sie also für die Nutzer und Teilnehmer unkenntlich zu machen? Wie könnte das technisch umgesetzt werden? Ist es möglich, Daten spurenlos physisch zu löschen? Wenn ja, wie? In welchen Fällen könnte dies erforderlich sein?

- Losgelöst von Blockchains ist ein „Schwärzen“ technisch möglich, z.B., in dem illegale Inhalte verschlüsselt werden und anschließend der Schlüssel gelöscht wird. Ob dies zur Erfüllung von Löschansprüchen und -pflichten ausreicht hängt von der Art der Daten ab: Persönliche Daten wären dabei anders zu behandeln als beispielsweise Kinderpornographie. Diese Betrachtungen gelten unabhängig von der jeweiligen Technologie.
- Ein spurenloses physisches Löschen ist, wieder unabhängig von der Technologie, möglich, z.B. indem die Daten wiederholt mit Zufallszahlen überschrieben werden; so wird sichergestellt, dass sie nicht wiederhergestellt werden können.
- In permissioned (public oder private) Blockchains ist ein Löschen einfacher möglich, da sich die (bekannten und identifizierbaren) Teilnehmer einfacher („off-chain“) darauf einigen können, die entsprechenden Daten zu löschen. In permissionless Blockchains ist solch eine Form der Koordination auch deswegen sehr schwer, da Teilnehmer meist nicht identifizierbar sind.
- Man kann unterscheiden zwischen lokaler Löschung und globaler Löschung:
  - Lokale Löschung bezieht sich nur auf einzelne Knoten, während globales Löschen bedeutet, dass kein Knoten im System mehr die Daten besitzt.
  - In public & permissionless Blockchains ist eine globale Löschung nicht möglich ohne die Vertrauensannahmen des Systems massiv zu verändern, so dass sich die Frage stellt, ob eine public & permissionless Blockchain dann unter diesen Annahmen überhaupt noch sinnvoll ist.
  - Eine lokale Löschung auf einzelnen Knoten hingegen ist möglich, indem die Daten vom lokalen Datenträger gelöscht werden und die entsprechende Transaktion lokal als „gelöscht“ gekennzeichnet wird. Siehe dazu aktuelle Arbeiten von Florian et al. (voraussichtliche Veröffentlichung in 2019).

- Das Löschen von Daten ist beispielsweise bei in der Blockchain kodierter strafbarer Inhalte wie beispielsweise Kinderpornographie erforderlich, siehe dazu auch: Beaucamp; Henningsen; Florian, Strafbarkeit durch Speicherung der Bitcoin-Blockchain? MMR 2018, 501.

f) IT-Sicherheit

Welche Anforderungen an die IT-Sicherheit eines Blockchain-Systems stellen technologiebedingt eine besondere Herausforderung dar?

- Updates, insbesondere nach der Entdeckung von Sicherheitslücken, stellen eine besondere Herausforderung dar. Während die Dezentralität sowie die strengen Konsensregeln auf der einen Seite maßgeblich zum Vertrauen in ein Blockchain-System beitragen, so erschweren sie auf der anderen Seite notwendige Aktualisierungen im Fall von Sicherheitslücken.

    1. Es gibt keinen Zwang für Netzwerkteilnehmer ein Sicherheitsupdate durchzuführen.

    2. Änderungen der Protokolle können zu Hard-Forks führen, also einem Zustand in dem sich die Blockchain in zwei Stränge aufteilt, die nicht wieder zusammengeführt werden können.

    3. Angekündigte Sicherheits-Updates machen die Sicherheitslücke zwangsläufig publik und somit alle Knoten verwundbar, die noch keine Updates eingespielt haben; insbesondere diejenigen, die aus Vertrauensgründen den veränderten Quelltext zunächst selbst prüfen möchten.

- Eine Illustration für die Update-Problematik stellt ein aktueller Vorfall bei der Kryptowährung Zcash dar: https://z.cash/blog/zcash-counterfeiting-vulnerability-successfully-remediated/

- Die Kombination aus Irreversibilität und menschlichem Versagen ist eine weitere Herausforderung. Beispielsweise können Bugs in smart contracts aufgrund der „Code is law“-Semantik zu schwerwiegenden Verlusten führen, siehe z.B. die DAO- und Parity-Hacks bei Ethereum.

Wo und wie könnten „klassische“ Sicherheitsansätze (wie zum Beispiel eine Public Key Infrastructure) die Blockchain-Technologie ergänzen?

- Die Ergänzung im Sinne von „Verbesserung“ einer permissionless Blockchain mit einer PKI erscheint wenig sinnvoll. Permissionless Blockchains liefern durch Proof-of-Work (o.ä.) eine approximative Lösung für das Identitätsproblem. Eine PKI hingegen verbindet öffentliche Schlüssel mit Identitäten, was eine effizientere Lösung des Identitätsproblem darstellt und den effizienteren „permissioned“-Betrieb ermöglicht.

- Umgekehrt könnte eine Blockchain eine PKI ergänzen. Eine Blockchain kann Zeitstempel (Timestamps) für Zertifikate liefern und für den Widerruf von Zertifikaten (Certificate Revocation) genutzt werden. Eine Blockchain-basierte Organisation einer PKI könnte auch deren Transparenz erhöhen.

Sollte es eine Sicherheitszertifizierung für Blockchain-Produkte geben?

Können potenzielle technische IKT-Probleme, ungezielte oder gar gezielte Angriffe bei Einsatz von Blockchain-Lösungen in besonderer Weise Auswirkungen auf zentrale Komponenten, Kommunikationswege oder Clientsysteme haben und die notwendige Verfügbarkeit und Reaktionszeit gefährden?

- Die Risiken hängen auch hier von der Art der Blockchain ab.

- Bei permissionless Blockchains wie Bitcoin und Ethereum haben sich mehrere Sicherheitsrelevante Stellen herauskristallisiert; allerdings muss hervorgehoben werden, dass die verwendete Kryptographie die Manipulationsmöglichkeiten eines Angreifers stark einschränkt.
  - Die Netzwerkschicht hat sich als besonders empfindlich gegenüber gezielten Angriffen erwiesen. Diese Angriffe können benutzt werden, um das Netzwerk zu partitionieren oder einzelne Teile vom Rest auszuschließen; anschließend kann dieser Zustand ausgenutzt werden, um beispielsweise sogenannte Double Spends auszuführen.
  - Aufgrund der Irreversibilität wiegen Phishing-Angriffe (z.B. auf private keys) deutlich schwerer als in anderen Szenarien, da bewusst kein Raum für menschliche Intervention vorgesehen ist.
  - Gegen starke Angreifer (z.B. Nationalstaaten) reicht bei vielen öffentlichen Blockchains der Proof-of-Work nicht aus, um das System gegen Double-Spends zu schützen. Siehe dazu https://www.crypto51.app/ für eine Zusammenstellung der notwendigen Kosten eines Double-Spends in diversen Kryptowährungen.
- Im Falle von permissioned Blockchains gelten ähnliche Schlussfolgerungen wie bei bekannten IT-Systemen.

Wie könnte sich der Einsatz von Blockchains bei der Bekämpfung von Cybersicherheitsrisiken, insbesondere in Bereichen der kritischen Versorgung, zukünftig auswirken?

- Die meisten Sicherheitsvorfälle geschehen nicht, weil die passende Technologie noch nicht da ist um diese zu verhindern, sondern, weil bestehende Erkenntnisse unzureichend bis gar nicht umgesetzt werden. Sichere Passwörter, 2-Faktor-Authentifizierung, regelmäßige Updates, E-Mail Zertifikate zur Verschlüsselung sowie zum Schutz gegen Phishing; solche Maßnahmen sind bereits mit bestehender Technologie umzusetzen.
- Ob der Einsatz von Blockchain vorteilhaft für die Sicherheit sein könnte, hängt von den betrachteten Szenarien ab. Im Allgemeinen könnte die Redundanz von Blockchain-Systemen tatsächlich die Ausfallsicherheit erhöhen; allerdings basieren permissionless Blockchains auf der Annahme einer ehrlichen Mehrheit von 50% der Knoten. Damit sind sie verwundbar durch starke Angreifer (z.B. Nationalstaaten). Nichtsdestotrotz können die einzelnen Komponenten aus denen eine Blockchain zusammengesetzt ist für eine erhöhte Ausfallsicherheit verwendet werden: Redundanz und verteilte Datenspeicherung ist bei kritischer Infrastruktur häufig eine wünschenswerte Eigenschaft, Hash-Chains können für Datenintegrität und -versionierung verwendet werden.

2. Ökonomische Fragestellungen

a) Ökonomisches Potenzial

Wie schätzen Sie das ökonomische Potenzial der Blockchain-Technologie in den nächsten fünf Jahren ein?

Wie schätzen Sie das ökonomische Potenzial von privaten Blockchains im Vergleich zu öffentlichen Block-chains ein?

Welches sind die zentralen ökonomischen Herausforderungen für private Blockchain-Anwendungen bzw. Anwendungen auf öffentlichen Blockchains?

b) KMU

Wie kann das Potenzial der Blockchain-Technologie nicht nur in der Start-up-Szene, sondern auch bei mittel-ständischen Unternehmen, insbesondere kleinen und mittleren Unternehmen, gehoben werden?

Welche Einsatzmöglichkeiten und Potenziale sehen Sie insbes. bei kleinen und mittleren Unternehmen?

3. Ökologische Fragestellungen

In welchen Anwendungsfeldern werden zentrale ökologische Chancen bzw. Risiken durch die Nutzung der Blockchain-Technologie gesehen (Use Cases)?

- Chancen könnten beim Handel mit Emissionszertifikaten entstehen. Im internationalen Rahmen, in dem eine CO2-Bilanzierung besonders relevant erscheint, ist das Etablieren von global als vertrauenswürdig eingestuften Vertrauensankern bekanntlich schwierig. Eine technische Grundlage, die ohne zentrale Vertrauensanker auskommt, könnte somit zu einer breiteren Akzeptanz führen ohne auf die Effizienzvorteile einer vollständig digitalen Lösung verzichten zu müssen.
- Risiken entstehen insbesondere durch die wirtschaftliche Attraktivität von Proof-of-Work-Mining. Je nach Akzeptanz- und Wertentwicklung von Kryptowährungen wie Bitcoin sind hier noch weitere Steigungen des Energieverbrauchs vorstellbar.

Welche Lösungsansätze für das Ressourcenproblem von (öffentlichen) Blockchains sind erfolgversprechend? Wann ist die Umsetzung solcher Lösungsansätze zu erwarten?

- Viele etablierte Kryptowährungen, insbesondere Bitcoin, werden aus technischen und ideologischen Gründen voraussichtlich nicht in absehbarer Zukunft auf eine ressourcenschonende Alternative zu Proof-of-Work umsteigen. Dies hängt u.a. auch damit zusammen, dass vieldiskutierte Alternativen wie Proof-of-Stake nicht dieselbe Sicherheit bieten wie Proof-of-Work und zudem deutlich komplexer umzusetzen sind.
- Als Alternativen zu Konsensmechanismen, die wie Proof-of-Work oder Proof-of-Stake auf ökonomischen Anreizen basieren, werden z.Z. föderierte Ansätze für den Einsatz in öffentlichen Blockchains erprobt. Föderierte Ansätze bieten dezentral verwaltete Mitgestaltungsrechte bei geringem Ressourcenverbrauch und bilden somit einen Mittelweg zwischen „permissionless“ und „permissioned“. Siehe z.B. (Mazières, 2015) und das Projekt „Stellar“.
- Abgesehen von der Etablierung attraktiver ressourcenschonender Konkurrenzsysteme, kann der Umweltbelastung durch Proof-of-Work nur durch einen entschiedenen, weltweiten Stoß in Richtung stärkerer Besteuerung entgegengetreten werden.

Mazières, David. „The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus.“ Stellar Development Foundation (2015).

Durch welche Regelungs-, Regulierungs- und Anreizsysteme könnte eine nachhaltige Nutzung der Blockchain-Technologie unterstützt werden? Welche europäischen oder internationalen Governance-Strukturen sind denkbar?

Wie hoch wird der Stromverbrauch für Blockchain-Anwendungen heute und im erwarteten Trend eingeschätzt? Und wie verhalten sich demgegenüber mögliche Einsparungen?

Welche Änderungen in der Konstruktion der Blockchain, zum Beispiel zugunsten der Transaktionsgeschwin-digkeit und des Energieverbrauchs, unterwandern wiederum die Kerneigenschaften der Technologie wie zum Beispiel Transparenz und Manipulationssicherheit?

Viel wichtiger als die Frage, welche Kerneigenschaften einer Technologie unterwandert werden könnten, ist die Frage, welche Anforderungen in einem gegebenen Anwendungskontext konkret existieren, und wie bzw. mit welcher Kombination von Technologien und deren Abwandlungen diese am besten erfüllt werden können.

Sollte es ein Zertifizierungsverfahren für Blockchain-Technologien im Hinblick auf Energie-/Ressourcenver-brauch geben?

4. Rechtliche Fragestellungen

Welchen Unterschied sehen Sie mit Blick auf die rechtlichen Herausforderungen zwischen öffentlichen und privaten Blockchains?

- Bei permissioned Blockchains gibt es in der Regel eine natürliche oder juristische Person, die die Blockchain betreibt. Eine solche natürliche oder juristische Person kann bei permissionless Blockchains nicht ausgemacht werden.
- Auf eine private Blockchain können in vielen Punkten die zu Online-Plattformen etablierten Normen und die Rechtsprechung hierzu übertragen werden. Der Betreiber der Blockchain kann in der Regel als äquivalent zu dem Betreiber einer Online-Plattform angesehen werden.
- z.B. das datenschutzrechtliche Problem, wer im Rahmen eines öffentlichen Blochchain-Systems „Verantwortlicher“ im Sinne der DSGVO ist, stellt sich bei privaten Blockchains nicht oder in anderer Weise. Hier kann wohl der Betreiber der privaten Blockchain als Verantwortlicher angesehen werden.
- Das Fehlen eines Betreibers bzw. eines Verantwortlichen ist Grund für einen großen Anteil der Regulierungsprobleme bei öffentlichen Blockchains.
- Die scheinbare „Unregulierbarkeit“ von öffentlichen Blockchain wir dabei von manchen Proponenten als deren zentraler Vorteil gesehen.

a) Anwendbares Recht

Welches Recht soll etwa in den Fällen anwendbar sein, in denen herkömmlich an den Standort eines nun in der Blockchain verbrieften Rechts oder den Sitz eines durch die Blockchain entbehrlich gewordenen Intermediärs angeknüpft wird?

- Hier muss differenziert werden, zwischen permissioned und permissionless Blockchains.
- Bei privaten Blockchains kann an den Gerichtsstand der juristischen bzw. der natürlichen Person, die die Blockchain betreibt, angeknüpft werden, bzw. kann auf eine Rechtswahlvereinbarung zurückgegriffen werden.
- Bei öffentlichen Blockchains ist die Frage komplexer und kaum pauschal zu beantworten.
- Hier ist nach dem jeweiligen konkreten rechtlichen Zusammenhang (Rechtsgebiet, vertragliches Schuldverhältnis, außervertragliches Schuldverhältnis) zu differenzieren.
- Auch die konkrete technische Ausgestaltung, z.B. des jeweiligen Smart Contract, kann hier zu Unterschieden in der Bewertung führen.

- Das Kollisionsrecht stellt ein hoch ausdifferenziertes Gebiet dar, dessen Differenziertheit sich auch bei Sachverhalten im Zusammenhang mit der Blockchain-Technologie widerspiegeln muss, daher ist die Formulierung einer allgemeinen Lösung schwierig.
- Sofern die Identität der Akteure bekannt ist, so kann z.B. an deren gewöhnlichen Aufenthalt oder an deren Staatsangehörigkeit angeknüpft werden.
- Bei deliktischen Handlungen kann entsprechend dem sogenannten „fliegenden Gerichtsstand“ gemäß § 32 ZPO an den Ort des Schadens angeknüpft werden, hieraus ergibt sich aus deutscher Perspektive eine internationale Zuständigkeit.

Können Transaktionen, die verschiedenen Rechtsordnungen unterliegen, in einer Blockchain abgebildet werden und welche Herausforderungen stellt dies an die Blockchain?

Wie können in Blockchains wesentliche Verbraucherschutzrechte und rechtsstaatliche Grundsätze (Rule of Law) sichergestellt werden?

- Bei keiner Blockchain handelt es sich um einen „rechtsfreien Raum“.
  - Problematisch ist, welche Rechtsordnung Anwendung findet.
  - Im Zweifelsfall kollidieren mehrerer Rechtsordnungen, die alle anwendbar sind; zu klären ist dann, welche Rechtsordnung in dem konkreten Fall anzuwenden ist.
  - Auch besteht die Gefahr des „forum shopping“, also die Wahl eines für eine Partei günstigen Gerichtsstandes.
- die Durchsetzung von Verbraucherschutzrechten und rechtsstaatlichen Grundsätzen ist problematisch, insbesondere aufgrund der Pseudonymität der Akteure auf der Blockchain.
- Eine Auflösung der Pseudonymität würde nicht nur die Frage der Durchsetzbarkeit des Rechts erheblich vereinfachen, sondern auch die der Klärung der anwendbaren Rechtsordnung, da dann zumindest ein personeller Bezug zu einer bestimmten Rechtsordnung hergestellt werden kann. Eine Verpflichtung zur Auflösung der Pseudonymität ist wiederum schwer durchsetzbar. Zudem besteht die Problematik der Wahrung datenschutzrechtlicher Grundsätze.

b) Rechtliche Verantwortlichkeit und Rechtsdurchsetzung

Besteht Bedarf für ein technisches und regulatives Regime, mit dem auf der Blockchain festgehaltene Transaktionen rückgängig gemacht werden können?

- Hier muss differenziert werden danach, ob unter „rückgängig machen“ eine Löschung oder lediglich eine Umkehrung von Transaktionen gemeint ist.
- Aus rechtlichen Gründen besteht die Notwendigkeit bestimmte Transaktionen „rückgängig“ zu machen; in vielen Situationen reicht eine zweite Transaktion, welche die erste Transaktion rückgängig macht, z.B. eine Rücküberweisung.
  - So können beispielsweise bestimmte Güter mit Bitcoin oder mit anderen Kryptowährungen bezahlt werden; tritt der Käufer vom Vertrag zurück, muss er auch den Kaufpreis zurückerhalten.

  - Diesen erhält er durch eine zweite Transaktion zurück, die faktisch die erste Transaktion „rückgängig“ macht.
  - Die rechtliche Verpflichtung hierfür besteht zum Beispiel nach Gewährleistungsrecht, die Durchsetzung ist aufgrund des fehlenden Verantwortlichen in öffentlichen Blockchains und der Pseudonymität der Teilnehmer teilweise schwierig.

- In anderen Situationen besteht allerdings auch die Notwendigkeit der Löschung einer Transaktion.
  - Das Löschen von Daten ist beispielsweise bei in der Blockchain kodierten strafbaren Inhalte wie beispielsweise Kinderpornographie erforderlich, siehe dazu auch Beaucamp; Henningsen; Florian, Strafbarkeit durch Speicherung der Bitcoin-Blockchain? MMR 2018, 501.
  - Hinsichtlich eines Löschungsverlangens und einer daraus folgenden Löschungsverpflichtung auf Grundlage von Art. 17 DSGVO, ist unklar, ob ein Full Node als Verantwortlicher im Sinne der DSGVO gelten kann. Sofern dies der Fall ist, so wäre auch hier die Möglichkeit einer Löschung rechtlich erforderlich.

Ggf.: Wie könnte ein solches technisches und regulatives Regime aussehen?

Zu technischen Möglichkeiten der Löschung von Transaktionen siehe die Antworten zu III 1. e) („Irreversibilität“).

c) Smart Contracts

Sollte es Regelungen für Smart Contracts in unserer Rechtsordnung geben bzw. wie kann man sicherstellen, dass sich Smart Contracts einer Rechtsordnung und wesentlichen rechtsstaatlichen Grundgedanken unterordnen?

- Auch hier kommt es wiederum auf die konkrete Ausgestaltung des Smart Contracts an.
- Die wenigsten Smart Contracts haben Ähnlichkeit mit Verträgen im rechtlichen Sinne, es handelt sich hierbei um schlichte Computerprogramme.
- Hinsichtlich der Durchsetzung bestehender gesetzlicher Vorgaben und rechtsstaatlicher Grundsätze stellen sich bei öffentlichen Blockchains stets dieselben Probleme der Anonymität, des fehlenden Verantwortlichen, der Durchsetzbarkeit, des anwendbaren Rechts (s.o.).
- Der aktuelle Zeitpunkt ist zu früh, um über konkrete Gesetzesänderungen nachzudenken, da die Technologie hinsichtlich Anwendungsfällen, die über den Handel mit Kryptowährungen hinausgehen, noch nicht sehr weit entwickelt ist.
- Zudem müssen die Fragen der Durchsetzbarkeit gesetzlicher Regeln gelöst werden, bevor neue Regeln geschaffen werden.

Wie kann eine transparente Vertragsgestaltung und -abwicklung (insbesondere für Verbraucher) gewährleistet werden?

- Hinsichtlich der Bedeutung der Transparenz des Abschlusses von Verträgen ist wiederum auf die Dash-Button Entscheidung des OLG München vom 10.01.2019 (Az.: 29 U 1091/18) zu verweisen.
- Hier wurde die fehlende Erkennbarkeit von Preis und Produkt sowie das Fehlen des Hinweises, dass durch einen Knopfdruck ein Produkt zahlungspflichtig bestellt wird, gerügt.

- Diese Problematik kann auf den automatisierten Vertragsabschluss und Vertragsdurchsetzung durch einen sogenannte Smart Contract in einigen Fällen übertragen werden.
- Entscheidend ist aber auch hier die konkrete Ausgestaltung des Smart Contract.
- Wie auch aus der oben genannten Entscheidung ersichtlich wird, regelt das BGB sehr genau, wie Verbraucher bei Verträgen im elektronischen Geschäftsverkehr zu schützen sind.
- Problematisch ist, wie diese Regelungen im Zusammenhang mit Smart Contracts umgesetzt werden können.
- Zudem fügt die Umsetzung eines Vertrages in Form eines Smart Contracts, also Code, der Rechtsbeziehung eine zusätzliche Abstraktionsstufe hinzu, in welcher die Abreden in Code „übersetzt“ werden.
- Eine automatisierte Kontrolle, ob der Code auch dem Text AGB (sofern das geltende Recht zum Verbraucherschutz nicht geändert wird, müssen diese dem Verbraucher zur Verfügung stehen) entspricht ist technisch nicht möglich.
- Es ist offen, inwieweit sich die Blockchain Technologie im Geschäftsverkehr etablieren wird. Sollte dies aber der Fall sein, dann wird wohl auch die Impressumspflicht nach §5 TMG (zumindest analog) Anwendung finden müssen. Zudem haben nach § 312d BGB i.V.m. Art. 264a EGBGB Verbraucher das Recht Identität und Geschäftsanschrift des Unternehmers zu erfahren. Dies würde auf Seiten der Unternehmer rechtlich das Problem der Anonymität lösen.
- Ein verbleibender Schwarzmarkt, der sich nicht an die rechtlichen Vorgaben hält, kann auf öffentlichen Blockchains regulatorisch kaum vermieden werden. Auch technisch ist dies wohl ohne die Grundfesten der Technologie aufzulösen (Dezentralität, Pseudonymität) nicht möglich.

Ggf.: Welche Fragen sollten gesetzlich geregelt werden? Gibt es bereits Orakel, die Gegebenheiten der realen Welt in der Blockchain abbilden können?

Wie ist die grenzüberschreitende Wirksamkeit von Smart Contracts zu bewerten (zum Beispiel bei internationalen Lieferketten)? Ist eine Vereinheitlichung internationalen Rechts erforderlich?

Sollte es ein Zertifizierungsverfahren für Smart Contracts im Hinblick auf die versprochenen Funktionalitäten und die Cybersicherheit geben?

- Ein Zertifizierungsverfahren kann als zusätzliche Sicherheit für Verbraucher durchaus sinnvoll sein.
- Hierbei ist dann im Zusammenhang mit den obigen Fragen und Antworten, insbesondere mit dem Punkt der Problematik der Durchsetzbarkeit der geltenden gesetzlichen Regeln anzumerken, dass die Verpflichtung zur Zertifizierung zunächst wiederum nur eine weitere rechtliche Vorschrift ist, die in public permissionless Systemen, wie beispielsweise Ethereum kaum flächendeckend durchgesetzt werden kann.
- Wenn sich nun Anbieter von Smart Contracts „freiwillig“ der Zertifizierung stellen, so ist zunächst der Wille des rechtskonformen Verhaltens anzunehmen.
- Zudem kann hiermit eine Registrierung verbunden werden und damit auch eine Möglichkeit der Vereinfachung der Durchsetzung der gesetzlichen Vorschriften.

d) Ersetzbarkeit von Intermediären

Gibt es bereits Konzepte, wie dezentrale Handelsplattformen beaufsichtigt werden können?

Welche Möglichkeiten gibt es, die Funktion von Intermediären anderweitig sicherzustellen?

In welchen Bereichen sollte auf einen Intermediär nicht verzichtet werden und warum?

Wie bereits im Text genannt, kann bei Verträgen für welche die notarielle Form vorgeschrieben ist, kaum auf den Notar als „Intermediär" verzichtet werden, da die notarielle Form dem Schutz und der Beratung der Vertragsparteien dient; siehe hierzu auch die Antworten zu Formvorschriften, insbesondere zur Funktion von Formvorschriften.

e) Datenschutz (insbesondere Anforderungen nach der DSGVO)

Wie kann der Einsatz der Blockchain-Technologie kompatibel mit datenschutzrechtlichen Anforderungen (informationelle Selbstbestimmung) gestaltet werden?

- Blockchain-Technologie ist eine Offenlegung und Verteilung von Daten immanent. Datenschutzrechtkonforme Anwendungen von Blockchain-Technologie sind somit solche, bei denen keine personenbezogenen Daten verarbeitet und auf der Blockchain gespeichert werden.

- Es existieren zahlreiche technische Vorschläge, um die Eigenschaften von Blockchain-basierten Systemen in Bezug auf den Schutz der Privatheit zu verbessern. Da sie teils zu starken Einbußen bei der Dienstgüte führen, ist ihre Eignung im Einzelfall zu prüfen.

- Für eine Umsetzung der gesetzlich vorgeschriebenen Löschungspflichten müssen Knotenbetreiber in der Lage sein, von ihnen gespeicherte Daten zu löschen. Dies ist bei den meisten Blockchain-basierten Systemen nicht vorgesehen. Mit einer Datenlöschung kann daher einhergehen, dass der Löschende sich nicht mehr in gleichem Umfang im System einbringen kann und bei globalen Löschanfragen u.U. das gesamte System zusammenbricht. Auch zu diesem Problem existieren jedoch technische Lösungsmöglichkeiten. Siehe dazu z.B. den technischen Teil von (Beaucamp; Henningsen; Florian, Strafbarkeit durch Speicherung der Bitcoin-Blockchain? MMR 2018, 501), sowie aktuelle Arbeiten von Florian et al. (voraussichtliche Veröffentlichung in 2019).

Durch welche Methoden können personenbezogene Daten hinreichend anonymisiert werden (Verschlüsselung, Verschleierung, Aggregieren etc.)?

- Dies hängt sehr stark von der konkreten Anwendung und dem konkreten Kontext ab. Siehe auch vorherige Antwort.

- U.U. wird lediglich eine Zeitstempel-Funktionalität benötigt. Bei dem Erstellen von Zeitstempeln mithilfe eines Blockchain-Systems wird nur ein kryptographischer Hash verarbeitet - je nach konkreter technischer Ausgestaltung können somit datenschutzrechtliche Bedenken umschifft werden (s.a. https://opentimestamps.org).

- U.U. wird lediglich die Funktionalität benötigt, den Widerruf eines Daten-Objekts (bspw. eines Zertifikats) öffentlich bekannt zu machen. Auch hierbei reicht die Veröffentlichung eines kryptografischen Hashes aus (ob auf einer Blockchain oder über ein anderes Medium).

- Oft werden neuartige kryptographische Technologien wie Zero-Knowledge-Proofs als Allheilmittel für die Anonymisierung auf Blockchains präsentiert. Allerdings sind diese durch ihre hohe Komplexität und ihre Ineffizienz nur selten praktikabel einsetzbar.

- Selbst bei einem hochwertigen Entwurf einer technischen Anonymisierungsmaßnahme bleibt ein nicht zu vernachlässigendes Restrisiko durch die potentiell fehlerhafte praktische Umsetzung. Dies ist insbesondere bei komplexen technischen Lösungen der Fall. Bei Blockchain-basierten Systemen kommt dabei erschwerend hinzu, dass auf einer Blockchain gespeicherte Daten für alle Teilnehmer einsehbar sind, womit unkenntlich gemachte Daten bei Bekanntwerden einer Schwachstelle durch jedermann deanonymisierbar werden.

Gibt es eventuell auf indirektem Wege Berührungspunkte mit der DSGVO, selbst wenn alle personenbezogenen Daten „off-chain" gespeichert werden?

- Die Hashwerte der Daten müssen zur Verifizierung stets auf der Blockhchain gespeichert werden (bzw. ein Hashwert für eine Gruppe von Daten, bei Verwendung eines Verwahrens wie den Aufbau eines Merkle-Baums).
- Die Frage, ob es sich bei Hashwerten um personenbezogene Daten handelt, ist umstritten.
- Dies hängt auch von der konkreten Ausgestaltung der Hash-Prozedur ab. Also von der Art der verwendeten Hash-Funktion und davon, ob die Eingangsdaten mit zumutbaren Aufwand „erraten" werden können (was die Anonymisierung durch Hashing auflösen würde).
- Allgemein lässt sich jedoch festhalten, dass bei Kenntnis der Eingangsdaten stets eine Verbindung zum Hashwert und damit den Eintrag auf der Blockchain hergestellt werden kann. U.U. ist somit weniger der Hash selbst als personenbezogenes Datum zu werten, als die Tatsache, dass er zu einer bestimmten Zeit auf die Blockchain geschrieben wurde.

f) Formvorschriften

Was steht der Anerkennung von digitalen Nachweisen als gleichwertig mit der Schriftform entgegen?

- Nach § 126 Abs. 3 BGB kann die schriftliche Form auch durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz etwas anderes ergibt.
- In diesen Fällen ist die Verwendung elektronischer Nachweise auf der Blockchain unter Einhaltung der Vorgaben des § 126a BGB denkbar.
- Hinsichtlich solcher Dokumente, für die das Gesetz die elektronische Form ausschließt, kann als Anhaltspunkt hinsichtlich der Frage der Ersetzbarkeit der Schriftform durch digitale Nachweise an die Zwecke des Schriftformerfordernisses angeknüpft werden:
  - Warnfunktion
  - Beratungs- und Belehrungsfunktion
  - Klarstellungs- und Beweisfunktion
  - Dokumentationsfunktion
  - Kontrollfunktion
- Auf der Grundlage des Schwerpunktes der Funktion der Schriftform Einzelfall ist jeweils abzuwägen.

- Bei Schriftstücken, deren Funktion primär in der Dokumentationsfunktion besteht, sollte zunächst nicht auf die Form einer schriftlichen Urkunde verzichtet werden. Die Blockchain-Technologie steckt noch im Anfangs- und Entwicklungsstadium. Demgegenüber ist hinsichtlich schriftlicher Dokumente ein Überdauern in Archiven in der Regel gesichert. Ein *zusätzlicher* (datenschutzkonformer) digitaler Nachweis bietet zusätzliche Sicherung, sollte aber nicht die Schriftform ersetzen.
- Auch die Warnfunktion und den Schutz vor Übereilung kann der Nachweis auf einer Blockchain schwer erfüllen.

Kann die Blockchain die Textform ergänzen und hierfür zusätzliche Sicherheit hinsichtlich der Identitäten bieten?

Welche Beispiele gibt es, bei denen bereits von dem Erfordernis der Schriftform abgewichen wurde?

g) Steuern

Wie sind die – wirtschaftlichen – Ergebnisse der an (Trans)Aktionen Beteiligten umsatz- und ertragsteuerlich einzuordnen?

IV. Praxisbeispiele

Zum Abschluss des Konsultationsprozesses besteht die Möglichkeit, auf Projekte hinzuweisen, bei denen die Blockchain-Technologie bereits erfolgreich genutzt wird:

- Bitcoin
- OpenTimestamps - Software und offener Standard für das Erstellen und Verifizieren von Zeitstempeln mithilfe bestehender Blockchain-Systeme (inkl. Bitcoin). https://opentimestamps.org/