Hünseler M. et al., Digitale Verbraucherteilhabe bei Blockchain-Anwendungen,
In: Boden, A., Jakobi, T., Stevens, G., Bala, C. Hgg., Verbraucherdatenschutz – Technik und Regulation zur Unterstützung des Individuums. Schriften der Verbraucherinformatik Band 1, 2021. DOI: 10.18418/978-3-96043-095-7_01

Digitale Verbraucherteilhabe bei Blockchain-Anwendungen

Marco Hünseler[1], Kerstin Lemke-Rust[1], Eva Pöll[2], Katja Stoppenbrink[2]
[1] Hochschule Bonn-Rhein-Sieg, Institut für Cyber Security & Privacy
[2] Westfälische Wilhelms-Universität Münster, Philosophisches Seminar, und Hochschule München, Fakultät für Angewandte Sozialwissenschaften
marco.huenseler@h-brs.de
kerstin.lemke-rust@h-brs.de
eva.poell@uni-muenster.de
katja.stoppenbrink@uni-muenster.de und katja.stoppenbrink@hm.edu

Abstract. Die Blockchain-Technologie ist einer der großen Innovationstreiber der letzten Jahre. Mit einer zugrundeliegenden Blockchain-Technologie ist auch der Betrieb von verteilten Anwendungen, sogenannter Decentralized Applications (DApps), bereits technisch umsetzbar. Dieser Beitrag verfolgt das Ziel, Gestaltungsmöglichkeiten der digitalen Verbraucherteilhabe an Blockchain-Anwendungen zu untersuchen. Hierzu enthält der Beitrag eine Einführung in die digitale Verbraucherteilhabe und die technischen Grundlagen und Eigenschaften der Blockchain-Technologie, einschließlich darauf basierender DApps. Abschließend werden technische, ethisch-organisatorische, rechtliche und sonstige Anforderungsbereiche für die Umsetzung von digitaler Verbraucherteilhabe in Blockchain-Anwendungen adressiert.

Einleitung

In der aktuellen Diskussion um digitale Verbraucherteilhabe[1] kommen mehrere Stränge der Inklusions- und Verbraucherpolitik zusammen: Ziel ist nicht mehr die Inklusion einer Gruppe in die Öffentlichkeit, in Gesellschaft, Bildungswesen oder Politik, sondern ein von Anfang an inklusives und Diversität anerkennendes Verständnis aller gesellschaftlichen Teilsysteme. Das Leitbild des souveränen Verbrauchers, der als *homo oeconomicus* sein rationales Eigeninteresse durchsetzt, wird ersetzt durch die Einsicht, dass Verbraucher:innen unterschiedliche Rollen einnehmen, die unterschiedliche Förderung, Kompetenzbildung und Befähigung erforderlich machen (1). Ausgehend von der Kryptowährung Bitcoin ist ein neuartiges Technologiefeld entstanden, dessen Möglichkeiten und Anwendungen noch lange nicht ausreichend wissenschaftlich erforscht sind. Blockchain-basierte Systeme bauen auf einer offenen, dezentralen Netzwerkstruktur auf und nutzen ein Regelwerk mit Mehrheitskonsens. Grundlegend für die Sicherheitsgarantien sind kryptographische Funktionen; hierdurch lassen sich persistente Verfügbarkeit und Integrität des Hauptbuchs erreichen sowie eine Verbindlichkeit von Transaktionen und auch Resistenz gegen Zensur. Im Blockchain-Ökosystem, das aktuell eine immense Marktkapitalisierung aufweist, gibt es inzwischen eine nahezu unüberschaubare Vielzahl von Anwendungen in sehr unterschiedlichen Entwicklungsstadien. Die Basis von Blockchain-Anwendungen bildet die Blockchain-Technologie, welche diese als Datenspeicher und für die dezentrale Ausführung von anwendungsorientiertem Code nutzen. Decentralized Applications (DApps) der Ethereum-Blockchain sind von besonderem Interesse: Die Anwendungslogik wird in sogenannten Smart Contracts implementiert, mit denen die Nutzer:innen über web-basierte Nutzerschnittstellen interagieren. Wir stellen hier die wichtigsten aus einer Verbraucherschutzperspektive relevanten Eigenschaften von Blockchains und DApps vor und erläutern deren technische Grundlagen (2), bevor wir uns grundlegenden Anforderungen an DApps aus der Perspektive der Verbraucherteilhabe und aus rechtlicher Sicht widmen (3). Ein kurzes Fazit beschließt den Beitrag (4).

[1] Der Ausdruck ‚Verbraucherteilhabe' wird vorliegend als generisches Maskulinum verstanden. Bei alleinstehenden Begriffen möchten wir mit der (verkürzten) Doppelnennung alle Gender einschließen. Bei zusammengesetzten Worten wie ‚Verbraucherteilhabe' oder ‚Nutzerschnittstelle' werden wir allerdings, der Lesegewohnheit folgend, auch im Weiteren abkürzend das generische Maskulinum verwenden.

1 Digitale Verbraucherteilhabe als eine von multiplen Inklusionsdimensionen und öffentliche Aufgabe

Ziele und Instrumente von Verbraucherschutzpolitik haben sich seit der Herausbildung und Implementierung eines modernen Verbraucherbegriffs in Wissenschaft und Recht sehr gewandelt. Die Digitalisierung fordert gegenwärtig erneut sowohl das Verbraucherverständnis als auch die Annahmen über angemessene Maßnahmen zum Verbraucherschutz stark heraus. Mehr als um die klassische Frage einer Verhinderung oder Rückabwicklung unerwünschter, verbraucherunfreundlicher Vertragsabschlüsse geht es heutzutage ganz grundsätzlich um die Ermöglichung sozialer Teilhabe von Menschen in ihrer Rolle als Verbraucher:innen. Wir beschäftigen uns vorliegend mit digitaler Teilhabe als einer Dimension sozialer Teilhabe. Wir knüpfen dabei an ein weites Verständnis von sozialer Inklusion an und identifizieren digitale Teilhabe als eine Dimension in einer Vielzahl von Inklusionsdimensionen (a). Dem liegt ein differenziertes Verbraucherverständnis zugrunde, das unterschiedliche Grade von Inklusion und Teilhabe zulässt (b). Digitale Teilhabe ist in mindestens zweifacher Hinsicht eine öffentliche Aufgabe (c). Dies gilt auch für den bislang vor allem von privaten Akteur:innen beherrschten Bereich der Anwendung von Blockchain-Technologien, von denen die Kryptowährung *Bitcoin* sicher die gegenwärtig bekannteste ist.

(a) Digitale Teilhabe – Unterscheidung von Teilhabe und Inklusion – multiple Inklusionsdimensionen

Als Teilhabesubjekte sind Verbraucher:innen heutzutage in multiplen Kontexten auf ganz unterschiedliche Weisen integriert oder – besser – inkludiert. Bezeichnen wir diese Kontexte der Inklusion als Teilhabeobjekte, so zeichnen sich Verbraucher:innen in der Gegenwart dadurch aus, dass sie einer Vielzahl von Teilhabeobjekten gegenüberstehen, an denen sie mehr oder weniger partizipieren. Der Begriff der Teilhabe ist ein *gradueller*, es geht stets um ein Mehr oder Weniger an Teilhabe. Die Vorstellung von vollständiger Inklusion in ‚die' Gesellschaft ist praktisch unmöglich, kontextuell unangebracht und ethisch nicht erstrebenswert (Stoppenbrink, 2020, m. w. N.). Das begriffliche Verhältnis von ‚Teilhabe' und ‚Inklusion' wird deshalb vorliegend wie folgt verstanden: Teilhabe resultiert in Inklusion – ‚Inklusion' gibt es aber niemals als ‚Totalinklusion', sondern stets als ein fragmentiertes Verhältnis von Inklusionsbeziehungen zwischen Teilhabesubjekt und multiplen Teilhabeobjekten. Zum Beispiel kann eine Informatikstudentin zwar bestens in der Fachschaft inkludiert sein, in der Unisportgruppe aber nur sporadisch mitmachen und aus der Gruppe der potenziellen Studienabbrecherinnen ganz herausfallen. Als gewähltes Mitglied des Studierendenparlaments gehört die Studentin in einer bestimmten Wahlperiode

zwar formal ganz dazu, kann aber dieses Mandat unterschiedlich intensiv ausüben und mehr oder weniger ernst nehmen. Das Beispiel zeigt, dass ‚Inklusion' immer relativ zu einer bestimmten Gruppe, einem bestimmten Kontext vorliegt. Auch für digitale Teilhabe lassen sich multiple Inklusionsdimensionen unterscheiden. Geht es um Grundschulkinder, so wird sich digitale Teilhabe beispielsweise in den Möglichkeiten und Kompetenzen im Umgang mit kindgerecht ausgestatteten Tablets oder Spielrobotern mit ersten einfachen Codierübungen ausdrücken lassen. Für Verbraucher:innen mit einer Präferenz für eigenständig durchführbare Finanzgeschäfte wird die Möglichkeit zum Umgang mit Onlinebrokern als digitale Teilhabe zu verstehen sein. Dabei können digitale und finanzielle Kompetenzen (etwa im Sinne von *financial literacy*) auseinanderfallen. Es ergeben sich somit für den Ankauf ein- und desselben Wertpapiers unterschiedliche Teilhabeanforderungen je nachdem, ob die Transaktion bei einem niedergelassenen Kreditinstitut oder einem Onlinebroker auf dem Smartphone in Auftrag gegeben wird. Auch die Anforderungen an finanziellen Verbraucherschutz sind unterschiedlich je nachdem, ob ein Intermediär wie ein:e Bankberater:in eingeschaltet oder direkt gehandelt wird. Digitale Teilhabe ist ebenfalls im Sinne eines Mehr/Weniger als graduell zu verstehen. So mag Seniorin A zwar auf dem heimischen PC Onlinebanking betreiben; mangels Smartphone kann sie aber ihr Vermögen nicht über einen sog. ‚Neobroker' verwalten, der ausschließlich diesen Vertriebskanal anbietet. In dieser Hinsicht fehlt ihr digitale Teilhabe.

(b) Plädoyer für ein differenziertes Verbraucherverständnis

An die Stelle des Verständnisses des souveränen Verbrauchers der (neo-) klassischen Wirtschaftswissenschaft (zum Ausdruck *consumer sovereignty* vgl. zuerst Hutt 1940, dazu Persky 1993) ist die Auffassung getreten, dass sich die Position von Verbraucher:innen durch Vulnerabilität und eine inferiore Marktposition auszeichnet. Dieses Leitbild ist unseres Erachtens zu pauschal und entspricht nicht der realen Position von Verbraucher:innen in der heutigen Lebenswelt, die zunehmend von Fragmentierung und Digitalisierung[2] geprägt ist. In einem ersten Schritt (unter (a)) haben wir ein graduelles Verständnis digitaler Teilhabe skizziert. Dabei werden die Begriffe ‚Teilhabe' und ‚Inklusion' unterschieden, die gegenwärtig in der Literatur unterschiedlicher Fachrichtungen (vgl. z. B. Wansing 2015; Rudolf 2017) und in der Öffentlichkeit oft als deckungsgleich[3] verstanden werden. Aus unserer Bestimmung digitaler Teilhabe

[2] Beide Phänomene lassen sich unter das theoretische Konzept der Singularisierung subsumieren, wie es von Reckwitz (2017) zur Diagnose spätmoderner Gesellschaften entwickelt wird. Auch das hier vorgeschlagene differenzierte Verbraucherverständnis trägt einer zunehmenden gesellschaftlichen Individualisierung Rechnung.

[3] Inklusion wird dabei z. B. als Ergebnis gelungener Bemühungen um Teilhabe verstanden. Besonders irreführend sind verbreitete grafische Darstellungen, nach denen ‚Inklusion' dann vorliegt, wenn in einem bestimmten Inklusionsobjekt, das oftmals durch einen Kreis visualisiert und als ‚die' Gesellschaft verstanden wird, alle vorhandenen Inklusionssubjekte, oftmals als einzelne Punkte visualisiert, enthalten

als (normativer) Zieldimension ergibt sich ein Verbraucherverständnis, das sich v. a. dadurch auszeichnet, dass es nicht eindimensional Vulnerabilität und Inferiorität zuschreibt, sondern eine differenzierte Sichtweise zulässt. In einem zweiten Schritt ergibt sich daraus nun ein (normatives) Plädoyer für ein differenziertes Verbraucherverständnis. Verbraucher:innen sind unterschiedlich digital affin und unterschiedlich digital kompetent. Kompetenz und Affinität können, müssen aber praktisch nicht zusammenfallen und sind begrifflich zu unterscheiden. Es ist im Sinne der Entwicklung neuartiger Technologien wie in unserem Fall von Blockchain-Anwendungen wichtig, die Verbraucherschutzanforderungen mit Bezug auf bestimmte Annahmen in puncto Verbraucherkompetenz zu spezifizieren.

(c) Digitale Teilhabe als öffentliche Aufgabe vs. digitale Teilhabe an öffentlich-politischen Prozessen

Insofern Verbraucher:innen als *consumer citizen* verstanden werden, richten sie sich nach wie vor auf *eine* Entität aus, den Staat, der ihnen als Teilhabeobjekt gegenübertritt. Doch sind mindestens zwei Varianten des Verhältnisses von Verbraucherinnen und Verbrauchern sowie Öffentlichkeit und Politik zu unterscheiden; *erstens* Partizipation *an* Öffentlichkeit und Politik, *zweitens* Partizipation als öffentliches Anliegen oder öffentliche Aufgabe *der* Politik.

Erstens: Partizipation an öffentlichen (politischen) Prozessen. Die Partizipation an öffentlich-politischen Prozessen ist eine der Ausdrucksformen der *consumer citizens*. Diese bringen sich in ihrer klassischen Rolle als Staatsbürger:innen (*citoyens*) unter anderem auch deshalb ein, um in ihrer Rolle als Wirtschaftsbürger:innen (*bourgeois*) besser agieren zu können, ihre Interessen als Wirtschaftsbürger:innen besser vertreten zu wissen (Höffe (2004); Kneip (2010); m. w. N.). Im Rahmen des vorliegenden Projekts wird als Anwendungsfall u. a. auch untersucht, ob und wie politische Partizipation und Aktivismus von Verbraucher:innen mittels Blockchain-Anwendungen transparent und manipulationsresistent gestaltet werden können.

Zweitens: öffentliche Aufgabe digitale Teilhabe und Verbraucherschutz. Zudem geht es darum, Teilhabe in einer Vielzahl von Dimensionen zu ermöglichen. Digitale Teilhabe ist dabei (nur) eine von vielen Teilhabedimensionen. Ein Verständnis von Verbraucherschutz als öffentliche Aufgabe ist mittlerweile *common sense*. Während die Schutzwürdigkeit von Verbraucherinteressen breit geteilte Anerkennung findet, bleiben die Fragen nach Modi (z. B. ordnungspolitisch vs. freiwillig) und Ausmaßen (z. B. Schutzniveau, Eingriffstiefe in Privatautonomie) von Verbraucherschutz umstritten.

---

sind. Ein solches Verständnis von ‚Totalinklusion' ist zurückzuweisen. (Beispielhaft in einem negativen Sinne sind die Visualisierungen unter: https://de.wikipedia.org/wiki/Inklusive_Pädagogik; abgerufen am 01.09.2021.)

Aus dieser Unterscheidung ergeben sich generell zwei Stränge öffentlicher Aufgaben: Einmal geht es um die Einrichtung der erforderlichen Infrastruktur für digitale Teilhabe. Dabei lässt sich der Anspruch erheben, diese müsse flächendeckend, barrierefrei und für alle Bürger:innen bzw. *consumer citizens* gleichermaßen zugänglich sein. Es lässt sich mit Blick auf jeden einzelnen Punkt diskutieren, ob die Infrastruktur für digitale Teilhabe flächendeckend oder nur konzentriert auf Ballungsräume, barrierefrei oder nur für besonders befähigte, digital affine Gruppen eingerichtet werden soll, ob sie trotz unterschiedlicher Bedarfe, finanzieller Möglichkeiten und Kompetenzen für alle gleichermaßen Zugang bieten soll. Diese Fragen können hier nicht im Detail erörtert werden, sollen aber als wichtige *Policy*-Dimensionen digitaler Teilhabe zumindest kurz angesprochen werden. Im Einzelnen können sich auch mit Blick auf Blockchain-Anwendungen für Verbraucher:innen unterschiedliche infrastrukturelle Anforderungen aus den Weichenstellungen, die in diesen Hinsichten vorgenommen werden, ergeben. Beispielsweise könnte aus Schutzgründen eine zentralisierte, staatlich oder zumindest hoheitlich/öffentlich überwachte Blockchain in einem bestimmten Anwendungsbereich[4] vorzuziehen sein. Dies entspricht dann ggf. nicht den üblicherweise angenommenen Vorzügen dezentraler *Bottom-up*-Strukturen, sondern steht in einem Spannungsverhältnis zu diesen. Weiterhin ergibt sich die Forderung nach individueller oder gruppenbezogener Kompetenzbildung für digitale Teilhabe. Diese Aufgabe könnte in einem alternativen normativen Modell den Einzelnen überlassen bleiben. Wird die Ermöglichung digitaler Teilhabe aber als öffentliche Aufgabe und Facette von Verbraucherschutz verstanden, so ergibt sich daraus, dass auch die Kompetenzbildung bzw. die Schaffung von *Möglichkeiten zur Kompetenzbildung* als öffentliche Aufgabe aufzufassen ist. Schlagworte sind hier Befähigung bzw. Empowerment sowie *digital literacy*.[5] Wir gehen nun zunächst auf technische Grundlagen ein, erklären die Funktionsweise von Blockchains und sogenannten DApps und befassen uns genauer mit deren Eigenschaften (2). Anschließend formulieren wir aus rechtlicher und Verbraucherschutzperspektive Anforderungen an diese (3).

[4] Grundsätzlich kritisch zu der Untersuchung immer neuer Anwendungsbereiche insbesondere von Blockchain-Technologie sind Kloiber und Lindinger (2021, 397). Für die Autorinnen kommt dies einem „Solutionismus“ gleich, d. h., es „werden alle Probleme so definiert, als ließen sie sich mit technischen Mitteln lösen.“

[5] Dieses weiterführende Thema soll vorliegend nicht vertieft werden.

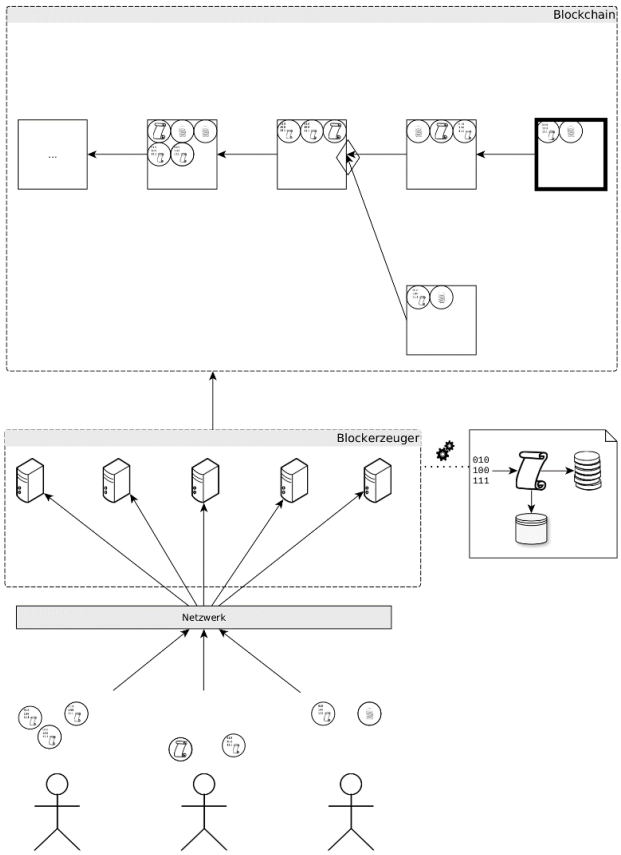

Abbildung 1. Funktionsweise eines Blockchain-Systems.

2 Technische Grundlagen: Funktionsweise und Eigenschaften von Blockchains und DApps

Als Blockchain wird eine Datenstruktur bezeichnet, die sich durch eine Organisation der in ihr gespeicherten Daten in Form einer Kette von Blöcken auszeichnet. Ausgehend von dem ersten Block (‚Genesis-Block') der Kette beinhaltet jeder nachfolgende Block den kryptographischen Hashwert des Vorgängerblocks (rückwärts verkettete Liste) sowie weitere kryptographische Sicherungsmaßnahmen zum Schutz vor Manipulationen des Datenbestands. *Bitcoin* (Nakamoto, 2008) war die erste Kryptowährung mit dem Ziel, ein dezentrales Peer-to-Peer-Bezahlsystem zu erschaffen, in dem Teilnehmer:innen untereinander und ohne die Beteiligung eines Intermediärs Geldbeträge transferieren können. Neue Transaktionen im Netzwerk werden dezentral in einem neuen Block zusammengefasst. Die Einigung über den aktuellsten Block in einer Kette erfolgt durch die Einhaltung von Konsensregeln der jeweiligen Blockchain.

Dies ist erforderlich, da verschiedene Knoten des Blockchain-Netzwerks eine unterschiedliche Sicht auf die jeweils aktuellsten Blöcke im Netzwerk haben können, beispielsweise aufgrund von Latenzzeiten. Aus den Inhalten aller Blöcke zwischen dem aktuellsten und ersten Block ergibt sich der aktuelle Datenbestand, der auch als das Hauptbuch (‚Ledger') der Blockchain bezeichnet wird. Die Blockchain-Struktur stellt somit probabilistisch sicher, dass Datensätze in Blöcken, die schon mehrere Nachfolgeblöcke aufweisen, in Zukunft unverändert bleiben werden. Außerdem ergibt sich hieraus eine zeitliche Ordnung der Datensätze, wodurch Aussagen darüber getroffen werden können, wann eine bestimmte Information hinzugefügt wurde (Nakamoto, 2008).

Es existieren zahlreiche Möglichkeiten zur konkreten Ausgestaltung einer Blockchain. Der grundsätzliche Ablauf unterscheidet sich zwischen den gebräuchlichen Implementierungen jedoch nur geringfügig. Abbildung 1 zeigt den grundsätzlichen Ablauf des Erweiterungsprozesses (Buterin, 2013):

(1) Ein:e Nutzer:in möchte die Blockchain um einen Datensatz erweitern. Verwaltet die Blockchain eine Kryptowährung, kann dies beispielsweise eine Transaktion sein, die einen gewissen Betrag der Währung an ein anderes Konto überweist. Unterstützt die Blockchain-Implementierung eine Ausführung von festgelegten Prozessen in Form von Programmcode (‚Smart Contracts'), könnte die Transaktion auch einen neuen Smart Contract enthalten oder eine Funktionalität eines bestehenden Smart Contracts nutzen. Die Inhalte der Transaktion werden durch den oder die Nutzer:in kryptografisch signiert. Nur mit dem eigenen privaten Schlüssel haben Nutzer:innen Zugriff auf ihre Werte in der Blockchain. Die eigenen kryptographischen Schlüssel sind von den Nutzer:innen in einem digitalen Schlüsselbund (‚Wallet') so aufzubewahren, dass unautorisierte Personen keinen Zugriff hierauf erhalten.

(2) Der oder die Nutzer:in sendet die Transaktion an Teilnehmer des Blockchain-Netzwerks (‚Nodes'), die sie im Blockchain-Netzwerk weiterverteilen, wodurch weitere Nodes eine Kopie des Datensatzes erhalten. Unter anderem wird die Transaktion auch Nodes zugestellt, die daran arbeiten, die Blockchain um neue Blöcke zu erweitern.

(3) Blockerzeugende Nodes (je nach Blockchain ‚Miner', ‚Minter', ‚Proposer' u. a.) prüfen die Transaktionen der Nutzer auf Gültigkeit und führen ggf. den Programmcode referenzierter Smart Contracts aus. Anschließend sammeln sie gültige Transaktionen und fassen sie in einem neuen Block zusammen. Dieser Block enthält u. a. einen Verweis in Form eines Hashwertes einer kryptografischen Hashfunktion auf den Block, den der Node als den aktuell letzten gültigen Block ansieht. Hierdurch wird eine Verkettung der Blöcke untereinander hergestellt, die bewirkt, dass Veränderungen in der Struktur der Kette ausgeschlossen werden. Wenn die Nodes ein kryptografisches Puzzle lösen können (‚Proof-of-Work')

oder durch ein alternatives Verfahren zur Erstellung eines Blocks ausgewählt werden (z. B. ‚Proof-of-Stake'), binden sie einen Nachweis in den Block ein und versenden ihn an das Netzwerk.

(4) Sobald die Nodes des Netzwerks den neuen Block empfangen, prüfen sie, ob die enthaltenen Daten regelkonform und insbesondere die digitalen Signaturen gültig sind. Ist dies der Fall, so wird der Block mitsamt der Transaktion der Nutzer:innen im Netzwerk weiterverteilt und probabilistisch in die Blockchain integriert. Hierbei ist zu ergänzen, dass es möglich ist, dass zeitgleich im Netzwerk ein alternativer Block derselben Blockhöhe (bzw. Blocknummer) erzeugt wird, der die Transaktion der Nutzer:innen nicht enthalten könnte, aber z. B. wegen schnellerer Verteilung im Netzwerk von der Mehrheit der Nodes als aktuellster Block angesehen wird. Sollte dieser Fall eintreten, müssen Nutzer:innen auf einen späteren Block warten, der die eigene Transaktion beinhaltet.

(5) Der aktuelle Zustand des Netzwerks ergibt sich aus den Transaktionen innerhalb des letzten aktuell gültigen Blocks und seiner Vorblöcke.

(a) Eigenschaften von Blockchains

Blockchains eigenen sich aufgrund ihrer Eigenschaften insbesondere für die Anwendungsfälle, in denen Daten mehrerer Teilnehmer:innen fälschungssicher abgespeichert werden müssen und keine einzelne Instanz existiert, der alle Beteiligten hinreichend viel Vertrauen entgegenbringen.

Zentrale Eigenschaften von Blockchains aus Sicht von Verbraucher:innen sind u. a. Dezentralität, Transparenz, Pseudonymität, Finalität und Integrität (Wu et al., 2019; Xiao et al., 2019).

Dezentral bedeutet in diesem Kontext, dass es eine Vielzahl von Teilnehmer:innen gibt, die die Blockchain potenziell um neue Daten erweitern können oder dem oder der Nutzer:in angeforderte Datensätze übermitteln können. Durch diese Eigenschaft wird sichergestellt, dass keine einzelne Partei dazu in der Lage ist, Transaktionen der Nutzer:innen zu zensieren, sodass sich Nutzer:innen darauf verlassen können, dass gültige Transaktionen zeitnah ein Teil des verteilten Datenbestandes werden. Zudem wird durch die Dezentralität die Verfügbarkeit von Daten erhöht, sodass Nutzer:innen auch beim Ausfall einzelner Nodes Daten abrufen können.

Transparenz entsteht durch die öffentliche Verfügbarkeit aller Datensätze und die Nachvollziehbarkeit des Regelwerks, durch das die Blockchain definiert ist. Während dies generell aus Verbrauchersicht eine wünschenswerte Eigenschaft darstellt, so kann die Transparenz aller gespeicherten Informationen auch zu einer Schwächung des Datenschutzes führen.

Integrität beschreibt die Eigenschaft, dass jede spätere Änderung an Daten festgestellt werden kann. Es ist damit nicht möglich, Daten in der Blockchain

unbemerkt zu ändern. In Verbindung mit der Transparenzeigenschaft ergibt sich hieraus eine öffentliche Verifizierbarkeit: Jede:r kann die Datensätze in der Blockchain auf Korrektheit prüfen und sicherstellen, dass keine Manipulation erfolgt ist (Wüst und Gervais, 2018).

Für viele Anwendungsfälle ist es unerlässlich, dass private Daten der Anwender:innen verarbeitet werden. An dieser Stelle besteht ein Konflikt zur Privatsphäre der Nutzer:innen: Vollständige Transparenz der gespeicherten Daten ist in diesem Fall nicht immer erwünscht. Es muss etwa vermieden werden, dass Dritte in den Besitz personenbezogener Daten gelangen, ohne dass die betroffene Person vorher zugestimmt hat (Wüst und Gervais, 2018). Lösungsmöglichkeiten bestehen an dieser Stelle in der Verwendung eines separaten Datenspeichers und der Verwendung von Pseudonymen oder sonstigen Referenzen auf die separate Datenbank, durch Verschlüsselung oder durch die Verwendung von anonymisierenden Transaktionsformaten (z. B. Noether, 2015).

Öffentliche Blockchains wie Bitcoin und Ethereum bieten Nutzer:innen konstruktionsbedingt Anonymität bzw. *Pseudonymität*. Konten für den Währungstransfer oder Smart Contracts werden durch kryptografische Schlüssel identifiziert, die Nutzer:innen selbst in beliebiger Anzahl erstellen können. Diese Schlüssel bzw. Pseudonyme lassen sich ohne weitere Informationen nicht mit der realen Identität der Nutzer:innen verbinden. Da Nutzer:innen mit dem Netzwerk interagieren müssen, fallen diverse Metadaten, u. a. IP-Adressen an, die zur Feststellung einer Identität herangezogen werden können (Koshy et al., 2014). Zudem müssen sich Nutzer:innen für den Kauf von Kryptowährung an einigen Handelsplattformen aufgrund von nationalen Gesetzen ausweisen. Hier entsteht durch die Transparenz der Transaktionen eine Nachverfolgbarkeit der Währungsbeträge, die auch Rückschlüsse auf die Identität der Nutzer:innen zulässt (Meiklejohn et al., 2016). Sofern eine wirksame Pseudonymisierung der Identitäten von Verbraucher:innen gewünscht ist, ist es aus diesem Grund erforderlich, bei der Implementierung eines Blockchain-Systems weitere Sicherheitsmaßnahmen zu ergreifen.

Neben der Transparenz kann auch die *Finalität* ein unerwünschtes Kriterium sein. Diese beschreibt die Eigenschaft, dass Daten, die Teil der Blockchain geworden sind, auch in Zukunft unabänderlich ein Teil der Kette bleiben werden. In der Interaktion zwischen Behörden, Verbraucher:innen, Firmen und anderen Entitäten können stets menschliche Fehler auftreten, beispielsweise bei der Bearbeitung eines Antrags oder beim Eintrag neuer Datensätze. Auch Programmierfehler in Smart Contracts können ruinöse Folgen für Nutzer:innen nach sich ziehen (Kühl, 2016). Durch die gegebene Finalität sind diese Fehler grundsätzlich unumkehrbar, was nachteilige Folgen haben kann. Für viele Anwendungsfälle besteht außerdem die Anforderung, dass Änderungen an Verträgen oder Gesetzen auch Änderungen der Datenverarbeitung nach sich ziehen. In diesem Fall müssen Mechanismen vorgesehen werden, die es

ermöglichen, nachträgliche Änderungen am Verhalten der DApps (zu diesen sogleich unter (d)) vorzunehmen (Kafeza et al., 2020).

Nachfolgend werden eine übliche taxonomische Unterscheidung von Blockchain-Netzwerken (b), das diesen zugrundeliegende Konsens-Verfahren (c) sowie DApps näher vorgestellt (d).

(b) Taxonomie

Blockchain-Netzwerke können in mehrere Kategorien eingeteilt werden (Xiao et al., 2020):

- Öffentliche Blockchains mit freiem Zugriff (*Public Permissionless*). Es existieren keine Beschränkungen zum Zugriff auf das und zur Teilnahme am Blockchain-Netzwerk. Alle Teilnehmer:innen können Daten erzeugen, die vom Netzwerk verarbeitet werden. Um die Kette um einen Block zu erweitern, wird ein Konsens-Mechanismus eingesetzt, der von allen Teilnehmer:innen verwendet werden kann. Dieser Algorithmus sichert die Blockchain auch gegen Angriffe vieler Teilnehmer:innen zur gleichen Zeit ab. Öffentliche Blockchain-Netzwerke weisen häufig hohe Transaktionskosten und einen geringen Datendurchsatz auf.
- Öffentliche Blockchains mit eingeschränktem Zugriff (*Public Permissioned*). Dieses Modell stellt eine Mischform aus öffentlichen und privaten Blockchains dar. Während auf die Daten der Blockchain frei zugegriffen werden kann, wird der schreibende Zugriff auf den Datenbestand limitiert.
- Private Blockchains (*Private Permissioned*). Ausschließlich ausgewählte Teilnehmer:innen können partizipieren. Die möglichen Ersteller neuer Blöcke und der Teilnehmerkreis, der neue Daten zur Aufnahme in die Blockchain vorschlagen kann, ist durch eine zentrale Instanz festgelegt. Damit ähneln private Blockchains zentralistischen Datenhaltungssystemen. Vorteile gegenüber öffentlichen Blockchains liegen in geringeren Kosten und höherem Datendurchsatz. Im Gegenzug gibt es Nachteile bei der Partizipation und Transparenz (Wüst und Gervais, 2018).

Je nachdem, welche funktionellen Anforderungen und Sicherheitsgarantien erfüllt werden müssen, können sich konkrete Implementierungen des Systems und der darin verwendeten Konsensmechanismen voneinander unterscheiden. Bei der Konzeptionierung eines Systems auf Blockchain-Basis ist es aus diesem Grund unerlässlich, die entsprechenden Anteilseigner:innen einzubinden und deren Anforderungen von Beginn an zu berücksichtigen. Welche Gestaltungsmöglichkeiten es gibt und welche Auswirkungen diese auf das Gesamtsystem haben, wird im Folgeabschnitt (c) erläutert.

(c) Konsens

Ein zentrales Element innerhalb eines Blockchain-Systems ist das zugrundeliegende Konsens-Verfahren. Mithilfe dieses Verfahrens einigen sich alle Teilnehmer:innen auf Basis der ihnen zur Verfügung stehenden Daten auf den aktuellen Zustand der Blockchain. Ein Konsens-Verfahren besteht aus den folgenden Komponenten (Xiao et al., 2020):

Bestimmung des Blockerstellers

Es wird festgelegt, welche:r Teilnehmer:in zur Erstellung eines Blocks berechtigt ist. Für öffentliche Blockchains werden häufig Algorithmen eingesetzt, die auf Proof-of-Work oder Proof-of-Stake basieren. Die Wahrscheinlichkeit, einen Block zu produzieren, steigt bei diesen Algorithmen mit der eingesetzten Rechenleistung (Proof-of-Work) oder mit dem Einsatz von Kryptowährung auf der jeweiligen Blockchain (Proof-of-Stake) (Buterin, 2013).

In privaten Blockchains kommen zusätzlich nachrichtenbasierte Algorithmen wie Raft oder Practical Byzantine Fault Tolerance (PBFT) zum Einsatz. Diese erfordern oft den Versand vieler Nachrichten, weshalb sie für große Netzwerke mit vielen Teilnehmer:innen nicht geeignet sind. Im Gegenzug erfordern sie im Vergleich mit Proof-of-Work nur einen geringen Einsatz von Rechenkapazität und ermöglichen es, einen höheren Transaktionsdurchsatz zu erreichen.

Nachrichtenbasierte Algorithmen werden häufig durch die Merkmale Crash Fault Tolerance (CFT) und Byzantine Fault Tolerance (BFT) charakterisiert. Während CFT-Algorithmen (z. B. Raft) lediglich die Operation der Blockchain bei Ausfällen einzelner Knoten sicherstellen, tolerieren BFT-Algorithmen (z. B. PBFT) darüber hinaus gezielt gefälschte Nachrichten, ohne den Betrieb zu beeinträchtigen (Bundesamt für Sicherheit in der Informationstechnik, 2019).

Verfahren zur Datenübertragung

Zur Übertragung von Blöcken, Transaktionen und anderen Nutzdaten wird ein Verfahren benötigt, das sicherstellt, dass alle berechtigen Teilnehmer:innen Zugriff auf die benötigten Daten erhalten. Hierzu kommen üblicherweise Protokolle auf Peer-to-Peer-Basis zum Einsatz. Das bedeutet, dass die Teilnehmer:innen untereinander verbunden sind und sich gegenseitig über neue Daten informieren (Xiao et al., 2020).

Validitätsprüfung

Eine Blockchain legt fest, welche Transaktionsdaten der Nutzer:innen als gültig angesehen werden. Wird die Blockchain für den Transfer von Währungen eingesetzt, wird z. B. festgelegt, dass eine Einheit der Währung nicht doppelt transferiert und nur dann übertragen werden kann, wenn der:die Nutzer:in auch tatsächlich in deren Besitz ist. Darüber hinaus können beliebige weitere Regeln

bestehen, etwa in Bezug auf den Transfer anderer Güter. Blockchains wie Ethereum legen zusätzlich Mechaniken fest, die die Erstellung und Verwendung von Smart Contracts, also auf der Blockchain gespeicherten Programmen (dazu sogleich unter (d)), regeln (Wood, 2021).

Bestimmung des aktuellsten Blocks

Um den aktuellen Zustand der Blockchain bestimmen zu können, benötigen Teilnehmer:innen einen Algorithmus, der festlegt, welcher der aktuellste gültige Block ist. Die Nutzdaten des so bestimmten Blocks und aller Vorgängerblöcke legen fest, auf welche Datenbasis (Kontostände, Smart Contracts) sich das Netzwerk geeinigt hat. Ein solcher Algorithmus wird insbesondere dann benötigt, wenn ein Block mehrere Nachfolger besitzt (siehe Abbildung 1, ◊). Beispiele sind die Longest-Chain-Rule von Bitcoin, welche die längste bekannte Kette auswählt (Nakamoto, 2008) und GHOST, das von Ethereum verwendet wird. GHOST bestimmt, ausgehend von einem Block, der durch mehrere mögliche Nachfolger referenziert wird, rekursiv die Anzahl der Nachfolgeblöcke und wählt als korrekten Nachfolger denjenigen aus, der insgesamt die meisten Folgeblöcke besitzt (Buterin, 2013).

Ökonomische Anreize

Insbesondere in öffentlichen Blockchains ist es erforderlich, ökonomische Anreize zu schaffen, die Teilnehmer:innen für korrektes Verhalten belohnen und bewirken, dass Fehlverhalten weniger lohnenswert ist als eine ehrliche Teilnahme. Die Bitcoin-Blockchain belohnt beispielsweise Teilnehmer:innen, die einen Block erschaffen, mit der Berechtigung zum Erzeugen neuer Währungseinheiten und der Gutschrift von Transaktionsgebühren der Teilnehmer:innen. Fehlverhalten wird implizit bestraft, indem Teilnehmer:innen, die bei der Durchführung eines Angriffes erfolglos bleiben, ihre Rechenleistung aufgewendet haben, ohne belohnt zu werden (Nakamoto, 2008).

Da in privaten Blockchains häufig alle Teilnehmer:innen bekannt sind und Vertragsverhältnisse oder andere rechtliche Rahmenbedingungen existieren, kann auf weitere ökonomische Anreize innerhalb des Blockchain-Systems ggf. verzichtet werden.

(d) Dezentrale Applikationen (DApps)

Als DApps (Dezentrale Applikationen) werden Anwendungen bezeichnet, die in einer Blockchain dezentral ausgeführt werden. Eine DApp besteht aus einer Nutzerschnittstelle (z. B. webbasiert) und einem Programmcode in der Blockchain. Die Nutzerschnittstelle der DApp übernimmt die Erstellung von Transaktionen, die an das Netzwerk übermittelt werden und interagiert im Auftrag des:der Nutzer:in mit ‚Smart Contracts' in der Blockchain (Ethereum Foundation, 2021).

Smart Contracts erlauben es, ein Blockchain-System um neue Funktionalitäten zu erweitern. Die Programme werden dem Netzwerk in Form einer Transaktion übermittelt und können nach Aufnahme in einen Block durch andere Teilnehmer:innen verwendet werden, indem diese die vom Smart Contract bereitgestellten Funktionen aufrufen. Smart Contracts haben einen eigenen Kontostand und können Daten abspeichern.

Der Aufruf von Funktionalität eines Smart Contracts durch eine:n Nutzer:in erfolgt durch eine Transaktion, die an das Netzwerk übermittelt wird. Alle Teilnehmer:innen, die Transaktionen prüfen, führen den Programmcode der Applikation mit den Eingabedaten der Transaktion durch und berechnen die Änderungen an den gespeicherten Daten und ggf. auftretende Zahlungsvorgänge, die sich daraus ergeben (Abbildung 1, rechts) (Wood, 2021).

Durch die Übertragung und Einbettung von Programmcode und Transaktionen in einen Block kann durch jede:n Nutzer:in der Blockchain transparent nachvollzogen werden, wann welche Funktionen durch welches Konto aufgerufen wurden.

```
Stimmen für Vorschlag 1: 0
Stimmen für Vorschlag 2: 0
Konten, die bereits abgestimmt haben: Liste[]

Auszählung: 01.01.2022, 12:00 UTC

Abstimmung (Transaktion):
  Wenn AktuelleZeit() >= Auszählung:
    Abbruch ("Die Auszählung hat bereits stattgefunden.")
  Wenn Transaktion.Absender in Teilnehmer, die bereits abgestimmt haben:
    Abbruch ("Konto hat bereits abgestimmt.")

    Wenn Transaktion.Stimme == Vorschlag 1:
      Stimmen für Vorschlag 1 += 1
    Wenn Transaktion.Stimme == Vorschlag 2:
      Stimmen für Vorschlag 2 += 1

    Konten, die bereits abgestimmt haben += Transaktion.Absender

Auszählung():
  Wenn AktuelleZeit() < Auszählung:
    Abbruch ("Die Abstimmung läuft noch.")

  Wenn Stimmen für Vorschlag 1 > Stimmen für Vorschlag 2:
    Rückgabe: "Vorschlag 1 hat gewonnen"
  Wenn Stimmen für Vorschlag 2 > Stimmen für Vorschlag 1:
    Rückgabe: "Vorschlag 2 hat gewonnen"
  Sonst:
    Rückgabe: "Unentschieden"
```

Listing 1. Beispiel für einen Smart Contract.

Ein kurzes Beispiel für einen Smart Contract ist in Listing 1 angegeben. Der vorliegende Smart Contract verwaltet eine Abstimmung, bei der Teilnehmer:innen zwischen zwei Vorschlägen wählen können. Sobald ein zuvor festgelegter Zeitpunkt („Auszählung“) erreicht ist, sind keine weiteren Stimmabgaben möglich und das Ergebnis kann abgerufen werden. In diesem vereinfachten Beispiel wird die Identität der Nutzer:innen nicht berücksichtigt, sodass ein:e Nutzer:in durch die Erzeugung weiterer Konten mehrfach abstimmen könnte. Die Pseudonyme, die bereits abgestimmt haben, werden in einer Liste verwaltet, sodass eine Mehrfachabstimmung durch dasselbe Konto verhindert wird. Eine einmal getätigte Entscheidung kann nicht korrigiert werden. Die Nutzer:innen agieren über den Versand von Transaktionen mit dem Vertrag, die eine der angegebenen Methoden („Abstimmung“ oder „Auszählung“) verwenden und ggf. die Stimmabgabe des:der Nutzer:in enthalten. Durch die Verwendung eines Blockchain-basierten Smart Contracts wird permanent festgehalten, welcher und wie viele Nutzer:innen für einen bestimmten Vorschlag abgestimmt haben.

Im Kontext des vorangegangenen Beispiels wäre etwa eine DApp zur Entscheidung über Vorschläge im Kontext einer öffentlichen und nicht-geheimen Abstimmung denkbar. Diese könnte den Nutzer:innen im ersten Schritt alle Vorschläge detailliert, einschließlich etwaiger Hintergrundinformationen, vorstellen und abschließend zur Stimmabgabe auffordern, die dann dauerhaft in der Blockchain abgespeichert wird.

Da der Programmcode von Smart Contracts und DApps beliebig ausgestaltet werden kann, ist es sinnvoll, die Anwendbarkeit der Technologie auch für Probleme in der Verbraucherinformatik zu untersuchen. Denkbar sind etwa Anwendungen zur Verwaltung von Daten über den Lebenszyklus eines Automobils, sodass z. B. Werkstattbesuche und Reparaturen transparent und fälschungssicher nachgehalten werden können. Eine weitere Möglichkeit ist die Implementierung virtueller Auktionen, die im Rahmen der dezentralen Energieerzeugung Anwendung finden könnte (Hahn et al., 2017).

3 Anforderungen an Blockchain-Anwendungen aus Verbraucherschutz-Perspektive

Dieser Abschnitt verfolgt das Ziel, Anforderungsbereiche an Blockchain-Anwendungen aus Verbraucherperspektive zu entwickeln. Es sollen technische (a), ethisch-organisatorische (b), rechtliche (c) und weitere (d) Bereiche dargestellt werden, die für eine Architektur von konkreten Blockchain-Anwendungen Hilfestellungen im Sinne von guter Praxis geben können.

(a) Technische Anforderungsbereiche

Intrinsische technische Eigenschaften von Blockchain-Basistechnologien

Die Blockchain-Basistechnologie verwaltet ein gemeinsames Hauptbuch auf den Netzwerkknoten. Gegen Manipulationsversuche im Hauptbuch werden nach dem Stand der Technik starke kryptographische Verfahren bei öffentlichen Blockchains eingesetzt. Zudem kann die Basistechnologie durch die dezentrale Verwaltung des Hauptbuchs Löschungen auf einer signifikanten Anzahl von Netzwerkknoten tolerieren und den Betrieb aufrechterhalten. Bei privaten Blockchains gibt es speziellere Konfigurationsmöglichkeiten für Blockchains, die u. U. leichtgewichtigere Verfahren enthalten können und deshalb speziell untersucht werden sollten (Cachin und Vukolić, 2017).

Weiterhin sollten Implementierungen auf Blockchain-Basis immer auch im Hinblick auf die der Technologie inhärenten Vor- und Nachteile für Verbraucher:innen geprüft und mit klassischen Implementierungen auf Basis herkömmlicher Datenbanken verglichen werden (Wüst und Gervais, 2018).

Finalität

Die Frage nach einer Finalität von Transaktionen im Hauptbuch wird in verschiedenen Blockchain-Basistechnologien unterschiedlich beantwortet. Traditionell wird Finalität von Transaktionen wie bei Bitcoin (Nakamoto, 2008) im probabilistischen Sinn verstanden: Die Wahrscheinlichkeit eine existierende Blockchain ausgehend von einem gemeinsamen Block in der Vergangenheit ab einem bestimmten Zeitpunkt mit einer parallelen Kette zu überholen, sinkt hinreichend stark mit der Anzahl der zu überholenden Blöcke und erfordert bei Proof-of-Work auch Rechenkapazität in der Größenordnung der gesamten Rechenkapazität des restlichen Netzwerks (Nakamoto, 2008). Andere Konsensverfahren, wie beispielsweise das in der Ethereum 2.0 Beacon Chain verwendete Verfahren Gasper (Buterin et al., 2020), beinhalten das Konzept der deterministischen Finalität, da bei Proof-of-Stake ein Aufbau einer Parallelkette keine außergewöhnlich hohe Rechenkapazität erfordert. Das Verfahren legt hierzu fest, dass nach einer festgelegten Anzahl vergangener Blöcke die zuvor erstellten Blöcke explizit als ‚final' deklariert werden.

Bei Blockchain-Anwendungen kann es erforderlich sein, Korrekturmöglichkeiten für Programmierfehler oder menschliche Fehler bei der Eingabe von Transaktionen bereitzustellen (Kühl, 2016). Dies könnte beispielsweise durch eine programmatische Rückabwicklung von Transaktionen oder durch die Referenzierung eines aktualisierten Smart Contracts realisiert werden (Kafeza et al., 2020). Andere verbraucherrelevante Fragen entstehen zu der Möglichkeit des Umtauschs und der Gewährleistung.

Klassifizierung von Informationen

In einer Blockchain-Anwendung sind sicherheits- und privatheitssensitive Daten besonders zu kennzeichnen. Die Vertraulichkeit von Informationen in einer Blockchain-Anwendung erfordert den Einsatz von Verschlüsselungsverfahren auf dem Stand der Technik und eine Konzeption für die Schlüsselverteilung.

Geprüfte Software

Qualität von Software zeichnet sich durch die nachgewiesene Abwesenheit von Programmierfehlern und Schwachstellen aus. Wesentlich für die Qualität von Softwareentwicklung ist der Umfang der durchgeführten funktionalen Tests und von Schwachstellentests. Besonders sensitiv ist bei Blockchain-Anwendungen der Code von Smart Contracts. Es ist eine gute Praxis, den Quellcode, insbesondere von Smart Contracts, von den Entwickler:innen manuell und automatisiert auf mögliche Schwachstellen zu prüfen (Trail of Bits, 2020). Weitere relevante Softwaremodule wie z. B. Nutzerschnittstellen sind zu identifizieren und ebenfalls manueller und automatisierter Prüfungen im Entwicklungsprozess zu unterziehen. Die Entwicklung und Bereitstellung von Software unter einer offenen Lizenz wäre

begrüßenswert, um unabhängige Verifikationen der Korrektheit des Codes und der Abwesenheit unerwünschter Funktionalitäten durch Verbraucher:innen sowie Dritte überprüfbar zu machen.

Öffentliche Dokumentation

Angesichts der Allgegenwärtigkeit von Smartphones ist in den letzten Jahren zu beobachten gewesen, dass eine sachgerechte Dokumentation von Anwendungen durch den Hersteller oft nicht mehr frei zugänglich für Benutzer:innen verfügbar ist. Es ist eine Erwartungshaltung seitens der Nutzer:innen aufgebaut worden, dass die Bedienung von Software benutzerfreundlich und selbsterklärend ist bzw. Nutzer:innen von Entwickler:innen durch eine vorgesehene, korrekte und fehlerfreie Bedienung geführt werden und das Lesen von Dokumentation überflüssig ist. Ebenso bleiben die Architektur und Implementierung einer Smartphone-Anwendung oft nebulös, den Verbraucher:innen vorenthalten und unabhängiger Expertise nicht zugänglich. Die Bereitstellung von Benutzerdokumentation für die korrekte Benutzung von Software-Anwendungen gilt heutzutage fast schon als überholt.

Dennoch ist öffentliche Dokumentation weiterhin eine gute Praxis – gerade im Bereich der IT-Sicherheit (Common Criteria, 2017) und des Datenschutzes (Europäische Union, 2016) –, die auch für Blockchain-Anwendungen für Verbraucher:innen umgesetzt werden sollte. Neben der Funktionsweise der Nutzerschnittstellen und ggf. Installationsbeschreibungen von weiteren Werkzeugen ist für ein grundlegendes Verständnis einer Blockchain-Anwendung auch ein Architekturentwurf wesentlich sowie wichtige Hinweise zur Beachtung seitens der Verbraucher:innen, die vor möglichen Risiken oder Implikationen einer Fehlbedienung ausdrücklich warnen.

(b) Ethisch-organisatorische Anforderungsbereiche

Partizipation von Verbraucher:innen

Der freie Zugang zu einer Blockchain-Anwendung ist elementar für die Partizipation von Verbraucher:innen an neuartigen Blockchain-Anwendungen und damit an innovativen Märkten wie z. B. dezentralen Energiemärkten. Ausgehend von einem differenzierten Verbraucherverständnis ergeben sich so verschiedene Arten des Zugangs. Für technik-affine Verbraucher:innen ist ein direkter Zugang ohne unterstützende Intermediäre selbstverständlich. Bei einem indirekten Zugang ist ein Intermediär zwischen Verbraucher:innen und Blockchain-Anwendung zwischengeschaltet. Dies kann verantwortbar sein, um technologischen Hemmnissen von Verbraucher:innen und den Konsequenzen von Fehlern bei der Benutzung seitens der Verbraucher entgegenzuwirken, sodass auch ein niederschwelliges Angebot für die Teilnahme ermöglicht wird. Intermediäre

zwischen Verbraucher:innen und dem Blockchain-Netzwerk nehmen eine verantwortliche Rolle eines Vertrauensdienstleisters für Verbraucher:innen wahr. Diese Verantwortlichkeiten können z. B. die Verwaltung der Wallets der Verbraucher:innen beinhalten. Die Anwendbarkeit der eIDAS-Verordnung (Europäische Union, 2014) auf Intermediäre von Blockchain-Anwendungen könnte auf ihre Eignung geprüft werden. Ebenfalls ist eine Haftung von Vertrauensdienstleistern für ihnen anvertrauten Werte von Verbraucher:innen, die z. B. im Fall von Cyberangriffen beim Intermediär entwendet werden könnten, vorzusehen. Der Erwerb und Verkauf von Werteinheiten (Tokens) – falls erforderlich für die Partizipation bei einer Blockchain-Anwendung – ist Verbraucher:innen niederschwellig zu ermöglichen.

Fairness

In der konkreten Ausgestaltung von Smart Contracts könnte eine Benachteiligung von Verbraucher:innen gegenüber ihren Vertragspartnern implementiert werden. Beispielsweise könnte die finanzielle Bindung von Geldwerten der Verbraucher:innen in Smart Contracts in Form einer Kaution unverhältnismäßig lange erfolgen oder im Vorfeld eines Vertragsabschlusses seitens des anderen Vertragspartners bereits gefordert werden. Aus Verbrauchersicht ist auf eine ausgewogene Vertragsausgestaltung der Vertragsparteien in Smart Contracts hinzuwirken. Konkrete Regelungen in Smart Contracts sind Verbraucher:innen transparent darzustellen.

Dezentralität

Während die Dezentralität bei öffentlichen Blockchain-Basistechnologien mit hoher Marktkapitalisierung wie Bitcoin und Ethereum eine ureigene Eigenschaft der Blockchain darstellt, so ist dies bei Blockchain-Anwendungen nicht selbstverständlich gegeben. Gerade bei Verwendung von privaten Blockchainlösungen und dedizierten Anwendungen ist Vorsorge dafür zu treffen, dass der Betrieb der Netzwerkknoten in der Blockchain-Basistechnologie dezentral mit mehreren Parteien oder Anteilseignern organisiert ist. Es ist regulativ darauf hinzuwirken, dass kein:e an der Blockchain-Anwendung Beteiligte:r eine monopolistische Stellung mit mehr als 50 % der Rechenkapazität bzw. des Marktvolumens der Blockchain-Anwendung erreichen kann (Dalheimer et al., 2017). Bei Rollen mit privilegierten Befugnissen, wie z. B. bei der zentralen Blockerzeugung in privaten Blockchains, ist eine sorgfältige Prüfung der Unabhängigkeit der beteiligten Institutionen zu den Marktteilnehmer:innen erforderlich. Dies könnte eine Aufgabe für Träger von Hoheitsrechten sein.

(Öffentliche) Transparenz des Hauptbuchs

In dem Hauptbuch der Blockchain werden die getätigten Transaktionen einer Blockchain-Anwendung nachgehalten. Unabhängige Prüfungen von

Verbraucher:innen oder Dritten erfordern direkte Lese-Zugriffsmöglichkeiten auf das Hauptbuch (‚Ledger') der Blockchain. Nur so ist es zu gewährleisten, dass unabhängige Prüfungen ohne Anmeldung bei Intermediären jederzeit erfolgen können und ein freier Zugang zu Informationen sichergestellt ist. Während technisch affine Verbraucher:innen eigene Werkzeuge für den Lesezugriff einsetzen können, ist für weniger technisch affine Verbraucher:innen ein für die Blockchain-Anwendung spezifisch entwickelter Blockchain-Explorer hilfreich, in dem die Transaktionen der Blockchain-Anwendung mit einer grafischen Webansicht nachverfolgt werden können.

Datenschutz

Die Gesetzgebung zum Datenschutz soll verhindern, dass Dritte in den Besitz personenbezogener Daten gelangen, ohne dass die betroffene Person vorher zugestimmt hat (Europäische Union, 2016, Artikel 5 und Artikel 6). Dies kann durch Vermeidung der Speicherung von personenbezogenen Daten in Transaktionen und die durchgängige Verwendung von Pseudonymen erfüllt werden. Medienbrüche zwischen digitaler und analoger Welt in Marktplätzen, die eine persönliche Kontaktaufnahme erfordern (z. B. beim Gebrauchtwagenkauf), bedürfen einer gesonderten Betrachtung. Eine Prüfung einer Blockchain-Anwendung auf Speicherung datenschutzsensibler personenbezogener Daten durch unabhängige Prüfer ist zu erwägen.

Pseudonymität/Anonymität

Die Transaktionen von Verbraucher:innen werden unter einem Pseudonym getätigt, das sich aus dem öffentlichen Schlüssel der Verbraucher:innen ableitet. Eine Aufdeckung der Identität der Verbraucher:innen zu einem Pseudonym gegenüber Dritten darf nur mit ausdrücklicher Zustimmung der Verbraucher:innen oder auf Basis von gesetzlichen Vorgaben erfolgen. Eine Registrierung der Nutzer:innen durch Hinterlegung der Zuordnung von Pseudonymen und Identitäten bei vertrauenswürdigen Stellen kann bei bestimmten Blockchain-Anwendungen vorgesehen sein, um Missbrauch oder Betrugsmöglichkeiten entgegenzuwirken. Auch bei einer Nutzerregistrierung ist eine sorgfältige Prüfung der Unabhängigkeit der beteiligten Institutionen zu den Marktteilnehmer:innen erforderlich, dies könnte eine Aufgabe für Träger von Hoheitsrechten sein.

Befähigung

Die vorhandene Kompetenz und technische Affinität von Verbraucher:innen ist als sehr unterschiedlich anzunehmen. Es ist davon auszugehen, dass für eine partizipative Teilnahme an Blockchain-Anwendungen der überwiegende Teil der Verbraucher:innen erst zu befähigen ist. Die Verbraucher:innen sind darauf zu sensibilisieren, dass sensitive Daten vor Preisgabe in und außerhalb einer Blockchain-Anwendung u. U. speziell zu schützen sind.

(c) Rechtliche Anforderungen

Bestehende Rechtsgrundlagen

Auch wenn wir nun ‚neue' Anwendungen für Blockchaintechnologie erforschen, so bedeutet dies nicht, dass wir in einem rechtsfreien Raum agieren.[6] Es ist im Detail zu prüfen, wie sich bestimmte Aufgaben mittels Blockchain-Technologien bewältigen lassen, welche Rechtslage dabei *de lege lata* besteht, welche Probleme dies womöglich birgt und wie diese *de lege ferenda* zu lösen sein könnten. Wenn wir einen Smart Contract in einer Blockchain-Anwendung vorsehen, so heißt dies nicht, dass wir es hier mit einem Vertragsschluss zu tun hätten, für den bislang noch keine Rechtsgrundlage vorhanden wäre; es ist nicht einmal *ex ante* selbstverständlich und sicher, ob durch eine selbstausführende (*self-executing*) Anwendung ein Vertrag auf der Grundlage des anzuwendenden Zivilrechts unserer Rechtsordnung zustände käme. Mit anderen Worten: Was ‚Contract' heißt, muss noch lange keinen ‚Vertrag' im Rechtssinne darstellen. Dafür kommt es nach dem Bürgerlichen Gesetzbuch (BGB) nach wie vor auf Angebot und Annahme, einander entsprechende Willenserklärungen von mindestens zwei Parteien, an. Ob und unter welchen Voraussetzungen ein ‚Vertrag' im Rechtssinn geschlossen wird, ob und wie dieser rückabgewickelt werden kann, welche Gewährleistungsrechte entstehen, wann ein Schadensfall vorliegt und wie die Beweislast für diesen ggf. verteilt ist, kann nur im Wege juristischer Interpretation ermittelt werden, nicht aber durch eine ‚Aussage', einen Output des technischen Systems selbst.[7]

Smart Contracts, Ethik und Recht

An dieser Stelle kann keine vertiefte Prüfung der rechtlichen Einordnung von Smart Contracts nach der deutschen oder einer anderen Rechtsordnung erfolgen. (Dazu siehe zum Beispiel Governatori et al. (2018); Durovic und Janssen (2019); DiMatteo und Poncibo (2019); De Filippi und Hassan (2016); Weber (2018). Klassisch noch immer: Szabo (1997).) Es soll lediglich ein gewisses Bewusstsein für die Fallstricke und Herausforderungen der rechtlichen Beurteilung von Smart Contracts geschaffen werden. Die Anforderungen an Blockchain-Technologie, die sich aus der geltenden Rechtslage ergeben, müssen zudem nicht mit Anforderungen aus ethischer bzw. aus einer Verbraucherschutzperspektive übereinstimmen. Vielmehr gehört es zu den Aufgaben der normativen Wissenschaften, das geltende Recht einer ethischen Prüfung zu unterziehen, dabei u. a. Verbraucherschutzinteressen als Maßstäbe und Kriterien anzusetzen, etwaige

---

6 Vgl. Oster (2021, 102): „Yet the absence of specific regulation concerning a technology, such as blockchain, does not mean that such systems operate outside the law." Anderer Auffassung ist Yeung (2019).

7 Vgl. Oster (2021, 10): „[…] machine cannot interpret a legal term or attribute a certain value to a legally protected interest." Ebenfalls ibid., 114: „[…] the technology of smart contracts does not constitute a new contract law; instead, the interpretation and validity of smart contracts has to be assessed against the backdrop of existing contract law." Dazu vgl. auch Azzopardi et al. (2016).

rechtliche Schutzlücken zu identifizieren und rechtspolitische Empfehlungen zu formulieren. Ethische Anforderungen, technische Möglichkeiten, die rechtlichen Möglichkeiten nach der geltenden Rechtslage und die rechtspraktischen Möglichkeiten, den ethischen Anforderungen *de lege ferenda* zu entsprechen, sind deutlich zu unterscheiden. Eine bestimmte Blockchain-Anwendung mag technisch umsetzbar sein – sollte sie rechtlich[8] nicht darstellbar sein oder ethischen Gesichtspunkten (z. B. Verbraucherschutzinteressen) widersprechen, so ergibt sich aus der bloßen Machbarkeit allein kein Argument zugunsten ihrer Implementierung (*feasibility argument*).[9]

Auch mit Blick auf eine ‚automatisch' vorgenommene Transaktion auf Grundlage einer Blockchain-Anwendung ist der Parteiwille zu ermitteln und zu untersuchen, welche Rechtsfolge(n) die Partei(en) herbeiführen woll(t)en. So lässt sich beispielsweise fragen, ob es als ein Angebot oder als eine Einladung zur Abgabe eines Angebots (*invitatio ad offerendum*) zu interpretieren ist, wenn eine Seite, z. B. ein Autohersteller, eine Blockchain-Anwendung mit einem ausführbaren Smart Contract zur Verfügung stellt und – untechnisch gesprochen – zur Nutzung einlädt. Diese ‚Nutzung' kann in der Registrierung des soeben gekauften Autos bestehen, die impliziert, dass bestimmte nachfolgende Veränderungen am Auto ebenfalls in der Blockchain niedergelegt werden. Das würde in eine irreversible ‚Buchführung' über Unfälle, Inspektionen, Reparaturen, Tachostand, Hauptuntersuchungen usw. über die Zeit hinweg entlang der gesamten Historie des Autos münden – solange diese Ereignisse mit der Herstellersoftware verbunden werden. Diese Möglichkeiten können aus der Perspektive eines:einer einzelnen Kraftfahrzeughalter:in wünschenswert sein. Doch ist im Einzelnen zu ergründen, ob Autokäufer:innen hinreichend über diese Implikationen informiert sind, wenn sie in die Nutzung der Blockchain-Anwendung einwilligen. Es könnten – ähnlich dem ‚Beipackzettel' von Finanzprodukten – bestimmte Informationspflichten in Bezug auf das Blockchain-‚Angebot' von dem Autohersteller zu erfüllen sein. An dieser Stelle soll dieses Beispiel nur der Illustration dienen.

Festzuhalten ist, dass generell bestehende Rechtspflichten auch bei der Zurverfügungstellung von Blockchain-Anwendungen zu beachten sind, dass ‚selbstausführende' Smart Contracts die rechtlichen Rahmenbedingungen nicht in Frage stellen oder außer Kraft setzen dürfen – nur weil durch sie ‚automatisch' Prozesse in Gang gesetzt werden, die bestimmte Rechtsfolgen haben (können).[10] Selbstverständlich müssen Grundrechte der beteiligten Rechtssubjekte beachtet werden – einschließlich des Rechts auf informationelle Selbstbestimmung, das u. a. im Datenschutzrecht konkretisiert wird. Die rechtsstaatlichen Grundsätze der

---

8 Ähnlich etwa Giancaspro (2017).

9 Dies widerspricht der Implikation einer üblichen Interpretation des Ausspruchs „Code is Law", der auf Lessig (1999) zurückgeht, nämlich, so Barker (2021, 431), „dass Programmierer Wertesysteme in Technologien einschreiben."

10 Vgl. Oster (2021, 115).

Gewaltenteilung und Verhältnismäßigkeit müssen respektiert werden. Recht gilt abstrakt-generell, während Smart Contracts Einzelfallregelungen treffen (können). Recht muss nachvollziehbar, überprüfbar und gestaltbar sein. Keine rechtliche Vorkehrung gilt ‚für die Ewigkeit'; alle Verträge sind grundsätzlich nachverhandelbar. Diesen Anforderungen müssen auch Smart Contracts und DApps entsprechen.

(d) Weitere Anforderungsbereiche

Kosten

Ein oft entscheidendes Kriterium für den Erfolg einer Anwendung sind die mit der Nutzung einer Anwendung verbundenen Kosten. Daher ist es wünschenswert, die Kosten zur Verwendung einer Blockchain-Anwendung für Verbraucher:innen *erstens* möglichst gering zu halten und *zweitens* vorhersehbar zu gestalten. Als kostengünstige Basistechnologien kommen Sidechains öffentlicher Blockchains, wobei die Mehrzahl der Transaktionen außerhalb der Blockchain („off-chain") durchgeführt werden, und private Blockchains infrage. Die Kosten sollten nicht als primäres Anforderungskriterium gesetzt werden; es ist vielmehr empfehlenswert, auf die Erfüllung auch anderer Anforderungsbereiche (z. B. Dezentralität, öffentliche Transparenz des Hauptbuchs) zu prüfen.

Mehrwert und Akzeptanz

Ein Mehrwert materieller oder ideeller Natur für Verbraucher:innen muss realistisch und ohne Inkaufnahme von intransparenten Risiken in einer Blockchain-Anwendung erzielbar sein, damit Verbraucher:innen den Einsatz einer Blockchain-Anwendung erwägen und danach auch weiterführen.

4 Zusammenfassung und Ausblick

In diesem Beitrag sind ausgehend von den Grundlagen generische Anforderungsbereiche an Blockchain-Anwendungen für die Umsetzung von digitaler Verbraucherteilhabe entwickelt worden. Die technischen, ethisch-organisatorischen und rechtlichen Anforderungen sollen nachfolgend anhand dedizierter ausgewählter Anwendungen (Gebrauchtwagenmarkt, Immobilientransaktionen, Energiezertifikate, Partizipative Verfahren) konkretisiert und auf ihre Umsetzbarkeit praktisch überprüft werden. Das resultierende Ziel dieser Arbeiten ist es, zukünftig ausgehend von generischen Anforderungskatalogen Blockchain-Anwendungen so gestalten zu können, dass digitale Verbraucherteilhabe *per design* integriert werden kann. Bei alledem gilt: Voraussetzung für die Nutzung von Blockchain-Anwendungen ist auch entsprechende Kompetenz auf Seiten der Verbraucher:innen. Der Erwerb von

digitaler Kompetenz (*digital literacy*) ist notwendiger Bestandteil digitaler Teilhabe. Befähigung (Empowerment) von Verbraucher:innen als Voraussetzung digitaler Teilhabe ist als eine gemeinwohlbezogene öffentliche Aufgabe zu verstehen, soll nicht durch den Betrieb von Blockchains neue Exklusion entstehen.

Danksagung

Die Autor:innen bedanken sich für die finanzielle Unterstützung beim Bundesministerium der Justiz und für Verbraucherschutz (BMJV) im Rahmen des Verbundprojekts BlockTechDiVer (Förderkennzeichen der Teilprojekte: 28V1401A20 und 28V1401B20).

Literatur

Azzopardi, S., Pace, G. J., Schapachnik, F. und Schneider, G. (2016): Contract Automata. An Operational View of Contracts between Interactive Parties. *Artificial Intelligence and Law*, vol. 24, no. 3, pp. 203-243. doi:10.1007/s10506-016-9185-2P

Barker, T. (2021): Kap. 3.5 Internationales. Geopolitische Diplomatie und die europäische Digitalstrategie. In: Chris Piallat (Ed.), Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt (pp. 415-431). transcript. Abgerufen am 09.09.2021 unter https://www.transcript-verlag.de/media/pdf/3d/91/9e/oa9783839456590.pdf

Bundesamt für Sicherheit in der Informationstechnik (2019): Blockchain sicher gestalten. Abgerufen am 01.09.2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.html

Bundesamt für Sicherheit in der Informationstechnik (2020): Projekt 374 (Studie Blockchain) - Abschlussbericht. Abgerufen am 01.09.2021 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html

Buterin, V. (2013): Ethereum Whitepaper. Abgerufen am 01.09.2021 unter https://ethereum.org/en/whitepaper

Buterin, V., Hernandez, D., Kamphefner, T., Pham, K., Qiao, Z., Ryan, D., Sin, J., Wang, Y. und Zhang, Y. X. (2020): Combining GHOST and Casper. arXiv. https://arxiv.org/abs/2003.03052

Cachin, C. und M. Vukolić (2017): Blockchain Consensus Protocols in the Wild. arXiv. https://arxiv.org/abs/1707.01873

Common Criteria (2017): Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components. Version 3.1. Abgerufen am 01.09.2021 unter https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

Dalheimer, M., Fridgen, G., Fritz, M., Guggenberger, M., Hoeren, T., Holly, S., Kreutzer, M., Leiner, U., Nouak, A., Otto, B., Prinz, W., Rose, T., Schulte, A., Schütte, J., Schwede, C., Sprenger, P., Urbach, N., Weimert, B., Welzel, C. und Wenzel, M. (2017): Blockchain und Smart Contracts. Abgerufen am 01.09.2021 unter https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf

De Filippi, P. und Hassan, S. (2016): Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday, vol. 21, no. 12. doi:10.5210/fm.v21i12.7113

DiMatteo, L. A. und Poncibó, C. (2019): Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies. European Review of Private Law, vol. 26, no. 6,

pp. 805–824.
http://www.kluwerlawonline.com/abstract.php?area=Journals&id=ERPL2018056
Durovic, M. und Janssen, A. (2018): The Formation of Blockchain-based Smart Contracts in the Light of Contract Law. European Review of Private Law, vol. 26, no. 6, pp. 753–771. http://www.kluwerlawonline.com/abstract.php?area=Journals&id=ERPL2018053
Europäische Union (2014) : Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Abgerufen am 01.09.2021 unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910
Europäische Union (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen am 01.09.2021 unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02016R0679-20160504
Ethereum Foundation (2021): Decentralized applications (dapps). Abgerufen am 01.09.2021 unter https://ethereum.org/en/dapps
Giancaspro, M (2017): Is a “smart contract” Really a Smart Idea? Insights from a Legal Perspective. Computer Law & Security Review, vol. 33, no. 6, pp. 825–835. doi:10.1016/j.clsr.2017.05.007
Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G. und Xu, X. (2018):, On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems. Artificial Intelligence and Law, vol. 26, no. 4, pp. 377-409. doi:10.1007/s10506-018-9223-3
Hahn, A., Singh, R., Liu, C.-C. und Chen, S. (2017): Smart contract-based campus demonstration of decentralized transactive energy auctions. In: 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-5). IEEE Computer Society. doi:10.1109/ISGT.2017.8086092
Höffe, O. (2004): Wirtschaftsbürger, Staatsbürger, Weltbürger: Politische Ethik im Zeitalter der Globalisierung. Beck.
Hutt, W. H. (1940): The Concept of Consumers' Sovereignty. The Economic Journal, vol. 50, no.197, pp. 66-77. doi:10.2307/2225739
Kafeza, E., Ali, S. J., Kafeza, I. und AlKatheeri, H. (2020): Legal smart contracts in Ethereum Blockchain: Linking the dots. In L. O‘Conner (Ed.), 2020 IEEE 36th International Conference on Data Engineering Workshops (ICDEW) (pp. 18-25). IEEE Computer Society. doi:10.1109/ICDEW49219.2020.00-12
Kloiber, J. und Lindinger, E. (2021): Kap. 3.4 Vielfalt. Gestalten statt reagieren – Was wir von der Zivilgesellschaft für eine gelungene Digitalisierung lernen können. In: Chris Piallat (Ed.), Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt (pp. 395-414). transcript. Abgerufen am 09.09.2021 unter https://www.transcript-verlag.de/media/pdf/3d/91/9e/oa9783839456590.pdf
Kneip, V. (2010): Consumer Citizenship und Corporate Citizenship. Bürgerschaft als politische Dimension des Marktes. Nomos.
Koshy, P., Koshy, D. und McDaniel, P. (2014): An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In: N. Christin und R. Safavi-Naini (Eds.), Financial Cryptography and Data Security (pp. 469–485). Springer. doi:10.1007/978-3-662-45472-5_30
Kühl, E. (2016): Und plötzlich fehlen 50 Millionen Dollar. ZEIT ONLINE. Abgerufen am 01.09.2021 unter https://www.zeit.de/digital/internet/2016-06/the-dao-blockchain-ether-hack
Lessig, L. (1999): Code and other laws of cyberspace. Basic Books.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M. und Savage, S. (2016): A Fistful of Bitcoins: Characterizing Payments among Men with No Names. Communications of the ACM, vol. 59, no. 4, pp. 86-93. doi:10.1145/2896384
Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. Abgerufen am 01.09.2021 unter https://bitcoin.org/bitcoin.pdf

Noether, S. (2015): Ring Signature Confidential Transactions for Monero. Cryptology ePrint Archive, Report 2015/1098. https://ia.cr/2015/1098

Oster, J. (2021): Code is code and law is law—the law of digitalization and the digitalization of law. International Journal of Law and Information Technology, vol. 29, no. 2, pp. 101-117. doi:10.1093/ijlit/eaab004

Persky, J. (1993): Retrospectives: Consumer Sovereignty. Journal of Economic Perspectives, vol. 7, no. 1, pp. 183-191. doi:10.1257/jep.7.1.183

Reckwitz, A. (2017): Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne. Suhrkamp.

Rudolf, B. (2017): Teilhabe als Menschenrecht - eine grundlegende Betrachtung. In: E. Diehl (Ed.), Teilhabe für alle?! Lebensrealitäten zwischen Diskriminierung und Partizipation (pp. 13-43). Schriftenreihe der Bundeszentrale für politische Bildung, Bd.10155. https://www.bpb.de/shop/buecher/schriftenreihe/256651/teilhabe-fuer-alle

Stoppenbrink K. (2020): Inclusion and Recognition. In: Siep L., H. Ikäheimo und M. Quante. (Eds.), Handbuch Anerkennung (pp. 1-9). Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-19561-8_15-1

Szabo, N. (1997): The Idea of Smart Contracts. Abgerufen am 01.09.2021 unter https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Trail of Bits (2020): A Guide To Smart Contract Security Tools. Abgerufen am 01.09.2021 unter https://ethereum.org/en/developers/tutorials/guide-to-smart-contract-security-tools

Wansing, G. (2015): Was bedeutet Inklusion? Annäherungen an einen vielschichtigen Begriff. In: Th. Degener und E. Diehl (Eds.), Handbuch Behindertenrechtskonvention. Teilhabe als Menschenrecht – Inklusion als gesellschaftliche Aufgabe (pp. 43-54). Schriftenreihe der Bundeszentrale für politische Bildung, Bd.1506.

Weber, R. H. (2018): "Rose is a rose is a rose is a rose"–What about Code and Law?. Computer Law & Security Review, vol. 34, no. 4, pp. 701-706. doi:10.1016/j.clsr.2018.05.005

Wood, G. (2021): Ethereum: A Secure Decentralised Generalised Transaction Ledger. Istanbul Version 80085f7. Abgerufen am 01.09.2021 unter https://ethereum.github.io/yellowpaper/paper.pdf

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M. und Rong, C. (2019): A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8114–8154. doi:10.1109/JIOT.2019.2922538

Wüst, K. und Gervais, A. (2018): Do you Need a Blockchain?. In: L. O'Conner (Ed.), 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45–54). IEEE Computer Society. doi:10.1109/CVCBT.2018.00011

Xiao, Y., Zhang, N., Li, J., Lou, W. und Hou, Y. T. (2019): Distributed Consensus Protocols and Algorithms. In: S. Shetty, C. A. Kamhoua und L. L. Njilla (Eds.), Blockchain for Distributed Systems Security (pp. 25-50). Wiley and IEEE Press. doi:10.1002/9781119519621.ch2

Xiao, Y., Zhang, N., Lou, W. und Hou, Y. T. (2020): A Survey of Distributed Consensus Protocols for Blockchain Networks. IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1432–1465. doi:10.1109/COMST.2020.2969706

Yeung, K (2019): Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code. Modern Law Review, vol. 82, no. 2, pp. 207-239. doi:10.1111/1468-2230.12399