Kompetenzzentrum Öffentliche IT

weizenbaum institut

FORSCHUNG FÜR DEN DIGITALEN STAAT

MYTHOS BLOCKCHAIN: ZWISCHEN HOFFNUNG UND REALITÄT

Fabian Kirstein, Philipp Lämmel, Anton Altenbernd

Gefördert durch:

Bundesministerium des Innern, für Bau und Heimat

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Fabian Kirstein, Philipp Lämmel, Anton Altenbernd

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-948582-06-7

1. Auflage Oktober 2021

Fotos: ÖFIT
Icons: fontawesome

Dieses White Paper ist in Kooperation mit dem Weizenbaum-Institut entstanden. Das Weizenbaum-Institut ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Verbundprojekt (Förderkennzeichen: 16DII128 – »Deutsches Internet-Institut«).

https://www.weizenbaum-institut.de

Weitere Informationen von Fraunhofer FOKUS rund um die Thematik Blockchain unter:

https://www.blockchain-werkstatt.de

VORWORT

Selten hat eine Technologie einen so schlagartigen Hype durchlebt wie die Blockchain. Vor vier Jahren erschien unser White Paper »Mythos Blockchain – Herausforderung für den Öffentlichen Sektor« und zu dieser Zeit hielten manche die Möglichkeiten der jungen Technologie für schier grenzenlos, insbesondere für den öffentlichen Sektor. Die Blockchain versprach den Aufbau von dezentralen Dateninfrastrukturen ohne die Notwendigkeit zentraler Vermittler und Instanzen – sogenannter Intermediäre –, Prozessoptimierungen über Organisationsgrenzen hinweg und ein erhöhtes Vertrauen durch Transparenz und Fälschungssicherheit. Nun ist es Zeit für eine erneute Bestandsaufnahme und Prüfung der Zukunftsaussichten der Blockchain.

Unzählige Organisationen, Unternehmen und Forschungseinrichtungen arbeiten an Anwendungsfällen und technischen Weiterentwicklungen. Doch der wirkliche Durchbruch und der weitreichende Einsatz der Blockchain lassen weiter auf sich warten. Unsere Welt ist augenblicklich immer noch vollständig abhängig von Intermediären, die Vertrauen schaffen, als Vermittler agieren und Richtlinien durchsetzen. Sogar produktive Blockchain-Anwendungen können bis heute nicht gänzlich auf zentrale Akteure verzichten. Ist die Blockchain also an ihren eigenen Ansprüchen gescheitert? War der Hype völlig unbegründet? Tatsächlich ist die Blockchain an ihren Ansprüchen gewachsen. Das Momentum des Hypes wurde genutzt, um die Vision der Blockchain zu erweitern und die vielfältigen Potenziale von Dezentralisierung, Unveränderbarkeit und verteilter Ausführung von Computerprogrammen zu ergründen. Dabei ist ein reichhaltiges Ökosystem von Lösungsansätzen entstanden, die unseren Umgang mit Daten, Prozessen und Kommunikation in Zukunft verändern werden. Es wird nur eben nicht unmittelbar passieren und weniger sichtbar sein als bisherige Vorhaben, da sich die Blockchain zu einem Technologiebaustein von vielen entwickeln wird.

Die vergangene Diskussion um die technische Umsetzung der Corona-Warn-App hat noch einmal aufgezeigt, welche wichtige Rolle eine Dezentralisierung und ein reduzierter Einsatz von zentralen Instanzen in der Umsetzung von Dateninfrastrukturen spielen. In der Zukunft des Web und der Datenverarbeitung werden entsprechende Fragestellungen zunehmend an Bedeutung gewinnen. Die Blockchain und verwandte Technologien bieten hierfür vielfältige Lösungsansätze, die eine große Bedeutung dieser Technologien in Zukunft erwarten lassen.

In diesem White Paper geben wir einen Überblick über die Entwicklungen der Blockchain in den letzten Jahren, um ein gemeinsames Verständnis zum aktuellen Stand der Dinge zu schaffen. Dabei stellen wir die technischen Entwicklungen und beispielhafte Anwendungsfälle in den Mittelpunkt. Schließlich haben wir konkrete Schlüsselfaktoren abgeleitet und Handlungsempfehlungen für den zukünftigen Einsatz der Blockchain zusammengestellt.

Wir wünschen eine anregende Lektüre!
Ihr Kompetenzzentrum Öffentliche IT

EIN GEMEINSAMES VERSTÄNDNIS DER BLOCKCHAIN IST FÜR IHRE ERFOLGREICHE WEITERENTWICKLUNG UNERLÄSSLICH.

INHALTSVERZEICHNIS

1. THESEN

Der Hype um die Blockchain ist vorbei – Das ermöglicht den Blick auf realistische Anwendungsfelder.
Die umfangreiche Medienpräsenz der Blockchain ist abgeflacht und die erwartete Umwälzung ist bisher ausgeblieben. Dennoch haben sich eine vielfältige, aktive Community und eine Start-up-Szene entwickelt, die praktische Lösungen und Produkte auf Basis der Blockchain entwickeln. Darüber hinaus untersuchen Forschungseinrichtungen zahlreiche Detailfragen, um einen produktiven Einsatz der Blockchain zu ermöglichen. Die Erkenntnisse und Erfahrungen ermöglichen eine neue Einschätzung potenzieller Anwendungen der Blockchain.

Es gibt kein einheitliches Verständnis von der Blockchain.
Der Hype um die Blockchain hat zu einem verschwommenen Einsatz des Begriffes geführt. Blockchain wird häufig als Synonym für verschiedenste Systeme verwendet: Kryptowährung, Datenbank, Register, verteilter Computer oder dezentrale Datenverarbeitung. Damit treten die tatsächlichen Eigenschaften in den Hintergrund und eine sinnvolle Bewertung von Anwendungsfällen wird erschwert. Andererseits unterliegt die Technologie einer dynamischen Entwicklung, die eine scharfe Definition erschwert.

Die Blockchain ersetzt keine zentralen Dienste.
Blockchain-Nutzung als vollständiger Ersatz für vertrauensbildende Intermediäre ist kaum umsetzbar und erzeugt neue Hürden. Bei vielen Anwendungsfällen zeigt sich daher ein Trend hin zu zentralen Vermittlern und Plattformen, wie beispielsweise Anbietern von Wallets für Kryptowährungen. Die Gründe dafür liegen hauptsächlich in der hohen Komplexität und geringen Nutzungsfreundlichkeit eines dezentralen Systems. Darüber hinaus hat sich gezeigt, dass eine Absicherung durch etablierte Institutionen weiterhin notwendig ist und verlangt wird. Die Blockchain ist eine ergänzende Technologie.

Die Blockchain ist eine Infrastruktur- und Basistechnologie.
Die Blockchain ist ein Technologiebaustein für den Aufbau von komplexen und modernen IT-Systemen und sollte nicht mit grundsätzlicher Digitalisierung gleichgesetzt werden. Analog zu Datenbanksystemen, Software-Frameworks oder Kommunikationsprotokollen erfüllt die Blockchain einen konkreten Zweck. Sie dient der Koordination und Vernetzung einer Vielzahl von Akteuren über Organisationsgrenzen hinweg und ermöglicht die sichere Dokumentation von Datenänderungen und Transaktionen. Ihr Einsatz ist sinnvoll in Umgebungen, in denen Manipulationsanreize bestehen oder Vertrauen rar ist. Ein Blockchain-Einsatz löst spezifische Probleme, ist aber kein Allerheilmittel für die Herausforderungen der digitalen Transformation, die auch organisatorische Veränderungen erfordern. Die Blockchain ersetzt keine notwendigen organisatorischen Transformationsprozesse.

DSGVO und Blockchain stehen in einem lösbaren Konflikt.
Die Datenschutz-Grundverordnung sieht ein »Recht auf Vergessen« vor. Dieser Grundsatz und die Unveränderbarkeit der gespeicherten Daten in der Blockchain stehen im Widerspruch. Jegliche Informationen, die einen Personenbezug aufweisen, können daher nicht in einer Blockchain gespeichert werden. Trotzdem kann eine Blockchain auch in Anwendungen eingesetzt werden, die personenbezogene und sensitive Daten verarbeiten. Aktuelle Forschungsprojekte geben erste Antworten auf dieses Dilemma.

Abseits von Kryptowährungen muss die Blockchain ihre Rolle noch finden.
Unabhängig von ihrem echten Nutzen haben sich zahlreiche Kryptowährungen als produktiv funktionierende Systeme auf Blockchain-Basis etabliert. Das Bitcoin-Netzwerk wird täglich von Millionen von Nutzer:innen verwendet, die hunderttausende von Transaktion ausführen. Über Kryptowährungen hinaus kann kein Szenario eine echte Community vorweisen. Typische Anwendungsfälle, wie Logistik, Produktionsketten, Dokumentenintegrität und Beweiswerterhaltung, befinden sich höchstens in einem prototypischen Stadium. Die Erprobung und Evaluation unter realen Bedingungen stehen weiterhin aus.

2. EINLEITUNG

Mehr als zehn Jahre sind seit der Veröffentlichung von Satoshi Nakamotos Paper »Bitcoin: A Peer-to-Peer Electronic Cash System« vergangen.[1] Seitdem hat sich die dadurch begründete Technologie Blockchain auf vielfältige Weise weiterentwickelt. Neben Bitcoin wurden mehrere Tausend Kryptowährungen veröffentlicht, deren Nutzer:innen häufig auf schnelle Spekulationsgewinne hofften.[2] Ähnlich viel Beachtung fanden Einsatzmöglichkeiten der jungen Technologie jenseits von digitalen Währungen. Die Blockchain versprach eine transparente und manipulationssichere Ausführung von Transaktionen zwischen verschiedenen Parteien ohne die Notwendigkeit einer zentralen Instanz oder Organisation. Aus einfachen Werttransaktionen wurden der Austausch ganzer Datensätze sowie die Ausführung digitaler Verträge. Die Blockchain wurde als die Lösung für sicheres Datenmanagement in jeder Form gehandelt, wobei die grundsätzlichen und ursprünglichen Charakteristiken der Technologie in den Hintergrund traten. Es entwickelten sich technische Abwandlungen und Ableger des ursprünglichen Konzeptes, um die neuen Anwendungsfälle aufzugreifen. Der Begriff Blockchain steht daher nicht mehr nur für eine Technologie, sondern hat sich zu einem Sammelbegriff für eine ganze Reihe von Produkten, Architekturen und Protokollen entwickelt. Diese Entwicklung ist zum einen positiv zu bewerten, da sie das Innovationspotenzial der Kernidee einer Blockchain zeigt. Zum anderen erschwert die Vielfalt der Aspekte eine generelle Beurteilung der grundlegenden Blockchain-Prinzipien für konkrete Anwendungsfälle. Darüber hinaus haben sich in den letzten Jahren zahlreiche praktische Hindernisse beim Einsatz einer Blockchain gezeigt. Dazu zählen technische Limitierungen wie die begrenzte Skalierbarkeit oder ein hoher Energieverbrauch. Außerdem existieren Barrieren für die praktische Nutzbarkeit wie das häufig komplexe Identitätsmanagement. Schließlich hat die Unveränderlichkeit und Transparenz der Blockchain für Verunsicherung bei rechtlichen und Datenschutz-relevanten Gesichtspunkten geführt.

2.1 BLOCKCHAIN ALS TREND UND INNOVATIONSMOTOR

Die Potenziale der Blockchain sind Gegenstand der Aktivitäten zahlreicher Organisationen, Unternehmen und Initiativen. Die Auseinandersetzung umfasst dabei neben technischen Fragestellungen insbesondere rechtliche und politische Gesichtspunkte. Sinnbildlich dafür ist, dass sich die finanziellen Investitionen in Blockchain-Start-ups in Europa bis 2018 auf fast acht Milliarden Euro summiert haben[3]. Zahlreiche etablierte Unternehmen, insbesondere aus der Finanzindustrie, haben Systeme auf Blockchain-Basis umgesetzt und evaluieren deren Nutzen. Dadurch sind bereits mehrere Hundert Live-Systeme bekannt.[4]

Die Relevanz, die der Blockchain zugemessen wird, zeigt sich zudem in der Gründung nationaler und europäischer Initiativen, die sich ihrer Förderung und Erforschung verschrieben haben. In Deutschland ist der Blockchain Bundesverband[5] ein Netzwerk mit über 100 Mitgliedern, dessen Ziel die Erhöhung des Bewusstseins für die junge Technologie auf politischer Seite ist. Dazu zählt auch die Initiative »Blockchain in der Verwaltung in Deutschland« (BiVD)[6], die insbesondere den Blockchain-Einsatz im öffentlichen Sektor untersucht. Im September 2019 wurde schließlich die Blockchain-Strategie der Bundesregierung verabschiedet.[7] Die Strategie beinhaltet detaillierte Maßnahmen, um die starke Position Deutschlands weiter auszubauen und umfasst Innovations- und Investitionsvorhaben zu nahezu allen bekannten Blockchain-Anwendungsfällen. Die Umsetzung der Strategie geht allerdings bisher nur langsam voran und nur wenige konkrete Projekte wurden umgesetzt[8]. Auch die Europäische Kommission hat vielfältige Impulse gesetzt. Das EU

[1] Nakamoto, S.: »Bitcoin: A peer-to-peer electronic cash system«, 2008.

[2] Coinranking: »Cryptocurrency Prices Live – Rates List Today«, https://coinranking.com/, abgerufen: 21. Juli 2020.

[3] Nascimento, S. et al.: »Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies«, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-08977-3.

[4] Rauchs, M. et al.: »2nd Global Enterprise Blockchain Benchmarking Study«, 2019, doi:10.2139/ssrn.3461765.

[5] Bundesblock: »Blockchain Bundesverband«, https://bundesblock.de/, abgerufen: 21. Juni 2020.

[6] Govchain-Blog: »BiVD – Blockchain in der Verwaltung in Deutschland«, https://govchain-blog.de/bivd-eine-initiative-fuer-deutschland/, abgerufen: 16. August 2021.

[7] Blockchain-Strategie: »Online-Konsultation zur Blockchain-Strategie der Bundesregierung«, https://www.blockchain-strategie.de/, abgerufen: 21. Juli 2020.

[8] Heise.de: https://www.heise.de/news/Blockchain-Strategie-der-Bundesregierung-lieferte-bislang-wenig-Ergebnisse-6114983.html, abgerufen: 23. Juni 2020.

EIN BLOCKCHAIN-SYSTEM BESTEHT IN DER REGEL AUS DREI ELEMENTEN: EINER BLOCKCHAIN, EINEM NETZWERK UND EINEM PROTOKOLL.

Blockchain Observatory and Forum[9] bietet einen zentralen Anlaufpunkt und eine Datensammlung für europäische Aktivitäten rund um die Blockchain und leitet aus den vielfältigen Aktivitäten Empfehlungen und fachliche Berichte ab. Die European Blockchain Services Infrastructure (EBSI)[10] plant den Aufbau einer rechtskonformen, staatenübergreifenden Infrastruktur für die öffentliche Verwaltung. Ein erster Prototyp ist bereits verfügbar und wird durch geförderte Forschungsprojekte evaluiert. Aufseiten der Industrie gilt die Region Berlin als Hotspot junger Unternehmen, die im Blockchain-Kontext aktiv sind. Zahlreiche Start-ups bieten Beratungsangebote, Anwendungsentwicklung oder Infrastrukturlösungen an.[11] Der Fokus liegt dabei auf typischen Anwendungsfällen, wie Geldtransaktionen, sicherer Nachverfolgung und neuartigen Handelsplattformen. Diese beispielhaften Aktivitäten zeigen, dass der Blockchain-Hype konkreten Entwicklungen und einem sachlichen Diskurs weicht. Akteure aus Wissenschaft, Wirtschaft und Politik sind sich der Potenziale der »Blockchain-Idee« bewusst und transformieren den Trend in innovative Lösungen und Konzepte.

2.2 WAS IST EINE BLOCKCHAIN?

Eine einheitliche und eindeutige Definition der Blockchain konnte sich bisher nicht etablieren. Eine klare Abgrenzung zu verwandten Technologien findet sich im öffentlichen Diskurs und in Produktinformationen häufig nicht. Am umfassendsten kann eine Blockchain als **Multi-Party Consensus System (Mehrparteien-Konsenssystem)**[12] beschrieben werden. Diese Definition ermöglich bereits eine Ableitung möglicher Anwendungsfälle. Allerdings haben sich weitere Begriffe und Definitionen im Blockchain-Kontext etabliert, die eine genauere Differenzierung ermöglichen. In Anlehnung an Xu et al.[13] werden im Folgenden die wichtigsten dieser Begriffe definiert.

Ein **Distributed Ledger** ist ein Register von Transaktionen, das über viele Computer verteilt gespeichert wird. Eine **Blockchain** ist ein Distributed Ledger, das als verkettete Liste von Blöcken organisiert ist, wobei jeder Block eine sortierte Liste von Transaktionen enthält. Ein **Blockchain-System** besteht in der Regel aus drei Elementen: einer Blockchain, einem Netzwerk und einem Protokoll. Das Netzwerk ist die Gesamtheit aller beteiligten Computer, auch **Nodes** (Knoten) genannt, und deren Verknüpfung. Das Protokoll spezifiziert die Kommunikation innerhalb des Netzwerkes und die zulässigen Aktionen der Knoten. Es umfasst Rechte, Pflichten, Verifikation, Validierung und Konsens zwischen den Teilnehmern. Eine **public Blockchain** ist ein Blockchain-System, bei dem das Netzwerk offen und eine Teilnahme ohne Genehmigung jederzeit möglich ist. Jeder Knoten kann neue Transaktionen verifizieren. Das konkrete Protokoll beinhaltet hier einen Anreizmechanismus, der das korrekte (protokollgemäße) Verhalten des Systems sicherstellt. Eine **Blockchain-Plattform** ist die technische Grundlage (das Framework), um ein konkretes Blockchain-System zu betreiben. Ein **Smart Contract** ist ein Computerprogramm, das auf einer Blockchain ausgeführt wird. Es verwaltet digitalen Besitz, der durch die Blockchain repräsentiert wird und wird häufig zur Abbildung von rechtlichen Verträgen verwendet. Eine Softwareanwendung, die hauptsächlich mit einem Smart Contract interagiert, wird als **Decentralized Application** oder **DApp** bezeichnet. Sie bildet damit die Anwendungsebene von Blockchain-Lösungen.

[9] EUBlockchain: »EU Blockchain Observatory and Forum«, https://www.eublockchainforum.eu, abgerufen: 22. Juli 2020.

[10] EBSI: »European Blockchain Services Infrastructure«, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI, abgerufen: 21. Juli 2020.

[11] BerChain: »BerChain – Connecting and promoting Blockchain for Berlin«, https://berchain.com/, abgerufen: 21. Juli 2020.

[12] Rauchs, M. et al.: »2nd Global Enterprise Blockchain Benchmarking Study«, 2019, doi:10.2139/ssrn.3461765.

[13] Xu, X.; Weber, I.; Staples, M.: »Architecture for blockchain applications«, 2019, Springer International Publishing, doi:10.1007/978-3-030-03035-3.

Allgemein hat sich eine Unterscheidung zwischen vier Blockchain-Typen etabliert. Eine **public permissionless** Blockchain ist öffentlich und (zumindest prinzipiell) weltweit zugänglich, eine Teilnahme ist uneingeschränkt möglich. Bei einer **public permissioned** Blockchain unterliegt die Teilnahme individuellen, festgelegten Beschränkungen. Analog dazu existieren **private permissionless** Blockchains, die nur innerhalb eines Konsortiums sichtbar, an denen aber alle Konsortialmitglieder uneingeschränkt teilnehmen können. Bei einer **private permissioned** Blockchain ist der Zugang innerhalb des Konsortiums zusätzlich limitiert und reguliert.

Eine zentrale Eigenschaft einer Blockchain und wichtiges Unterscheidungsmerkmal zu anderen Systemen ist die **Immutability (Unveränderlichkeit)**. Daten und Transaktionen, die in der Blockchain gespeichert werden, lassen sich in der Regel im Nachhinein nicht mehr ändern oder löschen, können aber durch weitere Transaktionen in einen »historischen« Zustand versetzt werden.

Neben diesen technischen Definitionen kann der Blockchain-Begriff auch als Synonym für Verhaltens- und Prozesswandel innerhalb und außerhalb einer Organisation gesehen werden. Dabei wirken die Grundideen der Blockchain von Dezentralisierung und Transparenz als Katalysator für Transformationen, die von der eigentlichen Blockchain-Technik losgelöst sind. Dieser Prozess wird als **Blockchain Meme** (in etwa: »Blockchain-Imitation«) bezeichnet. In der Realität handelt es sich bisher bei den meisten Blockchain-Projekten um diese organisatorische Ausprägung. Im Rahmen einer Untersuchung von über 60 Industrie-Blockchain-Netzwerken erfüllten nur zwei die Anforderungen an ein Blockchain-System im engeren Sinne.[14] Einer der Gründe hierfür sind die bestehenden, technischen Herausforderungen bei der Umsetzung von Blockchain-Anwendungen. Unternehmen möchten von den Blockchain-Potenzialen profitieren, ohne sich allen damit verbunden Herausforderungen zu stellen.

Die hier vorgestellten Definitionen sind bereits breiter gefasst als das ursprüngliche Konzept von Bitcoin und respektieren damit die Entwicklungen der letzten Jahre. Insbesondere ist festzuhalten, dass in der Weiterentwicklung der Blockchain-Idee Aspekte des Vertrauens eine untergeordnete Rolle spielen, während die Optimierung von Prozessen und Organisationsstrukturen in den Vordergrund rückt. Im Folgenden wird der Begriff Blockchain im weiteren Sinne für alle hier beschriebenen Varianten und Teilaspekte verwendet.

[14] Rauchs, M. et al.: »2nd Global Enterprise Blockchain Benchmarking Study«, 2019, doi:10.2139/ssrn.3461765.

3. STAND DER TECHNIK

Blockchain ist weiterhin eine junge Technologie und unterliegt ständigem technischen und konzeptionellen Wandel. Viele Defizite und Verbesserungspotenziale wurden früh erkannt und entsprechende Lösungsansätze werden aktiv entwickelt. Anhand dieser lassen sich die aktuellen technischen Entwicklungen nachzeichnen. Grundsätzliche Bedenken existieren in Bezug auf die allgemeine **Informationssicherheit** der Blockchain, insbesondere im Zusammenhang mit der **Datenschutzgrundverordnung (DSGVO)**. Die verteilte Struktur und die Unveränderbarkeit einer Blockchain erschweren die Durchsetzung zentraler Sicherheitskonzepte, die Durchsetzung von Ansprüchen bezüglich personenbezogener Daten und die schnelle Schließung von Sicherheitslücken. Durch die Komplexität der Mechanismen und Verteilung der Daten wird der Blockchain-Technik eine schlechte **Skalierbarkeit** für umfangreiche Anwendungsfälle unterstellt. Als besonders problematisch gilt der sehr hohe **Energieverbrauch** vieler Ausprägungen, der insbesondere im Zusammenhang mit dem sogenannten Mining im Rahmen der Kryptowährung Bitcoin diskutiert wurde. Hierbei spielen verschiedene **Konsensverfahren** eine entscheidende Rolle. Schließlich kann eine Blockchain hinsichtlich **Nutzungsfreundlichkeit** nicht mit zentralen Verfahren mithalten. Die Nutzer:innen tragen häufig mehr Verantwortung für ihre Zugangsdaten und müssen sich unmittelbar mit kryptografischem **Schlüsselmanagement** auseinandersetzen. Im Folgenden werden diese häufig diskutierten Hürden aufgegriffen und dem aktuellen technischen Stand der Blockchain-Entwicklung gegenübergestellt. Darüber hinaus werden weitere aktuelle Entwicklungen vorgestellt, wie Smart Contracts und eine Auswahl an produktiv einsetzbaren **Blockchain-Plattformen**.

3.1 ENERGIEVERBRAUCH UND KONSENSVERFAHREN

Ein grundsätzlicher Kritikpunkt an der Blockchain ist der hohe Energieverbrauch, den der Betrieb des Netzwerkes verursacht. Bei deutlich divergierenden Schätzungen wurde zum Beispiel der Energieverbrauch des Bitcoin-Netzwerkes im Juli 2020 mit fast 60 TWh pro Jahr beziffert.[15] Das entspricht ca. 0,2 Prozent des weltweiten Energieverbrauchs.[16] Angesicht der weltweiten Klimakrise kann dieser Umstand durchaus als K.-o.-Kriterium für den Einsatz einer Blockchain gesehen werden, zumal noch viele weitere energieintensive Blockchains existieren. Allerdings hängt der tatsächliche Energieverbrauch einer Blockchain-Lösung von ihrer konkreten technischen Umsetzung ab. Der mit Abstand bedeutendste Faktor für den Energieverbrauch ist das sogenannte Konsensverfahren. In einer Blockchain beschreiben die Blöcke mit den enthaltenen Transaktionen den Zustand des Systems. Das Konsensverfahren beschreibt den Prozess, wie sich die Knoten des Netzwerkes auf den Zustand einigen. Neben dem Energieverbrauch bestimmt das konkrete Konsensverfahren auch Eigenschaften wie Skalierbarkeit, Sicherheit und Grad der Dezentralität.

Bitcoin setzt auf das ausgereifte und bekannteste Konsensverfahren **Proof of Work (PoW)**, dessen Grundlage die Lösung eines sehr rechenintensiven mathematischen Rätsels für jeden neuen Block ist. Alle Knoten, die sich aktiv beteiligen, versuchen gleichzeitig, dieses Rätsel zu lösen. Durch die Schwierigkeit des Rätsels ist gewährleistet, dass die Generierung eines neuen Blockes stets eine gewisse Zeit dauert. Die Lösung des Rätsels erfordert den Einsatz von viel Rechenleistung und damit auch viel elektrischer Energie. Für die korrekte Lösung des Rätsels erhalten die Besitzer:innen des ersten erfolgreichen Knotens einen Gewinn in der jeweiligen Kryptowährung. Dadurch wird ein Anreiz geschaffen, die Integrität und Korrektheit des Blockchain-Systems zu erhalten. Der Einsatz von Rechenleistung, um falsche oder korrumpierte Blöcke zu generieren, ist nicht lohnenswert und wird aufgrund des protokollkonformen Verhaltens vieler Knoten mit sehr hoher Wahrscheinlichkeit und sehr schnell aufgedeckt.

Es gibt auch alternative Konsensverfahren, die einen weitaus geringeren Energieverbrauch aufweisen. Zu den bekanntesten Vertretern zählt **Proof of Stake (PoS)**, bei dem neue Blöcke von Teilnehmer:innen generiert werden, die das größte Vermögen (Kryptowährung) vorweisen können. Dieses Vorgehen folgt der Annahme, dass Nutzer:innen mit großem Vermögen nicht daran interessiert sind, die Blockchain zu manipulieren. Sie wet-

[15] CBECI: »Cambridge Bitcoin Electricity Consumption Index«, https://www.cbeci.org/, abgerufen: 21. Juli 2020.

[16] Baraniuk, C.: »Bitcoin's energy consumption ›equals that of Switzerland‹«, BBC, https://www.bbc.com/news/technology-48853230, abgerufen: 03. Juli 2019.

ten also mit ihrem Vermögen als Einsatz darauf, einen korrekten Block zu erzeugen. Es existieren verschiedene Umsetzungen des PoS-Mechanismus sowie Kombinationen aus PoS und PoW, wie beispielsweise Peercoin[17]. Bekannte Konsensverfahren, die auf PoS aufbauen, sind Ouroboros[18] und Snow White[19]. Diese bestimmen rundenweise randomisiert abhängig vom Vermögen ein Komitee, das dann einen neuen Block erstellt und dem Netzwerk vorschlägt.

Ein klassisches Konsensverfahren, das schon vor der Blockchain in verteilten Systemen verbreitet eingesetzt wurde, ist **Practical Byzantine Fault Tolerance (PBFT)**[20]. Es wird hauptsächlich in permissioned Blockchains (wie Hyperledger Fabric[21]) eingesetzt. Die Grundidee ist simpel: Alle aktiven Knoten kommunizieren miteinander und einigen sich per (demokratischer) Abstimmung auf den korrekten nächsten Block. Daher ist dieses Verfahren eher für geschlossene Systeme geeignet, in denen zwischen den Teilnehmer:innen ein Grundvertrauen besteht. Da der Kommunikationsaufwand mit der Anzahl der Knoten steigt, wird PBFT vorzugsweise bei kleineren Netzwerken eingesetzt. Im Vergleich zu PoW, wo mindestens die Hälfte der Rechenleistung aller aktiven Knoten auf ehrliche Weise verwendet werden muss, um Manipulation zu verhindern, sind es bei PBFT mindestens zwei Drittel aller Knoten, die jeweils über eine Stimme verfügen. In einer permissioned Blockchain sind normalerweise alle Knoten bekannt und die Wahrscheinlichkeit ist sehr gering, dass sich mehr als ein Drittel unehrlich verhält.

Häufig werden Weiterentwicklungen von PBFT eingesetzt. Beispielsweise setzt die Blockchain-Lösung Tendermint[22] auf eine Kombination aus PBFT und PoS und koppelt Stimmrechte an das Vermögen. Durch den Einsatz des sogenannten **Gossip-Protokolls** ist die Kommunikation stark optimiert. Dabei werden Informationen analog zu epidemiologischem Verhalten weitergetragen. Sobald ein Knoten eine neue Information erhält, wird diese an Knoten weitergetragen, zu denen eine Verbindung besteht. Dadurch muss nicht jeder Knoten mit jedem anderen Knoten kommunizieren und Informationen können indirekt weitergetragen werden.[23]

Im Wesentlichen versprechen alternative Konsensverfahren viele Vorteile gegenüber dem etablierten PoW-Ansatz, wie z. B. eine geringe Verzögerung bei der Bestätigung von Transaktionen sowie einen deutlich geringeren Energieverbrauch. Jedoch entstehen neue und andere Angriffsvektoren, wie zum Beispiel die Nothing-at-Stake- und Long-Range-Attacke, zumal sich die entsprechenden Lösungen noch in der Entwicklung befinden bzw. noch nicht ausgereift sind. Nur bei wenigen Algorithmen konnte die Korrektheit bisher mathematisch bewiesen werden. Darüber hinaus besteht beim PoS die Gefahr der Zentralisierung durch sogenannte Stake-Pools, in denen Teilnehmer:innen sich zusammenschließen, um mit höherer Wahrscheinlichkeit die Belohnung für einen neuen Block erhalten zu können.[24] Grundsätzlich gilt, dass die Wahl eines Konsensverfahrens immer auf einer Abwägung aus Sicherheit, Performanz, Energieverbrauch

[17] Peercoin: »Peercoin – Pionier des Proof of Stake«, https://www.peercoin.net/, abgerufen: 21. Juli 2020.

[18] Kiayias, A. et al.: »Ouroboros: A provably secure proof-of-stake blockchain protocol«, in: Advances in Cryptology – CRYPTO 2017 Part I, S. 357 – 388, Springer International Publishing, doi:10.1007/978-3-319-63688-7_12.

[19] Bentov, I.; Pass, R.; Shi, E.: »Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake«, International Conference on Financial Cryptography and Data Security. Springer, Cham, 2019, doi:10.1007/978-3-030-32101-7_2.

[20] Castro, M.; Liskov, B.: »Practical Byzantine fault tolerance«, in: 3rd Symposium on Operating Systems Design and Implementation (OSDI 99), 1999, S. 173 – 186.

[21] The Linux Foundation: »Hyperledger Fabric«, https://www.hyperledger.org/use/fabric, abgerufen: 01. Dezember 2020.

[22] Tendermint: »Tendermint Documentation«, https://docs.tendermint.com, abgerufen: 01. Dezember 2020.

[23] Tanenbaum, A. S.; Van Steen, M.: »Distributed systems: principles and paradigms«, 2007, Prentice-Hall, ISBN 978-0-13239-227-3.

[24] Nguyen, C. T. et al.: »Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities«, IEEE Access, Volume 7, 2019, S. 85727 – 85745, doi:10.1109/ACCESS.2019.2925010.

DER MIT ABSTAND BEDEUTENDSTE FAKTOR FÜR DEN ENERGIEVERBRAUCH IST DAS SOGENANNTE KONSENSVERFAHREN.

und weiteren Aspekten beruht. Gleichzeitig stellt das Konsensverfahren den zentralen Aspekt und die Grundlage einer konkreten Blockchain dar. Bisher konnte sich zumindest in öffentlichen Blockchains nur das energieintensive PoW behaupten. Es gibt also erheblichen Forschungs- und Entwicklungsbedarf insbesondere im Bereich der Grundlagen.

3.2 SKALIERBARKEIT

Die Blockchain bietet derzeit im Vergleich zu zentralisierten Systemen eine geringere Skalierbarkeit. Konkret nimmt ihre Leistungsfähigkeit, die über den Durchsatz und die Verzögerungszeit definiert ist, mit steigender Zahl von Nutzer:innen und Transaktionen ab.[25] Das hat direkte Auswirkungen auf die Einsatzfähigkeit für bestimmte Anwendungsfälle, da die Funktionalität ggf. nur für eine begrenzte Anzahl an Nutzer:innen gewährleistet werden kann. Beispielsweise ist die Kreditkartengesellschaft Visa in der Lage, weit über tausend Transaktionen pro Sekunde abzuwickeln[26]. Bitcoin bietet mit gerade einmal 7 Transaktionen pro Sekunde einen wesentlich geringeren Durchsatz[27]. Andere Blockchains mit Kryptowährungen (wie Ethereum) sind mit einem nur geringfügig höheren Durchsatz ebenfalls nicht konkurrenzfähig. Zudem werden Transaktionen, die über Visa getätigt werden, innerhalb weniger Sekunden abgewickelt[28]. Transaktionen, die über eine Blockchain getätigt werden, haben eine weitaus höhere Verzögerungszeit.

Die geringe Skalierbarkeit ist grundsätzlich systembedingt. Alle Knoten oder ein großer Teil der Knoten des Netzwerkes müssen miteinander kommunizieren und alle Daten austauschen, um jederzeit eine gemeinsame Sicht auf das System zu ermöglichen. Diese Übertragungen benötigen Zeit. Darüber hinaus haben Funktionsweise und Datenstruktur der Blockchain Einfluss auf die Skalierbarkeit. Wichtige Faktoren sind hier die **Blockgröße**, die **Blockzeit** und das **Konsensverfahren**. Die Blockgröße beschreibt, wie viele Transaktionen in einem Block zusammengefasst werden. Die Bestätigung einer Transaktion ist also von der Verarbeitung anderer Transaktionen abhängig. Die Blockzeit ist die Zeitperiode, in der ein neuer Block generiert wird, also die Zeit, in der sich das Netzwerk auf einen korrekten neuen Block einigt. Diese Zeit ist abhängig vom gewählten Konsensverfahren. Die Lösung des mathematischen Rätsels im etablierten Verfahren PoW benötigt beispielsweise Zeit, die im Wesentlichen von der Komplexität des zu lösenden Rätsels abhängt. Anpassungen der Blockgröße, der Blockzeit oder des Konsensverfahrens haben jedoch nicht nur Einfluss auf die Skalierbarkeit der Blockchain, sondern immer auch auf die Sicherheit und Dezentralität des Systems.[29]

In den letzten Jahren wurden verschiedene Verfahren entwickelt, um die Skalierbarkeit maßgeblich zu verbessern. Zu den vielversprechendsten zählen sogenannte **Off-Chain**-Lösungen, bei denen die Blockchain entlastet wird und Transaktionen außerhalb des eigentlichen Netzwerkes abgewickelt werden. Das hat den Vorteil, dass Parameter der Blockchain und damit die Sicherheit nicht beeinflusst werden. Zu den Off-Chain-Lösungen zählen Payment Channels und das Konzept der Sidechains.

[25] Zhou, Q. et al.: »Solutions to scalability of blockchain: A survey«, IEEE Access, Volume 8, 2020, S. 16440 – 16455, doi:10.1109/ACCESS.2020.2967218.

[26] Li, K.: »The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed«, Hackernoon, https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44, abgerufen: 26. Januar 2019.

[27] Bitcoin Wiki: »Scalability - Bitcoin Wiki«, https://en.bitcoin.it/wiki/Scalability, abgerufen: 21. Juli 2020.

[28] Visa: »Visa – Fact Sheet«, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf, abgerufen: 01. Dezember 2020.

[29] Antonopoulos, A. M.; Osuntokun, O.; Pickhardt, R.: »Mastering the Lightning Network«, 2020, https://github.com/lnbook/lnbook, abgerufen: 21. Juli 2020.

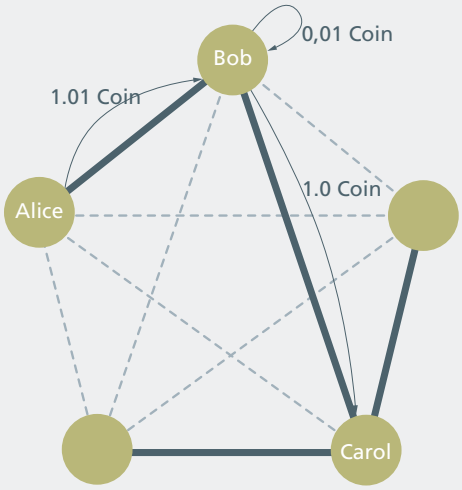


Abbildung 1:
Lightning Network

Payment Channels basieren auf der Grundidee, die Anzahl der Transaktionen auf das Nötigste zu reduzieren, wenn zwei Parteien mehrere Transaktionen miteinander durchführen wollen. Letztlich kann die Summe der Transaktionen auch zusammengefasst werden, solange sich die Parteien über den Zustand einig sind. Dafür wird ein direkter Transaktionskanal, also eine unmittelbare Kommunikation, zwischen zwei Parteien hergestellt. Innerhalb des Kanals können nahezu beliebig viele Transaktionen beinahe ohne Verzögerung durchgeführt werden.[30] Die Anzahl der Transaktionen, die auf die Blockchain geschrieben werden, wird damit auf bis zu zwei Transaktionen pro Kanal reduziert. Der Kanal ist über die Blockchain kryptografisch so abgesichert, dass der Gegenpartei nicht vertraut werden muss. Solange die Blockchain sicher ist, kann auch im Payment Channel nicht betrogen werden.[31] Um einen Payment Channel aufzubauen, wählen beide Parteien ein Guthaben, das sie potenziell austauschen möchten, und senden es an eine bestimmte Adresse, die unter der Kontrolle beider Parteien steht. Anschließend tauschen sie Transaktionen aus, die die Verteilung der Guthaben aktualisieren. Wird der Payment Channel abgebaut, wird das jeweilige aktuelle Guthaben an die zugehörige Partei zurückgezahlt.[32]

Auf Basis des Prinzips der Payment Channels wurde das so genannte **Lightning Network** entwickelt. Es bietet ein **Routing Protocol**, das den günstigsten Weg zwischen zwei Parteien im Netzwerk findet und die Verbindung etabliert.[33] Besteht ein Kanal zwischen Alice und Bob und ein Kanal zwischen Bob und Carol, kann Alice, indirekt über Bob, mit Carol eine Transaktion austauschen. Bob kann als Anreiz eine Transaktionsgebühr verlangen. Das Lightning Network bildet also ein Netzwerk aus Payment Channels. Das Lightning Network ist vielversprechend und löst tatsächlich das Problem der Skalierbarkeit. Es verspricht die Abwicklung von mehreren Millionen Transaktionen pro Sekunde und das nahezu ohne Verzögerung[34]. Darüber hinaus haben Transaktionen innerhalb der Payment Channels den Vorteil, dass sie privat sind[35]. Das Lightning Network wurde 2018 gestartet und hatte bis 2020 insgesamt über 100.000 aktive Kanäle. Untersuchungen haben jedoch gezeigt, dass einerseits die Suche nach dem günstigsten Weg und andererseits der Anreiz, die Transaktionsgebühren zu maximieren, zu sogenannten Hubs führen, die als stark vernetzte Knotenpunkte für das Lightning Network agieren.[36] Wie bei jeder Währung haben so einige Wenige die Kontrolle über den Großteil der Währung. Das Lightning Network führt daher auch wieder zu Zentralisierung.

Einen weiteren Lösungsansatz stellen **Sidechains** dar. Eine Sidechain ist eine unabhängige Blockchain, die die **Mainchain** um neue Funktionalitäten erweitern soll und die Mainchain entlastet. Entsprechend werden Sidechains parallel betrieben. Dabei werden Daten (Digital Assets oder Transaktionszustände) von der Mainchain auf die Sidechain überführt, indem sie an eine spezielle Adresse gesendet werden, die sinnbildlich als Schließfach fungiert. Der Zustand der Daten wird dann auf der Mainchain gesperrt und auf der Sidechain freigegeben. Transaktionen oder andere Prozesse werden dann auf der Sidechain durchgeführt und sind entsprechend unabhängig. Um die Daten wieder auf der Mainchain freizugeben, müssen diese auf der Sidechain zerstört oder gesperrt werden. Dieser Prozess

[30] Bitcoin Wiki: »Payment Channels – Bitcoin Wiki«, https://en.bitcoin.it/wiki/Payment_channels, abgerufen: 21. Juli 2020.

[31] Zhou, Q. et al.: »Solutions to scalability of blockchain: A survey.«, IEEE Access, Volume 8, S. 16440 – 16455, doi:10.1109/ACCESS.2020.2967218.

[32] Antonopoulos, A. M.: »Mastering Bitcoin: Programming the open blockchain«, O'Reilly Media, Inc., 2017, ISBN 978-1-49195-438-6.

[33] Antonopoulos, A. M.: »Mastering Bitcoin: Programming the open blockchain«, O'Reilly Media, Inc., 2017, ISBN 978-1-49195-438-6.

[34] Lightning Network, https://lightning.network/, abgerufen: 21. Juli 2020.

[35] Antonopoulos, A. M.; Osuntokun, O.; Pickhardt, R.: »Mastering the Lightning Network«,2020, https://github.com/lnbook/lnbook, abgerufen: 21. Juli 2020.

[36] Lin, J. H. et al.: »Lightning Network: a second path towards centralisation of the Bitcoin economy«, 2020, doi:10.1088/1367-2630/aba062.

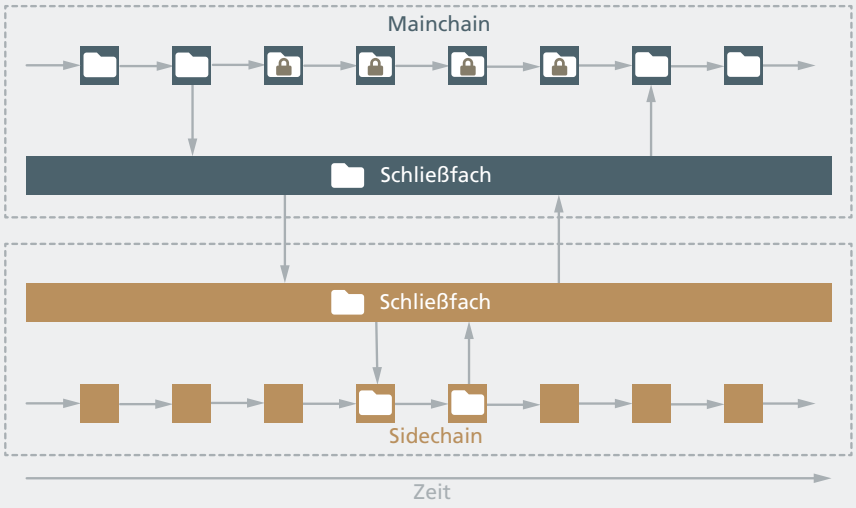


Abbildung 2: Sidechains

wird als **Two-Way Peg** bezeichnet. Grundsätzlich ist das Konzept Sidechain vielversprechend und zielt insbesondere auf **Interoperabilität** zwischen Blockchains ab. Es existieren verschiedene Ausprägungen für dieses Verfahren, die teilweise aber die sichere Ausführung der Transaktionen schwächen können, weil je nach Verfahren das Schließfach zentralisiert kontrolliert wird.[37] Darüber hinaus ist noch ungeklärt, ob der Betrieb von Sidechains ohne Vertrauen in Dritte durchgeführt werden kann[38]. Für Bitcoin werden zum Beispiel RootStock[39] und Liquid[40] als Sidechains eingesetzt.

Zusammengefasst kann festgehalten werden, dass die geringe Skalierbarkeit der Blockchain kurzfristig nur bedingt zu lösen ist. Das betrifft insbesondere public permissonless Blockchains wie Bitcoin. Alltagseinkäufe oder sogenannte Mikrotransaktionen über Bitcoin sind momentan nicht durchführbar. PoW als Konsensverfahren ist derzeit noch der De-facto-Standard und beeinflusst entsprechend die Skalierbarkeit. In geschlossenen Blockchains können hingegen andere Verfahren gewählt werden und unter Abwägung verschiedener Faktoren zu skalierbareren Lösungen führen. Off-Chain-Lösungen sind noch sehr experimentell und der Entwicklungs- und Forschungsbedarf ist entsprechend hoch. Speziell der Einsatz von Sidechains erfordert einen hohen Grad an Interoperabilität, die nur durch entsprechende Standardisierung erreicht werden kann.

3.3 SCHLÜSSELMANAGEMENT UND NUTZUNGSFREUNDLICHKEIT

Eine Blockchain ist ein komplett oder in großen Teilen verteiltes System. Die Authentifizierung der Nutzer:innen (also der Anmelde- oder Login-Prozess) ist daher besonders herausfordernd. Da eine zentrale Instanz grundsätzlich vermieden werden soll, ist die Anwendung von etablierten Verfahren (wie die Authentifizierung mit E-Mail-Adresse und Passwort) nicht umsetzbar, da diese Informationen an keiner Stelle gespeichert werden können und sollen. Daher wird für die Interaktion mit einer Blockchain fast immer auf ein kryptografisches Schlüsselpaar gesetzt: einen privaten und einen öffentlichen Schlüssel (**Public-Private Key Pair**). Üblicherweise ist dieses Schlüsselpaar mit dem Account in der Blockchain verknüpft oder gleichgesetzt. Dabei dient der öffentliche Schlüssel der Adressierung des Accounts, während der private Schlüssel benötigt wird, um Transaktionen zu signieren.[41] Der private Schlüssel dient entsprechend der Authentifizierung und kann in seiner Bedeutung einer E-Mail-Adresse-Passwort-Kombination gleichgesetzt werden. Im Gegensatz zu zentralen Lösungen ist ein Zurücksetzen oder eine Wiederherstellung dieses Zugangs grundsätzlich nicht möglich. Die Verantwortung für die sichere Aufbewahrung und die Umsetzung von Wiederherstellungsmechanismen verlagert sich damit vom System zu den Nutzer:innen. Dadurch sinkt zunächst grundsätzlich die Usability. Kommt es zum Verlust des privaten Schlüssels, ist es nicht mehr möglich, über den Account zu verfügen. Auch können über einen gestohlenen Schlüssel unautorisierte Transaktionen durchgeführt werden. Wird eine Blockchain zum Beispiel als Grundlage einer Kryptowährung eingesetzt, kann das dort gespeicherte Vermögen

[37] Singh, A. et al.; »Sidechain technologies in blockchain networks: An examination and state-of-the-art review«, Journal of Network and Computer Applications, Volume 149, doi:10.1016/j.jnca.2019.102471.

[38] Torpey, K.: »It's 2019, Where are Bitcoin's Sidechains?«, Forbes, https://www.forbes.com/sites/ktorpey/2019/02/27/its-2019-where-are-bitcoins-sidechains/#220f211353b4, abgerufen: 27. Februar 2020.

[39] RSK: »RootStock«, https://www.rsk.co/, abgerufen: 21. Juli 2020.

[40] Liquid: »Liquid Network«, https://blockstream.com/liquid/, abgerufen: 21. Juli 2020.

[41] Welzel, C. et al.: »Mythos Blockchain: Herausforderung für den öffentlichen Sektor«, Fraunhofer FOKUS, Berlin, 2017, ISBN 978-3-9816025-6-2.

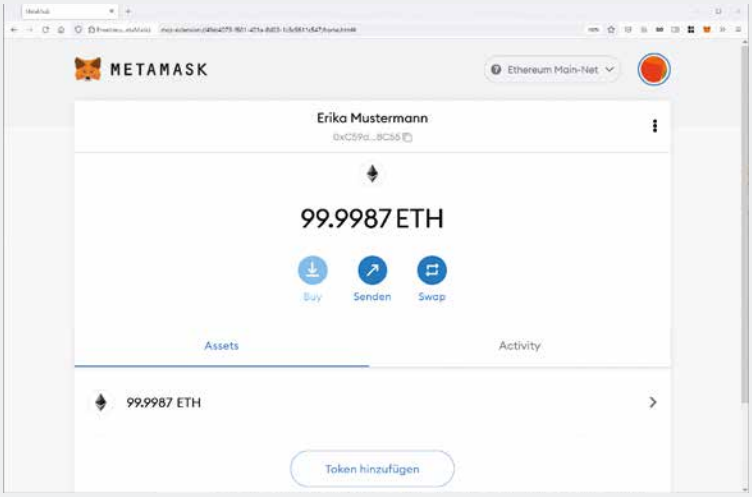


Abbildung 3: Oberfläche des Wallets MetaMask

problemlos von Dritten transferiert werden, sofern der private Schlüssel in falsche Hände gerät[42].

Üblicherweise wird die Verwaltung der privaten Schlüssel von einem sogenannten **Software-Wallet** übernommen. Darüber hinaus kann dieses **Wallet** oft auch Transaktionen signieren und mit der Blockchain kommunizieren.[43] Je nach Art des Wallets variieren die Art der Schlüsselverwaltung und die Usability.[44] Es wurden verschiedene Lösungen entwickelt, um eben diese Nutzungsschwelle zu verringern und eine praktische Anwendbarkeit der Blockchain zu gewährleisten. Ziel ist es, den Nutzer:innen die Sicherung des privaten Schlüssels zu erleichtern oder gänzlich zu abstrahieren.

Ein Beispiel für eine solche Lösung ist MetaMask[45], ein Software-Wallet für die Ethereum-Blockchain. MetaMask kann als Anwendung auf dem Smartphone oder als Browser-Plug-in installiert werden. Bei der ersten Anmeldung erstellt die Software das kryptografische Schlüsselpaar, wobei die Nutzer:innen lediglich ein im Vergleich zum privaten Schlüssel »einfaches« Passwort angeben müssen. Das Passwort wird benötigt, um sich anzumelden und den privaten Schlüssel lokal zu verschlüsseln. Das Ergebnis des Anmeldeprozesses ist eine sogenannte **Seedphrase**, eine Liste von 12 zufälligen Wörtern, mit denen MetaMask den privaten Schlüssel jederzeit wiederherstellen kann. Üblicherweise wird die Seedphrase auf ein Blatt Papier geschrieben und im Idealfall sicher und geschützt vor Fremdzugriff verwahrt. MetaMask ist einfach zu bedienen und erleichtert durch seine einfachere Darstellungsform den Umgang mit dem privaten Schlüssel. Angriffe durch Schadsoftware oder ein Verlust von Passwort und Seedphrase sind weiterhin möglich.

Ein weiterer Lösungsansatz ist die Offline-Speicherung des privaten Schlüssels, zum Beispiel auf einem speziellen USB-Stick. Ein solches Gerät wird als **Hardware-Wallet** bezeichnet. Der private Schlüssel wird auf diese Weise physisch isoliert, da der Signaturvorgang ebenfalls auf dem Stick ausgeführt wird. Im Allgemeinen gilt diese Variante als sehr sichere Lösung. Allerdings können auf dem Wallet ebenfalls Sicherheitslücken vorhanden sein, die unautorisierte Transaktionen ermöglichen. Darüber hinaus wird bei Verlust des Wallets auch hier eine Seedphrase benötigt, um den privaten Schlüssel wieder herstellen zu können.[46]

Zudem können private Schlüssel auch durch Dritte zentral gespeichert und verwaltet werden (**Hosted-Wallet**). Dabei werden die privaten Schlüssel offline gelagert, um sie gegen Angriffe zu schützen, und bei Bedarf temporär in den Online-Speicher verlagert, um den Nutzer:innen den Zugriff zu ermöglichen. Typischerweise authentifizieren sich die Nutzer:innen über die Webschnittstelle des Wallets mittels Loginname und Password oder mit Zweifaktor-Authentifizierung. Solche Wallets verfügen über bequeme Wiederherstellungsmechanismen, wodurch eine hohe Usability ermöglicht wird. Allerdings entsteht dadurch wiederum eine Zentralisierung, die gezielte Angriffe ermöglicht.[47]

Eine besonders sichere Möglichkeit zur Schlüsselverwaltung ist die Nutzung eines **Multisignatur-Wallets**. Dabei werden mehrere private Schlüssel generiert, wobei zur Authentifizierung

[42] Eriksson, N.: »10 Dramatic Stories of People Who Lost Their Bitcoin Private Keys«, Coinnounce, https://coinnounce.com/10-dramatic-stories-of-people-who-lost-their-bitcoin-private-keys/, abgerufen: 12. Februar 2019.

[43] Xu, X.; Weber, I.; Staples, M.: »Architecture for blockchain applications«, 2019, Springer International Publishing, S. 34, doi:10.1007/978-3-030-03035-3.

[44] Eskandari, S. et al.: »A first look at the usability of bitcoin key management«, 2018, https://arxiv.org/pdf/1802.04351.pdf, angerufen: 07. September 2021.

[45] MetaMask: »A crypto wallet & gateway to blockchain apps«, https://metamask.io/, abgerufen: 21. Juli 2020.

[46] Eskandari, S. et al.: »A first look at the usability of bitcoin key management«, 2018, https://arxiv.org/pdf/1802.04351.pdf, angerufen: 07. September 2021.

[47] Eskandari, S. et al.: »A first look at the usability of bitcoin key management«, 2018, https://arxiv.org/pdf/1802.04351.pdf, angerufen: 07. September 2021.

HOUSE NOODLE LAMP VACUUM
CAPABLE CAR COOK ARCH ALL
ENFORCE ELEFANT RACCOON

Abbildung 4: Beispielhafte Seedphrase zur Wiederherstellung eines Wallets

nur eine Teilmenge dieser Schlüssel benötigt wird, bspw. 2 von 3 Schlüsseln. Der Vorteil ist, dass die Schlüssel verteilt auf verschiedenen Geräten gespeichert werden. Eine Kombination aus verschiedenen Varianten ist denkbar. Ein Schlüssel könnte dabei lokal auf dem Computer der Nutzer:innen gespeichert werden, ein weiterer in einem Hardware-Wallet und der dritte in einem Hosted-Wallet. Der Verlust eines Schlüssels kann durch die Verteilung kompensiert werden, damit verringert sich das Risiko, keinen Zugang mehr zur Blockchain zu erhalten. Die Verteilung der Schlüssel erschwert auch einen Angriff. Allerdings ist die erhöhte Komplexität der Nutzungsfreundlichkeit nicht zuträglich.[48]

Schließlich existieren »soziale« Lösungskonzepte, die häufig in Blockchain-Anwendungen für Identitätsmanagement zum Einsatz kommen, wie Sovrin[49] und uPort[50]. Der private Schlüssel wird auf dem Smartphone lokal gespeichert und für die Wiederherstellung werden berechtigte Vertraute ausgewählt, die einen Teil des Schlüssels erhalten. Geht der private Schlüssel verloren, kann der Schlüssel auf Basis einer Teilmenge der ausgewählten Vertrauten wiederhergestellt werden.

Die vorgestellten Verfahren zeigen, dass die Verwaltung von privaten Schlüsseln ein entscheidender Punkt bei der Usability und damit der Massentauglichkeit von Blockchain-Anwendungen ist. Bisher gestaltet sich der Umgang noch zu kompliziert und kann realistischerweise nur von technisch versierten Nutzer:innen gehandhabt werden. Kurzfristig erscheint der Einsatz einer zentralen Instanz zur Verwaltung der Schlüssel als nutzbarste Lösung. Als vielversprechend und zukunftsweisend kann die Verteilung des Schlüssels auf verschiedene Speicherorte oder Vertraute gesehen werden. Eine große Verbreitung solcher Lösungen erfordert einen hohen Grad an Standardisierung, um die Verwaltung der Schlüssel über Anwendungs- und Gerätegrenzen hinweg einzusetzen.

3.4 SMART CONTRACTS UND DAPPS

Das ursprüngliche Konzept der Blockchain sah die Durchführung relativ einfacher Werttransaktionen einer virtuellen Währung vor und war somit auf den Anwendungsfall einer dezentralen Buchführung beschränkt. Mit der Weiterentwicklung der Blockchain entstanden schnell neue und komplexere Anwendungsfälle, die eine Abbildung von erweiterten Datenstrukturen und Algorithmen verlangen. Insbesondere soll eine Verwaltung von Werten, Daten und Prozessen ermöglicht werden, die auch außerhalb der Blockchain Gültigkeit haben. Die Blockchain wird damit zu einer Anwendungsplattform, die mit traditionellen Anwendungen interagiert und die Verwaltung physischer Güter abbildet. Solche Abbildungen werden als **Digital Assets** innerhalb der Blockchain bezeichnet. Die Verwaltung erfolgt über Programmcode, der in der Blockchain gespeichert und durch die Knoten ausgeführt wird. Solche Programme sind bekannt als **Smart Contracts**.[51] Ein anschauliches Beispiel für einen typischen Smart Contract ist ein von der Blockchain gesteuerter Beherbergungsvertrag: Wird die Miete ordnungsgemäß bezahlt, erhalten die Mieter:innen Zutritt zur Ferienwohnung über ein elektronisches Schloss. Andernfalls bleibt die Ferienwohnung gesperrt.[52] In diesem Fall wäre die Ferienwohnung ein Digital Asset, wobei ein Smart Contract den Zugang entsprechend verwaltet.

[48] Bitcoin Wiki: «Multisignature – Bitcoin Wiki«, https://en.bitcoin.it/wiki/Multisignature, abgerufen: 21. Juli 2020.

[49] Sovrin, https://sovrin.org/, abgerufen: 21. Juli 2020.

[50] uPort, https://uport.me/, abgerufen: 21. Juli 2020.

[51] Xu, X.; Weber, I.; Staples, M.: »Architecture for blockchain applications«, 2019, Springer International Publishing, S. 37 – 38, doi:10.1007/978-3-030-03035-3.

[52] Song, J.: »The Truth about Smart Contracts«, Medium, https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f, abgerufen: 11. Juni 2020.

DER UMGANG MIT PRIVATEN SCHLÜSSELN GESTALTET SICH NOCH ZU KOMPLIZIERT UND KANN REALISTISCHERWEISE NUR VON TECHNISCH VERSIERTEN NUTZER:INNEN GEHANDHABT WERDEN.

Smart Contracts werden häufig losgelöst von der Blockchain im Kontext der Automatisierung von juristischen Verträgen diskutiert. Es ist aber zu beachten, dass ein Smart Contract (noch) nicht mit einem rechtsgültigen Vertrag gleichzusetzen und unabhängig davon zu betrachten ist. Ein Smart Contract ist nicht besonders intelligent. Das Wort Smart bezieht sich vielmehr auf die Ausführung des Programmes ohne Eingreifen von Dritten.[53] Der Begriff Contract kann in den aktuellen Anwendungsfällen am besten als Algorithmus verstanden werden. Wird ein automatisierter Vollzug durch Anbieter in einer zentralisierten Umgebung umgesetzt, stellt sich immer die Frage, ob dem Anbieter vertraut werden kann. In einer Blockchain-Umgebung, in der Smart Contracts dezentral abgebildet werden können, ist eine Ausführung auch ohne Vertrauen in jeden einzelnen Akteur möglich.[54] Der Programmcode kann von allen Nutzer:innen gelesen und geprüft werden. So können Fehler oder betrügerisches Verhalten schnell entdeckt und kommuniziert werden. Darüber hinaus ist der Programmcode unveränderbar. Nutzer:innen können sich also sicher sein, dass sich der Smart Contract zu jeder Zeit wie erwartet verhält. Die Blockchain nimmt demzufolge die Rolle von unabhängigen Notar:innen ein.

Auf der technischen Seite wird ein Smart Contract immer von allen Knoten, die am Konsensverfahren beteiligt sind, validiert. In Ethereum sind dies die Miner. Zuerst wird eine Transaktion, die einem Smart Contract zugeordnet ist, von einem Miner ausgeführt und inklusive des Ergebnisses in den nächsten Block geschrieben. Um den Block zu validieren, führen alle anderen Miner den Programmcode des Smart Contracts mit den gegebenen Parametern durch und überprüfen, ob das Ergebnis stimmt. Falls das Ergebnis abweicht, gilt der Block als invalide.[55]

Des Weiteren bilden Smart Contracts die Grundlage für sogenannte dezentralen Applikationen (**DApp**). Das Backend (Verarbeitung, Logik) einer DApp basiert dabei vollständig auf Smart Contracts. Im Gegensatz zum Backend kann das Frontend (Eingabe, Interaktion) einer DApp auf einem zentralen Server laufen.[56]

Ein Beispiel für eine DApp ist die Plattform OpenSea[57]. Diese bietet einen Marktplatz für sogenannte Non-fungible Token (NFT), die sich im Gegensatz zu Kryptowährungen dadurch auszeichnen, dass sie einzigartig und nicht austauschbar sind. NFTs basieren auf Smart Contracts, die eine eindeutige Identifikationsnummer, eine Blockchain-Adresse und weitere Informationen in Kombination auf der Blockchain speichern. Durch die Zuordnung der Blockchain-Adresse bestehen klare Eigentumsverhältnisse an den Token. Darüber hinaus sind NFTs üblicherweise übertragbar und deren Handel wird zugelassen. Je nach Anwendungsfall können die gespeicherten Informationen genutzt werden, um zum Beispiel ein einzigartiges Bild zu konstruieren (CryptoKitties[58]) oder auf eine externe Ressource im Internet zu verweisen. Auch wenn die Idee nicht neu ist, war insbesondere im Frühjahr 2021 im Bereich der digitalen Kunst und der Sammelobjekte ein regelrechter NFT-Hype zu beobachten. Abschließend ist zu beachten, dass NFTs keine dinglichen Eigentumsrechte beschreiben. Verweist das NFT zum Beispiel auf ein externes, öffentlich zugängliches Bild, kann dieses belie-

[53] Xu, X.; Weber, I.; Staples, M.: »Architecture for blockchain applications«, 2019, Springer International Publishing, S. 37 – 38, doi:10.1007/978-3-030-03035-3.

[54] Song, J.: »The Truth about Smart Contracts«, Medium, https://jimmysong.medium.com/the-truth-about-smart-contracts-ae825271811f, abgerufen: 11. Juni 2020.

[55] Xu, X.; Weber, I.; Staples, M.: »Architecture for blockchain applications«, 2019, Springer International Publishing, S. 37 – 38, doi:10.1007/978-3-030-03035-3.

[56] Xu, X.; Weber, I.; Staples, M.: »Architecture for blockchain applications«, 2019, Springer International Publishing, S.39 – 40, doi:10.1007/978-3-030-03035-3.

[57] OpenSea: »Discover, collect, and sell extraordinary NFTs«, https://opensea.io/, abgerufen: 21. Juni 2021.

[58] CryptoKitties: »Collect and breed digital cats!«, https://www.cryptokitties.co/, abgerufen: 21. Juni 2021.

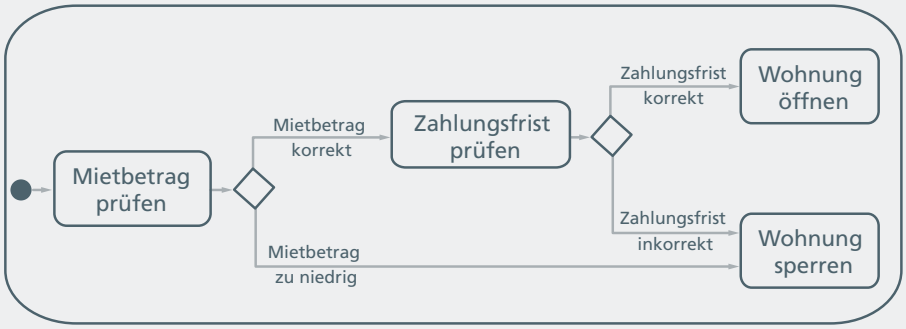


Abbildung 6: Vereinfachte Darstellung eines Smart Contracts

big kopiert, verteilt, ohne Exklusivität angeschaut und sogar entfernt werden.[59]

Smart Contracts und DApps bilden die Grundlage für die Bereitstellung von komplexeren Anwendungen auf Blockchain-Basis. Momentan sind sie aber nur ein Begriff für Softwareprogramme, die nicht auf einem zentralen Server, sondern eben dezentral durch die Blockchain-Knoten ausgeführt werden. Ihre Möglichkeiten sind noch stark eingeschränkt und ihre Anwendung als juristisches Instrument derzeit nicht umsetzbar. Insbesondere der dafür notwendige rechtliche Rahmen muss noch geschaffen werden und die Auswirkungen auf die Durchsetzung von Recht müssen diskutiert werden.

3.5. SICHERHEIT UND DATENSCHUTZ

IT-Sicherheit mit den Merkmalen **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** ist von zentraler Bedeutung für die Akzeptanz einer neuen Technologie, denn nur sichere und einfach zu verwendende Technologien werden alltagstauglich für eine massenhafte Anwendung sein. Die Merkmale Integrität und Verfügbarkeit werden über die inhärenten Eigenschaften der Blockchain abgesichert. Im Folgenden werden die jüngsten Entwicklungen hinsichtlich **Angriffsvektoren** und **Vereinbarkeit der Blockchain-Technologie mit der DSGVO** beschrieben, um einen aktuellen Überblick über noch offene Fragestellungen bzw. ungeklärte Herausforderungen zu geben.

3.5.1 Aktuelle Angriffsvektoren

Anna Katrenko und Mihail Sotnichek (Apriorit) klassifizieren die Angriffsvektoren in fünf große Kategorien[60]:

1. Angriffe auf Blockchain-Netzwerke,
2. Angriffe auf die Wallets der Nutzer:innen,
3. Angriffe auf Smart Contracts,
4. Angriffe auf den Transaktionsüberprüfungsmechanismus,
5. Angriffe auf den Miningpool.

Jede dieser Kategorien von Angriffsvektoren stellt die Blockchain-Technologie vor Herausforderungen. Insbesondere Angriffe auf die Wallets der Benutzer:innen sowie auf die Smart Contracts können die Akzeptanz der Blockchain-Technologie gefährden, daher werden sie hier kurz beschrieben.

3.5.2 Angriffe auf die Wallets der Benutzer:innen

Bei Blockchains sind Angriffe auf die Wallets der Nutzer:innen sehr häufig. Dabei werden die Anmeldedaten und andere sensible Informationen, die in den Wallets der Opfer gespeichert sind, »gestohlen«. Dies ermöglicht es den Angreifern, betrügerische Transaktionen zu initiieren und zu autorisieren, indem sie im Namen der Geschädigten handeln. Zu den Angriffsmethoden gehören bekannte Methoden wie Phishing, Wörterbuchangriffe, anfällige Signaturen, fehlerhafte Schlüsselgenerierung und die Ausnutzung von Softwarefehlern der Wallets. Bei erfolgreichen Angriffen können Transaktionen im Namen des Opfers getätigt werden, ohne dass die Transaktionen als inkorrekt oder nicht autorisiert zu identifizieren sind, da sie die korrekte Signatur des Geschädigten beinhalten.

[59] Chohan, U. W.: »Non-Fungible Tokens: Blockchains, Scarcity, and Value«, Critical Blockchain Research Initiative (CBRI) Working Papers, 2021, doi:10.2139/ssrn.3822743.

[60] Katrenko, A.; Sotnichek, M.: »Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology«. https://www.apriorit.com/dev-blog/578-blockchain-attackvectors, abgerufen: 30. Juli 2020.

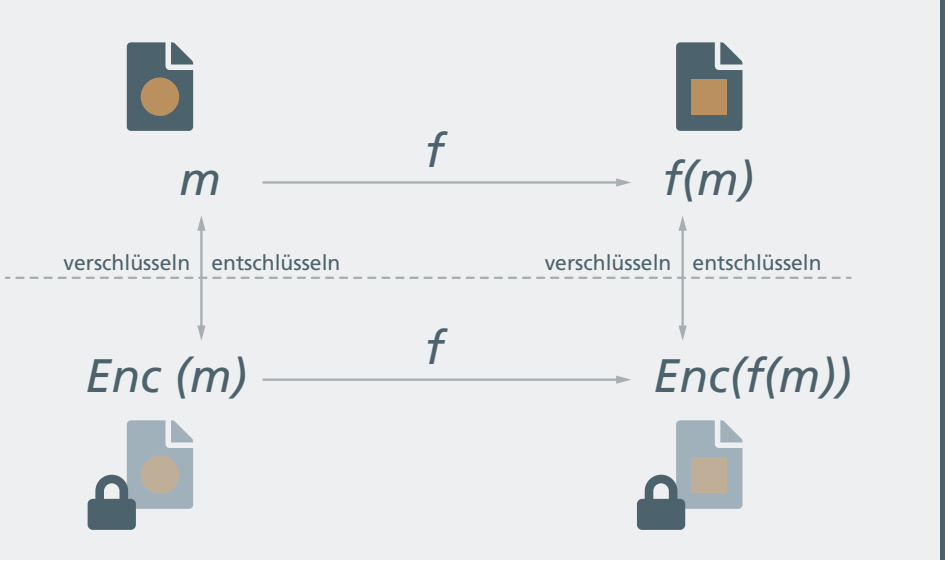


Abbildung 7: Datentransformationen bei homomorpher Verschlüsselung

3.5.3 Angriffe auf Smart Contracts

Angriffe auf Smart Contracts werden aufgrund von bestehenden Schwachstellen entweder im Quellcode des Smart Contracts oder in der Ausführungsumgebung des Programmcodes ermöglicht. Das Fehlverhalten – beispielsweise die Ausführung des Smart Contracts mit invaliden Daten - kann zum Verlust von Token[61] oder zur fehlerhaften Ausführung der Geschäftslogik führen, sodass die DApps, die auf diesen Smart Contracts aufbauen, ebenfalls fehlerhaft sind. Diese Angriffsmöglichkeiten sind jedoch nicht nur im Kontext der Blockchain-Technologie relevant, sie sind auch von anderen Programmiersprachen oder komplexen Anwendungen bekannt, da es fast unmöglich ist, eine komplexe Software fehlerfrei zu entwickeln.

Zusammenfassend ist zu sagen, dass für Blockchain-Ökosysteme ähnliche Angriffsvektoren wie für andere Software-basierte Technologien existieren. Meist zeigt sich, dass die verschiedenen Blockchain-Realisierungen robust mit technischen Angriffen umgehen, bzw. die jeweiligen Communities nach Attacken die Sicherheitslücken schnell schließen. Jedoch sind insbesondere Angriffe auf die Wallets der Nutzer:innen von großer Bedeutung, da die sichere Verwaltung des Schlüsselmaterials eine fundamentale Annahme der Technologie ist. Diese Aufgabe liegt bei den Nutzer:innen der Technologie, welche sich folglich der Wichtigkeit des Schlüsselmaterials und seines Schutzes bewusst sein müssen. Da das hierfür notwendige technische Verständnis nicht immer vorausgesetzt werden kann, stellt die sichere Verwaltung des Schlüsselmaterials eine noch offene Herausforderung dar.

3.5.4 Mögliche kryptografische Verfahren für den Umgang mit personenbezogenen Daten

Die Datenschutz-Grundverordnung (DSGVO) sieht ein **»Recht auf Vergessen«** vor. Wie bereits einleitend erwähnt, erschweren jedoch die verteilte Struktur und die Unveränderbarkeit der Blockchain die Realisierung von Ansprüchen an die Verwaltung personenbezogener Daten, sodass der Anschein entstehen kann, dass der Grundsatz der DSGVO und die Unveränderbarkeit der gespeicherten Daten in der Blockchain im Widerspruch stehen würden. Aktuelle Forschungsarbeiten zeigen jedoch, wie mit dieser Herausforderung umgegangen werden kann.

Diverse Ergebnisse schlagen zusätzliche Strategien vor, die zur Verbesserung der Sicherheits- und Datenschutzaspekte der bestehenden und zukünftiger Blockchain-Realisierungen eingesetzt werden können. Die Strategien umfassen 1) Mixing (Mischen), 2) Anonyme Unterschriften, 3) Homomorphe Verschlüsselung, 4) Attribut-basierte Verschlüsselung, 5) Nicht-interaktive Zero-Knowledge (NIZK)-Beweise, und 6) Smart Contracts, die auf einem Trusted Execution Environment (TEE) basieren[62/63]. In den folgenden Abschnitten werden zwei der vielversprechendsten Strategien näher erläutert.

3.5.5 Homomorphe Verschlüsselung

Mit der homomorphen Kryptografie können Berechnungen, wie zum Beispiel die grundlegenden mathematischen Operationen, direkt auf den verschlüsselten Daten (Chiffriertext) durchgeführt werden. Es werden dieselben Ergebnisse erzeugt, die

[61] Allgemein betrachtet sind Token im Zusammenhang mit Blockchains spezielle Einheiten, die den Inhaber zu einer Operation auf einer Blockchain berechtigen. Die Operation, die mit diesem Token autorisiert wird, kann z. B. eine digitale Zahlung oder aber eine Ausführung im Kontext einer dezentralen Anwendung sein.

[62] Zhang, R.; Xue, R.; Liu, L.: »Security and privacy on blockchain«, ACM Computing Surveys, Vol. 1, No. 1, Article 1, doi:10.1145/3316481.

[63] Eine Ausführungsumgebung wird als Trusted Execution Environment (TEE) bezeichnet, wenn sie eine vollständig isolierte Umgebung für die Ausführung von Anwendungen bereitstellt, die wirksam verhindert, dass andere Softwareanwendungen und Betriebssysteme den Zustand der darin laufenden Anwendung manipulieren und erfahren.

sich aus der Durchführung der entsprechenden Berechnungen auf den unverschlüsselten Daten ergeben würden (siehe Abbildung 7). Solche Verfahren ermöglichen folglich die Speicherung von verschlüsselten Daten auf der Blockchain und die korrekte Weiterverarbeitung auf Basis der verschlüsselten Daten, ohne dass diese vorher entschlüsselt werden müssten. Unter der Annahme, dass die personenbezogenen Daten verschlüsselt auf der Blockchain abgespeichert werden, bietet die Verwendung der homomorphen Verschlüsselungstechnik Schutz der Privatsphäre und ermöglicht den einfachen Zugriff auf verschlüsselte Daten über öffentliche Blockchains.

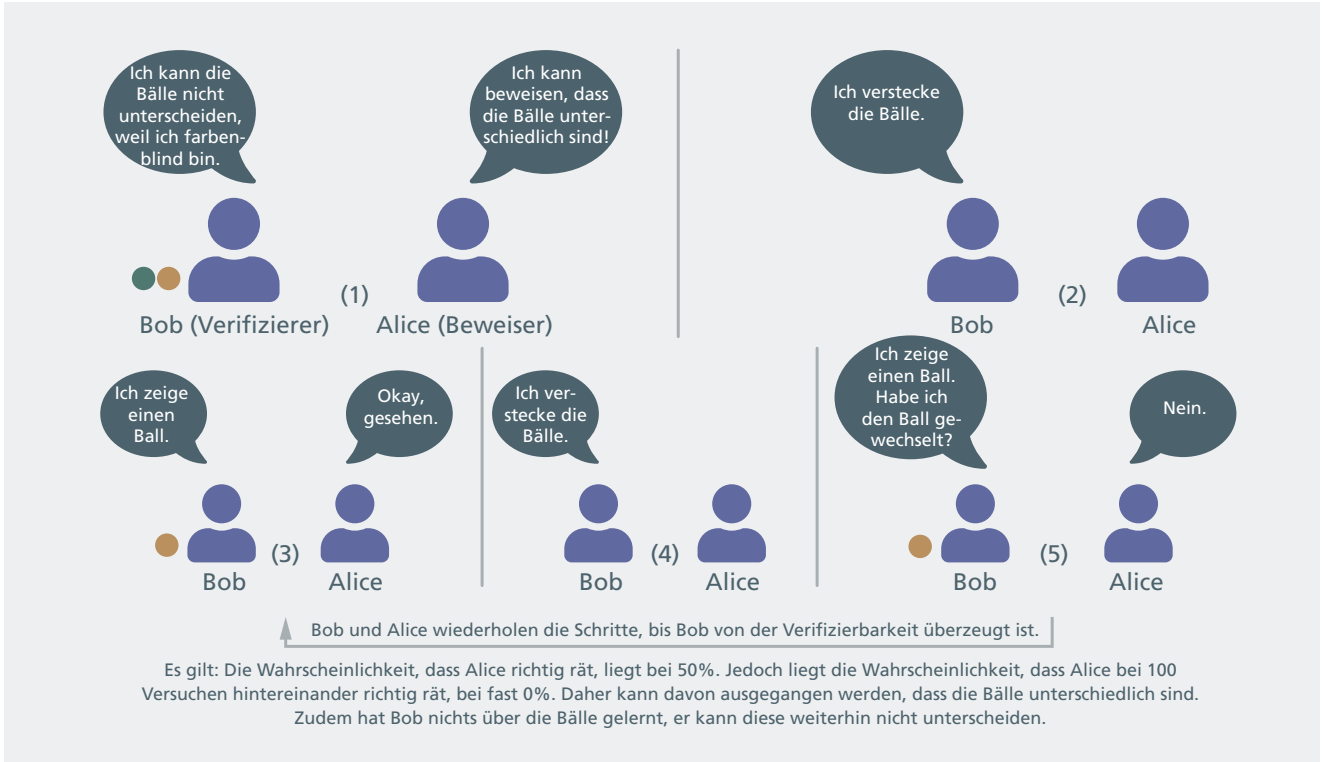
3.5.6 Nicht-interaktive Zero-Knowledge (NIZK)-Beweise

Die **Überprüfung der Korrektheit von Informationen**, die aus der Ausführung eines Programms mit **geheimgehaltenen Eingaben** resultieren, stellt eine komplexe Herausforderung dar. Zero-Knowledge-Beweise liefern Ansätze zum Umgang mit dieser Herausforderung. Bei Zero-Knowledge-Verfahren handelt es sich um spezielle Beweissysteme, die es Teilnehmer:innen (den Beweisenden) ermöglichen, andere Teilnehmer:innen (die Verifizierenden) zu überzeugen, über bestimmte geheime/private Informationen zu verfügen, ohne diese preisgeben zu müssen. **Interaktive Zero-Knowledge-Beweissysteme** ergeben sich stets aus einem **Dialog** zwischen den beiden Parteien. Der Dialog wird dazu als eine Art Frage-Antwort-Spiel geführt, wobei die Verifizierenden Fragen stellen, zu denen die Beweisenden die Antworten liefern. Beide Seiten können dazu beliebige Berechnungen durchführen und Zufallswerte bestimmen. Am Ende der Interaktion entscheiden die Verifizierenden, ob sie den Beweis akzeptieren, d. h. von der Korrektheit der Behauptung der Beweisenden überzeugt sind (siehe die Abbildung 8 für eine Illustration des Konzepts).

Die Abhängigkeit der Sicherheit des Verfahrens von den Interaktionen stellt jedoch hohe Anforderungen an die Ausführungsumgebung sowie an die Teilnehmer:innen, denn beide Parteien müssen während der gesamten Durchführung des Beweises miteinander Informationen austauschen. Die Möglichkeit, Zero-Knowledge-Verfahren mit schwächeren, jedoch weiterhin ausreichenden Sicherheitsanforderungen zu entwerfen, würde daher die Anwendbarkeit solcher Systeme stark erhöhen. Die Beweisvariante, bei der Beweisende und Verifizierende während des gesamten Prozesses nicht interaktiv sein müssen, wird als **nicht-interaktiver Zero-Knowledge-Beweis** bezeichnet. Nicht-interaktive Zero-Knowledge-Beweise reduzieren die notwendigen Interaktionen auf eine Richtung, d. h. es findet nur noch eine **unidirektionale Kommunikation zwischen den Beteiligten** statt.

[64] LinkedIn: »Demonstrate how Zero-Knowledge Proofs work without using math«, https://www.linkedin.com/pulse/demonstrate-how-zero-knowledge-proofs-work-without-using-chalkias/, abgerufen: 15. Juni 2021.

Abbildung 8: Zero-Knowledge-Beweis[64]



Es gilt: Die Wahrscheinlichkeit, dass Alice richtig rät, liegt bei 50%. Jedoch liegt die Wahrscheinlichkeit, dass Alice bei 100 Versuchen hintereinander richtig rät, bei fast 0%. Daher kann davon ausgegangen werden, dass die Bälle unterschiedlich sind. Zudem hat Bob nichts über die Bälle gelernt, er kann diese weiterhin nicht unterscheiden.

	Ethereum	Hyperledger Fabric	Corda
Eigenschaft	Generisch	Modular	Finanzsektor
Governance	Ethereum-Gemeinschaft/ Entwickler:innen	Linux Foundation	R3
Ausprägung	Public Permissionless oder Private Permissionless	Private Permissioned	Private Permissioned
Währung	Ether	Keine	Keine
Finalität der Einigung (Konsensverfahren)	Probabilistisch auf Blockebene	Deterministisch auf Transaktionsebene	Deterministisch auf Transaktionsebene
Programmiersprache	Solidity	Java, Go	Java, Kotlin
Datenprivatsphäre	Alle bzw. alle autorisierten Parteien	Alle autorisierten Parteien	Nur involvierte Parteien

Tabelle 1: Eigenschaften dreier bekannter Blockchain-Plattformen[65]

Die Vereinbarkeit von DSGVO – insbesondere im Hinblick auf das Recht auf Vergessen – und Blockchains ist eine nachträglich hinzugekommene Anforderung. Datenschutz hat in den letzten Jahren in der Blockchain-Entwicklung jedoch stark an Bedeutung gewonnen, sodass mittlerweile eine Vielzahl an vielversprechenden Strategien existiert, mit welchen personenbezogene und andere schützenswerte Daten auch im Kontext von Blockchain-Technologien sicher verarbeitet und verwendet werden können. Als Beispiel seien hier nochmals Zero-Knowledge-Beweise erwähnt, bei denen die privaten Daten erst gar nicht öffentlich preisgegeben werden müssen. Somit kann die ursprüngliche Herausforderung des fehlenden Einklangs zwischen DSGVO und Blockchains kann als erkannt und weitestgehend gelöst angesehen werden.

3.6 BLOCKCHAIN-PLATTFORMEN

Um konkrete Anwendungsfälle mit einer Blockchain umzusetzen, kann auf eine Vielzahl von bestehenden **Blockchain-Plattformen** zurückgegriffen werden. Solche Plattformen bieten einen weitaus größeren Funktionsumfang und mehr Möglichkeiten zur individuellen Anpassung als viele Kryptowährungs-Blockchains, die nur relativ einfache Transaktionen unterstützen. Sie sind in ihrer Funktion mit etablierten Elementen aus der Software- und Plattformentwicklung vergleichbar, wie Datenbanksystemen, Frameworks oder Programmierumgebungen. Die Blockchain kann dadurch als »Baustein« zur praktischen Umsetzung von Anforderungen in der Softwareentwicklung gesehen werden. Eine Blockchain-Plattform muss zum Anwendungsfall passen, entsprechend sollten mögliche Alternativen auch bewertet werden. Blockchain-Plattformen bieten in unterschiedlicher Ausprägung vielfältige Möglichkeiten, die Charakteristiken eines Blockchain Systems zu gestalten. Dazu zählen u. a. die Datenstrukturen, das Konsensverfahren und das Rechtemanagement. Aber insbesondere unterstützen sie das Bereitstellen und Durchführen von Programmen in Form von Smart Contracts und den darauf aufbauenden DApps. Wie viele andere Plattformlösungen kann eine Blockchain-Plattform auf eigenen Servern betrieben werden oder eine bestehende (Cloud-)Installation eingesetzt werden. Im Folgenden werden drei bekannte Blockchain Plattformen genauer beleuchtet: **Ethereum**, **Hyperledger Fabric** und **Corda**.[65]

3.6.1 Ethereum

Ethereum ist grundsätzlich eine public permissionless Blockchain, die stark auf die Ausführung von DApps spezialisiert ist[66]. Die inhärente Kryptowährung, die in der Ethereum-Blockchain gehandelt wird, wird Ether genannt. Zentraler Bestandteil von Ethereum sind Smart Contracts, die hier immer aus einem Blockchain-Account, ausführbarem Programmcode, einem internen Zustand und einem Saldo bestehen. Darüber hinaus sind Funktionen eines Smart Contracts über Transaktionen aufzurufen. Als Konsensverfahren bei der Generierung neuer Blöcke setzt Ethereum hauptsächlich auf PoW.

Die Transaktionsgebühren werden in dem abstrakten Mittel **Gas** bezahlt. Dabei sind die Gebühren für eine Transaktion immer aus festen und variablen Gaswerten zusammengesetzt. Die variablen Gaswerte sind durch die benötigten Ressourcen zur Ausführung eines Smart Contracts bestimmt, wie Datenspeicher und Prozessorleistung. Das Konzept Gas soll also die erforderlichen Ressourcen beim Validieren von Transaktionen widerspiegeln. Der Gaspreis wiederum ist definiert als Ether pro Gas und wird durch die Nutzer:innen bzw. durch Angebot und Nachfrage bestimmt. Je nach Dringlichkeit und durchschnittlichem Gaspreis können Nutzer:innen angeben, wieviel Ether sie bereit sind, pro Gas zu bezahlen. Neben dem Gaspreis muss auch das Gaslimit angegebenen werden. Das Gaslimit gibt an,

[65] Saraf, C.; Sabadra, S.: »Blockchain platforms: A compendium«, 2018, IEEE International Conference on Innovative Research and Development (ICIRD), S. 1 – 6, doi:10.1109/ICIRD.2018.8376323.

[66] Ethereum Whitepaper, https://ethereum.org/en/whitepaper/, abgerufen: 22. Juli 2020.

wieviel Gas für die Ausführung eines Smart Contracts verwendet werden soll. Wird eine Transaktion erfolgreich von einem Miner einem Block hinzugefügt, bekommt dieser die Anzahl an Gas, die zur Ausführung benötigt wurde, multipliziert mit dem Gaspreis als Belohnung. Übersteigt das benötigte Gas allerdings das Gaslimit, wird die Ausführung abgebrochen und ist als ungültig anzusehen. Transaktionen, die das Gaslimit übersteigen, werden trotzdem in die Blockchain geschrieben. Das Überschreiten des Gaslimits wird daher als Geldverlust für die Nutzer:innen und als Verschwendung von Ressourcen angesehen[67].

Als Blockchain-Plattform zur Bereitstellung von DApps hat Ethereum eine große Bedeutung. In einem Vergleich wurden 2.836 von insgesamt 3.451 DApps auf der Ethereum Blockchain angeboten. Darüber hinaus steht Ethereum mit etwa 27.760 aktiven Nutzer:innen pro Tag auch hier an oberster Stelle. Die meist genutzen DApps auf der Ethereum-Plattform kommen vor allem aus dem Finanz- und Spielesektor.[68]

Die Software der Ethereum-Plattform kann auch jenseits des öffentlichen Produktivsystems als Grundlage für eigene Blockchain-Anwendungen (private Blockchain) eingesetzt und entsprechend angepasst werden.

3.6.2 Hyperledger Fabric

Hyperledger ist ein Open-Source-Dachverband, der unter der Leitung der Linux Foundation an der Entwicklung von Blockchain und Distributed Ledger Frameworks, Bibliotheken und Werkzeugen arbeitet. Die Vision ist, einen akzeptierten und etablierten Standard zu schaffen. Die Zielgruppe sind insbesondere Unternehmen, Organisationen und Konsortien. In Hyperledger finden sich aktuell (2021) über 200 Mitglieder aus verschiedensten Domänen zusammen. Derzeit umfasst das Angebot 6 Frameworks, 5 Bibliotheken und viele weitere Tools.[69] Mit einer modularen Architektur zur Entwicklung von Blockchain-basierten Anwendungen ist Hyperledger Fabric eines dieser Projekte.

Hyperledger Fabric ist ein auf Konsortial-Blockchains spezialisiertes Framework für den Aufbau privater permissioned Blockchain-Plattformen. Es ist geeignet für Umgebungen, in denen bereits ein bestimmtes Grundvertrauen existiert. Dabei setzt Hyperledger Fabric bis zu einem gewissen Grad auf zentralisierte Dienste. Die Verwaltung und die Authentifizierung der Mitglieder werden vom Membership Service Provider durchgeführt. Zertifikate, die öffentliche Schlüssel beinhalten und die jeweiligen Eigentümer:innen bestätigen, werden hier verwaltet, um Teilnehmer:innen im Netzwerk zu identifizieren. Insbesondere die Vergabe von Zertifikaten wird in der Standardimplementierung von einer vertrauenswürdigen, zentralen Certificate Authority pro Organisation durchgeführt. Die Certificate Authorities der Organisationen müssen sich demnach untereinander vertrauen. Um private und vertrauliche Information zu schützen, existieren in Hyperledger Fabric sogenannte Channels. Jeder Channel ist dabei einer Gruppe von Teilnehmer:innen zugeordnet und hat einen separaten Transaktionsspeicher. Smart Contracts werden in Hyperledger Fabric in sogenannten Chaincodes zusammengefasst und in Containern (z. B. Docker) ausgeführt. Die Funktionalität der Smart Contracts kann anschließend von Anwendungen innerhalb des Netzwerks genutzt werden.[70] Hyperledger Fabric verfügt über kein festgelegtes Konsensverfahren, sondern ermöglicht den flexiblen Einsatz

[67] Liu, C. et al.: »Studying gas exceptions in blockchain-based cloud applications«, Journal of Cloud Computing, 9(1), S. 1 – 25, doi:10.1186/s13677-020-00176-9.

[68] State of the DApps, https://www.stateofthedapps.com, abgerufen: 19. Mai 2020.

[69] The Linux Foundation: »Hyperledger – Open Source Blockchain Technologies«, https://www.hyperledger.org/, abgerufen: 10. Juni 2021.

[70] The Linux Foundation: »Smart Contracts and Chaincode in Hyperledger Fabric«, https://hyperledger-fabric.readthedocs.io/en/release-2.0/smartcontract/smartcontract.html, abgerufen: 22. Juli 2020.

DIE BLOCKCHAIN IST EIN TECHNOLOGIEBAUSTEIN FÜR DEN AUFBAU VON KOMPLEXEN UND MODERNEN IT-SYSTEMEN.

verschiedener Verfahren. In der aktuellen Langzeitunterstützungsversion (v2.2.x) wird jedoch mit RAFT lediglich ein gängiges deterministisches Konsensverfahren unterstützt, das ähnliche Eigenschaften wie PBFT aufweist.

Hyperledger Fabric findet bereits praktische Anwendung, beispielhaft sei hier TradeLens genannt. TradeLens ist eine Plattform zur Digitalisierung von Lieferketten und wird in Kooperation von IBM und GTD Solution Inc. entwickelt. Hyperledger Fabric wird von TradeLens genutzt, um eine unveränderbare Protokollierung der Lieferkette umzusetzen und Vertrauen unter Teilnehmer:innen zu stärken oder zu schaffen. Darüber hinaus nutzt TradeLens die Channels von Hyperledger Fabric, um den Informationsaustausch zwischen den Teilnehmer:innen zu separieren.[71]

Corda[72]

Corda ist eine Open-Source-Distributed-Ledger-Lösung, die vom Konsortium R3 entwickelt wird. Die über 300 Mitglieder stammen überwiegend aus dem Finanzsektor. Daher ist die Architektur von Corda auch vorwiegend auf dessen Bedürfnisse angepasst. Ähnlich wie in Hyperledger Fabric werden Zertifikate durch zentralisierte Certificate Authorities ausgestellt. Sogenannte CorDapps (Corda Distributed Applications) definieren die Programmlogik in Corda. Diese werden in Java programmiert und als Java Archiv (JAR) in der Java Virtual Machine (JVM) ausgeführt. Der in der CorDapp definierte Programmfluss spezifiziert, welche Informationen an wen und in welcher Reihenfolge gesendet werden müssen, um eine Transaktion durchzuführen. Grundsätzlich gilt in Corda, dass ausschließlich notwendige Informationen geteilt werden. Dazu wird im Vergleich zu anderen Blockchain-Lösungen in Corda-Netzwerken ausschließlich von Punkt zu Punkt kommuniziert. Das Ergebnis einer neuen Transaktion wird von den Beteiligten selbst validiert. Dazu wird durch die Beteiligten das Ergebnis mittels Ausführens der jeweiligen CorDapp überprüft und anschließend signiert. Darüber hinaus muss ein Notary Service überprüfen, ob die Transaktion auf Grundlage vergangener Transaktionen erlaubt ist. Hierzu muss der Notary Service jedoch nicht in der Lage sein, die Inhalte der Transaktionen zu lesen. Je nach Anwendungsfall kann dem Notary Service auch die Erlaubnis erteilt werden, Transaktionen zu lesen und die Validierung der Transaktion zu unterstützen.

Corda wird von der Schweizer Plattform Cardossier[73] genutzt. Diese soll für mehr Transparenz und Sicherheit beim Autokauf sorgen. Dabei soll der Lebenszyklus von Gebrauchtwagen in der Blockchain gespeichert und so ein **Single Point of Truth**[74] für Käufer:innen und Verkäufer:innen gebildet werden. Cardossier wird unter anderem von der AdNovum Informatik AG und der Universität Zürich entwickelt. Ursprünglich war die Plattform auf Hyperledger Fabric umgesetzt und wurde später auf Corda umgestellt, da nach Angaben der Entwickler Corda bessere Eigenschaften in Skalierbarkeit und Datenschutz vorweisen kann.[75]

[71] TradeLens Documentation, https://docs.tradelens.com, abgerufen: 22. Juli 2020.

[72] Corda Documentation, https://docs.corda.net, abgerufen: 22. Juli 2020.

[73] Cradossier: »Managing the life cycle of a car with blockchain technology«, https://cardossier.ch/, abgerufen: 22. Juli 2020.

[74] Wikipedia: »Single Point of Truth«, https://de.wikipedia.org/wiki/Single_Point_of_Truth, abgerufen: 03. August 2021.

[75] Schwabe, G.: »The role of public agencies in blockchain consortia: Learning from the Cardossier«, Information Polity, 24(4), 2020, S. 437 – 451, doi:10.3233/IP-190147.

4. AUSSICHTSREICHE ANWENDUNGSFÄLLE

Die vorgehenden Kapitel haben die vielfältigen Ausprägungen und Eigenschaften, aber auch die umfassenden Herausforderungen an die Blockchain-Technologie aufgezeigt. Das Interesse an der praktischen Anwendung in konkreten Projekten ist groß. Als zentrale Blockchain-Vorteile werden dabei folgende Eigenschaften wahrgenommen:

- Die Möglichkeit, Daten innerhalb eines Ökosystems von Akteuren, deren Interessen nicht strikt aufeinander abgestimmt sind, verlässlich auszutauschen.
- Die Möglichkeit, eine Infrastruktur zu nutzen, über die keine einzelne Organisation die vollständige Kontrolle hat.
- Die Fähigkeit, Informationen auf eine Art und Weise zu hinterlegen, die stark widerstandsfähig gegen Modifikationen ist.
- Die Fähigkeit, Transaktionen (einschließlich Finanztransaktionen) auf Basis vordefinierter Bedingungen zu automatisieren.

Im Folgenden werden repräsentativ drei aussichtsreiche Anwendungsfälle aus diesen Branchen genauer beschrieben und erläutert: E-Voting, Blockchain-basierter Stromhandel, und maritime Transportversicherung. Die konkreten Anwendungsfälle wurden auf Basis ihres Reifegrades ausgewählt und danach, ob der Einsatz der Blockchain einen tatsächlichen Mehrwert bietet. Für jeden Anwendungsfall werden neben der Beschreibung des potenziellen Mehrwerts auch die größte Herausforderung identifiziert sowie mögliche Auswirkungen bei erfolgreichem Einsatz aufgezeigt. Diese Auswirkungen werden aus verschiedenen Perspektiven – der technischen, der Sicherheits- sowie der gesellschaftlichen Perspektive – betrachtet.

In folgenden Branchen und Anwendungsgebieten wird dabei der größte Nutzen der Blockchain gesehen:[76/77/78]

Finanzdienstleistung

Energiebranche

Versicherungsbranche

Logistikbranche

E-Government und E-Voting

Identitätsmanagement

Digitale Inhalte und Urheberrecht

[76] Rawat, D. B.; Chaudhary, V.; Doku, R.: »Blockchain: Emerging Applications and Use Cases«, 2019, https://arxiv.org/abs/1904.12247, abgerufen: 03. August 2021.

[77] Chen, W. et al.: »A survey of blockchain applications in different domains«, Proceedings of the 2018 International Conference on Blockchain Technology and Application, S. 17 – 21, doi:10.1145/3301403.3301407.

[78] Nascimento, S. et al.: »Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies«, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-08977-3.

4.1 E-VOTING

E-Voting-Systeme haben das Potenzial, Wahlen und Abstimmungen effizienter, kostengünstiger und nachvollziehbarer zu gestalten. Sie agieren an der Schnittstelle von Bürger:innen, Politik und öffentlichen Organisationen. Der Sicherheit dieser Systeme hat eine weitreichende gesellschaftliche Bedeutung. E-Voting-Systeme sind daher ein interessanter Anwendungsfall für die Blockchain im Kontext des öffentlichen Raumes. Bisher stehen E-Voting-Systeme noch in der Kritik, nicht die nötigen Sicherheitskriterien zu erfüllen.[79] Das gilt sowohl für politische Wahlen als auch für Wahlen in Organisationen und Vereinen. Darüber hinaus sind die technischen Realisierungen für Laien oft nicht nachvollziehbar, und im Gegensatz zu Papier-basierten Wahlen ist eine Manipulation durch eine kleine Gruppe denkbar.

Die Blockchain als Grundlage für E-Voting-Systeme einzusetzen, zählt mit zu den originären Anwendungsfällen. Die Blockchain-Eigenschaften und das Konzept von Smart Contracts eröffnen neue Möglichkeiten und Mechanismen, um die Einsatzgebiete von E-Voting-Systemen maßgeblich zu erweitern. E-Voting ist bereits in zahlreichen Forschungsprojekten untersucht (theoretische Ausarbeitungen oder Proofs-of-Concept) und von einigen Unternehmen umgesetzt worden[80].

Bekannte kommerzielle Anbieter sind Polys[81], Follow My Vote[82] und Agora[83]. Polys ist eine Abstimmungsplattform des russischen Softwareunternehmens Kaspersky Lab. Das Unternehmen wirbt hauptsächlich mit der Transparenz und Sicherheit der Blockchain und hat seine Lösung bereits in einigen Einsätzen erprobt. Das US-amerikanische Unternehmen Follow My Vote entwickelt ebenfalls ein Online-Abstimmungssystem auf Basis von Blockchain und verwandten Technologien. Das Unternehmen adressiert eine breite Spanne an Anwendungsfällen. Das Schweizer Unternehmen Agora bietet ein eigenes Blockchain-Ökosystem inklusive Token, der eine dezentrale und anonyme Wahl ermöglichen soll. Diese Lösungen haben gemeinsam, dass sie sich derzeit auf die technologischen Eigenschaften der Blockchain als Marketingmittel konzentrieren. Organisatorische und rechtliche Randbedingungen oder die Abbildung von bestehenden Wahlregeln und Identifizierungsverfahren spielen derzeit weniger eine Rolle.

4.1.1 Herausforderungen

Aufgrund der Sensibilität des Anwendungsfalls gelten besondere Herausforderungen bei der Umsetzung von E-Voting-Systemen. Eine besondere Rolle spielt dabei das Identitätsmanagement, das eine sichere und manipulationssichere Abbildung der realen Identitäten der Wähler:innen ermöglichen muss.[84] Im Fall politischer Wahlen bedeutet das eine umfassende Anpassung bestehender Prozesse der Wähler:innenregistrierung und Benachrichtigung, beispielsweise durch die Anbindung an Melderegister.[85] Dabei muss ausreichende Anonymität gewährleistet werden können, wobei auch die Administrator:innen des Systems nicht in der Lage sein dürfen, individuelle Stimmen zurückzuverfolgen. Etablierte Blockchains bieten bisher nur Pseudoanonymität, die den Anforderungen an E-Voting-Systemen nicht gerecht wird. Gleichzeitig müssen die einzelnen Wähler:innen in die Lage versetzt werden, die Berücksichtigung

[79] Hjálmarsson, F. Þ. et al.: »Blockchain-based e-voting system«, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), S. 983 – 986, IEEE, doi:10.1109/CLOUD.2018.00151.

[80] Abuidris, Y.; Kumar, R.; Wenyong, W.: »A Survey of Blockchain Based on E-voting Systems«, Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications (ICBTA 2019), S. 99 – 104, ACM, doi:10.1145/3376044.3376060.

[81] Polys: »Polys is a Secure Online Voting System«, https://polys.me/, abgerufen: 22. Juli 2020.

[82] Follow My Vote: https://followmyvote.com/, abgerufen: 16. August 2021.

[83] Agora: https://www.agora.vote/, abgerufen: 22.Juli 2020.

[84] Çabuk, U. C.; Adiguzel, E.; Karaarslan, E.: »A survey on feasibility and suitability of blockchain techniques for the e-voting systems«, https://arxiv.org/abs/2002.07175, abgerufen: 16. August 2021.

[85] Der Bundeswahlleiter: https://www.bundeswahlleiter.de/, abgerufen: 22. Juli 2020.

SCHLÜSSELFAKTOREN FÜR DEN EINSATZ DER BLOCKCHAIN ALS GRUNDLAGE FÜR E-VOTING SIND TRANSPARENZ UND NACHVOLLZIEHBARKEIT.

ihrer individuellen Stimme nachzuvollziehen, und sie dürfen natürlich nur ein einziges Mal abstimmen können.[86] Schließlich stellen die noch limitierte Skalierbarkeit und der technische Reifegrad der Blockchain-Technologie Hindernisse dar, um zuverlässige Wahlen oder Abstimmungen in großem Umfang durchzuführen.

4.1.2. Technische Perspektive

Das wichtigste Unterscheidungsmerkmal zu traditionellen E-Voting-Systemen stellt die Dezentralität der technischen Infrastruktur dar. Zudem ermöglicht die freie Verfügbarkeit verschiedener Blockchain-Plattformen die Anpassung an konkrete Wahl- oder Abstimmungsvorhaben. Wichtige Funktionalitäten für elektronische Wahlen bietet die Blockchain bereits inhärent, was eine Konzentration auf organisatorische und sicherheitsrelevante Aspekte ermöglicht. Für E-Voting-Systeme wird in der Regel eine public permissioned Blockchain eingesetzt, da die Wahldaten zwar transparent und nachvollziehbar sein sollen, aber die Autorisierung und Kontrolle für den Schreibzugriff bei einer zentralen Instanz liegen. Dadurch wird der Einsatz von energiesparsamen und schnellen Konsensverfahren ermöglicht, wie bspw. Proof-of-Authority (PoA), bei dem die Validierung der Blöcke auf Basis von bestimmten verifizierten Accounts bzw. Nutzer:innen erfolgt.

4.1.3. Sicherheitsperspektive

Prinzipiell gilt E-Voting mit der Blockchain als sicherer im Vergleich zu traditionellen E-Voting-Verfahren. Lokale elektronische Wahlautomaten können physisch manipuliert werden und dadurch einen bestimmten Anteil an Stimmen verfälschen. Zentralisierte Systeme stehen in der Kritik, durch eine kleine Gruppe vollständig korrumpiert werden zu können.[87] Eine Manipulation der Blockchain ist grundsätzlich ebenfalls möglich, aber aufgrund der Dezentralität um ein Vielfaches aufwendiger. Das zentralisierte Identitätsmanagement stellt aber auch hier ein Angriffsziel dar, wodurch beispielsweise falsche Stimmberechtigungen generiert werden könnten. Die Transparenz der Blockchain ermöglicht die Aufdeckung möglicher Inkonsistenzen. Generell hat die Transparenz der Blockchain das Potenzial, das Vertrauen in E-Voting-Lösungen zu stärken und dadurch gängige Sicherheitsbedenken auszuräumen. Natürlich kann eine absolute Manipulationssicherheit nie gewährleistet werden. Insbesondere bei elektronischen Wahlen vom eigenen Computer kann dieser manipuliert worden sein oder eine fremde Person führt den Wahlvorgang durch.

4.1.4. Gesellschaftliche Perspektive

Eine erfolgreiche Umsetzung von elektronischen Wahlen auf Blockchain-Basis hätte unmittelbare Auswirkungen auf die Gesellschaft und die Art und Weise, wie politische und organisationelle Wahlen durchgeführt werden können. Offensichtlich sind hier massive Effizienzsteigerungen durch die Verringerung von physischen Ressourcen und die fast augenblickliche Auszählung der Stimmen. Die initiale Beschaffung und Einrichtung eines E-Voting-Systems ist mit hohem organisatorischem und finanziellem Aufwand verbunden, während die Nutzung ungleich ökonomischer im Vergleich zu traditionellen Verfahren ist. Dadurch können Wahlen häufiger und kurzfristiger durchgeführt werden.[88] So ist beispielsweise eine Stärkung der direkten Demokratie denkbar. Des Weiteren können die Flexibilität und die Ortsunabhängigkeit zu einer Erhöhung der Wahlbetei-

[86] Çabuk, U. C.; Adiguzel, E.; Karaarslan, E.: »A survey on feasibility and suitability of blockchain techniques for the e-voting systems«, https://arxiv.org/abs/2002.07175, abgerufen: 16. August 2021.

[87] Hjálmarsson, F. Þ. et al.: »Blockchain-based e-voting system«, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), S. 983 – 986, IEEE, doi:10.1109/CLOUD.2018.00151.

[88] Çabuk, U. C.; Adiguzel, E.; Karaarslan, E.: »A survey on feasibility and suitability of blockchain techniques for the e-voting systems«, https://arxiv.org/abs/2002.07175, abgerufen: 16. August 2021.

ligung beitragen. Ein essenzieller Vorteil liegt auch in der Möglichkeit, spezifischere Abstimmungs- und Wahlverfahren umzusetzen. Smart Contracts ermöglichen zum Beispiel die Anwendung von Delegated Voting oder ähnlichen Entscheidungsfindungsformen[89]. Als Schlüsselfaktor ist allerdings die Transparenz und Nachvollziehbarkeit zu betrachten, insbesondere in Ländern mit einem fragilen demokratischen System eröffnen sich neue Möglichkeiten zur Vertrauensbildung.

[89] Hjálmarsson, F. Þ. et al.: »Blockchain-based e-voting system«, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), S. 983 – 986, IEEE, doi:10.1109/CLOUD.2018.00151.

4.2 BLOCKCHAIN-BASIERTER STROMHANDEL

Der effiziente Ausgleich von Energieüberschüssen und -bedarfen spielt eine zentrale Rolle für eine erfolgreiche Energiewende. Üblicherweise ist dieser Ausgleich mit einem vorherigen Handel verbunden. Um einen vertrauenswürdigen Handel zu ermöglichen, müssen sowohl Angebot als auch Nachfrage informationstechnisch sicher und effizient abgebildet werden. Hierfür stellt der Einsatz der Blockchain eine mögliche Lösung dar, denn sie kann als **gemeinsamer Vertrauensraum** für die Handelspartner betrachtet werden. Dieser Ansatz wurde zusammen mit Übertragungsnetzbetreibern im Rahmen eines Forschungsprojekts[90] prototypisch umgesetzt. Der Fokus des Prototyps lag hierbei auf dem **Flexibilitätenhandel**: Eine Flexibilität bezieht sich in diesem Zusammenhang auf eine Energie-Produktions- beziehungsweise -Verbrauchseinheit, die plan- und kontrollierbar ist. Die Anlagenbetreiber bieten zwei Arten von Flexibilitäten an – **positive** und **negative Flexibilität**. Dies entspricht einer Erhöhung der Produktion beziehungsweise einer Erhöhung des Verbrauchs. Diese Angebote werden von Netzbetreibern zur Netzstabilisierung bei Netzengpässen eingesetzt. Die konkreten Teilprozesse für die Gebotsabgabe und Gebotsannahme des Flexibilitätenhandels wurden auf Basis der Blockchain umgesetzt, was in den folgenden Absätzen näher erläutert wird.

Grundsätzlich existieren bei diesem Handel Flexibilitäten mit unterschiedlicher zeitlicher Granularität: mit Gebotsabgabe am Vortag (Day-Ahead) und mit Gebotsabgabe bis 2 Stunden vor der Erbringung (Intraday). Der Inhalt der Angebote ist dabei jeweils eine positive oder negative Flexibilitätenmeldung sowie eine Kostenmeldung. Diese Angebote sowie deren Verarbeitung werden mittels Smart Contracts auf der Blockchain umgesetzt. Dies hat den Vorteil, dass die übertragenen Daten für alle Teilnehmer des Netzwerks einsehbar und fälschungssicher sind. Außerdem liegen Verarbeitung und Datenhaltung der Gebote nicht zentral bei einem einzelnen Plattformanbieter, sondern sind prinzipiell auf jedem Knoten des Netzwerks vorhanden und abrufbar.

Im Demonstrator wird zwischen zwei Arten von Teilnehmenden unterschieden: Anlagenbetreiber (die Gebote abgeben) und Netzbetreiber (die Gebote verarbeiten). Die Anlagenbetreiber können Gebote abgeben, welche transparent auf einer privaten Blockchain gespeichert werden. Auf Basis dieser Gebote können die Netzbetreiber Anteile der Gebote sicher und transparent kaufen, um Netzstabilität zu gewährleisten. Die (teilweise) Annahme bzw. Nichtannahme der Gebote wird ebenfalls auf der Blockchain festgehalten und ist somit für alle Netzwerkteilnehmer nachvollziehbar.

4.2.1 Herausforderungen

Einer der größten Vorteile – Schaffung von Transparenz der Prozesse – kann auch gleichermaßen als große Herausforderung gedeutet werden, da es sich um anlagenscharfe Gebote seitens der Anlagenbetreiber handelt. Dies bedeutet, dass man aus den Geboten Rückschlüsse über Aktivitäten bzw. fehlende Aktivitäten von Anlagen ziehen kann. Dies wiederum kann für manche Marktteilnehmer geschäftskritisch sein, sodass diese dazu geneigt sein könnten, ihre Angebote nicht mit Konkurrenten zu teilen. Um diesem Problem zu entgehen, könnte man die Gebote verschlüsseln. Dies ist aber ein komplexes Problem und impliziert gleichermaßen, dass man sich über die Verwaltung von zusätzlichem Schlüsselmaterial Gedanken machen muss. Daher ist eine genaue Abwägung zwischen den Vor- und Nachteilen der Alternativen unabdingbar und muss auf die jeweilige Situation, in der dieser Anwendungsfall umsetzt werden soll, zugeschnitten sein.

4.2.2 Technische Perspektive

Wie bereits in der Einleitung des Anwendungsfalls erwähnt, spielt die Schaffung eines gemeinsamen, dezentralen Vertrauensraums eine wichtige Rolle in diesem Anwendungsgebiet. Es

[90] WindNODE: https://www.windnode.de, abgerufen: 14. Juni 2021.

WISSEN ÜBER DIE HERKUNFT VON PRODUKTEN KANN EINFLUSS AUF DAS KAUFVERHALTEN HABEN.

sollten nur Technologien für den Handel eingesetzt werden, mit denen Vertrauen in die Angaben Dritter geschaffen werden kann. Genau dieser Vorteil zählt zu den inhärenten Blockchain-Eigenschaften. Im Anwendungsfall wird die Blockchain für den transparenten und gleichzeitig fälschungssicheren Austausch von Stromgeboten eingesetzt. Da die Blockchain bei allen Netzwerkteilnehmer repliziert wird, gibt es folglich keinen einzelnen Ausfallpunkt, wodurch die Verlässlichkeit des Handels über eine Blockchain gewährleistet werden kann. Für den Blockchain-basierten Stromhandel sollte eine private permissioned Blockchain eingesetzt werden, wodurch es leichter möglich wird, die Netzwerkteilnehmer einer Entität zuzuordnen. Denn es ist nicht wünschenswert, wenn unbekannte Teilnehmer Gebote abgeben oder annehmen können, da dies die Integrität des Handels und im nächsten Schritt die Netzstabilität verletzen könnte.

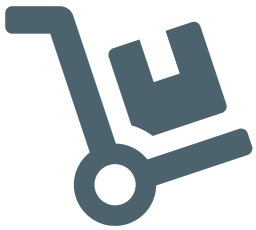
4.2.3 Sicherheitsperspektive

Im Allgemeinen ist Vertrauen in die eingesetzte Lösung – in diesem Beispiel auf Blockchain-Basis – für den Handel von enormer Wichtigkeit für dessen Erfolg. Dies hat wiederum Implikationen für Sicherheitsaspekte wie Vertraulichkeit, Integrität und Verfügbarkeit. Folglich sollten auch aus einer Sicherheitsperspektive nur bekannte Netzwerkteilnehmer die Möglichkeit haben, Stromgebote abzugeben bzw. anzunehmen. Die Verwendung eines privaten Netzwerks wäre dahingehend hilfreich, denn es liefert die notwendige Voraussetzung, dass nur bekannte Netzwerkteilnehmer partizipieren können. Aufgrund der Replikation der Daten sowie der inhärenten Eigenschaften der Blockchain sind die Aspekte Integrität und Verfügbarkeit von Daten sichergestellt. Eine noch offene Frage, die auch schon in der Herausforderung angesprochen wurde, dreht sich um die ggf. geschäftskritische Natur der Gebote. Da diese Gebote anlagenscharf sind, muss geklärt werden, ob diese unter Umständen verschlüsselt auf der Blockchain gespeichert werden sollten, um somit eine zu weit gehende Offenbarung (an Konkurrenten) zu vermeiden. Dies wiederum würde die Vertraulichkeit enorm steigern, würde aber gleichermaßen bedeuten, dass eine zusätzliche Komplexität aufgrund der sicheren Verwaltung des Schlüsselmaterials entsteht. Da dies aber auf Kosten der Transparenz wäre, muss diese Alternative genau abgewogen und an die Situation angepasst werden.

4.2.4 Gesellschaftliche Perspektive

Es ist davon auszugehen, dass bei erfolgreicher Einführung der Blockchain in den Stromhandel viele gesellschaftliche Vorteile entstehen: Mithilfe der Technologie kann die Sicherheit des Energiemarktes steigen, indem eine gemeinsame, konsistente, fälschungssichere Datengrundlage für alle Marktteilnehmer geschaffen wird. Durch die Nachvollziehbarkeit der Transaktionen auf der Blockchain entsteht gleichermaßen auch eine Transparenz der Prozesse. Dies wiederum führt dazu, dass eine bessere Kommunikation zwischen den involvierten Marktteilnehmer ermöglicht wird. Schließlich ist festzustellen, dass die Herkunft von Produkten – dies gilt gleichermaßen für Strom – Einfluss auf das Kaufverhalten haben kann. Demnach könnte bei Erweiterung des Anwendungsfalls auf den Stromhandel mit Privatkund:innen lokal produzierter Strom bevorzugt eingekauft werden, was zugleich zu einer geringeren Belastung des Transmissionsnetzes beitragen würde.

4.3 MARITIME TRANSPORTVERSICHERUNG



Die maritime Transportversicherung ist eine lieferkettenspezifische Versicherung, um die mit Frachtgütern verbundenen Risiken (wie Schäden oder Transportverzögerungen) zu kompensieren. Die Versicherungsart schützt Frachtschiffe und deren Ladung während ihrer gesamten Reise und ist ein wesentlicher Bestandteil des internationalen Handels. Das komplexe multinationale Ökosystem des internationalen Frachttransports umfasst verschiedene Interessengruppen, mehrere Gerichtsbarkeiten und eine hohe Anzahl von Transaktionen. Die Koordinierung aller Prozesse und Akteure bei gleichzeitiger Einhaltung der unterschiedlichen rechtlichen Anforderungen ist für die Seeversicherungsbranche eine große Herausforderung. Darüber hinaus stellt menschliches Versagen aufgrund der Komplexität des Versicherungsprozesses eine Herausforderung für die zuverlässige Ausführung dar. Des Weiteren können sich Verzögerungen, die sich aus den administrativen Fragen rund um die Transportversicherung ergeben, auf die gesamte Lieferkette auswirken. Außerdem kann die Herausforderung, die Versicherungsbedingungen dynamisch an sich ändernde Bedingungen (beispielsweise Gesetzesänderungen) anzupassen, zusätzliche Kosten für die Versicherungsunternehmen und den Handel als Ganzes verursachen.

Eine ganz konkrete Implementierung, um diese Herausforderungen anzugehen, bietet beispielsweise die aktuelle Version von Insurwave[91]. Hierbei soll die Verwendung einer private permissioned Blockchain – im konkreten Beispiel wird die von Guardtime entwickelte Guardtime KSI Plattform eingesetzt – allen Teilnehmern der maritimen Transportversicherungsbranche die Gewissheit geben, dass sie jederzeit auf die gleichen Informationen zugreifen können, während sie in einem sicheren und privaten Netzwerk verbunden sind. Dieses Versicherungssystem für den Seehandel digitalisiert alle Schritte des Versicherungsprozesses, von der Automatisierung der Zahlungen bis hin zum Austausch von Echtzeit-Sendungsinformationen zwischen Handelspartnern, Versicherern und Schadensbearbeitern. Beispielsweise werden Original-Seeversicherungszertifikate, Kopien von Frachtbriefen, Schadensrechnungen usw. in Echtzeit über die Blockchain zwischen allen Vertragsparteien ausgetauscht, wodurch insbesondere die Informationssuch- und Vertragskontrollkosten gesenkt werden und gleichzeitig Transparenz geschaffen wird. Durch den Einsatz von Smart Contracts für den Erfüllungsprozess löst die Blockchain darüber hinaus bestehende Konformitäts- und Vertragsdurchsetzungsprobleme. Ebenfalls verbessern diese Smart Contracts Ineffizienzen im Zusammenhang mit der Aufdeckung von Betrug, ungenauen Produktpreisen und anderen spezifischen Risiken für die Transportversicherung. Dies wiederum führt zur schnelleren, präziseren und kostengünstigeren Bearbeitung von Ansprüchen und Auszahlungen.

In Partnerschaft mit Maersk und mehreren Hafenbehörden bietet die Plattform derzeit Versicherungen für eine Vielzahl von Transportschiffen an und automatisiert gleichzeitig eine große Anzahl von Transaktionen. Der aktuelle Entwicklungsstand der Plattform ist der eines Beta-Produkts. Obwohl die bestehenden Systeme noch nicht ersetzt werden, sind die ersten Tests nach Angaben der Projektpartner äußerst positiv verlaufen, sodass die Blockchain-basierte Lösung neben der herkömmlichen im kommerziellen Einsatz getestet wird.

4.3.1 Herausforderungen

Die Skalierung des Anwendungsfalls auf den globalen maritimen Versicherungsmarkt wird die zentrale Herausforderung sein, da die Kommunikationsmöglichkeit aller relevanten Teilnehmer mit dem Netzwerk durchweg gesichert sein muss. Dies wiederum impliziert, dass jedes Transportschiff, jeder Hafen, jede Aufsichtsbehörde, jede Versicherung etc. Zugang zum Netzwerk haben muss. Im kleineren Rahmen der initialen Ausbaustufe ist dies noch relativ leicht umsetzbar. Bei größeren Fall-

[91] Insurewave: »Digital Pathway for Commercial Insurance«, https://insurwave.com/, abgerufen: 22. Juli 2020.

zahlen wird das jedoch eine enorme Herausforderung sein, die nicht nur technische, sondern auch organisatorische und rechtliche Komplexität beinhaltet.

4.3.2 Technische Perspektive

Neben der Schaffung von Vertrauen und einer verbesserten Verfügbarkeit des Gesamtsystems im Vergleich zum zentralisierten Bestandssystem ist absehbar, dass im Rahmen dieses Anwendungsfalles die Blockchain hauptsächlich für die Speicherung von Daten und die zeitnahe Bereitstellung dieser Daten eingesetzt wird. Die Antwortzeiten können jedoch zwischen den verschiedenen Blockchain-Lösungen stark variieren. Daher müssen der Aspekt der Nutzungsfreundlichkeit und die entsprechenden Antwortzeiten evaluiert und eine Blockchain gewählt werden, die diese Anforderungen erfüllt, was einige Blockchain-Lösungen ausschließt.

Ein weiterer, entscheidender Aspekt ist die Art der Blockchain in Bezug auf die Berechtigungen. Im Kontext dieses Anwendungsfalls ist eine private permissioned Blockchain vorteilhaft. Immer dann, wenn eine neue Technologie in einem grundlegenden Bereich (wie hier dem Versicherungswesen) eingesetzt wird, sollte sie von einer Gruppe einander bekannter Mitwirkenden getestet und bewertet werden.

4.3.3 Sicherheitsperspektive

Wie bereits dargelegt, ist es von größter Bedeutung, dass man der vorgeschlagenen Lösung für die maritime Transportversicherung vertrauen kann. Dies hat Auswirkungen auf Sicherheitserwägungen zu Vertraulichkeit, Integrität und Verfügbarkeit. Demnach sollten nur bekannte Knotenpunkte in der Lage sein, am Akteursnetzwerk im Versicherungsbereich teilzunehmen und die Informationen einzusehen. Das gewährleistet einen ersten Grad an Vertraulichkeit. Integrität und Verfügbarkeit von Daten sind inhärente Eigenschaften der Blockchain. Darüber hinaus gewährleistet eine private permissioned Blockchain in Kombination mit Verschlüsselung der Daten die Wahrung der Geschäftsgeheimnisse der beteiligten Interessengruppen, seien es Einzelpersonen oder Unternehmen. Nur autorisierte Teilnehmer:innen sind so in der Lage, Informationen einzusehen und entsprechend zu agieren.

4.3.4 Gesellschaftliche Perspektive

Kleinere Unternehmen haben aufgrund komplizierter Versicherungspolicen, langwieriger Schadensregulierungsverfahren und unflexibler Prämienzahlungen, die nicht mit ihrem Cashflow im Einklang stehen, bisweilen nur schweren Zugang zu maritimen Transportversicherungen. Neue Unternehmen sind ebenfalls schwer zu versichern, da es an Informationen über ihre Aktivitäten, ihren wirtschaftlichen Status und zu Risikoprofilen im Zusammenhang mit dem Transport ihrer Waren mangelt.

Mit zunehmender Datenverfügbarkeit über Versicherungsnehmer:innen können jedoch die Prämien und damit die Transportkosten gesenkt werden, wodurch die Seeversicherung (und damit der internationale Handel) für kleinere Unternehmen leichter zugänglich wird. Darüber hinaus kann durch den besseren Informationsaustausch zwischen den relevanten Stakeholdern der Unternehmen und den Versicherern die Prämienzahlung flexibler angepasst werden.

Ein weiterer wichtiger Aspekt im Bereich der Transportversicherung ist der Zugriff auf historische und aktuelle Daten. In erster Linie die Versicherer, aber auch andere Beteiligte, müssen die Möglichkeit haben, sowohl auf aktuelle als auch auf historische Daten zuzugreifen, beispielsweise auf frühere Ansprüche und deren Status. Für den Bereich der Transportversicherung ist dies besonders relevant, um die Schäden an Gütern, Fahrzeugen usw. zurückverfolgen und die Glaubwürdigkeit und Verantwortlichkeit bestimmter Interessengruppen und ihrer potenziellen Ansprüche beurteilen zu können. Laut einem kürzlich

BLOCKCHAIN-EINSATZ IM VERSICHERUNGSSEKTOR KANN DIE STANDARDISIERUNG DER VERSICHERUNGSPROZESSE SOWIE DIE ALLGEMEINE TRANSPARENZ ERHÖHEN.

erschienenen WTO-Bericht[92] ist Betrug bei Versicherungsansprüchen weit verbreitet – er wird auf 5 bis 10 Prozent aller Ansprüche geschätzt.[93] Die Blockchain kann auf zwei verschiedene Arten helfen: 1) bei der Konsistenz- und Plausibilitätsprüfung der Versicherungsansprüche und 2) zusätzlich durch automatisierte Sicherstellung, dass für ein und denselben Vorfall nur ein Antrag eingereicht werden kann. Damit wird der Arbeitsaufwand für die Versicherungsunternehmen insgesamt verringert und die mehrfache Einreichung betrügerischer Anträge erschwert.

Im Vergleich zum traditionellen Versicherungsmarkt, der durch papierlastige Prozesse und schwerfällige Verfahren gekennzeichnet ist, die darüber hinaus auch die Transparenz behindern, kann ein Blockchain-Einsatz im Versicherungssektor die Standardisierung der Versicherungsprozesse sowie die allgemeine Transparenz des gesamten Versicherungsprozesses erhöhen. Im Ergebnis trägt Blockchain-Einsatz dazu bei, die Vertragssicherheit zu gewährleisten, doppelte Datenerfassung zu vermeiden und die Möglichkeiten der Risikohandhabung zu verbessern.

Auch könnte eine Blockchain-basierte Lösung den Prozess der Schadensregulierung erheblich vereinfachen, indem es mehreren Unternehmen ermöglicht wird, relevante Datensätze gemeinsam zusammenzustellen. Das Distributed-Ledger-System könnte Versicherer und Kundschaft bei der Vereinbarung von Ansprüchen und Entschädigungen unterstützen. Die Gesamttransparenz des Prozesses würde angesichts der Zugänglichkeit der Daten für alle beteiligten Parteien das Vertrauen stärken und die Usability insgesamt verbessern.

---

[92] Ganne, E.: »Can Blockchain revolutionize international trade?«, World Trade Organization, 2018, ISBN 978-92-870-4761-8.

[93] Lorenz, J. T. et al.: »Blockchain in Insurance–Opportunity or Threat?«, McKinsey & Company, 2017, https://www.mckinsey.com/~/media/mckinsey/industries/financial services/our insights/blockchain in insurance opportunity or threat/blockchain-in-insurance-opportunity-or-threat.ashx, abgerufen: 22. Juli 2020.

5. SCHLÜSSELFAKTOREN FÜR DEN EINSATZ DER BLOCKCHAIN

Auf Basis der technischen Eigenschaften, bekannter Anwendungsfälle und praktischer Erfahrungen lassen sich Schlüsselfaktoren für den erfolgreichen Einsatz einer Blockchain ableiten. Neue Digitalisierungsprojekte wie auch Modernisierungsvorhaben sollten die Blockchain als einen möglichen Baustein effizienter und zielorientierter Lösungen betrachten. Obwohl die möglichen Ausprägungen und Funktionsweisen einer Blockchain sehr vielfältig sind, sollten potenzielle Anwendungsgebiete und Einsatzszenarien bestimmte Kerncharakteristiken erfüllen[94], die im Folgenden erläutert werden. Potenzielle Anwendungsfälle, die einen großen Teil der Faktoren erfüllen, lassen am ehesten einen fundierten und nachhaltigen Einsatz der Blockchain erwarten.

Gemeinsamer Zugriff auf Daten erforderlich.
Die grundsätzliche Ausgangssituation für den Einsatz einer Blockchain ist das Bedürfnis verschiedener Parteien, auf eine bestimmte Auswahl von Daten einen gemeinsamen Zugriff zu gewähren. Wichtig ist hierbei, dass sich die Gesamtheit der Daten für alle Teilnehmer zu einem gegebenen Zeitpunkt exakt gleich darstellt. Änderungen oder Ergänzungen der Daten durch einzelne Teilnehmende sind für alle anderen feststellbar. Es entsteht eine kollektive Datenbasis, die die Grundlage für vielfältige Prozess- und Kommunikationsoptimierungen bilden kann.

Verteilte Organisationsstruktur mit mehreren Teilnehmenden.
Der sinnvolle Einsatz einer Blockchain setzt eine vorhandene oder angestrebte verteilte Organisationsstruktur respektive eine verteilte Struktur zwischen verschiedenen Organisationen und Personen beispielsweise in Konsortien voraus. Innerhalb dieses Netzwerkes interagieren mehrere Teilnehmer mit der Blockchain. Essenziell ist, dass ein klares Governancemodell für das Netzwerk etabliert werden sollte, bevor mit der Umsetzung einer Blockchain begonnen wird. Das bedeutet, dass potenzielle Teilnehmenden, Rollen und Rechte sowie deren Verwaltung definiert werden müssen.

Zentrale Instanzen nicht wünschenswert oder praktikabel.
Ein potenzieller Anwendungsfall sollte immer eingehend dahingehend geprüft werden, ob der Einsatz einer zentralen Lösung nicht ebenfalls möglich ist. Aus technischer Sicht spricht in den meisten Fällen nichts gegen ein solches Vorgehen. Die Entscheidung gegen eine zentrale Instanz sollte aus dringenden organisatorischen, rechtlichen oder politischen Gründen getroffen werden. Aktuell lassen sich zentrale Ansätze deutlich ökonomischer und schneller umsetzen.

Notwendigkeit eines Vertrauensankers.
Die Blockchain spielt ihre Stärken aus, wenn kein zentraler Intermediär verfügbar ist, dem alle Teilnehmenden oder Organisationen gleichzeitig vertrauen. Damit besteht zumindest ein kleines Vertrauensdefizit innerhalb des verteilten Netzwerkes. Das kann auch gelten, wenn alle Beteiligten bekannt sind und sich prinzipiell auf organisatorischer Ebene bereits vertrauen. Denn auf technischer Ebene kann ein Angriff oder ein Fehlverhalten nie restlos ausgeschlossen werden, wodurch die Notwendigkeit eines Vertrauensankers entsteht. Können sich aber alle Beteiligten auf eine zentrale Vertrauensinstanz einigen, sind eventuell Lösungen ohne Blockchain passender.

Verifizierbarkeit und Transparenz von Transaktionen.

Eine wichtige Triebfeder für Blockchain-Anwendungen ist der Wunsch, dass alle Transaktionen für alle Teilnehmenden transparent, d. h. zeitnah und dauerhaft einsehbar sind. Dies schließt auch ein, dass vergangene Zustände des Datenbestandes abrufbar sind. Dies gewährleistet Verifizierbarkeit, die wiederum das Vertrauen innerhalb eines Netzwerkes steigert. Erfordert ein Anwendungsfall ein genau gegenteiliges Verhalten, also die explizite und vollständige Einschränkung von lesenden Zugriffen Dritter, ist die Blockchain in den meisten Fällen keine geeignete Lösung.

Widerstandsfähigkeit und Verfolgbarkeit von Manipulationsversuchen.
Das Design der Blockchain macht sie sehr widerstandsfähig gegenüber Manipulationen. Wie bei jedem Softwareprodukt kann ein Angriff nie restlos ausgeschlossen werden. Diesem Risiko wird bei der Blockchain durch ein sehr effektives und schnelles Verfahren zur Verfolgung und Entdeckung von Manipulationen begegnet. Anwendungsfälle, bei denen Manipulati-

[94] Wüst, K.; Gervais, A.: »Do you need a blockchain?«, 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), S. 45 – 54, IEEE, doi:10.1109/CVCBT.2018.00011.

ANWENDUNGSFÄLLE, DIE EINEN GROSSEN TEIL DER FAKTOREN ERFÜLLEN, LASSEN AM EHESTEN EINEN FUNDIERTEN UND NACHHALTIGEN EINSATZ DER BLOCKCHAIN ERWARTEN.

onssicherheit eine primäre Anforderung ist, profitieren von der Blockchain und können so sehr sicher umgesetzt werden. Es ist trotzdem wichtig, sich zu vergegenwärtigen, dass eine 100-prozentige Manipulationssicherheit bei einer Softwarelösung nie gewährleistet ist.

Validierung von Transaktionen erforderlich.
Eine besondere Eigenschaft der Blockchain ist die Vielfalt der Konzepte zur Konsensbildung über die Validität von Transaktionen innerhalb des Netzwerkes. Neben dem bekannten Proof-of-Work sind weitere Verfahren verfügbar oder können individuell angepasst werden. Im Kern können bestehende Prozesse für organisatorische Entscheidungsfindung technisch abgebildet und durchgesetzt werden. Anwendungen auf Basis der Blockchain können dadurch auch verteilte Prozesse abbilden, die mit traditionellen Lösungen nicht darstellbar sind.

Abwägung zwischen Offenheit und Vertraulichkeit.
Beim Entwurf jedes potenziellen Blockchain-Anwendungsfalles sollte eine Abwägung zwischen der systembedingten Offenheit und eventuell durch Regularien oder den Teilnehmenden geforderte Vertraulichkeit erfolgen. Das bedeutet, dass vor der Umsetzung sichergestellt werden muss, dass ein Blockchain-Einsatz Datenschutz oder Geheimhaltungsbedarf nicht zuwiderläuft. Ein konkreter Plan für das Datenmanagement sollte mit allen Beteiligten ausgearbeitet werden.

Vermeidung der Disruption bestehender Prozesse und Strukturen.
Eine unmittelbare Abbildung bestehender und etablierter Prozesse und Daten(management)strukturen auf eine Blockchain-Lösung ist meist nicht möglich. Bei der Umsetzung von Anwendungsfällen mit einer Blockchain-Lösung müssen existierende Verfahren eventuell durch von Grund auf neu entwickelte ersetzt werden. Nur so können die Vorteile der Blockchain nutzbar gemacht und grundlegende Fehler vermieden werden. Da für diesen Ersetzungsprozess noch Erfahrungswerte fehlen, ist es ratsam, sich zunächst auf gänzlich neue Anwendungsfälle zu konzentrieren. So kann vermieden werden, dass zum jetzigen Zeitpunkt möglicherweise erhebliche Ressourcen für einen Umstieg aufgebracht werden, die sich eventuell zukünftig durch einen teilweise standardisierten und automatisierten Umstieg mit deutlich geringerem Aufwand realisieren ließe. Ebenso kann erst die Erfahrung zeigen, wann ein vornehmlich ökonomisch motivierter Umstieg überhaupt sinnvoll ist.

Investitions- und Innovationsbereitschaft.
Organisationen sollten über eine hohe Investitions- und Innovationsbereitschaft verfügen, wenn sie die Blockchain einsetzen wollen und langfristig als Lösungsbaustein einplanen. Die Realisierung entsprechender Anwendungen ist kein kurzfristiges Vorhaben und der aktuelle technische Stand der Blockchain erlaubt keine Erfolgsgarantie. In den allermeisten Fällen können derzeit mit zentralen Lösungen schneller und kostengünstiger Ergebnisse erzielt werden. Langfristig bietet die Blockchain allerdings große Potenziale für Prozessoptimierung und Kosteneinsparungen.

Abschließend ist festzuhalten, dass sich die Blockchain und verwandte Technologien kontinuierlich weiterentwickeln, wodurch sich auch mögliche Anwendungsfälle und Schlüsselfaktoren wandeln und weiterentwickeln bzw. eine Neubewertung erforderlich machen werden.

6. HANDLUNGSEMPFEHLUNGEN

Gemeinsames Verständnis schaffen.
In aktuellen Diskussionen ist immer wieder erkennbar, dass verschiedene Akteur unterschiedliche Vorstellungen von Begriffen wie »Blockchain«, »Distributed Ledger« etc. haben. Ohne ein gemeinsames Grundverständnis ist eine Weiterentwicklung der Diskussion jedoch nur schwer möglich. Es ist wünschenswert, dass übergeordnete und einheitliche Definitionen der wichtigsten Begriffe in einem gemeinschaftlichen Begriffskanon festgehalten werden, um eine gemeinsame Grundlage für zukünftige Diskussionen zu schaffen. Im Idealfall wird diese Bestrebung von neutralen Organisationen, wie Normungsgremien oder Verbänden, koordiniert.

Die Blockchain-Technologie in Pilotprojekten erkunden.
Wie dargestellt, existieren bereits vielversprechende Anwendungsfelder, in denen der Einsatz einer Blockchain vorteilhaft erscheint. Pilotprojekte in diesen Anwendungsfeldern sollten weiter beobachtet und evaluiert werden, um den praktischen Blockchain-Einsatz weiter zu erkunden. Darüber hinaus müssen weiterhin neue Projekte, Reallabore oder Testzentren initiiert und gefördert werden. Forschungseinrichtungen und Unternehmen müssen hierfür mit entsprechenden (Förder-)Mitteln ausgestattet werden. Öffentliche Förderprogramme und Risikokapital spielen hier eine entscheide Rolle. Denn nur mit einem vertieften und praktischen Verständnis der Blockchain-Technologie können die optimalen Anwendungsfelder identifiziert und die Technologie bestmöglich genutzt werden.

Forschung und Entwicklung zur Lösung rechtlicher Anforderungen vorantreiben.
Auch wenn durch die Blockchain-Strategie der Bundesregierung und durch erste Standardisierungsaktivitäten und Rechtsentscheidungen der Weg für einen klareren rechtlichen Rahmen geebnet wird, ist ein Blockchain-Einsatz weiterhin mit rechtlichen Unklarheiten verbunden. Auch die Strategien und Möglichkeiten zur Vereinbarkeit von DSGVO und Blockchain müssen weiter untersucht und bekannter gemacht werden, um offene Fragen zu beseitigen. Denn aktuell führen diese noch dazu, dass Industrie und Verwaltung weitere Entscheidungen abwarten, was einen möglichen Blockchain-Einsatz verzögert. Höchste Priorität sollte sein, durch weitere Forschung und Entwicklung sowie auf Basis eines Dialogs mit Vertreter:innen aus Industrie und Verwaltung einen rechtssicheren Blockchain-Einsatz zu ermöglichen.

Standardisierung sowie Interoperabilität von Blockchain-Ansätzen fördern.
Die Entwicklung von Blockchain-Lösungen ist von proprietären Lösungen und Schnittstellen dominiert. Einheitliche Standards und Spezifikationen existieren nicht. Daraus resultiert die Gefahr, dass nicht-interoperable Insellösungen mit Abhängigkeiten zu proprietären Implementierungen und einzelnen Herstellern entstehen. Diese Gefahren wirken sich negativ auf die technische Souveränität der Anwendenden und auf die Nachhaltigkeit der einzelnen Lösungen aus. Die Standardisierung hat bereits begonnen, was allen Akteuren die Möglichkeit bietet, sich aktiv an den Standardisierungsaktivitäten zu beteiligen und so die weitere Entwicklung zu beeinflussen.

Entwicklung von Leitfäden und Best Practices für den Blockchain-Einsatz.
Wie im Kapitel »Schlüsselfaktoren für den Einsatz der Blockchain aufgezeigt, sollten potenzielle Anwendungsszenarien für die Blockchain bestimmte Charakteristiken aufweisen. Die Komplexität verfügbarer Blockchain-Ansätze und -Ausprägungen erschwert eine optimale Auswahl für angedachte Anwendungsfälle. Erfolgreiche Anwendende aus Industrie und Forschung sollten daher praktische Leitfäden und Erfolgsrezepte entwickeln, damit zukünftige Anwendungsszenarien von deren Erfahrungswerten profitieren können.

Zertifizierungsstellen für Smart Contracts aufbauen.
Smart Contracts sind der zentrale Baustein für den Transfer realer Wertobjekte mithilfe von Blockchain-Technik. Entsprechend hoch sind die Anforderungen an Sicherheit und Qualität der Smart Contracts. Bisher wird nur eine geringe Zahl von Smart Contracts unabhängig und qualifiziert überprüft, daher sind Fehler und Sicherheitslücken nicht selten. Um die Akzeptanz und das Vertrauen für Blockchain-Lösungen zu erhöhen, sollten einheitliche Prüfverfahren sowie Instanzen zur Prüfung und Zertifizierung von Smart Contracts aufgebaut werden, wie sie für andere Softwarelösungen existieren. Denn Vertrauen in die Korrektheit von Smart Contracts ist eine wesentliche Bedingung für deren Nutzung.

BEGRIFFE

Anreizmechanismus
Wird genutzt, um in einem Blockchain-System die Generierung neuer Blöcke attraktiv zu machen. Dies wird üblicherweise über Transaktionsgebühren gelöst.

Blockchain
Spezielle Form eines Distributed Ledgers, in der Transaktionen in Blöcke zusammengefasst und diese in einer Liste verlinkt werden. Die Verlinkung ist durch kryptografisches Hashing so abgesichert, dass die Manipulation eines Blocks durch einfache Prüfung aller Nachfolgeblöcke bemerkbar wird.

Blockchain-Plattform
Technische Grundlage oder Framework, um ein konkretes Blockchain-System zu betreiben.

Blockchain-System
Spezielle Form eines verteilten Systems, in der Nodes nach einem bestimmten Protokoll interagieren. Insbesondere wird eine Blockchain als Datenstruktur verwendet. Idealerweise handelt es hierbei auch um ein dezentrales System.

Blockgröße
Legt im Protokoll fest, wie viele Transaktionen in einem Block zusammengefasst werden können.

Blockzeit
Beschreibt, in welchem Zeitrahmen ein neuer Block generiert wird. Dies wird üblicherweise durch das Konsensverfahren implizit festgelegt.

Coin
Inhärente Kryptowährung, die innerhalb eines Blockchain-Systems gehandelt wird. Diese ist im Protokoll des Blockchain-Systems festgelegt. Initiale Guthaben werden hierbei im Genesis Block festgelegt. Üblicherweise existiert in einem Blockchain-System nur eine Art von Coin.

Dezentrale Anwendung (DApp)
Anwendung, die in einem dezentralen System ausgeführt wird. Üblicherweise basiert das Backend einer dezentralen Anwendung auf Smart Contracts, die in einem öffentlichen dezentralen Blockchain-System eingesetzt werden. In diesem Fall ist der Programmcode des Backends öffentlich sichtbar. Das Frontend hingegen kann eine zentralisierte Anwendung sein, deren Programmcode nicht veröffentlicht wird.

Dezentrales System
Verteiltes System, in dem die Nodes nicht von einer zentralen Instanz kontrolliert werden. Dabei ist die Verwaltung der Zugehörigkeit der einzelnen Nodes zum dezentralen System nicht zwangsweise unter dezentraler Kontrolle, diese kann auch durch eine zentrale Instanz erfolgen.

Digital Asset
Besitzgut, das in einem Blockchain-System mittels Transaktionen gehandelt wird. Ein typischer Anwendungsfall ist eine Kryptowährung.

Distributed Ledger
Spezielle Form eines verteilten Registers zur Speicherung authentifizierter Transaktionen. Der Zustand des Distributed Ledgers ist durch vorhandene Transaktionen und deren Reihenfolge definiert.

Fork
Entsteht, wenn zwei oder mehr Blöcke auf denselben Vorgänger-Block verlinken. Dieser Konflikt wird durch das Konsensverfahren aufgelöst.

Genesis Block
Der erste Block in der Blockchain. Der Genesis Block hat keinen Vorgänger-Block und beschreibt den initialen Zustand der Blockchain.

Hard-Fork
Bei einem Hard-Fork steigen Teile des Blockchain-Systems auf ein neues Protokoll um, zum Beispiel Erhöhung der Blockgröße. Neue Blöcke, die nach dieser Art erstellt werden, sind dann von dem anderen Teil des Blockchain-Systems nicht mehr interpretierbar. Das Blockchain-System wird hierbei in zwei Teile aufgeteilt.

Hashing
Beim kryptografischen Hashing wird für Eingabedaten durch eine sogenannte Hashfunktion eine Kurzfassung der Eingabedaten (ein Hashwert) produziert. Dabei ist die Hashfunktion so entworfen, dass der Hashwert keinerlei Rückschlüsse auf die Eingabedaten zulässt.

Initial Coin Offering/Initial Token Offering

Ähnlich wie beim Börsengang wird Nutzer:innen angeboten, in ein Projekt zu investieren. In Abhängigkeit von der Investitionssumme werden den Nutzer:innen eine Anzahl an Coins bzw. ein oder mehrere Token gutgeschrieben und die Nutzer:innen durch etwaige Wertsteigerungen der Gutschriften ggf. am Erfolg des Projekts beteiligt. Bei Coins wird die initiale Anzahl für die Nutzer:innen im Genesis Block festgehalten, bei Token in einem Smart Contract.

Konsensverfahren/Consensus Algorithm

Prozess zur Einigung über den Zustand der Blockchain. Je nach Konsensverfahren wird das Ergebnis der Einigung deterministisch oder probabilistisch erzielt.

Merkle-Tree

Datenstruktur, in der Transaktionen abgelegt werden und aus der ein eindeutiger Hashwert produziert wird, sodass bei Manipulation einer Transaktion die Veränderung im Hashwert bemerkbar ist.

Mining

Beschreibt das Suchen/Finden bzw. Generieren eines neuen Blocks bei Einsatz des Proof-of-Work-Mechanismus. Beim Proof-of-Stake-Mechanismus wird dieser Prozess analog als Forging bezeichnet.

Mining-Pool

Zusammenschluss von Nodes, um gemeinsam schneller einen Block zu finden und die Belohnung zu teilen. Im Zusammenhang mit dem Proof-of-Stake-Mechanismus wird ein solcher Zusammenschluss analog als Stake-Pool bezeichnet.

Node

Ein Computer, der in einem verteilten System interagiert. Full-Nodes verfügen über eine Kopie des gesamten Registers. Light-Nodes benötigen keine Kopie oder nur Teile des Registers, interagieren aber auch nur eingeschränkt mit dem System.

Off-Chain

Prozesse in einem Blockchain-System, die den Zustand der Blockchain nicht verändern.

On-Chain

Prozesse in einem Blockchain-System, die den Zustand der Blockchain verändern.

Protokoll

Die Regeln eines verteilten Systems. Dies beinhaltet insbesondere Rechte, Verantwortlichkeiten und wie die Nodes miteinander kommunizieren und interagieren.

Smart Contract

Programmcode, der in der Blockchain gespeichert wird. Die Aufruftransaktion mit Eingabeparametern und das Ergebnis einer Ausführung werden in der Blockchain festgehalten. Zur Validierung führen die Knoten des Blockchain-Systems den Programmcode mit den Eingabeparametern aus und prüfen so das Ergebnis.

Soft-Fork

Bei einem Soft-Fork steigen Teile des Blockchain-Systems auf ein neues Protokoll um. Neue Blöcke, die nach dieser Art erstellt werden, sind jedoch von dem anderen Teil des Blockchain-Systems weiterhin interpretierbar.

Token

Ähnlich wie Coins sind Token Nutzer:innen zugeordnet und können übertragen werden. Üblicherweise wird eine Token-Art durch einen Smart Contract erstellt und kann zusätzliche Informationen beinhalten oder auf externe Ressourcen verweisen. Theoretisch können beliebig viele Arten von Token in einem Blockchain-System existieren.

Transaktion

Veränderung des Registerzustandes aus Sicht von Nutzer:innen. Je nach Register kann eine Transaktion beliebige Daten betreffen.

Verteiltes Register/Verteilte Datenbank

Datenbank, deren Daten auf mehreren Computern konsistent gespeichert werden.

Verteiltes System

Ein Netzwerk aus Computern, die miteinander interagieren und im Kontext dieses Dokumentes ein verteiltes Register teilen. Insbesondere erscheint ein verteiltes System aus Sicht der Nutzer:innen als einheitliches System.

Wallet

Software, die genutzt wird, um Schlüssel zu verwalten und Transaktionen zu signieren. Bei einem Hardware-Wallet befindet sich diese Software auf einer speziell dafür ausgelegten Hardware.

KONTAKT

Jens Tiemann
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-948582-06-7