KONRAD ADENAUER STIFTUNG

Token Studie

#KAS4 INNOVATION

Grundlagen und Anwendungsszenarien der Blockchain-Technologie

Token Studie

Grundlagen und Anwendungsszenarien
der Blockchain-Technologie

Impressum

Herausgeberin:
Konrad-Adenauer-Stiftung e. V., 2023, Berlin

Ansprechpartner in der Konrad-Adenauer-Stiftung:
Jason Chumtong
Referent Künstliche Intelligenz
Analyse und Beratung
T +49 30 26996-3989
jason.chumtong@kas.de

Gestaltung und Satz: Kaluza + Schmid Studio GmbH
Die Printausgabe wurde bei der Druckerei Kern GmbH, Bexbach, klimaneutral produziert und auf FSC-zertifiziertem Papier gedruckt.
Printed in Germany.

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-124-3

Auf einen Blick

- Der Einsatz der Blockchain-Technologie erfolgt, abseits der Kryptowährungen, in immer mehr Anwendungsgebieten. Im Rahmen dieser Studie wird ein umfassender und detaillierter Überblick über alle wesentlichen Elemente und Entwicklungen rund um die Blockchain-Technologie gegeben.

- Die dezentrale Architektur der Blockchain-Technologie ermöglicht mithilfe von Konsensmechanismen die eindeutige Zuordenbarkeit von Besitz sowie die Peer-to-Peer-Übertragbarkeit von Werten über das Internet. Nutzerinnen und Nutzer von Blockchain-basierten Anwendungen können auf die Datenintegrität der Blockchain vertrauen, da Transaktionen nur nach fest definierten Regeln durchgeführt und fälschungssicher aufgezeichnet werden. Auf Basis der Technologie sind zukunftsweisende, innovative Applikationen entstanden. Hier sind insbesondere Smart Contracts für die Automatisierung von Prozessen sowie die Möglichkeiten zur Digitalisierung von Werten durch die Tokenisierung zu nennen.

- Besonders in der Finanzindustrie findet der Einsatz der Blockchain-Technologie Anklang. Hervorzuheben sind Deutschland und die Europäische Union. Beide haben auf regulatorischer Ebene, wenn auch in unterschiedlicher Ausprägung und Geschwindigkeit, sowohl die Weichen für Dienstleistungen im Bereich Kryptowährungen als auch für den Einsatz der Blockchain-Technologie im Kontext traditioneller Wertpapiere gestellt.

- Des Weiteren sind erste Anwendungsfälle aus der Realwirtschaft im Markt zu beobachten, die das Potenzial für eine breite Markttauglichkeit bieten. Diese sind vielfältig und reichen von nutzungsabhängiger Bezahlung von Maschinen in der verarbeitenden Industrie (Pay-per-Use) bis hin zu Möglichkeiten, die Vorteile der Technologie im Lieferkettenmanagement auszuschöpfen. Auch die Nutzung der Blockchain-Technologie zur Abbildung von CO_2-Zertifikaten kann für die nähere Zukunft erwartet werden. Anhand des Beispiels Lieferkettenmanagement zeigt sich allerdings auch, dass die Blockchain-Technologie nicht als Allheilmittel verstanden werden darf. Die Manipulation der Daten ist nicht möglich, wenn sich die Daten auf der Blockchain befinden. Manipulationsmöglichkeiten entstehen jedoch, wenn die Blockchain auf Daten von der Außenwelt angewiesen ist, die nur schwierig oder überhaupt nicht messbar sind und gegebenenfalls eine subjektive menschliche Einschätzung benötigen.

- Als Basisinfrastruktur für eine Vielzahl an Anwendungsgebieten sind digitale, Blockchain-basierte Identitäten zwingend erforderlich. Der Staat hätte auf dieser Grundlage die Möglichkeit, behördliche Leistungen für die Bürgerinnen und Bürger digital zugänglich zu machen und Kosteneffizienzen zu realisieren, indem manuelle, administrative Tätigkeiten abgebaut werden. Fehlende Lösungen im Bereich der digitalen Identitäten werden für Nutzerinnen und Nutzer künftig vermehrt zu Medienbrüchen bei der Nutzung digitaler Dienstleistungen oder Applikationen führen. Der Staat sollte dieses Thema auch deshalb stark vorantreiben, um die Datensouveränität der Bürgerinnen und Bürger gegenüber den großen Technologieunternehmen zu sichern.
- Aufkommende Trends und Neuentwicklungen zeigen, dass die Innovationskraft der Blockchain-Technologie bei Weitem nicht ausgeschöpft ist. Das Web 3.0 als weitere Ausbaustufe des Internets ermöglicht es Nutzerinnen und Nutzern, auf Basis der Blockchain-Technologie die Kontrolle über ihre eigenen Daten zu erlangen. Die Marktmacht von großen zentralisierten Plattformen wird verstärkt in Richtung der Anwenderinnen und Anwender verlagert. Das sich im frühen Entwicklungsstadium befindliche Metaverse schafft miteinander verbundene, virtuelle 3-D-Erlebniswelten, die eine von seinen Anwenderinnen und Anwendern kontrollierte Internetökonomie darstellt, um tokenisierte Werte zu handeln und zu besitzen. Hier sind insbesondere NFTs zu nennen, die im letzten Jahr durch die Tokenisierung von digitalen und physischen Kunstwerken oder Sammlerstücken in Onlinespielen auf sich aufmerksam gemacht haben.

Inhalt

Vorwort 8

Einleitung 10

Grundlagen
der Blockchain-Technologie 12

Regulatorik
in Deutschland und Europa 24

Anwendungsfälle
der Blockchain-Technologie 30

Ausblick 38

Fazit 44

Literaturverzeichnis
und Glossar 48

0

Vorwort

0 — Vorwort Prof. Dr. Sandner, Leiter des Frankfurt School Blockchain Center

Die Blockchain-Technologie eignet sich ausgezeichnet für die digitale Abbildung von Werten – das können Aktien, Immobilien, Schuldtitel, Währungen oder Krypto-Assets sein, zum Beispiel NFT, Decentralized Finance. Aus diesem Grund sind Anwendungsfälle im Bereich der Finanzen in den vergangenen Jahren stark gewachsen.

Das bisher prominenteste Anwendungsgebiet sind die Krypto-Assets, in deren Kontext besonders drei Innovationen der Blockchain-Technologie zu nennen sind.

1. Dezentrale Infrastrukturen wie Bitcoin, in denen es keine zentrale Instanz gibt, die über eine Kontrollhoheit verfügt.
2. Smart Contracts, elementare Bestandteile von Ethereum und ähnlichen Plattformen, mit deren Hilfe Zahlungsströme programmiert und automatisch ausgeführt werden können.
3. Die Tokenisierung, also die digitale Darstellung von Rechten und Pflichten jeglicher Vermögenswerte auf einer Blockchain.

In der Summe haben wir also eine dezentrale Basisinfrastruktur wie etwa Ethereum, auf welcher sich Vermögenswerte tokenisieren lassen. Der Austausch dieser Token ist dann programmierbar. Diese grundlegenden Vorteile der Blockchain-Technologie erkennen zunehmend auch Unternehmen. Und wir stehen erst am Anfang der Revolution. Die Themen Web 3.0, Metaverse und NFTs versprechen enormes Potenzial einer digitalen, dezentralen Ökonomie.

Um die Blockchain-Technologie zu fördern und als Wirtschaftsstandort Deutschland beziehungsweise Wirtschaftszone Europäische Union (EU) attraktive Bedingungen für Nutzerinnen und Nutzer sowie Unternehmen zu schaffen, braucht es adäquate Regulatorik. Dabei kann die Blockchain-Technologie selbst nicht reguliert werden – denn sie ist dezentralisiert und von einzelnen Staaten unabhängig. Es geht also darum, die Interaktion zwischen Nutzerinnen und Nutzern sowie Unternehmen in diesem Bereich rechtssicher zu gestalten, um Verbraucherschutz zu fördern und kriminelle Aktivitäten wie Geldwäsche zu verhindern. Um dem grenzübergreifenden Charakter der Technologie gerecht zu werden, muss dies auf internationaler Ebene geschehen. Deutschland und die EU sollten hier Vorreiter werden.

Die Schaffung eines Rechtsrahmens für die Blockchain-Technologie und die staatliche Förderung von Anwendungsfällen, zum Beispiel durch digitale, Blockchain-basierte Identitäten, sind elementar, um die digitale Souveränität der Bürgerinnen und Bürger gegenüber den globalen Technologieunternehmen in der nächsten Evolutionsstufe des Internets zu schützen. Dies zu verpassen, bedeutete auch, beim digitalen Transfer von Werten technologisch abgehängt zu werden und signifikante wirtschaftliche Potenziale ungenutzt zu lassen. Die bisher auf den Weg gebrachte deutsche Gesetzgebung hat im Bereich von Kryptowerten bereits gezeigt, wie es gehen kann. Die EU folgt durch die 2024 in Kraft tretende Verordnung über Märkte für Kryptowerte (MiCAR).

1

Einleitung

1 — Einleitung

Mit dem Begriff „Blockchain“ werden häufig sogenannte Distributed-Ledger-Technologien (DLT) beschrieben. Obwohl die DLT per se keine neue Technologie ist, hat sie doch in den vergangenen Jahren durch die stetig wachsende Popularität von Kryptowerten signifikant an Bedeutung im ökonomischen Kontext und an Aufmerksamkeit im öffentlichen Diskurs gewonnen.

Doch die DLT ist mehr als Kryptowerte: Auch abseits von Bitcoin, Ethereum und Co. existieren viele Bestrebungen, die Vorzüge der DLT gewinnbringend einzusetzen. Besonders im Finanzmarkt entstehen derzeit mehrere DLT-basierte Anwendungsszenarien, unterstützt durch eine fortschreitende Regulierung in Deutschland und der Europäischen Union (EU). Zu nennen sind auf deutscher Ebene die Emission und Abwicklung von Kryptowertpapieren, nach dem Gesetz über elektronische Wertpapiere (eWpG), und Kryptofondsanteilen, durch die im Juni 2022 in Kraft getretene Verordnung über Kryptofondsanteile (KryptoFAV). Auf europäischer Ebene ist die Verordnung über Märkte für Kryptowerte (MiCAR) hervorzuheben, die einen einheitlichen Rechtsrahmen für Marktteilnehmer im Umgang mit Kryptowerten schaffen wird. Auch aufseiten der klassischen Finanzinstrumente (Aktien, Anleihen und Investmentfonds) ist Bewegung innerhalb der EU: Die am 23. März 2023 in Kraft tretende Pilotregelung ermöglicht den Handel und die Abwicklung von DLT-basierten Marktinfrastrukturen.

Auch außerhalb des Finanzmarktes wird der Einsatz DLT-basierter Anwendungen branchenübergreifend getestet. Automobilhersteller versuchen, DLT-basierte Bezahlvorgänge zwischen Elektroladestationen und Lkw zu realisieren[1] oder die Kfz-Versicherungsbeiträge anhand der tatsächlich gefahrenen Kilometer zu berechnen.[2] Ebenso kommt die DLT auch bei Pay-per-Use-Konzepten zum Einsatz, bei der Maschinen nutzungsabhängig mithilfe von eindeutigen und manipulationssicheren Datensätzen abgerechnet werden.[3] Allerdings fehlt hierzu noch der Euro auf Blockchain-Basis (Stablecoin).

Wie relevant das Thema ist, zeigt sich auch in der Blockchain-Strategie der Bundesregierung. Besonderes Potenzial wird der Blockchain-Technologie hier im Bereich Lieferketten zugesprochen.[4] In der heutigen globalisierten Welt verspricht die Blockchain-Technologie Transparenz und Nachvollziehbarkeit von Daten, die letztlich zu einer besseren Produktqualität führen soll. Ebenso bei Themen rund um das Identitätsmanagement bietet die Blockchain-Technologie ein erhebliches Potenzial. Das Konzept der Self-Sovereign Identity (SSI) auf Blockchain-Basis ermöglicht es Nutzerinnen und Nutzern, eine eigene digitale Identität vollständig selbst zu verwalten, ohne sich auf Dritte verlassen zu müssen. SSIs machen Nutzerinnen und Nutzer zu endgültigen Eigentümern der persönlichen Daten.

In der vorliegenden Studie werden die technischen Eigenschaften der DLT anhand ihres bisher bedeutendsten Anwendungsfalls, den Kryptowährungen, erläutert. Hinsichtlich der technologischen Architektur wird insbesondere die Rolle der Konsensmechanismen thematisiert. Ferner differenziert die Studie zwischen verschiedenen Arten von DLT-basierten Infrastrukturen: nicht zugangsbeschränkte, öffentliche sowie zugangsbeschränkte, private und konsortiale Blockchains. Zusätzlich wird ein Einblick in aktuelle regulatorische Entwicklungen, auch mit Fokus auf die Rechtsprechung in Deutschland und der EU, vermittelt. Darauf aufbauend werden die Auswirkungen der DLT auf die Industrie und den Finanzsektor anhand ausgewählter Anwendungsbeispiele erläutert. Abschließend gibt die Studie einen Ausblick auf die weitere Entwicklung der DLT zu den Themen Metaverse, Non-Fungible Token (NFT) und Web 3.0.

1 Vgl. Commerzbank, 2019.
2 Vgl. The Ford Motor Company, 2021.
3 Vgl. Godenrath, 2022.
4 Vgl. Bundesministerium für Wirtschaft und Energie, 2019.

2

Grundlagen der Blockchain-Technologie

2 — Grundlagen der Blockchain-Technologie

Die Blockchain-Technologie ist eine Unterform der DLT und bezeichnet eine dezentrale IT-Infrastruktur (siehe Abbildung 1) zur Validierung, Speicherung und Aktualisierung von Datensätzen (zum Beispiel Transaktionen). In einer Blockchain werden Daten in Datenblöcken (Blocks) gespeichert. Jeder Block dieser Datenbank ist mit einem Zeitstempel versehen und mit dem vorhergehenden Block kryptografisch verknüpft, wodurch eine chronologische und unveränderliche Reihenfolge der Datensätze entsteht. Innerhalb dieser Studie werden die Begriffe „Blockchain“ und „DLT“ synonym verwendet.

Mit einer Blockchain können Werte und Informationen direkt zwischen den Teilnehmerinnen und Teilnehmern übertragen werden (Peer-to-Peer) – ohne zentrale Akteure oder Administratoren (siehe Abbildung 2). Um sicherzustellen, dass die vorhandenen Daten im Netzwerk korrekt sind, bedarf es daher eines Regelwerks, das alle Teilnehmenden der Blockchain befolgen. Hierfür verwenden Blockchains Konsensmechanismen. Sie legen die Bedingungen fest, unter denen die Datensätze und Blöcke in die Blockchain aufgenommen werden. Mithilfe des Konsensmechanismus können die Teilnehmenden eines Netzwerks Transaktionen prüfen, bestätigen und unwiderruflich kryptografisch miteinander verknüpfen, um sie letztendlich verteilt abzuspeichern.[5]

Hashfunktionen

Um die Sicherheit und Datenintegrität innerhalb einer Blockchain sicherzustellen, kommen kryptografische Hashfunktionen zum Einsatz. Sie können eine Zeichenfolge von variabler Länge in eine Zeichenfolge fixer Länge umwandeln (siehe Abbildung 3). Bei genau gleichen Inputdaten ergeben Hashfunktionen somit immer dieselben Outputdaten (Hashwert). In der Blockchain-Architektur dienen Hashfunktionen als vertrauenswürdige Prüfsumme eines Datenblocks. Eine spätere Änderung eines in der Blockchain gespeicherten Datenblocks hat zwangsläufig auch immer eine Änderung des Hashwerts zur Folge (siehe Abbildung 4). Da alle Datenblöcke in der Blockchain kryptografisch aufeinander aufbauen, verändern sich demnach auch alle auf den geänderten Block folgenden Datenblöcke. Durch dieses Verfahren sichern Blockchains – bei über die Zeit hinweg anfallenden Transaktionen – ihre Integrität, denn die fälschungssicheren Daten ermöglichen es den Netzwerkteilnehmenden, sich untereinander zu vertrauen, ohne sich zu kennen.

5 Vgl. Bundesnetzagentur, 2019.

2 — Grundlagen der Blockchain-Technologie

Folgend ein Beispiel, um die Nutzung von Hashwerten in Blockchains zu demonstrieren: Mehrere Unternehmen eines Konsortiums einigen sich auf einen Vertragstext und nutzen dabei eine Blockchain zur manipulationssicheren Speicherung des Inhalts.[6] Das Konsortium bildet dazu aus dem Vertragsinhalt einen Hashwert, der zum Beispiel „0x8L8Z210P“ heißt. Änderungen am originalen Vertragsinhalt, auch wenn nur marginal, würden zu einem anderen Hashwert führen. Das Konsortium speichert den Hashwert in der Blockchain ab, jedoch nicht den Vertragsinhalt. Nun hat ein weiteres Unternehmen zu einem späteren Zeitpunkt Interesse an einer Aufnahme in das Konsortium. Möchte es sich zuvor sicher sein, dass für dieses Unternehmen die gleichen vertraglichen Bedingungen wie für alle anderen gelten, könnte das neue Unternehmen zur Überprüfung aus dem ihm zur Verfügung gestellten Vertragsinhalt selbst noch einmal den Hashwert bilden. Ist der obere Hashwert in der Blockchain abgelegt, kann das Unternehmen, das in das Konsortium aufgenommen werden möchte, sicher sein, dass genau dieser Vertragsinhalt auch zwischen den übrigen Mitgliedern des Konsortiums vereinbart wurde.

Zusätzlich haben Hashfunktionen noch zwei weitere Vorteile: Erstens kann eine dritte Person aus dem in der Blockchain abgelegten Hashwert nicht den Vertragsinhalt rekonstruieren. Zweitens ist es mit vertretbarem Aufwand nicht möglich, zwei verschiedene Dateninputs zu finden, die denselben Hashwert ergeben.[7]

Konsensmechanismen

Der dezentrale Charakter einer Blockchain macht ein Regelwerk notwendig, um die Bedingungen für das Hinzufügen von Daten präzise festzulegen. Die Datenintegrität einer Blockchain ist essenziell, da sie füreinander unbekannte Akteure die Grundlage bildet, um miteinander interagieren zu können. Es gilt also, unbefugtes Hinzufügen sowie nachträgliche Veränderungen von Daten zu verhindern. Zwar fällt eine nachträgliche Veränderung von Daten in einer Blockchain sofort durch die Einzigartigkeit der Hashwerte auf (siehe vorheriger Abschnitt), sollte ein Angreifer allerdings die Mehrheit des Stimmgewichts in einem Netzwerk besitzen, so hätte er die Macht, die Daten zu manipulieren. Um ein solches Szenario zu verhindern und die Gültigkeit der Daten innerhalb eines verteilten Netzwerks sicherzustellen, werden Konsensmechanismen verwendet.

Ein Konsensmechanismus ist ein Algorithmus, der garantiert, dass alle Akteure eines Netzwerks Einigung hinsichtlich des aktuellen Zustands der Blockchain erzielen und somit über identische Datensätze verfügen. Hierzu gehören *Teilnehmerinnen und Teilnehmer*, die transaktionsberechtigten Nutzerinnen und Nutzer der Blockchain und *Nodes*[8] (mit dem Netzwerk verbundene Rechenknoten), die Prüfaufgaben übernehmen und mit ihrer Tätigkeit die Integrität der Blockchain sichern. Beim Bitcoin-Netzwerk fügen *Miner*, ebenfalls mit der Blockchain verbundene Computer, der Blockchain neue Blöcke hinzu. Sie erhalten für das erfolgreiche Hinzufügen eines Blocks neu geschaffene Anteile des Kryptowerts (zum Beispiel Bitcoin[9]) und die von den Teilnehmerinnen und Teilnehmern bezahlten Transaktionsgebühren.

6 Vgl. Bundesnetzagentur, 2019.
7 Vgl. Bundesministerium für Verkehr und digitale Infrastruktur, 2019.
8 Unter dem Begriff „Nodes“ sind im Kontext der DLT elektronische Geräte zu verstehen, die an das dezentrale Netzwerk als Kommunikationsendpunkte angeschlossen sind. Nodes können Transaktionen prozessieren und sich am Validierungsprozess des Netzwerks beteiligen.
9 Alle 210.000 Blöcke wird der Wert der Belohnung halbiert. Zu Beginn 2012 betrug die Block-Belohnung 50 Bitcoins, momentan liegt die Belohnung für die Erstellung eines neuen Blocks bei 6,25 Bitcoins.

Eigenschaften einer Blockchain

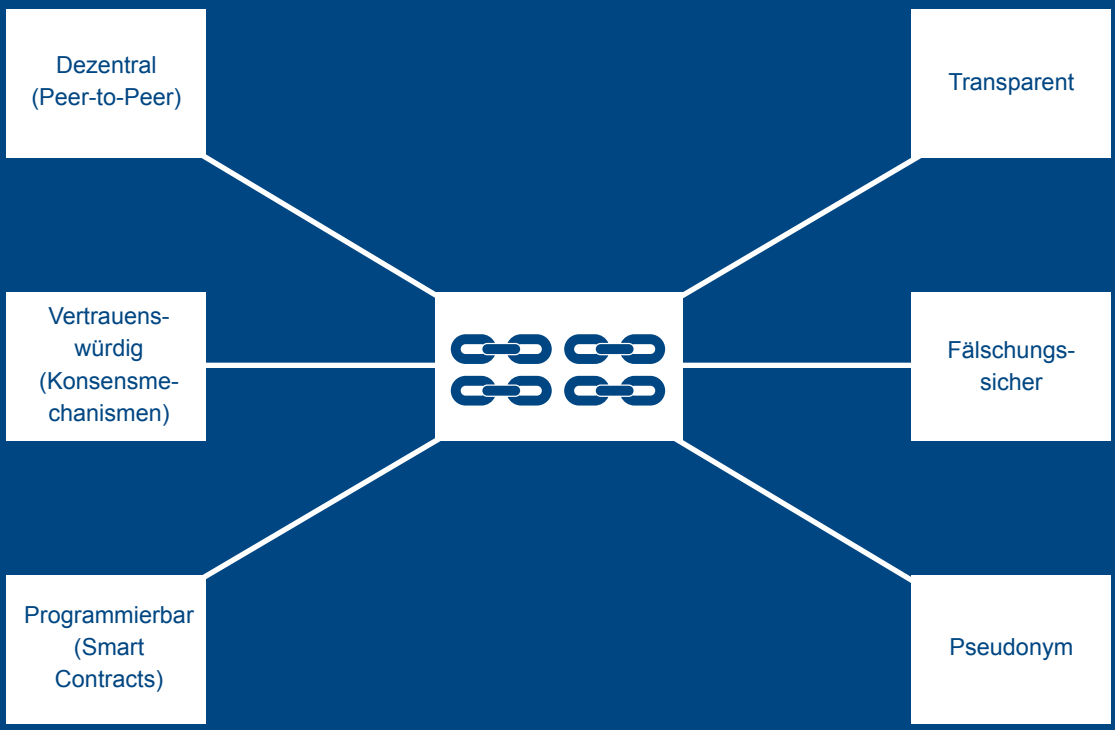

Abbildung 1

Quelle: Eigene Darstellung

2 — Grundlagen der Blockchain-Technologie

Konsensmechanismen dienen auch dem Schutz einer Blockchain. Der Konsensmechanismus Proof-of-Work (PoW), beispielsweise von Bitcoin genutzt, verwendet energieintensive Rechenaufgaben, die von den Minern zu lösen sind, um den Abstimmprozess gegenüber Angreifern zu schützen. Das Stimmgewicht wird beim PoW an eine knappe Ressource in Form von Energie, die für die Rechenleistung benötigt wird, gekoppelt. Denn eine Blockchain könnte manipuliert werden, wenn ein Angreifer die Mehrheit an Stimmrechten in einem Netzwerk besitzt (Sybil-Attacke[10]). In diesem Fall könnten beispielsweise Guthaben mehrfach ausgegeben werden oder bereits durchgeführte Transaktionen nachträglich geändert werden. Doch der PoW-Konsensmechanismus macht solche Attacken ökonomisch unrentabel. Zum einen haben Miner den ökonomischen Anreiz, sich regelkonform zu verhalten, um mit neu geschaffenen Anteilen an Kryptowerten belohnt zu werden. Zum anderen müsste ein Angreifer, um ausreichend Stimmgewicht bei der Konsensfindung zu erreichen, zwischen 25 und 50 Prozent an Rechenkapazität und den dazugehörigen Anteil an Energieverbrauch aufbringen, damit eine Chance auf einen erfolgreichen Angriff existiert.[11] Scheitert der Angriff jedoch, so sind die eingesetzten Ressourcen verloren.

Der Konsensmechanismus Proof-of-Stake (PoS) hingegen koppelt das Stimmgewicht innerhalb des Netzwerks an den eigenen Anteil am Gesamtkapital der Blockchain. Dies erfolgt über die nativen Token der jeweiligen Blockchain, bei Ethereum etwa über Ether (ETH). Beim PoS-Konsensmechanismus wird einem Validator (vergleichbar mit Minern bei PoW-basierten Blockchains) das Recht erteilt, einen Block zu validieren. Die Wahrscheinlichkeit ausgewählt zu werden, steigt dabei proportional mit dem Einsatz der zugrunde liegenden Token: Je mehr Token eingesetzt werden, desto höher die Wahrscheinlichkeit. Die beim PoS eingesetzten Token dienen auch als Sicherheit. Denn sie können verloren gehen, sollte ein Teilnehmer oder eine Teilnehmerin des Netzwerks sich nicht an die Regeln halten, etwa durch häufige Abstimmung gegen die Mehrheit. Auch der PoS-Konsensmechanismus schützt das Netzwerk vor Attacken. Ein Angreifer, der die Mehrheit im Netzwerk übernehmen möchte, müsste hierfür 51 Prozent an den insgesamt eingesetzten Token hinterlegen. Ein solcher Angriff würde beispielsweise bei Ethereum Kosten in Milliardenhöhe verursachen, um eine Chance auf einen erfolgreichen Angriff zu haben. Beim PoS-Konsensmechanismus führt ein gescheiterter Angriff zum Verlust der eingesetzten Token.

Der Konsensmechanismus Proof-of-Authority (PoA) ist etwa in privaten und konsortialen Blockchains vorzufinden. Hier wird die Vertrauenswürdigkeit eines Teilnehmers oder einer Teilnehmerin an seine oder ihre Identität geknüpft. Die Teilnehmerinnen und Teilnehmer des Netzwerkes besitzen gleichwertige Stimmrechte beziehungsweise reputationsbasierte Stimmrechte, die bei der Konsensfindung verwendet werden.[12] Grundsätzlich dient der PoA-Konsensmechanismus als Oberbegriff und ist in unterschiedlichen Ausprägungen und Sicherheitslevels anzutreffen.[13]

10 Angreifer, die das System überstimmen möchten, erstellen eine Vielzahl an Accounts, um die Mehrheit im Netzwerk zu übernehmen (vgl. Douceur, 2002).

11 Vgl. Eyal & Sirer, 2014.

12 Vgl. EU Blockchain Observatory and Forum, 2021.

13 Diese lassen sich aufteilen in Crash Fault-Tolerance (CFT) und Byzantine Fault-Tolerance (BFT) Konsensmechanismen. Die Fehlertoleranz erlaubt es DLT-Systemen, die Konsensfindung bei fehlerhaften oder nicht funktionierenden Nodes sicherzustellen (vgl. de Angelis, 2018).

Zentralisierte vs. dezentralisierte Architektur

Zentralisiert

Dezentralisiert

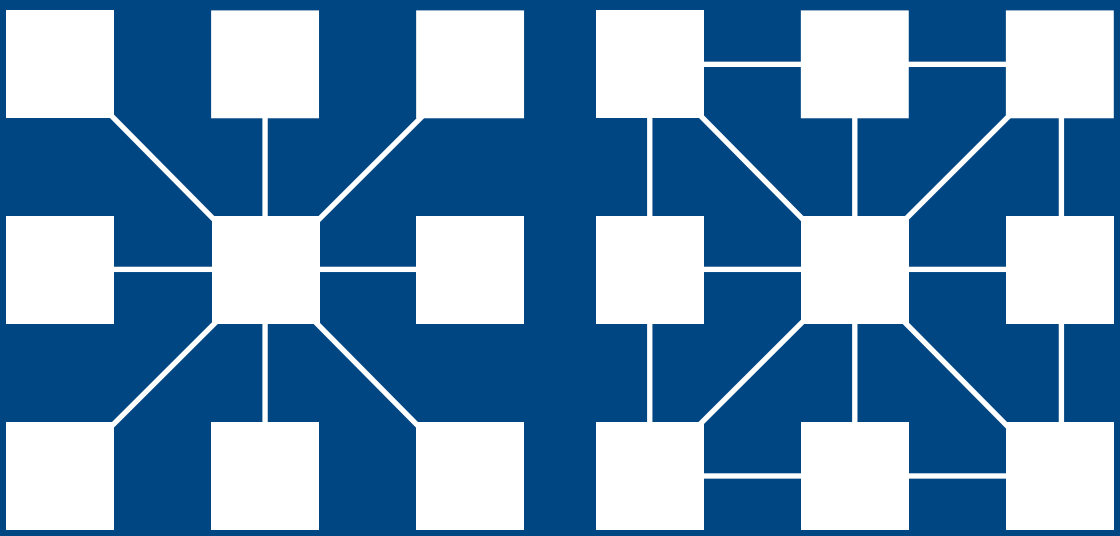

Abbildung 2

Quelle: Eigene Darstellung, nach Campbell et al., 2011

2 — Grundlagen der Blockchain-Technologie

Energieverbrauch von Blockchains

Wie zuvor dargestellt, arbeiten Miner energieintensive Rechenaufgaben ab. Die Miner versuchen in hoher Geschwindigkeit, eine Zufallszahl zu erraten, die sogenannte Nonce (siehe Abbildung 4). Der Schutz des Netzwerks und somit der Datenintegrität hat bei PoW-basierten Blockchains daher eine bewusst gewählte hohe Energieintensität. Mehr noch – je höher der Energieeinsatz, desto sicherer ist das Netzwerk. Denn der hohe Energieverbrauch schützt PoW-basierte Blockchains, sollte ein Angreifer versuchen, ausreichend Rechenkapazität eines Netzwerks zu erlangen, um – wie oben beschrieben – Datensätze einer Blockchain nachträglich zu verändern. Ein solches Vorhaben würde einen Angreifer prohibitive Mengen an Hardware und Energie kosten.

Vor dem Hintergrund der oftmals kritischen Aussagen über den hohen Stromverbrauch von Bitcoin sollte berücksichtigt werden, was dadurch aus technologischer Perspektive erreicht wird: ein sicheres, dezentrales Netzwerk. Weiterhin sollte die Herkunft und Art der Stromerzeugung, die für das Bitcoin-Mining verwendet wird, zugrunde gelegt werden. Denn heute findet das Bitcoin-Mining überwiegend in Rechenzentren statt, die auf möglichst kostengünstige Stromquellen setzen. Dabei kann es sich auch um geothermale Quellen und Wasserkraft handeln oder abgelegene Gas- und Ölkraftwerke. Studien zufolge stammt bereits mehr als die Hälfte des für das Bitcoin-Mining verwendeten Stroms aus erneuerbaren Quellen.[14] Dies deutet wiederum auf einen wichtigen Sachverhalt hin: Nicht der Stromverbrauch allein ist entscheidend, sondern auch der damit einhergehende CO_2-Ausstoß.

Blockchain bedeutet allerdings nicht immer gleich hoher Stromverbrauch: Der Konsensmechanismus PoS weist beispielsweise einen signifikant geringeren Stromverbrauch auf.[15] PoS-Mechanismen setzen nicht auf die energieintensive Rechenarbeit PoW-basierter Blockchains. Hier dient das eingesetzte Kapital in Form von Token als Schutz für das Blockchain-Netzwerk. Auch PoA-basierte Blockchains zeigen einen um Größenordnungen niedrigeren Stromverbrauch im Vergleich zum PoW-Konsensmechanismus.[16] Doch der Stromverbrauch PoA-basierter Blockchains steigt mit wachsender Anzahl von Netzwerkteilnehmenden und ist somit deutlich abhängiger von der Netzwerkgröße im Vergleich zu PoW- und PoS-basierten Blockchains.[17]

Öffentliche, private und konsortiale Blockchains

Blockchains wie Bitcoin und Ethereum werden auch als *öffentliche*, *nicht zugangsbeschränkte* Blockchains bezeichnet. Diese Art von Blockchains ermöglicht es allen Nutzerinnen und Nutzern, die Transaktionsdaten des Netzwerks pseudonymisiert einzusehen (siehe Abbildung 5). Durch webbasierte Tools ist es jedem möglich, Transaktionsdaten auf einer öffentlichen Blockchain auszulesen.[18] Somit ist für jede Partei im Netzwerk pseudonymisiert erkennbar, welche Netzwerkteilnehmenden zu welcher Zeit welche Transaktion durchgeführt haben.

14 Vgl. Sandner et al., 2021.
15 Vgl. Sedlmeir et al., 2020
16 Vgl. EU Blockchain Observatory and Forum, 2021.
17 Vgl. Gola & Sedlmeir, 2022.
18 Vgl. Blockchain.com, 2022.

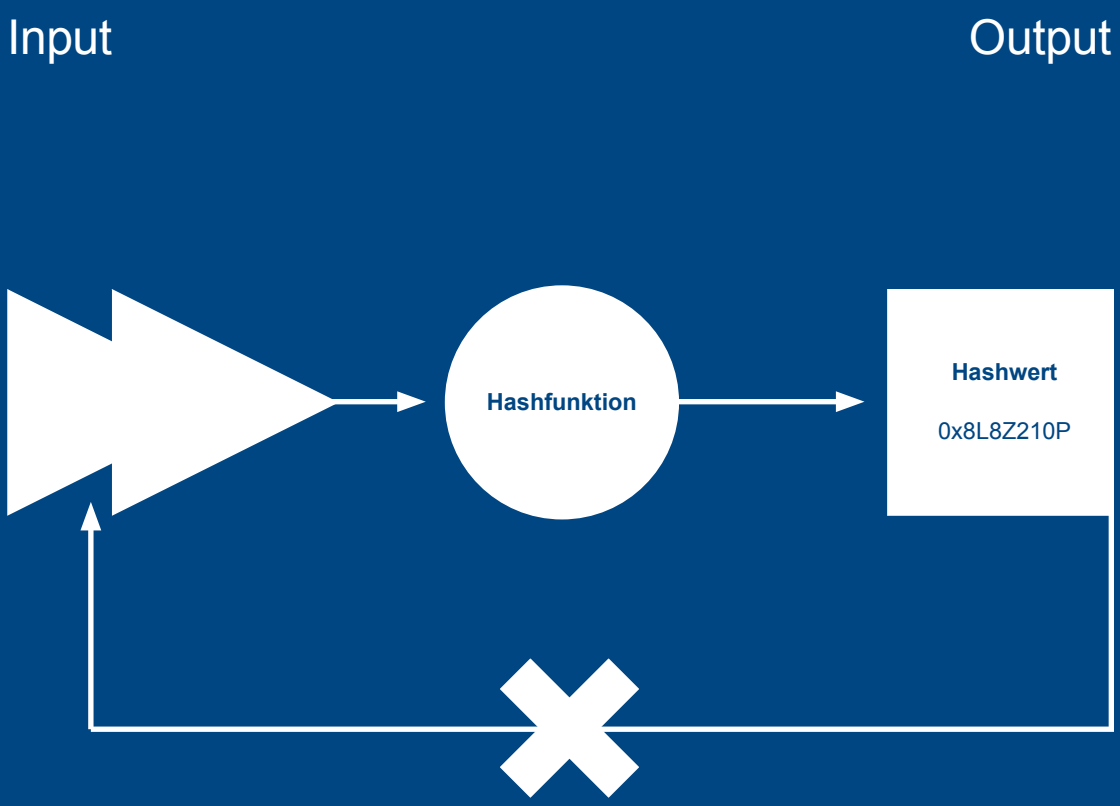

Abbildung 3

Quelle: Eigene Darstellung in Anlehnung an Forschungsstelle für Energiewirtschaft e. V. (FfE), 2018

2 — Grundlagen der Blockchain-Technologie

Im Gegensatz zu öffentlichen Blockchains nutzen *private* und *konsortiale* Blockchains meist andere Konsensmechanismen, da die Teilnehmerinnen und Teilnehmer hier von einer zentralen Instanz, beispielsweise einem Unternehmen oder Konsortium, zugelassen werden. Der in diesen Fällen oftmals verwendete PoA-Konsensmechanismus beinhaltet aufgrund der Netzwerkzusammensetzung deutlich geringere Abstimmungsaufwände, wodurch diese Netzwerke deutlich energieeffizienter und skalierbarer im Hinblick auf die Transaktionsgeschwindigkeit sind als PoW-basierte Blockchains. Durch den Einsatz einer privaten Blockchain behalten Unternehmen und Organisationen auch die Kontrolle darüber, wer ihre internen Unternehmensaktivitäten auf der Blockchain einsehen kann.

Grundsätzlich vereinen *konsortiale* Blockchains Eigenschaften aus beiden genannten Varianten. Hier verwaltet ein Konsortium die Zulassung der Teilnehmerinnen und Teilnehmer. Aus diesem Grund sind konsortiale Blockchains flexibler als öffentliche Blockchains, allerdings nicht so flexibel wie private Blockchains. Lese- und Schreibberechtigungen werden in der Regel nach interner Abstimmung und nur auf Einladung erteilt. Private und konsortiale Blockchains bieten den Nutzerinnen und Nutzern somit weiterhin die Vorteile einer Blockchain in Bezug auf die Datenintegrität und können zugleich energieeffizient betrieben werden.

Smart Contracts

Ein Smart Contract ist ein selbstausführender Computercode, in dem die Bedingungen einer Vereinbarung zwischen zwei oder mehreren Parteien festgeschrieben sind. Der Code und die darin enthaltenen Bestimmungen existieren in einem verteilten, dezentralen Blockchain-Netzwerk. Da kein Akteur die Ausführung verhindern kann, werden in Smart Contracts niedergelegte Bedingungen garantiert ausgeführt. Smart Contracts basieren auf Wenn-dann-Logiken: Beim Eintreten von vordefinierten Umständen werden festgelegte Aktionen ausgelöst. In öffentlichen Blockchains, beispielsweise Ethereum, spielen Smart Contracts eine große Rolle. Hier können fremde Teilnehmerinnen und Teilnehmer wirtschaftlich interagieren, ohne einander vertrauen zu müssen: Der Smart Contract garantiert die Ausführung der Transaktionen, wenn vorher definierte Bedingungen eintreten.

Ein Beispiel hierfür könnte eine Zinszahlung sein, die eine Nutzerin oder ein Nutzer automatisch erhält, wenn er oder sie einen Kryptowert zu einem gewissen Stichtag besitzt. Dieser Smart Contract würde zu gegebenem Datum eine Information erhalten und entsprechend die Transaktion abwickeln oder nicht durchführen, in Abhängigkeit davon, ob die Nutzerin oder der Nutzer besagten Kryptowert hält oder nicht hält. Wichtig ist dabei zu betonen, dass Smart Contracts oftmals auf Informationen angewiesen sind, die sich nicht in der Blockchain, sondern in der Außenwelt befinden. Dementsprechend können Smart Contracts ihre Qualitäten nur dann entfalten, wenn sichergestellt ist, dass die Informationen aus der Außenwelt korrekt sind (siehe Abschnitt „Oracles“).

Obwohl Smart Contracts eine revolutionäre Technologie sind, können sie jedoch noch nicht den Willen der Parteien interpretieren und sind keine Verträge im juristischen Sinne. In unserer Gesellschaft sind rechtmäßige Verträge darauf angewiesen, dass Menschen interpretieren, was die Vertragsparteien beabsichtigt haben. Computer können – zumindest bisher – nur den ihnen gegebenen Code verstehen, nicht aber die Absicht der Parteien.

Struktur einer Blockchain

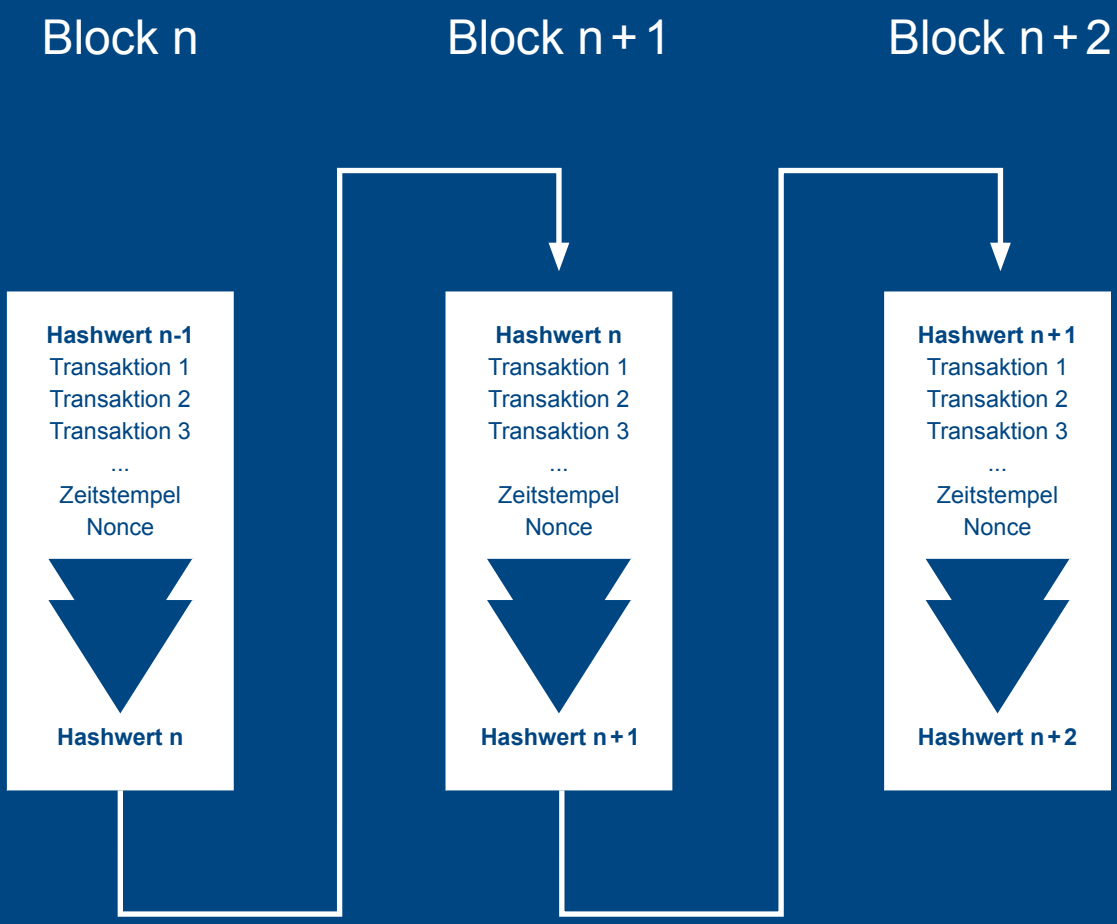

Abbildung 4

Quelle: Eigene Darstellung in Anlehnung an Bundesnetzagentur (2019)

2 — Grundlagen der Blockchain-Technologie

Oracles

Als Oracles werden externe Informationsquellen bezeichnet, die Informationen der Außenwelt in die Blockchain einspeisen. Oracles sind ein elementarer Bestandteil für Smart Contracts, da sie dafür verantwortlich sind, externe Datenquellen auszulesen und diese Informationen in einer für die Blockchain verständlichen Sprache bereitzustellen sowie die Daten auf Richtigkeit zu prüfen. Oracles schlagen damit eine Brücke zwischen Blockchain und Außenwelt.

Smart Contracts benötigen Informationen, um die in ihnen festgelegten Bedingungen zu erfüllen. Daher sind Smart Contracts bei ihrer Ausführung auf die Richtigkeit der Daten von Oracles angewiesen. Tritt eine festgelegte Bedingung ein, so soll die bestimmte Transaktion ausgeführt werden. Diese Bedingungen sind häufig in Bezug auf Zustände der realen Welt definiert. Wird zum Beispiel eine landwirtschaftliche Ernteausfallversicherung als Smart Contract definiert, die bei Frost zwischen Mai und August den verursachten Ernteausfall nach einer vorab festgelegten Metrik versichert, so benötigt der Smart Contract zuverlässige Informationen über die Temperatur auf der versicherten landwirtschaftlichen Nutzfläche. Diese Information stellen sogenannte Oracles zur Verfügung, indem sie mehrere Quellen (zum Beispiel Wetter- und Temperaturdatenbanken) abfragen, sie gegeneinander vergleichen und eigene Algorithmen zur Validierung implementieren.

Tokenisierung

Mithilfe der Blockchain-Technologie können beliebige Rechte und Pflichten an physischen oder digitalen Vermögenswerten digitalisiert in Form von Token repräsentiert werden.[19] Neben Smart Contracts sind Token eine der wichtigsten Innovationen in diesem Technologiebereich. Durch die Blockchain-Technologie kann der Besitz eines Token eindeutig zugeordnet und übertragen werden. Die Tokenisierung ermöglicht es, Vermögenswerte sowie die dazugehörigen Rechte und Pflichten global, durch Nutzung einer Internetinfrastruktur, zu transferieren und das dezentral, ohne Intermediär. Branchenübergreifend beinhaltet die Tokenisierung damit enormes Potenzial. Dies gilt für den Finanzmarkt und dessen klassische Finanzinstrumente wie Aktien, Anleihen und Investmentfonds sowie für Kunst, Sammlerstücke oder digitale Gegenstände (siehe Kapitel „Ausblick“).

Die Tokenisierung verspricht, wenig liquide oder nicht liquide Wertgegenstände liquide zu machen. Denn bei austauschbaren, fungiblen[20] Token muss keine Eins-zu-eins-Beziehung zwischen Wertgegenstand und Token bestehen. Somit können eine Vielzahl von Token die Rechte und Pflichten eines großen Bürokomplexes oder einer hochpreisigen Maschine repräsentieren. Hierdurch ergeben sich für Anleger völlig neue Möglichkeiten: Die Tokenisierung erlaubt den Erwerb von Bruchteilen eines Ganzen. Die Tokenisierung ermöglicht, im Zusammenspiel mit der Peer-to-Peer-Übertragbarkeit der Blockchain-Technologie, bisher nicht handelbare Wertgegenstände global investier- und handelbar zu machen. Durch Smart Contracts werden die Zahlungsströme der tokenisierten Vermögenswerte zusätzlich programmierbar und erlauben die Automatisierung von Prozessen.

19 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht, 2019.

20 Ein Vermögenswert gilt als fungibel, wenn die Möglichkeit besteht, ihn sowohl qualitativ als auch quantitativ durch einen identischen Vermögenswert (zum Beispiel Geld) zu ersetzen. Ein fungibler Wertgegenstand ist also ein Wertgegenstand, der mit jedem anderen seiner Art gleichwertig ist und gegenseitig ausgetauscht werden kann.

Vergleich zwischen öffentlichen, privaten und konsortialen Blockchains

	Öffentlich	Privat	Konsortial
Zugang	Nicht zugangsbeschränkt	Zugangsbeschränkt	Zugangsbeschränkt
Identität	Pseudonyme Nutzung	Bekannt	Bekannt
Erstellung neuer Blöcke	Dezentral (Miner)	Zentral	Je nach Ausgestaltung
Konsensmechanismus	Proof-of-Stake, Proof-of-Work	Proof-of-Authority, Proof-of-Stake	Je nach Ausgestaltung
(IT-)Security	Kein Single-Point-of-Failure, Manipulationen kaum möglich	Single-Point-of-Failure, Eingriffe durch zentralen Akteur möglich	Je nach Ausgestaltung
Stromverbrauch	Hoch (Proof-of-Work)	Niedrig (Proof-of-Authority)	Je nach Ausgestaltung
Transparenz	Sämtliche Transaktionen einsehbar	Ausgewählte Teilnehmende sehen relevante Informationen	Ausgewählte Teilnehmende sehen relevante Informationen
Systemupdates	Niedrige Flexibilität	Hohe Flexibilität	Konsens im Konsortium notwendig
Transaktionsgeschwindigkeit	Gering (Proof-of-Work)	Tendenziell schnell	Je nach Ausgesaltung; Tendenziell schnell
Native Kryptowährung	Als Anreizmechanismus zur Bildung neuer Blöcke	Optional	Optional

Abbildung 5

Quelle: Bundesnetzagentur (2019)

3

Regulatorik in Deutschland und Europa

3 — Regulatorik in Deutschland und Europa

In den vergangenen Jahren sind Kryptowährungen durch die stetig wachsende Nachfrage und Bedeutung in den Fokus der Regulatoren gerückt. Sowohl auf deutscher als auch auf EU-Ebene existieren mittlerweile Bestrebungen, um Kryptowerte und klassische Finanzinstrumente wie Aktien, Anleihen und Investmentfonds auf DLT-Basis zu regulieren. Hierdurch soll ein einheitlicher rechtlicher Rahmen innerhalb der EU für Nutzerinnen und Nutzer sowie Unternehmen geschaffen werden. Auch der Aufbau regulierter Marktplätze für den Handel mit DLT-basierten Finanzinstrumenten soll gefördert werden, um somit einen funktionierenden Sekundärmarkt zu schaffen. Besonders im Finanzwesen zeigt sich, dass der Einsatz der Blockchain-Technologie nicht nur auf Kryptowährungen beschränkt ist, sondern die Finanzmarktinfrastruktur in den kommenden Jahren prägen wird. Es ist zu begrüßen, dass die Regulatorik in Deutschland und auf EU-Ebene hier frühzeitig Marktteilnehmern Möglichkeiten einräumt, die Technologie in einem rechtssicheren Rahmen zu nutzen.

In Deutschland wurde ein Sonderweg eingeschlagen – bereits frühzeitig wurden nationale Gesetze zu Kryptowerten und anderen DLT-basierten Anlageklassen auf den Weg gebracht. Hierdurch hat Deutschland international eine Vorreiterrolle eingenommen und macht bereits eine Vielzahl von DLT-basierten Anwendungsfällen möglich, die im Folgenden erläutert werden. Die zeitlich nachfolgend in Kraft tretende EU-Regulierung wurde von der deutschen Regulierung inspiriert. Weitergehend wird die deutsche Regulierung, die zeitlich früher geschaffen wurde, später durch die EU-Regulierung ersetzt – sobald letztere in Kraft getreten ist. Insofern kann man den Zeitpunkt, die Abfolge und den materiellen Inhalt der Regulierung in Deutschland und in der EU weitestgehend als einen guten Weg klassifizieren.

Regulatorische Ausgangslage in Deutschland

In Deutschland wurde 2019 im Kontext der Umsetzung der 5. EU-Geldwäscherichtlinie das Kryptoverwahrgeschäft als neue Finanzdienstleistung in das Kreditwesengesetz (KWG) aufgenommen. Im KWG ist die Kryptoverwahrung unter Paragraf 1 Abs. 1a Satz 2 Nr. 6 KWG definiert. Zu dieser Finanzdienstleistung gehört die Verwahrung, Verwaltung und Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die zur Haltung, Speicherung oder Übertragung von Kryptowerten dienen. Entsprechend ist seit dem 1. Januar 2020 eine Kryptoverwahrlizenz seitens der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) notwendig.

Ebenfalls im Zuge der 5. EU-Geldwäscherichtlinie wurden Kryptowährungen als Kryptowerte bezeichnet und als Finanzinstrument im Sinne des KWG eingestuft (Paragraf 1 Abs. 11 Satz 1 Nr. 10 KWG). Demnach sind Kryptowerte in Deutschland legale Finanzinstrumente, die an Börsen und multilateralen Handelssystemen gehandelt werden dürfen. Kryptowerte werden in Paragraf 1 Abs. 11 Satz 4 KWG definiert als: „Digitale Darstellung eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.“[21]

21 Vgl. Bundesministerium der Justiz, 2022.

3 — Regulatorik in Deutschland und Europa

Gesetz über elektronische Wertpapiere

Mit dem Gesetz über elektronische Wertpapiere (eWpG) wird der Blockchain-Technologie in Deutschland auch für klassische Finanzinstrumente der Weg geebnet. Bisher bestand in Deutschland für Aktionäre und Anteilsinhaber ein Anspruch auf Globalverbriefung. Da physische Globalurkunden typischerweise in der Sammelverwahrung bei einem Zentralverwahrer hinterlegt sind, war dieser aufwendige Prozess traditionell mit mehreren Intermediären sowie Herausforderungen im Sachenrecht bezüglich der Übertragung verbunden. Mit dem eWpG, das am 10. Juni 2021 in Kraft trat, wird der Handel von elektronischen Wertpapieren und Kryptowertpapieren, zunächst für Inhaberschuldverschreibungen, ermöglicht. Auch die Begebung elektronischer Fondsanteile ist auf Basis des eWpG möglich. Im Zuge des Zukunftsfinanzierungsgesetzes soll das eWpG auch auf Aktien erweitert werden.[22] Grundsätzlich soll durch die Abschaffung der Globalurkunde der Kapitalmarkt schneller und kosteneffizienter werden.

Die Unterscheidung zwischen elektronischen Wertpapieren und Kryptowertpapieren spiegelt sich in der Ausgestaltung der Register wider. Elektronische Wertpapiere werden in zentralen Registern eingetragen und können von einer Wertpapiersammelbank (zum Beispiel Zentralverwahrer) oder einem Verwahrer (zum Beispiel Depotbank) geführt werden (Paragraf 12 Abs. 2 eWpG). Aufgabe der registerführenden Stelle ist unter anderem die Sicherstellung der Vollständigkeit aller Angaben der elektronischen Wertpapiere (Paragraf 13 Abs. 1 eWpG). Für die Ausgabe eines elektronischen Wertpapiers muss der Emittent eine Eintragung im Wertpapierregister anstatt der Erstellung der Papierurkunde (Paragraf 2 Abs. 1 eWpG) bewirken. Nach dem eWpG müssen Kryptowertpapierregister auf fälschungssicheren Aufzeichnungssystemen geführt werden. Auch wenn das eWpG an dieser Stelle eine technologieneutrale Formulierung wählt, sind die aufgeführten Merkmale typisch für die Blockchain-Technologie. Unternehmen, die solch ein Register führen möchten, benötigen seit dem 10. Juni 2021 eine Erlaubnis der BaFin als Kryptowertpapierregisterführer. Diese Dienstleistung wurde entsprechend als Finanzdienstleistung dem KWG hinzugefügt.

Verordnung über Kryptofondsanteile

Nach der Veröffentlichung der Verordnung über Kryptofondsanteile Mitte Juni 2022 ist diese mittlerweile in Kraft getreten. Die darin geregelten Neuerungen sind ein weiterer konsequenter Schritt, um die dringend nötige Digitalisierung der Fondsindustrie und des Fondsvertriebs voranzutreiben.

Die sogenannten Kryptofondsanteile sind eine Form der bereits durch das eWpG in Deutschland erlaubten elektronischen Anteilscheine. Im Gegensatz zu den elektronischen Anteilscheinen, die ein zentrales elektronisches Anteilscheinregister erfordern, sind Kryptofondsanteile in einem Kryptowertpapierregister einzutragen. Die Führung des Kryptowertpapierregisters für Kryptofondsanteile obliegt künftig der Verwahrstelle oder einem von der Verwahrstelle beauftragten Unternehmen, das über die Lizenz als Kryptowertpapierregisterführer verfügt. Ziel ist es, durch diese Gesetzesänderungen Deutschland als Fondsstandort attraktiver zu machen, neue Marktteilnehmer anzuziehen und innovative Geschäftsmodelle zu fördern. Auch für die Registerführung von Fondsanteilen kann die Blockchain-Technologie nun zur Erreichung einer höheren Markteffizienz verwendet werden. Denn durch ihren Einsatz können einzelne Intermediäre, wie in diesem Fall der Zentralverwahrer, ersetzt werden.

Fondsstandortgesetz

Der Gesetzgeber hat für die Fondsbranche in Deutschland am 2. August 2021 auch Neuerungen zugunsten von Kryptowerten mit dem Inkrafttreten des Fondsstandortgesetzes (FoStoG) durchgeführt. Hiernach dürfen offene inländische Spezialfonds mit festen Anlagebedingungen erstmals bis zu 20 Prozent ihres Fondsvolumens in Kryptowerten anlegen. Das Fondsstandortgesetz legitimiert Kryptowerte somit auch gegenüber institutionellen Investoren und erhöht die Möglichkeiten für Asset-Manager in dieser innovativen Anlageklasse.

Regulatorische Entwicklung in Europa

Verordnung über Märkte für Kryptowerte

Die von der EU vorgeschlagene Verordnung über Märkte für Kryptowerte[23] (MiCAR) soll einen harmonisierten Rechtsrahmen für Kryptowerte und damit verbundene Dienstleistungen schaffen. Außerdem soll sie das Vertrauen in den EU-Markt für Kryptowerte stärken. Emittenten können Kryptowerte europaweit anbieten. Die geplante Passporting-Regelung wird es Unternehmen ermöglichen, ihre Dienstleistungen grenzüberschreitend in der EU zu erbringen, ohne weitere Genehmigungen einholen zu müssen. Am 30. Juni 2022 kam es zu einer vorläufigen Einigung zur MiCAR, die abschließend noch vom Europäischen Rat sowie dem Europäischen Parlament gebilligt werden muss, bevor das förmliche Annahmeverfahren eingeleitet wird.[24]

Die MiCAR-Anforderungen sind breit gefächert und umfassen Bereiche wie Verbraucherschutz, Kapital- und Liquiditätsanforderungen, Betriebsorganisation und Governance sowie die Verhinderung von Marktmissbrauch. Danach müssen EU-Firmen, die E-Geld-Token[25] (die nicht unter die E-Geld-Richtlinie fallen), wertreferenzierte Token[26] und andere Kryptowerte ausgeben sowie alle Firmen, die Dienstleistungen im Zusammenhang mit diesen Kryptowerten erbringen, MiCAR-konform sein.

22 Vgl. Bundesministerium der Finanzen, 2022.

23 Ein Kryptowert ist eine digitale Darstellung von Werten oder Rechten, die unter Verwendung der DLT oder einer ähnlichen Technologie elektronisch übertragen werden können.

24 Vgl. European Council, 2022.

25 „Ein E-Geld-Token ist ein Kryptowert, dessen Hauptzweck darin besteht, als Tauschmittel zu dienen, und bei dem eine Nominalgeldwährung, die gesetzliches Zahlungsmittel ist, als Bezugsgrundlage verwendet wird, um Wertstabilität zu erreichen.“ (vgl. Europäische Kommission, 2020).

26 „Ein wertreferenzierter Token ist ein Kryptowert, bei dem verschiedene Nominalgeldwährungen, die gesetzliches Zahlungsmittel sind, oder eine oder mehrere Waren oder ein oder mehrere Kryptowerte oder eine Kombination solcher Werte als Bezugsgrundlage verwendet werden, um Wertstabilität zu erreichen.“ (vgl. Europäische Kommission, 2020).

3 — Regulatorik in Deutschland und Europa

Unternehmen, die in den Anwendungsbereich der neuen Regelung fallen, müssen von einer national zuständigen Behörde in einem EU-Mitgliedstaat zugelassen und beaufsichtigt werden. Die MiCAR zielt dabei nicht nur auf Kryptowerte ab, sondern reguliert auch E-Geld- und Stablecoin-Emittenten.[27] Diese müssen gewisse Verhaltensvorschriften einhalten und werden von den zuständigen Behörden des jeweiligen EU-Mitgliedstaats beaufsichtigt. Sobald die MiCAR in Kraft tritt, müssen Unternehmen, die Kryptowerte in der EU ausgeben wollen, als juristische Person eingetragen sein. Außerdem müssen sie ein MiCAR-konformes Whitepaper herausgeben.[28] Grundsätzlich beabsichtigt die MiCAR, ein höheres Schutzniveau von Investoren durch Bereitstellung risikorelevanter Informationen durch die Emittenten sicherzustellen.

Es wird damit gerechnet, dass die MiCAR im Jahr 2022 in Kraft treten und nach einer 18-monatigen Übergangsfrist unmittelbare Anwendung in allen Mitgliedstaaten finden soll. Ab 2024 ist damit ein harmonisiertes Regelwerk für Produkte und Dienstleistungen im Zusammenhang mit Kryptowerten in der gesamten Europäischen Union zu erwarten.

DLT-Pilotregime

Das DLT-Pilotregime ist eine EU-weite regulatorische Sandbox,[29] die auf eine Laufzeit von sechs Jahren ausgelegt ist. Gegenüber der MiCAR zielt das DLT-Pilotregime auf traditionelle Wertpapiere im Sinne der europäischen Finanzmarktrichtlinie MiFID II ab. Hierzu gehören beispielsweise Aktien, Anleihen und Investmentfonds. Das Pilotregime ist eine Testumgebung und ermöglicht es den infrage kommenden Finanzunternehmen, zum Beispiel Marktbetreibern, Wertpapierfirmen und Zentralverwahrern, ein DLT-basiertes Handelssystem und/oder ein Abwicklungssystem zu betreiben. Auch neue Marktteilnehmer (nicht regulierte Teilnehmerinnen und Teilnehmer) können sich eine befristete Genehmigung für den Betrieb einer solchen DLT-basierten Marktinfrastruktur einholen.

Das sichere regulatorische Umfeld und die Möglichkeit, von zugelassenen Marktteilnehmern unter dem Pilotregime ihre Dienstleistung innerhalb der EU anzubieten, birgt großes Potenzial. Für den Einsatz der Blockchain-Technologie spricht auch im Kontext des DLT-Pilotregimes die effizientere Abwicklung und der mögliche Wegfall von Intermediären. In den unterschiedlichen Ausbaustufen des Pilotregimes ist es nämlich einzelnen Finanzunternehmen möglich, Funktionen innerhalb des Finanzmarktes zu übernehmen, die bisher in den Tätigkeitsbereich anderer Institutionen fielen, beispielsweise die Wertpapierabwicklung eines Zentralverwahrers. Es ist zu hoffen, dass sich das DLT-Pilotregime bewährt und sodann die Sandbox-typischen Limitierungen sukzessive aufgehoben werden.

27 Stablecoins werden laut MiCAR als Untergruppe von Kryptowerten definiert, die entweder E-Geld-Token oder wertreferenzierte Token sind (vgl. Europäische Kommission, 2020).

28 Mit der MiCAR werden Emittenten von Kryptowerten verpflichtet, ein Informationsdokument zu veröffentlichen, das mit verbindlichen Offenlegungspflichten einhergeht. Das Whitepaper hat folgende Informationen zu enthalten: Beschreibung des Emittenten und Vorstellung der beteiligten Akteure, Beschreibung des Projekts des Emittenten und der Art des Kryptowerts, Beschreibung der Merkmale des öffentlichen Angebots (Anzahl und Ausgabepreis), Beschreibung der mit den Kryptowerten verknüpften Rechte und Pflichten, Informationen über die zugrunde liegenden Technologien und Standards sowie eine Beschreibung der Risiken (vgl. Europäische Kommission, 2020).

29 Als Sandbox werden abgegrenzte Bereiche bezeichnet, in denen Unternehmen technologische Innovationen testen können. Dabei können solche Unternehmen ihre Dienstleistungen in einem begrenzten Rahmen für einen ebenfalls begrenzten Zeitraum erbringen. Ziel ist es u. a., die Umsetzungsauswirkungen einer Technologie in der Realität zu erproben.

4

Anwendungsfälle der Blockchain-Technologie

4 — Anwendungsfälle der Blockchain-Technologie

Lieferketten

Auch außerhalb des Finanzmarktes wird der Einsatz der Blockchain-Technologie erprobt. Hierzu gehören beispielsweise Anwendungsfälle für Unternehmen im Bereich des Lieferkettenmanagements. Denn globale wie regionale Lieferketten stehen vor Herausforderungen in Bezug auf Herkunft, Qualität und Lieferung von Produkten.

Komplexe Lieferkettennetzwerke bestehen aus zahlreichen Zwischenhändlern, die oft keine gemeinsame Infrastruktur nutzen, um Informationen zur Rückverfolgbarkeit auszutauschen, was zu einem Mangel an Transparenz führt. Die Produktqualität auf jeder Stufe der Lieferkette hängt von der Qualität der vorangegangenen Stufen ab, sodass die Qualität des Endprodukts auf die ordnungsgemäße Rückverfolgbarkeit in der gesamten Lieferkette angewiesen ist. Dabei fällt es Unternehmen oftmals nicht leicht, anderen Parteien hinsichtlich der Qualität und des aktuellen Status eines Produkts zu vertrauen.[30] Ein Grund dafür ist, dass die Teilnehmerinnen und Teilnehmer keine gemeinsame Datenbank nutzen und relevante Informationen oftmals manuell und papierbasiert übermittelt werden. Weiterhin steigt die Komplexität der Lieferketten durch die Globalisierung und einen hohen Konsumentendruck stetig an.[31] Digitale Technologien setzen genau hier an. Sie haben das Potenzial für Unternehmen, Wettbewerbsvorteile zu erlangen: Risiken innerhalb der Lieferkette werden verringert und das Vertrauen der Konsumentinnen und Konsumenten in Sicherheit und Qualität von Produkten zurückgewonnen (siehe Abbildung 6).

Blockchain-Technologie bietet transparente und unveränderliche Register. Blockchains können im Lieferkettenmanagement verwendet werden, um Produktaktivitäten in der gesamten Lieferkette automatisch zu protokollieren und allen Teilnehmenden innerhalb des Wertschöpfungsprozesses zur Verfügung zu stellen. Auf Basis des Internets der Dinge (IoT) können die relevanten Informationen der realen Welt mittels Sensoren (siehe Abschnitt „Oracles“) in nachvollziehbare, digitale Datensätze einer Blockchain überführt werden.[32] Berechtigte Akteure können beispielsweise mittels einer privaten oder konsortialen Blockchain (siehe Abschnitt „Öffentliche, private und konsortiale Blockchains“) mit einer entsprechenden Genehmigung auf das DLT-basierte Register zugreifen. Die Mitglieder des Netzwerks kontrollieren dann, wer über welche Rechte im Netzwerk verfügt und wer welche Daten einsehen darf.

Besonders die Rückverfolgbarkeit bis zum Ursprung einer Lieferkette ist in vielen Branchen von großer Bedeutung. Etwa immer dann, wenn Probleme auftreten – beispielsweise in der Arzneimittelsicherheit und Lebensmittelversorgung. Auch können durch transparente Lieferketten gegebenenfalls Kosten gesenkt werden, wenn durch den Einsatz der Blockchain-Technologie Prozesse digitalisiert und automatisiert werden. Eine Manipulation der Daten ist durch die Verwendung der Blockchain-Technologie nicht möglich, sobald sich die Daten auf der Blockchain befinden. Dadurch wird das Vertrauen in die Lieferkette gesteigert. Solange jedoch die Blockchain auf Daten aus der realen Welt zurückgreifen muss, besteht weiterhin das Risiko, dass Daten zuvor manipuliert oder gefälscht werden.

Um diesem Umstand entgegenzuwirken, müssen Prozesse und Governance-Regeln definiert werden, die Daten aus der realen Welt in Form von Sensoren oder unabhängigen Validatoren fälschungssicher in die Blockchain transportieren. Dies stellt weiterhin eine große Herausforderung dar, da die erforderlichen Datensätze und respektiven Prozesse je nach Anwendungsbereich, Industrie und sogar Protokollstandards stark variieren. Um es zu verdeutlichen: Sobald die Blockchain auf Daten von der Außenwelt angewiesen ist, die nur schwierig oder überhaupt nicht messbar sind, sondern eine subjektive menschliche Einschätzung benötigen (zum Beispiel Umweltprobleme bei der Produktion eines Gutes), kann die Technologie nicht als Allheilmittel verstanden werden.

30 Vgl. Deutsches Global Compact Netzwerk (DGCN), 2012.
31 Vgl. Schäffner et al., 2021.
32 Vgl. Landesbank Baden-Württemberg, 2021.

4 — Anwendungsfälle der Blockchain-Technologie

Ein Pilotprojekt im Bereich des Lieferkettenmanagements mit integrierten Zahlungsverkehrslösungen wurde durch die Unternehmen BASF, Commerzbank und Evonik aufgesetzt.[33] Auf Basis einer gemeinsamen Blockchain-Plattform wurden Lieferkettenprozesse im Kontext des Forderungsmanagements automatisiert. Das gegenseitige Lieferantenverhältnis zwischen den Industrieunternehmen BASF und Evonik bedingt den regelmäßigen Zahlungsausgleich von Lieferungen und Leistungen. Auf Basis der Blockchain und mithilfe des für diesen Zweck zur Verfügung gestellten elektronischen Geldes wurde die Zahlungsabwicklung zwischen beiden Unternehmen automatisiert. Dies gelang durch die Nutzung von Smart Contracts, die die Zahlungen dank der Programmierbarkeit von elektronischem Geld vollautomatisiert prüften und verbuchten.

Ein weiteres Pilotprojekt wird von einem Joint Venture des Technologieunternehmens IBM und dem Anbieter für Container-Logistik Maersk[34] geleitet. Zusammen haben die Unternehmen eine digitale Plattform namens TradeLens entwickelt, die alle Transaktionen vollständig und in Echtzeit verzeichnet. Alle involvierten Parteien, vom Sender über Reedereien, Spediteure, Hafen- oder Terminalbetreiber, Zollbehörden bis hin zum Empfänger oder zur Empfängerin, erhalten Echtzeitzugriff auf Versanddaten, Dokumente und den aktuellen Standort der Sendung.[35]

Relevant kann der Einsatz der DLT auch bei der Einführung des deutschen Lieferkettengesetzes sein, das ab 2023 in Kraft treten soll, wenn es darum geht, Daten fälschungssicher aufzuzeichnen, die nicht auf menschlichen Einschätzungen beruhen. Das Gesetz verpflichtet Unternehmen ab einer bestimmten Größe, ihren ESG-bezogenen Verantwortungen und Sorgfaltspflichten innerhalb ihrer Lieferketten nachzukommen. Damit sollen Missstände wie Zwangsarbeit, Kinderarbeit, Umweltverschmutzungen oder die Zahlung von Hungerlöhnen reduziert werden.[36]

Maschinenbau

Die verarbeitende Industrie und ihre Zulieferer erleben schwierige Zeiten: Mehrere sich in den letzten Jahren abzeichnende globale Entwicklungen führen zu einem erheblichen Wettbewerbs- und Kostendruck. Besonders spürbar sind die Auswirkungen in Bereichen mit einem hohen Einsatz von Maschinen und Anlagen. Bleiben diese aufgrund einer rückläufigen Auftragslage ungenutzt, verursachen sie lediglich hohe Kosten, statt zur Rentabilität und Wertschöpfung des Unternehmens beizutragen, wie es auch während der Corona-Pandemie festgestellt werden konnte. Hier setzen neue Eigentumsmodelle wie das nutzungsabhängige Konzept Pay-per-Use in Verbindung mit der Blockchain-Technologie an.

In einem solchen Modell kaufen die Nutzenden der Industrieanlagen nicht das Produkt, sondern zahlen eine Gebühr, die von der Nutzung abhängt; die also anhand bestimmter, dem Nutzungskontext entsprechender Parameter gemessen wird. Die Messung der nutzungsspezifischen Daten kann mittels Sensoren erfolgen (siehe Abschnitt „Oracles“), die anschließend in ein DLT-basiertes System übertragen werden. Auch in diesem Anwendungsfall steht die Fälschungssicherheit der Daten durch die Blockchain-Technologie im Vordergrund. Der Maschinenbauer kann so den erhobenen Daten vertrauen. Weitere Effizienzen sind realisierbar, wenn mittels Smart Contracts beispielsweise die Zahlungsströme automatisiert werden. Das Sammeln und Analysieren von nutzungsbezogenen Maschinendaten kann auch eine vorausschauende Wartung ermöglichen und das Risiko von Produktionsausfällen für Nutzende und Herstellende reduzieren.

Die Verwendung des Pay-per-Use bringt dabei sowohl für Maschinenbauer als auch Maschinennutzer Vorteile. Maschinenbauer können ihre Einnahmen während des Produktlebenszyklus maximieren und einen konstanten Cashflow generieren. Aus Sicht des Maschinennutzers sind keine sonst üblichen Vorabinvestitionen erforderlich, wodurch die Kapitalbindung und das Risiko sinken.

33 Vgl. Commerzbank AG, 2021.
34 Vgl. van Kralingen, 2018.
35 Vgl. TradeLens, 2022.
36 Vgl. Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, 2022.

DLT als Fundament für mehr Transparenz in Lieferketten

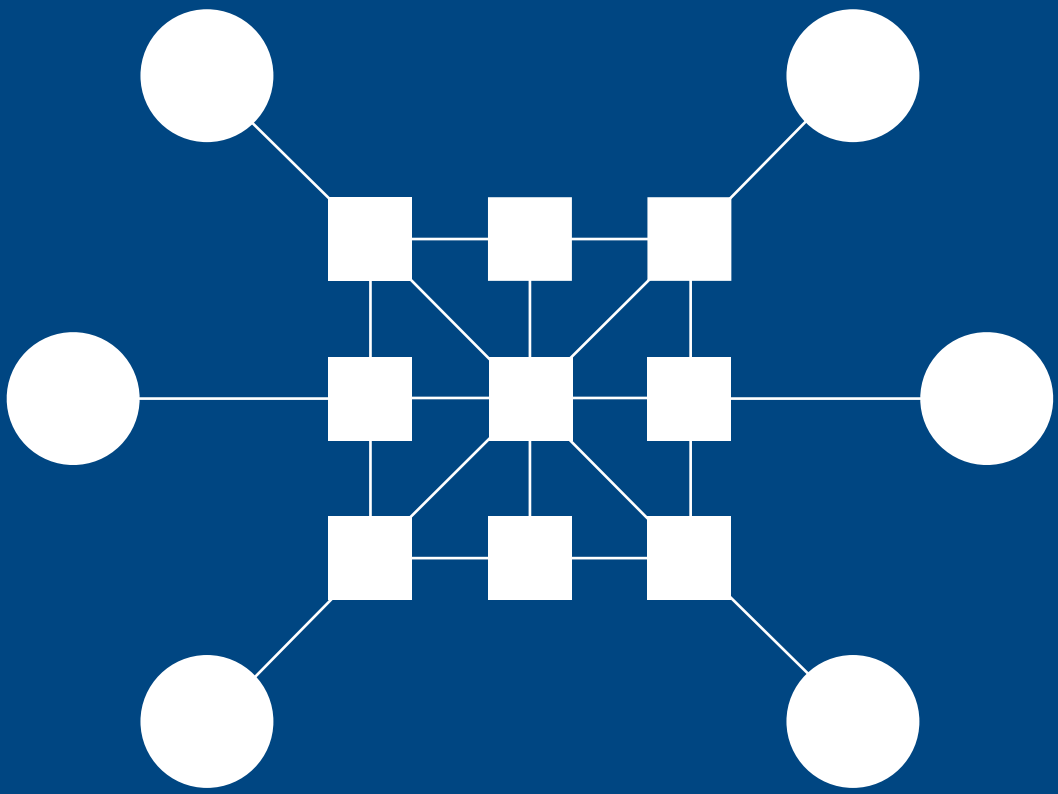

Abbildung 6

Quelle: Eigene Darstellung in Anlehnung an Fraunhofer-Institut, 2017

4 — Anwendungsfälle der Blockchain-Technologie

Ein Beispiel ist das Projekt vom Fraunhofer-Institut in Zusammenarbeit mit Miele für gewerbliche Geschirrspülmaschinen.[37] Da die Anschaffungskosten einer Geschirrspülmaschine eine hohe Investition darstellen, erhofft sich Miele, mit der Einführung eines Pay-per-Use-Geschäftsmodells neue Kundengruppen zu erschließen und bestehenden Kunden weitere Leistungen anzubieten. Hier geht es jedoch zunächst darum, die Tragbarkeit eines solchen Geschäftsmodells zu prüfen.

Ein weiteres Beispiel zum Pay-per-Use-Verfahren ist ein Pilotprojekt zwischen der Trumpf-Gruppe und der Munich Re-Gruppe. Beide Unternehmen erwägen eine strategische Partnerschaft mit der Intention, ein Pay-per-Part-Geschäftsmodell zu entwickeln. Kunden können demnach Laservollautomaten der Trumpf-Gruppe nutzen, ohne diese kaufen oder leasen zu müssen. Es wird für jedes zugeschnittene Blechteil gezahlt und der Preis dafür zuvor vereinbart.[38]

Ford arbeitet beispielsweise in England zusammen mit dem Versicherungsanbieter By Miles an einem Pay-as-you-drive-Ansatz. Grund hierfür war, dass im Zuge der Corona-Pandemie viele Ford-Kundinnen und -Kunden mehr von zu Hause arbeiten und das Auto entsprechend weniger nutzen. Ziel ist es nun, Kfz-Versicherungskosten für Kundinnen und Kunden zu senken, die weniger pendeln müssen, als es noch zuvor der Fall war. Die Versicherungskosten können sich demnach in Zukunft aus den tatsächlich zurückgelegten Kilometern berechnen.[39]

Staatsmodernisierung

Elektronische Identitäten

Angesichts der Corona-Pandemie mussten viele öffentliche und private Organisationen Wege finden, um ihre Dienstleistungen für Kundinnen und Kunden sowie Geschäftspartner aufrechtzuerhalten. Da der persönliche Kontakt entweder eingeschränkt oder sogar verboten wurde, haben digitale Prozesse an Bedeutung gewonnen. Um sich zum Beispiel bei elektronischen Behördendiensten zu authentifizieren und anzumelden, benötigen Nutzerinnen und Nutzer zuverlässige digitale Identitäten. Eine wichtige Möglichkeit hierfür ist die Verwendung nationaler elektronischer Identitäten (eIDs). In Europa trat 2016 die Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS) in Kraft.[40] Sie definiert einen Rechtsrahmen zur Harmonisierung digitaler Identitäts- und Vertrauensdienste im Europäischen Wirtschaftsraum (EWR). Aktuell ist eine umfassende Überarbeitung von eIDAS im Gange, bei der die gewonnenen Erkenntnisse und Paradigmenwechsel im Bereich des Identitätsmanagements berücksichtigt werden.

Selbstbestimmte Identitäten

Der Begriff „selbstbestimmte Identitäten“ (Self-Sovereign Identity oder SSI) wird häufig für DLT-basierte Ansätze zum Identitätsmanagement verwendet. In den letzten Jahren hat das SSI-Modell in der Forschung und in der Praxis an Aufmerksamkeit gewonnen, denn es ermöglicht Nutzerinnen und Nutzern eine eigene digitale Identität vollständig selbst zu verwalten, ohne sich auf Dritte verlassen zu müssen. Dadurch kann SSI als ein neues evolutionäres Identitätsmodell neben dem traditionellen zentralisierten, föderierten und nutzerzentrierten Identitätsmanagement gesehen werden (siehe Abbildung 7).[41]

37 Vgl. Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM, 2022.
38 Vgl. Munich Re, 2020.
39 Vgl. The Ford Motor Company, 2021.
40 Vgl. Europäische Union, 2014.
41 Vgl. Tobin & Reed, 2017.

Ein Beispiel für einen Anwendungsfall von SSI besteht im Zusammenhang mit Bildungszertifikaten, die im Laufe des Lebens gesammelt werden. Für den Arbeitgeber wird es besonders in Zeiten der Globalisierung stetig schwieriger, den Bildungsweg von potenziellen Arbeitnehmerinnen und -nehmern zu überprüfen. Ein Fälschen dieser Bildungs- und Abschlusszertifikate stellt demnach ein lukratives Geschäft für Betrüger dar. Ein von der ConsenSys Academy entwickeltes Software-Tool namens Ethense ermöglicht es Bildungseinrichtungen, Zertifikate an ihre Absolventinnen und Absolventen auszustellen. Ein solches Zertifikat wird kryptografisch signiert und ist damit fälschungssicher. Nachdem die Absolventinnen und Absolventen dieses Zertifikat erhalten haben, speichern sie es in ihrer Wallet[42] und müssen keine Papierkopie mehr vorlegen, um ihre Bildungsnachweise zu validieren. Die Frankfurt School of Finance & Management war die erste Hochschule in Deutschland, die ein solches Zertifikat für die Absolventinnen und Absolventen des Kurses „Certified Blockchain Expert“ erstellte.[43]

Ein weiterer Anwendungsfall ergibt sich für Stammdatensysteme.[44] Für Unternehmen ist es heutzutage sehr aufwändig und kostenintensiv, eine hohe Datenqualität zu erreichen. Eine ungenügende Datenqualität führt nicht nur zu mehr Kosten, sondern auch zu Problemen in Liefer- und Bezahlprozessen.[45] Bosch und Siemens versuchen in einem Pilotprojekt, Adress- und Bankdaten sowie Lieferantenzertifikate erstmals kryptografisch zu verifizieren, um die Integrität der Herkunft zu gewährleisten.[46] Mittels einer Unternehmenssoftware, die den Nutzerinnen und Nutzern zur Verfügung gestellt wird, können Geschäftspartner die Unternehmensdaten (sogenannte Verifiable Credentials) bei sich selbst speichern, nach Bedarf verteilen und empfangen sowie deren Authentizität prüfen. Interne Datenbanken werden ebenso an die Unternehmenssoftware angebunden. Sollten sich Daten ändern, werden die entsprechenden Geschäftspartner benachrichtigt. Stammdaten und Lieferantenzertifikate zwischen Unternehmen werden somit automatisch validiert und aktualisiert.

Es gilt festzuhalten, dass digitale, Blockchain-basierte Identitäten zwingend erforderlich sind für eine Vielzahl an Anwendungsszenarien. Der digitale Identitätsnachweis muss also als Basisinfrastruktur verstanden werden. Darauf aufbauend können beispielsweise verschiedene behördliche Leistungen durch die Bürgerinnen und Bürger problemlos über das Internet in Anspruch genommen werden. Der Staat könnte durch die Digitalisierung seiner hoheitlichen Aufgaben Kosteneffizienzen realisieren, indem manuelle, administrative Tätigkeiten abgebaut werden, und den Bürgerinnen und Bürgern gleichzeitig eine signifikante Zeitersparnis ermöglichen. Fehlende Lösungen im Bereich der digitalen Identitäten werden für Nutzerinnen und Nutzer künftig vermehrt zu Medienbrüchen bei der Nutzung digitaler Dienstleistungen oder Applikationen führen. Aus deutscher Sicht sollte der Staat dieses Thema auch deshalb stark vorantreiben, um die Datensouveränität der Bürgerinnen und Bürger gegenüber den großen Technologieunternehmen zu sichern.

42 Wallets stellen den Ausgangspunkt für die Interaktion mit einer Blockchain dar. Mithilfe der Wallet können Transaktionen ausgeführt werden. Eine Wallet kann als Speichermedium, auf dem Transaktionsdaten gespeichert werden, verstanden werden (vgl. Suratkar et al., 2020).

43 Vgl. Frankfurt School of Finance & Management, 2018.

44 Vgl. Bitkom e. V., 2020.

45 Vgl. Haug et al., 2013.

46 Vgl. Bitkom e. V., 2020.

4 — Anwendungsfälle der Blockchain-Technologie

Blockchain im Kontext behördlicher Dienste

Grundsätzlich besteht im Bereich behördlicher Dienste immenses Potenzial zur Staatsmodernisierung durch Digitalisierung. Die Blockchain-Technologie bietet hierfür, basierend auf den zuvor beschriebenen Eigenschaften, eine Infrastruktur für eindeutige und manipulationssichere Daten. Folglich kommen auf staatlicher Ebene Anwendungsszenarien im Kontext der SSI infrage, in denen bestimmte Daten eindeutig einer Person zugeordnet werden können, zum Beispiel Führerschein, Geburtsurkunde, Grundbuch, Kfz-Zulassung und vieles mehr.

In diesen Anwendungsfällen wäre der Staat der Betreiber einer konsortialen Blockchain-Infrastruktur, die öffentlich zugänglich und nutzbar ist. Die Konsensfindung innerhalb der Blockchain kann so auf staatlich kontrollierte Instanzen beschränkt werden. In dieser Rolle definiert der Staat somit das Regelwerk der zugrunde liegenden Blockchain mit entsprechendem Berechtigungskonzept, das Lese- und Schreibzugriff für Behörden sowie Nutzerinnen und Nutzer festlegt.

Folgend wird am Beispiel des Grundbuchs der mögliche Einsatz der Blockchain-Technologie aufgezeigt. In diesem Anwendungsfall muss der eindeutige Eigentumsnachweis gewährleistet werden. Es existieren rund um die Eigentumsübertragung und der damit zusammenhängenden Eintragung in das Grundbuch viele manuelle, papierbasierte Arbeitsschritte. Das Zusammenspiel zwischen Anwälten, Banken, Eigentumskäufern/-verkäufern, Grundbuchämtern und Notarinnen und Notaren ist ein langwieriger und teurer Prozess. Durch die Blockchain-Technologie können verschiedene Prozesse im Kontext des Grundbuchs und somit der Eigentumsübertragung digitalisiert, automatisiert, beschleunigt und für Nutzerinnen und Nutzer transparent gestaltet werden. Technisch könnte der Grundbucheintrag über die Nutzung eines NFTs (siehe Abschnitt „NFT“) vonstattengehen. Dabei repräsentiert der Besitz des NFTs das Eigentum am Grundstück. Die Übertragung des NFTs kann digital auf einen anderen Eigentümer beziehungsweise eine andere Eigentümerin erfolgen und durch die Blockchain transparent nachvollzogen werden.

Inwiefern in so einem Prozess die Notwendigkeit einer Notarin beziehungsweise eines Notars besteht, muss diskutiert werden. Da es in Deutschland eine gesetzliche Vorgabe gibt, kann die Rolle der Notarin beziehungsweise des Notars neu gedacht werden, zum Beispiel in Form eines digitalen Signaturprozesses, der Änderungen zuerst prüfen muss, bevor diese auf die Blockchain gegeben werden. Eine genaue Ausgestaltung von Grundbuchprozessen auf Basis der Blockchain muss genau geprüft werden. Im Rahmen des Koalitionsvertrages der Ampel-Regierung im Jahr 2021 wurde die Durchführung einer Machbarkeitsstudie für die Nutzung der Blockchain-Technologie für das Grundbuch beschlossen.[47]

47 Vgl. Koalitionsvertrag, 2021.

Digitale, Blockchain-basierte Identitäten

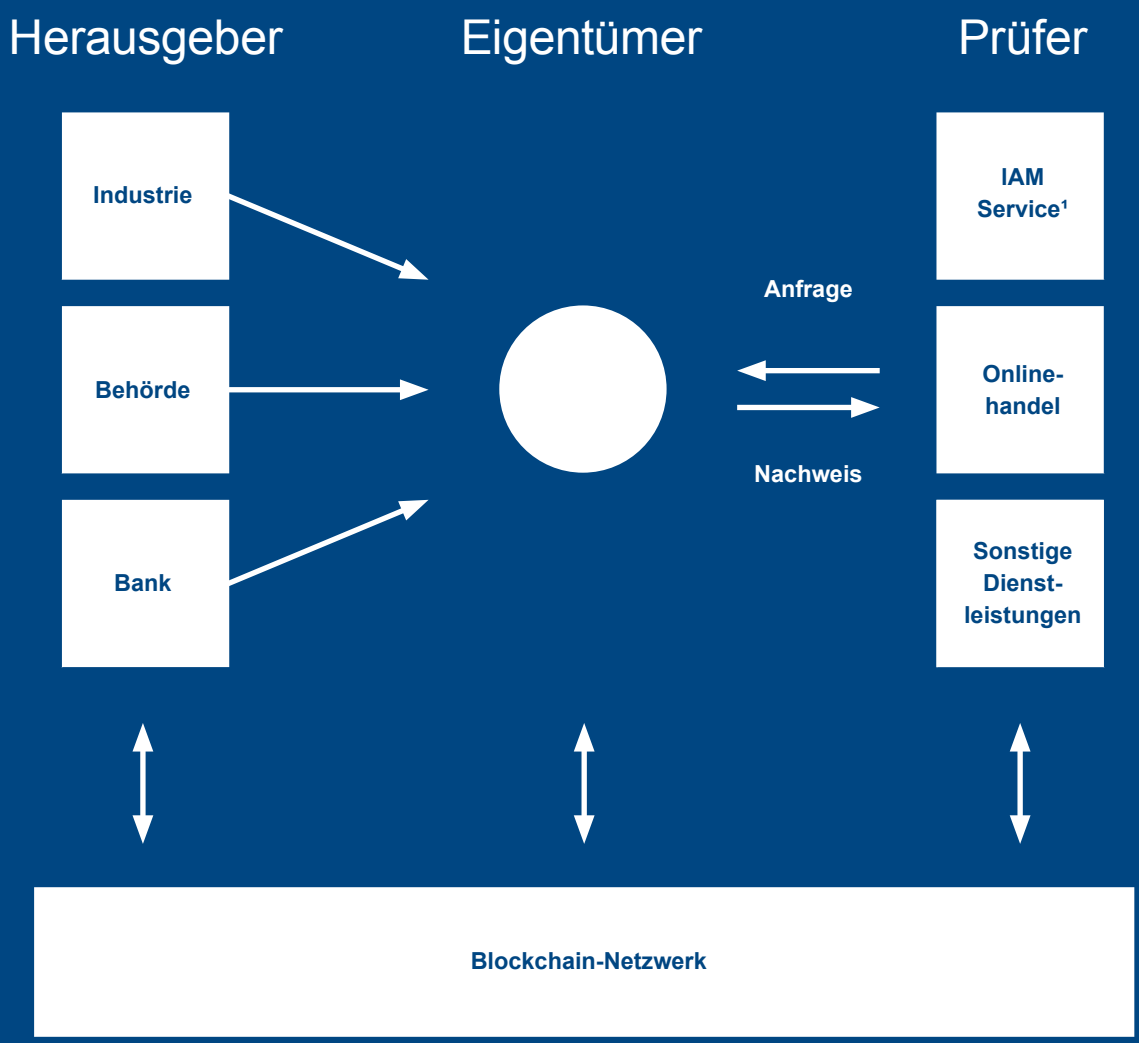

Abbildung 7

Quelle: Eigene Darstellung

5

Ausblick

5 — Ausblick

Web 3.0

Rund um die Blockchain-Technologie entstehen aktuell auch abseits des traditionellen Finanzmarktes (siehe Kapitel „Regulatorik in Deutschland und Europa“) und der Realwirtschaft (siehe Kapitel „Anwendungsfälle der Blockchain-Technologie“) einige Trendthemen, die enormes Potenzial bieten und das Internet und dessen Nutzung revolutionieren können. In der ersten Version des Internets (Web 1.0) haben die Nutzerinnen und Nutzer lediglich digitale Inhalte konsumiert, die von den jeweiligen Verlegern erstellt wurden. Das Web 2.0 ermöglicht es den Nutzerinnen und Nutzern, eigene Inhalte zu erstellen und zu konsumieren. Diese Ausbaustufe des Internets wird von zentralisierten Anbietern kontrolliert, zum Beispiel Social-Media-Plattformen, die für die Verbreitung von Inhalten verantwortlich sind und diese entsprechend monetarisieren. In der aktuell entstehenden Version des Web 3.0 (oftmals auch Web3 genannt) erhalten Nutzerinnen und Nutzer hingegen die Möglichkeit, Inhalte zu konsumieren, zu erstellen und erstmals auch zu besitzen (siehe Abbildung 8).

Das Ziel des von Gavin Wood vorgeschlagenen Konzepts des Web 3.0 basiert auf dezentralisierten Netzwerken und sieht vor, Nutzerinnen und Nutzern Dienstleistungen ohne vertrauenswürdige dritte Partei bereitzustellen. Unklare Definitionen und fehlender Konsens darüber deuten darauf hin, dass es sich beim Web 3.0 bisher entweder nur um ein gehyptes Konzept ohne praktische Entwicklung handelt oder dass es mehr als nur eine Richtung für die Entwicklung gibt. Das elementare Prinzip von Anwendungen im Web 3.0 ist, Nutzerinnen und Nutzern die volle Kontrolle über ihre eigenen Daten zu geben, ohne dass zentralisierte Organisationen diese Daten verwalten.[48] Dabei soll die Marktmacht von großen zentralisierten Plattformen verstärkt in Richtung der Nutzergruppen verlagert werden, indem die vertrauensbildenden Aktivitäten der zentralen Instanz über Bestandteile der Blockchain abgebildet werden. Erste Web-3.0-Anwendungen sind bereits entstanden, haben jedoch nur eine kleine Nutzerschaft. Insofern ist die Abschätzung von Wachstum oder gar Quantifizierung eines Trends noch nicht möglich.

Durch den Einsatz der Blockchain-Technologie können sich Nutzerinnen und Nutzer sowohl im Hinblick auf den Konsum als auch den Austausch von Inhalten und Werten vertrauen.[49] Das Web 3.0 ist zusätzlich eine Plattform der nächsten Generation an Anwendungen (DApps[50]), die auf einem Fundament ausgereifter Protokolle wie Ethereum aufbauen und ein Ökosystem leicht zugänglicher dezentralisierter Anwendungen schaffen.

48 Vgl. Wang et al., 2022.

49 Vgl. Boston Consulting Group, 2022.

50 DApps sind dezentrale Anwendungen auf einer Blockchain. Die Nutzerinnen und Nutzer agieren hier ohne zentrale Instanz (Peer-to-Peer). Eine DApp besteht aus dem Zusammenspiel mehrerer Smart Contracts, die relevante Daten und erforderliche Logiken beinhalten.

5 — Ausblick

NFT

NFT steht als Akronym für „Non-Fungible Token“. Ein NFT ist ein einzigartiger und somit nicht fungibler digitaler Besitznachweis an einem spezifischen digitalen oder physischen Vermögenswert. Anwendungsfälle von NFTs sind beispielsweise tokenisierte digitale und physische Kunstwerke oder Sammlerstücke in Onlinespielen. Im Metaverse spielen NFTs eine besondere Rolle, da sie Verfügungsrechte und somit Besitz innerhalb virtueller Welten ermöglichen (siehe Abbildung 9).

Im Gegensatz zu fungiblen Token wird ein NFT durch seine Nichtfungibilität und Nichtaustauschbarkeit charakterisiert: NFTs können nicht gegen dieselbe Menge desselben Typs getauscht werden, eben weil sie einzigartig sind und unterschiedliche Merkmale aufweisen. Wie bei den fungiblen Token ermöglicht die Blockchain-Technologie die eindeutige Zuordnung und Übertragbarkeit eines NFT. Im Kontext der NFTs geht es im Unterschied zu fungiblen Token darum, schwer austauschbare Güter und Rechte im Ganzen digital handelbar zu machen. Denn NFTs sind nicht teilbar und können dementsprechend nur als Ganzes gehandelt werden.

Insgesamt ist der NFT-Markt im vergangenen Jahr schnell gewachsen und hat die Attraktivität in diesem Bereich des Blockchain-Ökosystems untermauert. Einhergehend mit den Kurseinbrüchen im Kryptomarkt in den letzten Monaten, war auch ein starker Rückgang im NFT-Markt zu verzeichnen. NFT-Sammler haben 2022 bereits über 37 Milliarden US-Dollar an NFT-Marktplätze transferiert (Stand 1. Mai 2022). Im Jahr 2021 waren es insgesamt 40 Milliarden US-Dollar.[51] Während NFTs einerseits bei Sammlerinnen und Sammlern ein starkes Wachstum verzeichnen, haben sich die Anwendungsfälle auch auf andere Bereiche wie Avatare, Gaming, Sport und sogar physische Kunst ausgeweitet.

Mit dem Aufkommen und den Möglichkeiten des Web 3.0 beschleunigt sich die Entwicklung der NFTs, denn sie besitzen beispielsweise das Potenzial, die Medienbranche und Industrie für kreative Inhalte zu revolutionieren. Um dies allerdings zu ermöglichen, ist es von entscheidender Bedeutung, dass eine angemessene Unterstützung aus rechtlicher und unternehmerischer Sicht gewährleistet wird, zum Beispiel durch klar definierte regulatorische Vorgaben. Die Leitlinien zu verschiedenen rechtlichen, regulatorischen, buchhalterischen und steuerlichen Fragen im Zusammenhang mit NFTs sind bisher spärlich und nur wenige Rechtsordnungen haben Vorgaben für diesen Bereich ausgearbeitet.

51 Vgl. Chainalysis Inc., 2022.

Eigenschaften des Web 1.0, Web 2.0 und Web 3.0

	Web 1.0	Web 2.0	Web 3.0
Interaktion	Lesen	Lesen-Schreiben	Lesen-Schreiben-Besitzen
Medium	Statischer Text	Interaktiver Inhalt	Virtuelle Ökonomien
Organisation	Unternehmen	Plattformen	Netzwerke
Infrastruktur	Computer	Cloud & mobile Endgeräte	Blockchain-Cloud
Kontrolle	Dezentral	Zentral	Dezentral

Abbildung 8

Quelle: Eigene Darstellung in Anlehnung an Grayscale Investments (2021)

5 — Ausblick

Metaverse

Das Metaverse befindet sich aktuell in einem frühen Entwicklungsstadium, daher existiert noch keine allgemeingültige und abschließende Definition des Begriffs. Grundsätzlich handelt es sich beim Metaverse um miteinander verbundene, virtuelle 3-D-Erlebniswelten, in denen Menschen an beliebigen Orten in Echtzeit miteinander in Kontakt treten können, um eine dauerhafte, von den Nutzerinnen und Nutzern kontrollierte Internetökonomie zu schaffen, die die digitale und physische Welt verbindet.[52] Die Blockchain-Technologie dient im Metaverse als Infrastruktur und macht eine digitale Ökonomie erst möglich. Sie erlaubt es Nutzerinnen und Nutzern, digitale, tokenisierte Werte zu schaffen, die gehandelt und besessen werden können (siehe Abschnitte „Tokenisierung“ und „NFT“).

Auch wenn das Metaverse erst in der sehr frühen Entstehung ist, zeigen erste Beispiele, wie dieses neue virtuelle Konzept funktionieren kann: Decentraland, eine auf der Ethereum-Blockchain basierende virtuelle Welt, erlaubt es Nutzerinnen und Nutzern, Inhalte und Anwendungen zu erstellen, zu konsumieren und zu besitzen. Dort können Nutzerinnen und Nutzer mit Kryptowerten digitale Güter wie Kleidung und sogar Land kaufen. Unternehmen aus der Modebranche haben begonnen, mit virtueller Kleidung zu experimentieren, die Avatare in der Metaverse-Umgebung tragen können. So kommen auf Basis des Web 3.0 das Metaverse und NFTs zusammen.

Zur Feier des 200. Jahrestages der Gründung der Luxusmarke Louis Vuitton hat das Unternehmen das digitale Erlebnisspiel „Louis the Game“ ins Leben gerufen, in dem rund 30 NFTs integriert sind.[53] Nike hat das Unternehmen RTFKT Studios übernommen, ein Start-up, das sich auf virtuelle Schuhe und Sammlerstücke spezialisiert hat.[54] Das Unternehmen Gucci versteigerte im Juni 2021 ein neues NFT, das von seiner Herbst-Winter-Kollektion inspiriert war.[55] Im Januar 2022 brachten Adidas und Prada die Kollektion Adidas for Prada Re-Nylon als NFT ins Metaverse.[56]

52 Vgl. Bitkom e. V., 2022.
53 Vgl. CoinDesk, 2022.
54 Vgl. Reuters, 2021.
55 Vgl. Hanschke, 2021.
56 Vgl. Prada, 2022.

Unterscheidung: fungibel – nicht fungibel

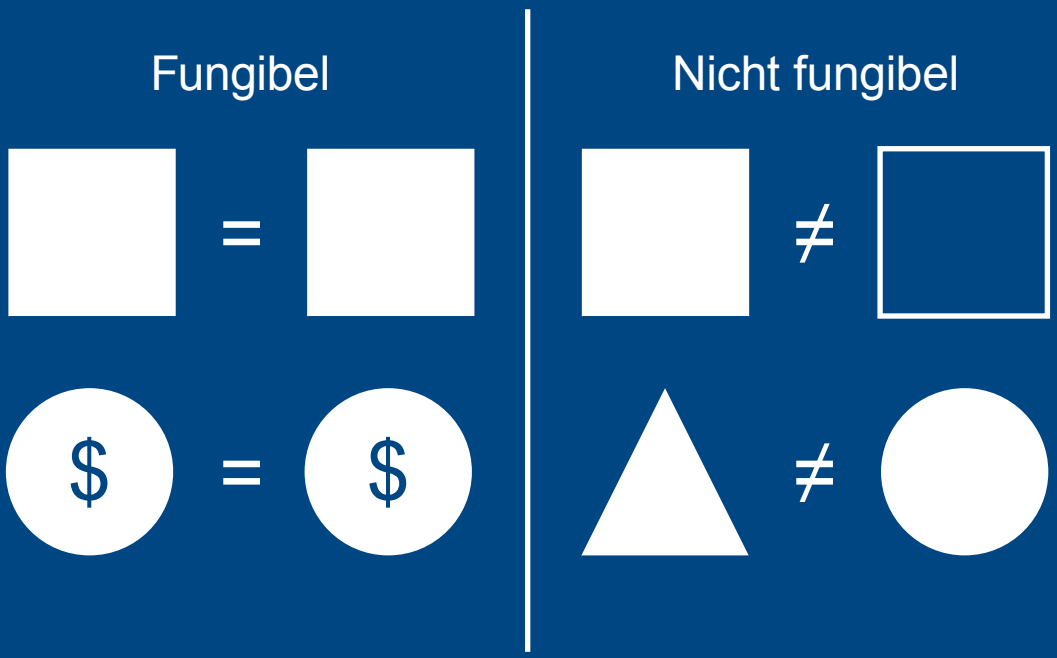

Abbildung 9

Quelle: Eigene Darstellung in Anlehnung an Crypto.com (2020)

6

Fazit

6 — Fazit

Im Rahmen dieser Studie wurden die Eigenschaften und Potenziale der DLT ausführlich dargestellt. Ihre dezentrale Architektur zeichnet sich durch die fälschungssichere Speicherung von Daten und eindeutige Zuordenbarkeit von Besitz aus. Daten können der Blockchain nur nach fest definierten Regeln hinzugefügt werden (Konsensmechanismus). Auf Basis der Blockchain-Technologie entstehen durch die Tokenisierung bislang nicht dagewesene Möglichkeiten zur Digitalisierung und Übertragung von Werten über das Internet. Zudem können mittels Smart Contracts Prozesse automatisiert werden, zum Beispiel durch programmierbare Zahlungsströme.

Bislang findet die Blockchain-Technologie besonders im Bereich der Kryptowerte in verschiedenen Facetten ihre Verwendung. Durch progressive Regulatorik rücken zunehmend aber auch Anwendungsmöglichkeiten für die traditionelle Finanzindustrie in Verbindung mit Wertpapieren wie Aktien, Anleihen und Investmentfonds in den Fokus. Deutschland nimmt an dieser Stelle eine Vorreiterrolle durch die Einführung diverser Regelungen ein und sorgt für viel regulatorische Klarheit in diesem Umfeld. Auch die EU, wenngleich etwas später, verfolgt ein ähnliches Vorgehen, um den Wirtschaftsstandort zu vereinheitlichen und zu stärken. Beide ebnen hierdurch der Blockchain-Technologie den Weg, sowohl für Dienstleistungen im Bereich Kryptowährungen, als auch für klassische Wertpapiere.

Vermehrt sind auch Anwendungsfälle außerhalb der Finanzindustrie zu beobachten. Ein an Bedeutung gewinnender Bereich für den Einsatz der Blockchain-Technologie ist das Lieferkettenmanagement. Durch die transparente Natur der Blockchain können Informationen entlang der Lieferkette für alle involvierten Parteien zur Verfügung gestellt und zurückverfolgt werden. Grundsätzlich jedoch können durch die Nutzung der Blockchain-Technologie nicht alle einhergehenden Herausforderungen des Lieferkettenmanagements adäquat adressiert werden. In gewissen Bereichen bedarf es für den Betrieb einer Blockchain-basierten Lieferkette weiterhin externer Daten, deren Authentizität nicht durch die Blockchain geprüft werden kann. Beruhen diese Daten auf nicht messbaren, subjektiven Einschätzungen von Menschen, kann die Technologie selbst dieses Problem nicht lösen.

6 — Fazit

In der verarbeitenden Industrie wie im Maschinenbau befinden sich nutzungsbasierte Pay-per-Use-Konzepte in der Testphase beziehungsweise bereits im Livebetrieb. Die Blockchain ist hierbei für die Datenintegrität verantwortlich, kann aber auch Zahlungsprozesse durch die Nutzung von Smart Contracts automatisieren. Derartige Modelle begünstigen sowohl Nutzerinnen und Nutzer als auch die Produzierenden einer Maschine. Nutzerinnen und Nutzer profitieren von einer deutlich geringeren Kapitalbindung und bezahlen lediglich das, was auch tatsächlich in Anspruch genommen wurde, während die Produzierenden auf einen stetigen Kapitalfluss vertrauen können.

Auch im öffentlichen Dienst können durch die Nutzung der Blockchain-Technologie Anwendungsfälle geschaffen werden, die bislang technisch nicht möglich waren. Behördengänge und andere Leistungen, die von Bürgerinnen und Bürgern in Anspruch genommen werden, können in weiten Teilen digitalisiert und automatisiert werden. Der elementare Faktor hierfür ist eine digitale Identität, die mit hohen Sicherheitsanforderungen einhergeht. Blockchain-basierte, digitale Identitäten (SSI) sind die Basisinfrastruktur für die Digitalisierung solcher Dienstleistungen. Es ist absehbar, dass sich innerhalb kurzer Zeit privatwirtschaftliche Unternehmen etablieren, die derartige Ansätze für digitale Identitäten entwickeln. Der Gesetzgeber muss zügig agieren, um die Datensouveränität der Bürgerinnen und Bürger zu schützen.

Auf Basis der Blockchain-Technologie entstehen fortwährend weitere Innovationen, die Aspekte der realen sowie virtuellen Welt abdecken. Das auf Blockchain-Technologie basierende Web 3.0 soll zukünftig das plattformgetriebene und zentralisierte Internet sukzessive ablösen. Auf dieser technologischen Grundlage entsteht das Metaverse, das eine virtuelle Welt abbildet, in der Nutzerinnen und Nutzer miteinander interagieren können und mittels NFTs beliebige digitale oder physische Vermögenswerte handeln. Um dieser dynamischen Entwicklung Rechnung zu tragen, sollte der Gesetzgeber diesen Sektor aufmerksam beobachten, damit auch hier rechtlich sichere Rahmenbedingungen für Nutzerinnen und Nutzer sowie Unternehmen entstehen.

7

Literatur-verzeichnis und Glossar

7 — Literaturverzeichnis

Bitkom e. V. (2020). *Self Sovereign Identity Use Cases – von der Vision in die Praxis*. https://www.bitkom.org/sites/main/files/2020-07/200703_lf_self-sovereign-identity-use-cases.pdf (zuletzt abgerufen am 1. Dezember 2022).

Bitkom e. V. (2022). *Wegweiser in das Metaverse*. https://www.bitkom.org/sites/main/files/2022-07/220714_LF_Metaverse.pdf (zuletzt abgerufen am 1. Dezember 2022).

Blockchain.com. (2022, 21. Juli). *Blockchain Explorer*. https://www.blockchain.com/explorer/ (zuletzt abgerufen am 21. Juli 2022).

Boston Consulting Group (2022, April). *The Corporate Hitchhiker's Guide to the Metaverse*. https://web-assets.bcg.com/85/18/a876a489473c98a41f406aa5ddfb/bcg-the-corporate-hitchhikers-guide-to-the-metaverse-27-apr-2022.pdf (zuletzt abgerufen am 1. Dezember 2022).

Bundesanstalt für Finanzdienstleistungsaufsicht (2019, 15. April). *Tokenisierung*. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2019/fa_bj_1904_Tokenisierung.html%3Bjsessionid=5D84F8E143824C1FCC7AB429102CDCA0.1_cid500#doc12342268bodyText1 (zuletzt abgerufen am 21. Juli 2022).

Bundesministerium der Finanzen (2022, 29. Juni). *Eckpunkte für ein Zukunftsfinanzierungsgesetz*. https://www.bundesfinanzministerium.de/Content/DE/Downloads/Finanzmarktpolitik/2022-06-29-eckpunkte-zukunftsfinanzierungsgesetz.html (zuletzt abgerufen am 22. Juli 2022).

Bundesministerium der Justiz (2022). *§ 1 KWG – Einzelnorm*. Gesetze im Internet. https://www.gesetze-im-internet.de/kredwg/__1.html (zuletzt abgerufen am 26. Juli 2022).

Bundesministerium für Verkehr und digitale Infrastruktur (2019, Mai). *Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik*. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1106/wi-1106.pdf (zuletzt abgerufen am 1. Dezember 2022).

Bundesministerium für Wirtschaft und Energie (2019, September). *Blockchain-Strategie der Bundesregierung*. https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=22 (zuletzt abgerufen am 1. Dezember 2022).

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) (2022). *Lieferkettengesetz*. https://www.bmz.de/de/themen/lieferkettengesetz (zuletzt abgerufen am 14. August 2022).

Bundesnetzagentur (2019, November). *Die Blockchain-Technologie: Grundlagen, Potenziale und Herausforderungen*. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Blockchain/Links_Dokumente/einfuehrung_bc.pdf?__blob=publicationFile&v=12 (zuletzt abgerufen am 1. Dezember 2022).

Campbell, A., Kunisch, S. & Müller-Stewens, G. (2011, 1. Juni). *To centralize or not to centralize?* McKinsey & Company. https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/to-centralize-or-not-to-centralize (zuletzt abgerufen am 21. Juli 2022).

7 — Literaturverzeichnis

Chainalysis Inc (2022, Juni). *The Chainalysis Web3 Report*. https://go.chainalysis.com/2022-web3-report.html (zuletzt abgerufen am 1. Dezember 2022).

CoinDesk (2022, 18. April). *Louis Vuitton Releases New NFTs, Continues Blockchain Gaming Experiment*. https://www.coindesk.com/videos/all-about-nfts/louis-vuitton-releases-new-nfts-continues-blockchain-gaming-experiment/ (zuletzt abgerufen am 14. August 2022).

Commerzbank AG (2019, 8. August). *Commerzbank testet erstmals Blockchain-basierte Maschine-zu-Maschine-Zahlung*. (c) 2022 Commerzbank AG. https://www.commerzbank.de/de/hauptnavigation/presse/pressemitteilungen/archiv1/2019/quartal_19_03/presse_archiv_detail_19_03_82762.html (zuletzt abgerufen am 21. Juli 2022).

Commerzbank AG (2021, 20. Mai). *Commerzbank, Evonik und BASF testen erstmals Blockchain-Technologie und programmierbares Geld zur Abwicklung von Supply-Chain-Prozessen zwischen Unternehmen*. (c) 2022 Commerzbank AG. https://www.commerzbank.de/de/hauptnavigation/presse/pressemitteilungen/archiv1/2021/2__quartal/presse_archiv_detail_21_02_97290.html (zuletzt abgerufen am 9. August 2022).

Crypto.com (2020, November). *Non-Fungible Tokens – A Brief Introduction and History*. https://assets.ctfassets.net/hfgyig42jimx/6A8K5H6VrTydTDuEFHXQ5P/3cca896ad77bd967859a7a1256a5a91f/Crypto.com_Macro_Report_-_Non-Fungible_Tokens.pdf (zuletzt abgerufen am 1. Dezember 2022).

de Angelis, S (2018, Mai). *Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains*. https://doi.org/10.48550/arXiv.1805.03490 (zuletzt abgerufen am 1. Dezember 2022).

Deutsches Global Compact Netzwerk (DGCN) (2012, August). *Nachhaltigkeit in der Lieferkette – Ein praktischer Leitfaden zur kontinuierlichen Verbesserung*. https://www.globalcompact.de/migrated_files/wAssets/docs/Lieferkettenmanagement/nachhaltigkeit_in_der_lieferkette.pdf (zuletzt abgerufen am 1. Dezember 2022).

Douceur, J. R. (2002). *The Sybil Attack*. *Peer-to-Peer Systems*, S. 251–260. https://doi.org/10.1007/3-540-45748-8_24 (zuletzt abgerufen am 1. Dezember 2022).

EU Blockchain Observatory and Forum (2021, September). *Energy Efficiency of Blockchain Technologies*. https://www.eublockchainforum.eu/sites/default/files/reports/Energy%20Efficiency%20of%20Blockchain%20Technologies_1.pdf (zuletzt abgerufen am 1. Dezember 2022).

Europäische Kommission (2020, September). *Verordnung des Europäischen Parlaments und des Rates on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0593&from=EN (zuletzt abgerufen am 1. Dezember 2022).

Europäische Union (2014, 28. August). *EUR-Lex - 32014R0910 - EN - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2014/910/oj (zuletzt abgerufen am 11. November 2021).

European Council (2022, 30. Juni). *Digital finance: agreement reached on European crypto-assets regulation (MiCA)*. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/ (zuletzt abgerufen am 26. Juli 2022).

Eyal, I. & Sirer, E.G. (2014). *Majority is not enough: Bitcoin mining is vulnerable*. In: *International conference on financial cryptography and data security*, S. 436–454. https://doi.org/10.1007/978-3-662-45472-5_28 (zuletzt abgerufen am 1. Dezember 2022).

Forschungsstelle für Energiewirtschaft e. V. (FfE) (2018, Juni). *Die Blockchain-Technologie: Chance zur Transformation der Energieversorgung?* https://www.ffe.de/wp-content/uploads/2017/11/Blockchain_Teilbericht_Technologiebeschreibung.pdf (zuletzt abgerufen am 1. Dezember 2022).

Frankfurt School of Finance & Management (2018, 23. Oktober). *Frankfurt School relies on Blockchain. https://www.frankfurt-school.de/en/home/newsroom/news/2018/September/blockchain-zertifikate* (zuletzt abgerufen am 14. August 2022).

Fraunhofer-Institut (2017, November). *Blockchain und Smart Contracts – Technologien, Forschungsfragen und Anwendungen*. https://www.iuk.fraunhofer.de/content/dam/iuk/de/documents/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf (zuletzt abgerufen am 1. Dezember 2022).

Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM (2022). *Digitalisierung von Geschäftsmodellen – Pay-per-Use-Geschäftsmodell für gewerbliche Geschirrspülmaschinen*. https://www.iem.fraunhofer.de/de/referenzen/industrieprojekte/pay-per-use-geschaeftsmodell-gewerbliche-geschirrspuelmaschinen.html (zuletzt abgerufen am 1. Dezember 2022).

Godenrath, B. (2022, 23. Mai). *DZ Bank setzt auf Pay per Use*. In: *Börsen-Zeitung*. https://www.boersen-zeitung.de/dz-bank-setzt-auf-pay-per-use-6b4895b2-da9a-11ec-a618-e6cf6e61a04f (zuletzt abgerufen am 21. Juli 2022).

Gola, C. & Sedlmeir, J. (2022). *Addressing the Sustainability of Distributed Ledger Technology*. In: *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4032837 (zuletzt abgerufen am 1. Dezember 2022).

Grayscale Investments (2021, November). *The Metaverse – Web 3.0 Virtual Cloud Economies*. https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf (zuletzt abgerufen am 1. Dezember 2022).

Hanschke, K. (2021, 1. Dezember). *Die digitalen Sneaker sind los*. In: *Faz.net*. https://www.faz.net/aktuell/stil/mode-design/wie-modemarken-blockchain-und-nft-technologie-nutzen-17625642.html (zuletzt abgerufen am 14. August 2022).

Haug, A., Stentoft Arlbjørn, J., Zachariassen, F. & Schlichter, J. (2013). *Master data quality barriers: an empirical investigation*. In: *Industrial Management & Data Systems*, 113(2), S. 234–249. https://doi.org/10.1108/02635571311303550 (zuletzt abgerufen am 1. Dezember 2022).

Koalitionsvertrag (2021). *Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP*. https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800 (zuletzt abgerufen am 13. September 2022).

Landesbank Baden-Württemberg (2021, Mai). *Mogeln unmöglich: Ressourcen schonen mit der Blockchain*. https://www.lbbw.de/artikelseite/maerkte-verstehen/ressourcen-schonen-mit-blockchain_ac6o5rxg9a_d.html (zuletzt abgerufen am 9. August 2022).

7 — Literaturverzeichnis

Munich RE (2020, 14. Oktober). *Pay-per-Part: TRUMPF und Munich Re planen neues Geschäftsmodell für die produzierende Industrie*. https://www.munichre.com/de/unternehmen/media-relations/medieninformationen-und-unternehmensnachrichten/medieninformationen/2020/2020-10-14-pay-per-part.html (zuletzt abgerufen am 21. Juli 2022).

Prada (2022). *adidas for Prada Re-Nylon*. https://www.prada.com/at/de/pradasphere/special-projects/2022/adidas-for-prada-re-nylon.html (zuletzt abgerufen am 14. August 2022).

Reuters (2021, 13. Dezember). *Nike buys virtual sneaker maker RTFKT in metaverse push*. https://www.reuters.com/markets/deals/nike-buys-virtual-sneaker-maker-rtkft-metaverse-push-2021-12-13/ (zuletzt abgerufen am 14. August 2022).

Schäffner, M., Lichti, C., Gross, J. & Sandner, P. (2021, März). *KOSMoS Private Blockchain Toolkit: How to Use Hyperledger in an Industrial DLT Project*. http://explore-ip.com/KOSMOS-Blockchain-Toolkit.pdf (zuletzt abgerufen am 1. Dezember 2022).

Sedlmeir, J., Buhl, H. U., Fridgen, G. & Keller, R. (2020). *The Energy Consumption of Blockchain Technology: Beyond Myth*. In: *Business & Information Systems Engineering*, 62(6), S. 599–608. https://doi.org/10.1007/s12599-020-00656-x (zuletzt abgerufen am 1. Dezember 2022).

Suratkar, S., Shirole, M. & Bhirud, S. (2020). *Cryptocurrency Wallet: A Review*. In: *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. https://doi.org/10.1109/icccsp49186.2020.9315193 (zuletzt abgerufen am 1. Dezember 2022).

The Ford Motor Company (2021, 24. Juni). *Commuting Less? Ford Teams up with Pay-As-You-Drive Car Insurance Provider That Could Save Drivers Money.* https://media.ford.com/content/fordmedia/feu/gb/en/news/2021/06/24/commuting-less--ford-teams-up-with-pay-as-you-drive-car-insuranc.html (zuletzt abgerufen am 21. Juli 2022).

Tobin, A. & Reed, D. (2017, März). *The Inevitable Rise of Self-Sovereign Identity*. Sovrin Foundation. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (zuletzt abgerufen am 1. Dezember 2022).

TradeLens (2022). *Pioneer a new class of customer support*. https://www.tradelens.com/tradelens-use-cases/customer-service (zuletzt abgerufen am 14. August 2022).

van Kralingen, B. (2018, 16. Januar). *IBM, Maersk Joint Blockchain Venture to Enhance Global Trade*. THINK Blog. https://www.ibm.com/blogs/think/2018/01/maersk-blockchain/ (zuletzt abgerufen am 14. August 2022).

Wang, Q., Li, R., Wang, Q., Chen, S., Ryan, M., Hardjono, T. (2022, Juli). *Exploring Web3 From the View of Blockchain*. https://doi.org/10.48550/arXiv.2206.08821 (zuletzt abgerufen am 1. Dezember 2022).

7 — Glossar

Blockchain
Die Blockchain ist eine Unterform der Distributed-Ledger-Technologie (DLT). Sie ist eine dezentral verteilte, verschlüsselte und unveränderliche Datenbank. Datensätze, zum Beispiel Transaktionen, werden in Form von Blöcken gespeichert. Die miteinander nach bestimmten Regeln kryptografisch verknüpften und aneinandergereihten Blöcke ergeben die Blockchain.

Distributed-Ledger-Technologie (DLT)
DLT ermöglicht, Informationen über eine bestimmte Kategorie von Vermögenswerten in einer gemeinsamen Datenbank, die verteilt abgelegt ist, zu speichern und für alle Nutzerinnen und Nutzer zugänglich zu machen. Diese Informationen werden unter den Nutzerinnen und Nutzern verteilt, die sie dann für die Abwicklung ihrer Transaktionen nutzen können, ohne sich auf ein vertrauensvolles zentrales Validierungssystem verlassen zu müssen.

Hashfunktion
Hashfunktionen können eine Zeichenfolge von variabler Länge in eine Zeichenfolge fixer Länge umwandeln. Bei identischen Inputdaten ergeben Hashfunktionen immer dieselben Outputdaten (Hashwert).

Internet of Things (IoT)
Das Internet der Dinge (IoT) bezieht sich auf physische Objekte, die beispielsweise mittels Sensorik mit dem Internet verbunden sind, um Daten auszutauschen und Funktionen zu aktivieren.

Mining
Beim Mining werden energieintensive Rechenaufgaben gelöst. Dabei versuchen die Miner, in hoher Geschwindigkeit eine Zufallszahl zu erraten (sogenannte Nonce). Sie erhalten für das erfolgreiche Hinzufügen eines Blocks neu geschaffene Anteile eines Kryptowerts (zum Beispiel Bitcoin).

Nodes
Nodes sind mit dem Netzwerk verbundene Rechenknoten, die Prüfaufgaben übernehmen und mit ihrer Tätigkeit die Integrität der Blockchain sichern.

Peer-to-Peer
Ein Peer-to-Peer-Netzwerk zeichnet sich dadurch aus, dass Teilnehmerinnen und Teilnehmer direkt von Person zu Person interagieren können, ohne dass eine dritte Partei dazwischensteht.

Proof-of-Authority (PoA)
Der Konsensmechanismus Proof-of-Authority (PoA) ist häufig in privaten und konsortialen Blockchains vorzufinden. Hier wird die Vertrauenswürdigkeit von Teilnehmenden an ihre Identität geknüpft. Die Teilnehmenden des Netzwerks besitzen gleichwertige beziehungsweise reputationsbasierte Stimmrechte, die bei der Konsensfindung verwendet werden. Grundsätzlich dient der PoA-Konsensmechanismus als Oberbegriff und ist in unterschiedlichen Ausprägungen und Sicherheitslevels anzutreffen.

Proof-of-Stake (PoS)

Der Konsensmechanismus Proof-of-Stake (PoS) koppelt das Stimmgewicht innerhalb des Netzwerks an den eigenen Anteil am Gesamtkapital der Blockchain. Dies erfolgt über die nativen Token der jeweiligen Blockchain, bei Ethereum etwa über Ether (ETH). Beim PoS-Konsensmechanismus wird einem Validator (vergleichbar mit Minern bei PoW-basierten Blockchains) das Recht erteilt, einen Block zu validieren. Die Wahrscheinlichkeit ausgewählt zu werden, steigt dabei proportional mit dem Einsatz der zugrunde liegenden Token: Je mehr Token eingesetzt werden, desto höher die Wahrscheinlichkeit. Die beim PoS eingesetzten Token dienen auch als Sicherheit. Denn sie können verloren gehen, sollte eine Teilnehmerin oder ein Teilnehmer des Netzwerks sich nicht an die Regeln halten, etwa durch häufige Abstimmung gegen die Mehrheit.

Proof-of-Work (PoW)

Der Konsensmechanismus Proof-of-Work (PoW) verwendet energieintensive Rechenaufgaben, die von den Minern zu lösen sind, um den Abstimmprozess gegenüber Angreifern zu schützen. Das Stimmgewicht wird beim PoW an eine knappe Ressource in Form von Energie, die für die Rechenleistung benötigt wird, gekoppelt. Miner erhalten für das erfolgreiche Hinzufügen eines Blocks neu geschaffene Anteile des Kryptowerts (zum Beispiel Bitcoin).

Smart Contracts

Ein Smart Contract ist ein selbstausführender Computercode, in dem die Bedingungen einer Vereinbarung zwischen zwei oder mehreren Parteien festgeschrieben sind. Der Code und die darin enthaltenen Bestimmungen existieren in einem verteilten, dezentralen Blockchain-Netzwerk. Da die Ausführung basierend auf externen Triggern stattfindet, werden in Smart Contracts niedergelegte Bedingungen garantiert ausgeführt.

Stablecoin

Ein Stablecoin ist ein Kryptowert, der Mechanismen zur Preisstabilisierung nutzt, um Schwankungen zu minimieren, und häufig an eine offizielle Währung wie den US-Dollar gekoppelt ist.

Tokenisierung

Unter Tokenisierung wird die mithilfe von Blockchain-Technologie digitalisierte Darstellung von Rechten und Pflichten an physischen oder digitalen Vermögenswerten in Form von Token verstanden.

Über die Autoren

Prof. Dr. Philipp Sandner

ist Gründer des Frankfurt School Blockchain Centers. Weiterhin war er an der Technischen Universität München und der Ludwig-Maximilians-Universität München tätig und forschte am Berkeley Center for Law & Technology. Er war Mitglied im FinTechRat und dem Digital Finance Forum des Bundesministeriums der Finanzen und hat mehrere Stipendien und Best Paper Awards erhalten. Zu seinen Themengebieten gehören die Blockchain-Technologie im Allgemeinen, Krypto-Assets wie Bitcoin und Ethereum, Decentralized Finance, der digitale Euro, Tokenisierung von Assets und der Bereich digitale Identität.

Benjamin Schaub

ist Chief Digital Officer bei intas.tech und berät Finanzinstitute zu den Themen Digital Assets und Blockchain-Technologie. Durch seine vorherige Position als wissenschaftlicher Mitarbeiter des Frankfurt School Blockchain Centers verfügt er über mehrjährige Erfahrung bei der Integration von Blockchain-Anwendungsfällen in der Finanzindustrie. Zu seinen Schwerpunktthemen gehört der Aufbau von Geschäftsmodellen für Kryptowerte sowie die regulatorischen möglichen Anwendungsfelder der Blockchain-Technologie im Kapitalmarkt wie zum Beispiel Kryptowertpapiere und Kryptofondsanteile.

Um digitale Werte wie beispielsweise Aktien, Immobilien, Schuldtitel, Währungen oder Krypto-Assets abzubilden, ist die Blockchain-Technologie ausgezeichnet geeignet. Aus diesem Grund sind Anwendungsfälle im Bereich der Finanzen in den vergangenen Jahren stark gewachsen. In der vorliegenden Studie werden die technischen Eigenschaften der Distributed-Ledger-Technologie (DLT) als zentrales Element einer Blockchain erläutert. Zusätzlich wird ein Einblick in aktuelle regulatorische Entwicklungen, auch mit Fokus auf die Rechtsprechung in Deutschland und der EU, vermittelt. Darauf aufbauend zeigen ausgewählte Anwendungsbeispiele die Auswirkungen der DLT auf die Industrie und den Finanzsektor. Abschließend gibt die Studie einen Ausblick auf die weitere Entwicklung der DLT zu den Themen Metaverse, Non-Fungible Token (NFT) und Web 3.0.

kas.de