Mittelstand 4.0
Kompetenzzentrum
eStandards

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

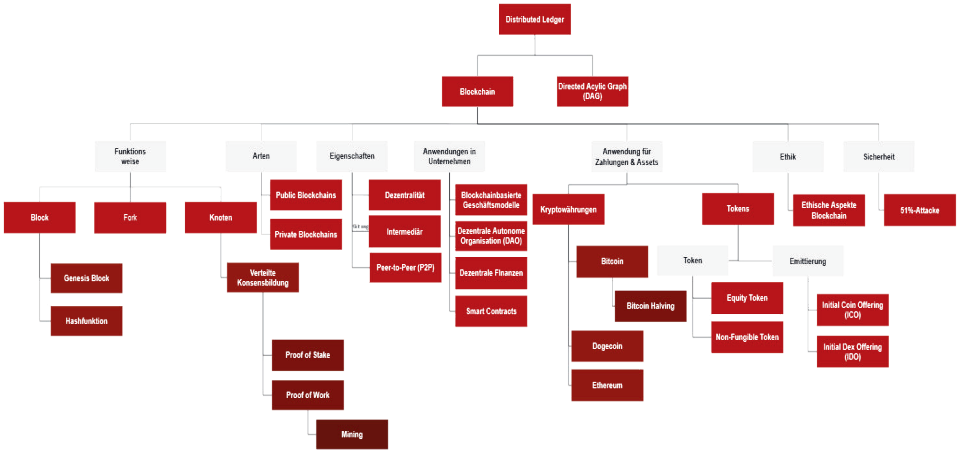
Begriffe rund um Blockchain

Faktenblatt

Im Fokus

Blockchain ist eine Technologie zum dezentralen, sicheren und nicht manipulierbaren Transfer von Daten.

In der nachfolgenden Übersicht sind die wichtigsten Begriffe und Themen rund um die Blockchain-Technologie kurz und knapp erläutert.



51%-Attacke

Bei einer 51%-Attacke soll die Kontrolle über eine Blockchain erhalten werden. Der Angreifende versucht, mindestens 51% der Gesamtrechenleistung des Netzwerkes (Hashing-Kraft) aufzubringen, um die Blockchain steuern und ändern zu können. Je größer das Blockchain-Netzwerk ist, desto schwieriger und kostspieliger wird ein Angriff.

Bitcoin

Bitcoin ist die erste weltweit verbreitete digitale Währung (Kryptowährung) und wurde 2009 von Satoshi Nakamoto initiiert. Im Gegensatz zu herkömmlichen elektronischen Geldsystemen ist für Bitcoin keine vertrauenswürdige Instanz (Intermediär) erforderlich. Anstelle einer Zentralbank verwendet Bitcoin die Blockchain-Technologie, um Transaktionen zwischen Benutzer:innen abzuwickeln und zu speichern. Bitcoin basiert auf dem Proof-of-Work-Konzept und ist im Unterschied zu klassischen Zahlungsmitteln nicht reguliert.

Bitcoin Halving

Jedes Mal, wenn in einem Bitcoin-Netzwerk eine Transaktionseinheit/ein Block neu generiert wird, bekommt ein Miner eine Belohnung. Durch das Bitcoin Halving wird diese Belohnung in regelmäßigen Abständen halbiert. Dies ist ein Sicherheitsmechanismus gegen Inflation.

Block

Bei der Blockchain-Technologie werden alle Daten als Transaktionen gespeichert und zu Blöcken zusammengefasst. Ein Block besteht mindestens aus den Transaktionsdaten und dem Hashwert des vorangegangen Blocks. Neue Blöcke werden durch diese kryptografische Verkettung manipulationssicher mit ihrem Vorgänger verbunden. Es entsteht eine stetig wachsende Kette von Datenblöcken, die sogenannte Blockchain.

Blockchain

Vereinfacht lassen sich Blockchains als verteilte Datenbanken beschreiben, die durch die Teilnehmer:innen in einem Netzwerk organisiert werden. Alle Teilnehmer:innen eines Blockchain-Netzwerkes haben eine Kopie der Datenbank bei sich gespeichert. Es handelt sich somit um ein dezentrales System. Soll ein neuer Block der Blockchain hinzugefügt werden, müssen die Teilnehmer:innen des Netzwerkes diesen verifizieren und bestätigen (mind. 51%). Die Blöcke sind über den Hashwert miteinander verkettet, wodurch von einem Block immer auf die vorherigen Blöcke geschlossen werden kann. Das macht die Blockchain transparent und manipulationssicher.

Blockchainbasierte Geschäftsmodelle

Mit Hilfe von Blockchain lassen sich neue Geschäftsmodelle etablieren. Blockchain erlaubt eine lückenlose Dokumentation; Produkte können somit problemlos in einer Lieferkette identifiziert und verfolgt werden. Auch systemübergreifende Prozesse werden sicherer und transparenter. Durch den Blockchain-Einsatz fallen zudem Intermediäre weg, was zu Kostensenkungen führt. Durch erhöhte Effizienz und reduzierte Kosten kann Blockchain in zahlreichen Branchen gewinnbringend eingesetzt werden.

Dezentrale Autonome Organisation (DAO)

Eine dezentrale autonome Organisation (DAO) basiert auf der Blockchain-Technologie und ist eine eigenständige und lokal strukturierte Organisationseinheit. Auf Basis eines Algorithmus werden selbstständig Entscheidungen getroffen. DAOs agieren ohne menschlichen Einfluss. Die Handlungen der DAO beruhen auf Smart Contracts, Geschäftsregeln, Prozessen und Besitzverhältnissen, die in einer Blockchain registriert sind. Besitzt die Organisationseinheit ein Profitziel, spricht man von einer DAC (Decentralised Autonomous Corporation).

Dezentrale Finanzen

Insbesondere der Finanzsektor wird durch Blockchain verändert. Durch Dezentralisierung und Disintermediation (d. h. durch die Unabhängigkeit von Intermediären bei Transaktionen) sind neue Geschäftsmodelle entstanden. Die Blockchain-Technologie kann die Notwendigkeit zentraler Institutionen für Finanztransaktionen überflüssig machen, da Peer-to-Peer-Transaktionen durch Vertrauen und dezentrale Plattformen erleichtert werden können. Infolgedessen kann die Blockchain-Technologie den Umfang und die Effizienz von Peer-to-Peer-Transaktionen erheblich steigern und bisher unwirtschaftliche Geschäftsmodelle realisierbar machen. Mit Hilfe der Blockchain werden Finanzdienstleistungen dezentral, innovativ, interoperable, grenzüberschreitend und transparent.

Dezentralität

Dezentral bedeutet, dass das Netzwerk über Mitglieder, die ihre Rechenleistung und Speicherkapazität zur Verfügung stellen, betrieben und wenig auf einem Server zentral gespeichert wird. Die Informationen sind daher verteilt gesichert und somit besonders gut vor Attacken und Ausfällen geschützt.

Directed Acyclic Graph (DAG)

Directed Acyclic Graph (DAG) kann als alternative Architekturmöglichkeit zu Blockchain-Technologien gesehen werden. DAG teilt die essentiellen Eigenschaften von Blockchain-Technologien, hat allerdings das Ziel, Kosten zu reduzieren und Speicherplatz zu erhöhen, indem lange redundante Ketten vermieden werden.

Distributed Ledger

Ein Distributed Ledger ist eine Art verteiltes Register/Kassenbuch, in dem Informationen gespeichert sind. Das Besondere ist, dass es ein öffentliches und dezentrales System ist. Dadurch können Werte, wie Währungen oder Informationen, direkt zwischen den Teilnehmenden ausgetauscht werden. Verifiziert werden die Austauschprozesse durch systemweit festgelegte dezentrale Prozesse und nicht durch eine zentrale Institution. Die Blockchain-Technologie ist ein Art von Distributed Ledger, in der die Informationen in Blöcken gespeichert sind.

Dogecoin

Dogecoin wurde 2013 ursprünglich als „Scherzwährung“ eingeführt und besetzt mittlerweile die Nische als Online-System für Trinkgelder, bei dem Nutzer:innen auf Social-Media-Plattformen anderen Personen Dogecoin-Trinkgelder geben. Wie Bitcoin wird auch bei Dogecoin nach dem Proof-of-Work-Konzept der schnellste Miner belohnt.

Equity Token

Ein Equity Token weist wertpapier- bzw. eigenkapitalähnliche Eigenschaften auf, ähnlich wie eine Aktie oder eine Unternehmensbeteiligung. Der Equity Token ist somit ein Vehikel zur Investition in Unternehmen. Besitzende von Equity Token haben oft Mitsprache- und Beteiligungsrechte innerhalb des Unternehmens und werden am Gewinn beteiligt.

Ethereum

Ethereum ist eine dezentrale Plattform auf Basis der Blockchain-Technologie. Der Zweck von Ethereum ist es, die Entwicklung und Implementierung von Applikationen zu ermöglichen, die von der Blockchain Gebrauch machen. Ethereum verfügt über eine eigene Kryptowährung, die Ether heißt und für die Bezahlung bestimmter Dienste im Ethereum-Netzwerk eingesetzt werden kann. Darüber hinaus ermöglicht Ethereum Smart Contracts.

Ethische Aspekte von Blockchain

Die Blockchain-Technologie weist eine Reihe an ethischen Aspekten auf. So kann mittels Blockchain die Transparenz und Nachverfolgbarkeit in den Lieferketten hergestellt werden. Darüber hinaus gewährleistet die Dezentralität, dass niemand von der Teilnahme an der Blockchain ausgeschlossen wird. Die Nutzenden können selbstbestimmt handeln, ohne unter Kontrolle einer zentralen Instanz zu stehen. Blockchain fördert durch seine Dezentralität zudem die Kontrolle von Nutzer:innen über die preisgegebenen persönlichen Daten. Da Blockchains unveränderbar und transparent sind, können die Daten im Nachgang nicht mehr eingesehen und gelöscht werden. Es ergibt sich dadurch ein Spannungsfeld mit dem Recht auf Vergessen bzw. mit dem Recht auf Löschen von Daten.

Fork

Ein Fork (= Gabelung) ist eine Aufsplittung der Blockchain in verschiedene Pfade. Zu Forks kommt es beispielsweise bei Updates oder Upgrades, um neue Funktionen hinzuzufügen oder Sicherheitsrisiken zu beseitigen. Bis zum Zeitpunkt der Aufsplittung teilen die Pfade ihren Transaktionsverlauf. Anschließend entwickeln sie sich jeweils unabhängig weiter. Bei diesem Prozess unterscheidet man zwischen Soft Forks und Hard Forks. Bei Soft Forks akzeptiert die alte Blockchain weiterhin Blöcke aus dem neu aktualisierten Blockchain-Protokoll, auch wenn sich die Regeln aufgrund der neuen Software geändert haben. Bei einer Hard Fork werden die Regeln des Blockchain-Protokolls so verändert, dass die alte Blockchain und die neue Blockchain nicht kompatibel sind.

Genesis Block

Der Genesis Block ist der erste Block in der Blockchain. Der Genesis Block initiiert bzw. startet eine Blockchain.

Hashfunktion

Die Hashfunktion generiert mit Hilfe von mathematischen Verfahren aus Daten/Informationen (z. B. einem beliebig langen Text) einen Hashwert. Der Hashwert ist dabei immer eindeutig. Werden die Daten verändert, ändert sich auch der Hashwert. Durch den Hashwert werden die ursprünglichen Daten gegen betrügerische Veränderungen abgesichert. In einer Blockchain sind die einzelnen Blöcke über die jeweiligen Hashwerte miteinander verknüpft. Wird einer neuer Block generiert, wird immer auch ein Hashwert erzeugt.

Initial Coin Offering (ICO)

Der Begriff des Initial Coin Offering (auch „Token Sale“ oder „Token Generating Event“) lehnt sich an den Begriff des Initial Public Offerings (IPO) an – also einen Börsengang. Beim ICO werden anstelle von Aktien sogenannte „Tokens“ emittiert. Diese Tokens besitzen allerdings eine andere Funktion und Struktur als herkömmliche Aktien. ICO-Tokens werden oft gegen herkömmliches Geld oder Kryptowährungen getauscht. Ein ICO bietet also Unternehmen eine Möglichkeit zur Kapitalaufnahme, ohne den streng regulierten herkömmlichen Prozess.

Initial DEX Offering (IDO)

IDOs sind Tokens, die von einem Projekt auf einer dezentralen Liquiditätsbörse an den Markt gebracht werden. Sie können sofort von jedem gehandelt werden – ohne Mindestvolumen. Dieser dezentrale Austausch wird als DEX (Abkürzung für “decentralized exchange”) bezeichnet. DEX ermöglicht den Austausch von Tokens und Kryptowährung ohne einen Intermediär. Dabei wird jede Transaktion unveränderlich in einer öffentlichen Blockchain gespeichert. Durch die Dezentralität des Austausches sind die Notierungskosten an der DEX-Börse günstiger als bei ICOs an zentralisierten Marktplätzen.

Intermediär

Intermediäre sind zwischengeschaltete Vermittler zwischen zwei Transaktionspartnern. Sie genießen ein hohes Vertrauen der beiden Transaktionspartner und garantieren die Korrektheit des Transaktionsablaufes. Intermediäre können durch die Blockchain-Technologie in Zukunft abgelöst werden.

Knoten

Knoten sind individuelle Systeme (z. B. ein Computer) innerhalb eines (Blockchain-)Netzwerkes und dienen als Verbindungspunkte für Datenübertragungen im Zusammenspiel mit weiteren Teil-

nehmenden (Knoten) des Netzwerkes. Bei Blockchains halten die Knoten jeweils eine Kopie der Blockchain gespeichert, die automatisch bei erneuter Verbindung mit dem Blockchain-Netzwerk aktualisiert wird.

Kryptowährungen

Bei Kryptowährungen handelt es sich um virtuelle und digitale Währungen. Diese Währungen verwenden eine Blockchain als Transaktionsprotokoll und setzen kryptographische Verfahren zur Manipulationssicherheit ein. Kryptowährungen sind keine staatlichen Währungen und werden dementsprechend auch nicht von einer Zentralbank oder öffentlichen Stellen emittiert. Trotzdem werden Kryptowährungen zum Teil von natürlichen und juristischen Personen als Tauschmittel akzeptiert.

Mining

Mining ist innerhalb des Proof-of-Work-Konsensmodells anzusiedeln und beschreibt das Verfahren zur Lösung eines Kryptorätsels. Ein Miner löst Rätsel möglichst schnell, um dafür eine Belohnung zu bekommen. Die Belohnung kann verschiedene Formen annehmen, bei Kryptowährungen oftmals in Form ebenjener Währung (z. B. Bitcoin).

Non-Fungible Token

Der Begriff fungibel beschreibt die Austauschbarkeit jedweder Einheit einer Ware mit weiteren Einheiten der gleichen Ware, d. h. zwei Parteien können den gleichen Betrag ohne Gewinn oder Verlust tauschen. Nicht-Fungibilität (non-fungibility) ist das Gegenteil davon: Jeder Token ist unterscheidbar und kann daher auch nicht geteilt, ersetzt oder umgetauscht werden. Dies wirkt sich auf die Nachverfolgbarkeit von Tokeneigentümern aus. Jeder Non-Fungible Token (NFT) muss separat nachverfolgt werden. Mit ERC-721 wurde ein Standard etabliert, der jedem NFT eine eindeutige ID zuweist. NFTs erfüllen den Zweck, Eigentum von digitalen oder physischen Vermögenswerten (z. B. Kunstwerke, Bilder oder Objekte) zu repräsentieren. Neben der eindeutigen Besitzzuweisung können NFTs zum Beispiel auch die Anwesenheit bei Events dokumentieren.

Peer-to-Peer (P2P)

Peer-to-Peer (P2P) beschreibt das Zusammenspiel Gleichberechtigter („Peers“), die einander wechselseitig Ressourcen wie Informationen, CPU-Laufzeiten, Speicher und Bandbreite zugänglich machen. So setzt ein P2P-Computernetzwerk auf die Rechenleistung und Bandbreite der Teilnehmenden, statt auf die von wenigen Servern. Diese kollaborativen Prozesse werden unter Verzicht auf zentrale Koordinationsinstanzen durchgeführt.

Private Blockchain

Private Blockchains sind Systeme, die nur für ein abgeschlossenes Konsortium, z. B. für bestimmte Unternehmen, verfügbar sind. Während Public Blockchains häufig genehmigungsfrei (permissionless) sind, sind bei Privaten Blockchains Zugriffsrechte in der Regel administriert bzw. auf ein Konsortium beschränkt. Populärstes Beispiel für eine Private Blockchain ist Hyperledger.

Proof of Stake

Mit dem Proof-of-Stake-Verfahren wird innerhalb eines Blockchain-Netzwerks ein Konsens darüber erzielt, wer den nächsten Block einer Blockchain hinzufügen darf. Für jeden neuen Block wird ein neuer Nutzender per gewichteter Zufallswahl bestimmt.

Proof of Work

Beim Proof-of-Work-Verfahren geht es wie beim Proof-of-Stake-Verfahren um das Recht, den nächsten Block einer Blockchain hinzuzufügen. Beim Proof-of-Work-Verfahren investieren die Knoten dabei Zeit, Energie und Rechenzyklen, um ein schwer zu lösendes, aber leicht zu verifizierendes Problem zu lösen. Der Miner, der als erster die Aufgabe löst, darf den nächsten Block generieren. Im Gegensatz zum Proof of Stake kann damit beim Proof of Work jeder Knoten die Chance nutzen, einen neuen Block hinzuzufügen.

Public Blockchain

Public Blockchains sind öffentliche Systeme, auf die theoretisch jeder zugreifen kann. Beispiele für öffentliche Systeme sind z. B. Ethereum oder die First Generation Blockchain, auf der Bitcoins basieren.

Smart Contracts

Ein Smart Contract ist ein digitales Transaktionsprotokoll bzw. ein computerbasierter Vertrag. Im Smart Contract werden zum einen die Bedingungen des Vertrages bestimmt (Zahlungskonditionen, Pfandrechte, Durchsetzung, etc.) und zum anderen die Aktivitäten, welche bei Erfüllung automatisch ausgeführt werden. Da Smart Contracts in Blockchains protokolliert werden, sind nachträgliche Veränderungen an Smart Contracts nahezu unmöglich. Smart Contratcs reduzieren den Bedarf an vertrauenswürdigen Intermediären.

Tokens

Tokens sind digitale Vermögenswerte, die auf Blockchain basieren. So können Tokens analog zu Aktien bei einem Börsengang gesehen werden, haben jedoch nicht die einfache Funktion eines reinen Anteils am Unternehmen. Tokens fungieren als eine Art digitaler Gutschein/Coupon, der für Dienstleistungen des Unternehmensprojektes steht. Im Gegensatz zu Krypotwährungen sind Tokens keine Zahlungsmittel. Darüber hinaus nutzen sie eine bereits bestehende Blockchain-Infrastruktur als Basis, besitzen also keine eigene Blockchain, Nodes und Miner. Tokens können ohne diese Infrastruktur nicht existieren.

Verteilte Konsensbildung

Im Kontext von Blockchain wird die Validität einer Transaktion (Hinzufügen eines neuen Blockes) über eine verteilte Konsensbildung sichergestellt. Diese spiegelt einen Beurteilungsprozess wieder, bei dem die einzelnen Knoten sich einigen müssen, ob eine Transaktion gültig ist. Dafür muss die Mehrheit der Knoten (mind. 51%) die Korrektheit der Transaktion bestätigen. Erst dann kann die Transaktion der Blockchain hinzugefügt werden.

Literaturverzeichnis

Brühl, V. (2017). Bitcoins, blockchain und distributed ledgers. Wirtschaftsdienst, 97(2), 135-142.

Berghoff, C., Gebhardt, U., Lochter, M., & Maßberg, S. (2019). Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen. Bundesamt für Sicherheit in der Informationstechnik (Hrsg) Bundesamt für Sicherheit in der Informationstechnik, Bonn.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37).

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

Dai, C. (2020). DEX: A DApp for the Decentralized Marketplace. In Blockchain and Crypt Currency (pp. 95-106). Springer, Singapore.

Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and business ethics. Journal of Businnes Ethics, 152(1), 1-14

Korschinowski, S., Forster, M., & Reulecke, L. (2018). Blockchain–wie Banken die Technologie aus Prozess-und Produkt-Sicht nutzen können. In Praxishandbuch Digital Banking (pp. 277-290). Springer Gabler, Wiesbaden.

Gyr, E. (2017). Dezentrale Autonome Organisation DAO - Eine juristische Betrachtungsweise. In Jusletter.

Hahn, C., & Wons, A. (2018). Initial Coin Offering (ICO): Unternehmensfinanzierung auf Basis der Blockchain-Technologie. Springer-Verlag.

Jakob, S., Schulte, A. T., Sparer, D., Koller, R., & Henke, M. (2018). Blockchain und Smart Contracts: Effiziente und sichere Wertschoepfungsnetzwerke. Whitepaper: Fraunhofer Gesellschaft.

Regner, F., Urbach, N., & Schweizer, A. (2019). NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application.

Ross, A. (2016). Die Wirtschaftswelt der Zukunft: wie Fortschritt unser komplettes Leben umkrempeln wird. Plassen Verlag.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 9(9), 1788.

Schlatt, V., Schweizer, A., Urbach, N., & Fridgen, G. (2016). Blockchain: Grundlagen, Anwendungen und Potenziale.

Schütte, J., Fridgen, G., & Prinz, W. (November 2017). Blockchain und Smart Contracts - Technologien, Forschungsfragen, Anwendungen.

Tang, Y., Xiong, J., Becerril-Arreola, R., & Iyer, L. (2019). Ethics of blockchain: a framework of technology, applications, impacts, and research directions. Information Technology & People.

Živić, N., Kadušić, E., & Kadušić, K. (2020). Directed Acyclic Graph as Hashgraph: an Alternative DLT to Blockchains and Tangles. In 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-4). IEEE.

Impressum:

Autor: Nick Harnau, Lorenz Laderick
Redaktion: Sarah Kilz
Grafik: Nick Harnau

Mittelstand 4.0-Kompetenzzentrum eStandards
Offene Werkstatt Leipzig
c/o Fraunhofer-Zentrum für Internationales Management und Wissensökonomie IMW

Kontakt:

Tel: +49 341 231039 122
leipzig@kompetenzzentrum-estandards.digital
www.kompetenzzentrum-estandards.digital

Das Mittelstand 4.0-Kompetenzzentrum eStandards gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter
www.mittelstand-digital.de