# I. Die Blockchain

*Alexandra Ciarnau*

## A. Einleitung

Die Blockchain ist eine der faszinierendsten technischen Innovationen der letzten Jahre. Sie trifft mit den damit verbundenen Möglichkeiten der Digitalisierung, bei gleichzeitig erhöhtem Vertrauen in das System, den Nerv der Zeit. Mit Hilfe der Blockchain lassen sich digitale Informationen fälschungssicher, transparent und unveränderbar dokumentieren. Diese Funktionalitäten sind in unterschiedlichsten Konstellationen gefragt. 1

Um eine detaillierte juristische Beurteilung der rechtlichen Rahmenbedingungen von Blockchain-Anwendungen vornehmen zu können, ist es unerlässlich, die grundlegenden Funktionsweisen der Technologie zu verstehen. Dementsprechend fassen wir die wichtigsten technischen Punkte einleitend zusammen, um in den weiteren Kapiteln auf dieser Basis die rechtlichen Implikationen zu beleuchten. 2

### 1. Entwicklung der Blockchain

An der Idee einer kryptografischen Verkettung von Datenblöcken wird schon seit den frühen 90er-Jahren gearbeitet. Den Durchbruch erlangte die Blockchain-Technologie jedoch erst 2008 mit der Etablierung und dem Höhenflug einer ihrer Anwendungen, nämlich des Bitcoins.[1] 3

Einen weiteren Meilenstein stellt die Entwicklung der Ethereum-Blockchain im Jahr 2013 dar: Dabei handelt es sich um eine Blockchain-Anwendung, die anders als das Bitcoin-Netzwerk das Hosting von NFTs und DApps sowie den Abschluss von Smart Contracts ermöglicht.[2] DApps sind dezentrale, an Smart Contracts gekoppelte Programme, die nicht wie übliche Apps (zB WhatsApp) von einem Anbieter betrieben werden, sondern dezentral über das Blockchain-Netzwerk laufen.[3] Smart Contracts sind auf Basis der Blockchain implementierte Automatismen, die bei Eintritt einer bestimmten Bedingung ein vertraglich festgelegtes 4

1 *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (zuletzt aufgerufen am 14. 2. 2024).

2 *Vitalik Butarin*, Ethereum White-Paper, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (zuletzt aufgerufen am 14. 2. 2024).

3 Vgl Kapitel I.C.6.c.

Ereignis auslösen.[4] Aufgrund dieser technologischen Weiterentwicklungen kommt die Technologie nunmehr **in diversen Bereichen** – auch abseits des Finanzmarktes – wie etwa im Kunst- und Immobilienhandel, Lieferkettenmanagement, als Grundlage des Metaverse, am Energiemarkt, bei der Ausgabe von Zertifikaten (zB in der Aus-/Fortbildung, am Arbeitsmarkt, bei Luxusgütern), Beschlussfassungen oder für digitale Identitäten zum Einsatz.[5]

5 Einer der bedeutendsten Momente in der Geschichte der NFT ereignete sich im März 2021. Der Digitalkünstler Mike Winkelmann, auch bekannt als *Beeple*, verkaufte sein digitales Kunstwerk „*Everydays – The First 5000 Days*" bei einer Christie's-Auktion für USD 69 Mio. Das war die erste Versteigerung eines digitalen Kunstwerks durch ein großes Auktionshaus. Dieser bahnbrechende Verkauf zeigte den potenziellen Wert, der mit digitalen Inhalten verbunden werden kann, und brachte NFTs in die Schlagzeilen der Mainstream-Medien. Darauf folgten viele weitere NFT-Anwendungen im kreativen Bereich, wie etwa in der Musik- und Gamingbranche.

6 Im Jahr 2022 hat sich schließlich durch die Neuausrichtung der Ethereum Foundation nach der Kritik an klimaschädlichen Kryptowährungen ein neuer Konsensmechanismus für die Blockchain durchgesetzt und die Technologie weiter beflügelt – das Proof of Stake-Verfahren.[6] Dabei hängt die Erzeugung eines neuen Blocks nicht wie bei Bitcoin von der aufgewendeten Rechenleistung (vgl Proof of Work-Verfahren in Kapitel I.C.4.), sondern vom gewichteten Zufall ab. Durch die Einbindung eines nach dem Zufallsprinzip agierenden Algorithmus wird der Stromverbrauch massiv reduziert.[7] Das erhöhte grds die Attraktivität der Blockchain-Technologie.

---

**4** Vgl Kapitel I.C.6.a.

**5** Zahlreiche dieser Use Cases werden in den jeweiligen Fachkapiteln behandelt, so bspw NFTs in Kapitel IV., Security Token in Kapitel IX, Kryptowährungen (Coins) in Kapitel VI und Immo-Token in den Kapiteln XI. und XII.

**6** Aufgrund des enormen Energieverbrauchs steht das Konsensverfahren Proof of Work unter Kritik. Vgl zB *FAZ*, Kryptowährungen brauchen enorme Mengen Strom und Wasser, 29. 10. 2023, https://www.faz.net/aktuell/finanzen/finanzmarkt/energieintensive-produktion-kryptowaehrungen-brauchen-enorme-mengen-strom-und-wasser-19276506.html (zuletzt aufgerufen am 10. 2. 2024). Daher ist Ethereum zum Proof of Stake- Verfahren gewechselt, vgl *Neuhaus/Schwarz*, Die zweitgrößte Kryptowährung der Welt verbraucht jetzt bis zu 99,95 Prozent weniger Energie, Handelsblatt 15. 9. 2022, https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/ethereum-update-die-zweitgroesste-kryptowaehrung-der-welt-verbraucht-jetzt-bis-zu-99-95-prozent-weniger-energie/28683044.html (zuletzt aufgerufen am 10. 2. 2024).

**7** Vgl https://ethereum.org/de/energy-consumption (zuletzt aufgerufen am 10. 2. 2024).

Die beschriebenen Veränderungen konnten jedoch den Kryptowinter nicht aufhalten. Damit wird ein langer Abschwung der Preise für Krypto-Assets bezeichnet.[8] Analysten zufolge ist in der zweiten Jahreshälfte 2022 der Boom abgeflacht.[9] Das hängt mit dem Wertverlust der digitalen Vermögenswerte zusammen. Die Kurse der jeweiligen Krypto-Assets sind deutlich unter ihrem jeweiligen Höchststand. Das ist mit einem Bärenmarkt bei traditionellen Aktien vergleichbar. Seitdem hat sich Stand Anfang 2024 der Markt langsam erholt und sich dem bisherigen Höchststand angenähert. **7**

**Beispiel** **8**

Den Höchststand hatte Bitcoin im November 2021 mit zirka USD 56.000. Im Dezember 2022 war der Kurs nur mehr bei etwas über USD 15.000. Somit ein Wertverlust von fast 75 %. Umgekehrt stieg der Kurs bis Februar 2024 wieder auf fast USD 50.000. Diese Volatilität des Kurses ist mit ein Grund, warum die Aufsichtsbehörden gegenüber der Kryptowährung kritisch eingestellt sind.

## 2. Wesen der Blockchain

### a) Verkettung der Inhalte

Technologisch gesehen basiert die Blockchain auf der *Distributed Ledger Technologie* („*dezentral geführtes Geschäftsbuch*"), ergänzt durch diverse kryptografische Verfahren. Die Blockchain ist kurz gesagt eine Kette chronologisch aneinandergereihter und kryptografisch miteinander verknüpfter Datensätze (***Chain***), die nicht bei einer zentralen Stelle, sondern auf allen am Netzwerk teilnehmenden Endgeräten der Full Nodes gespeichert werden.[10] **9**

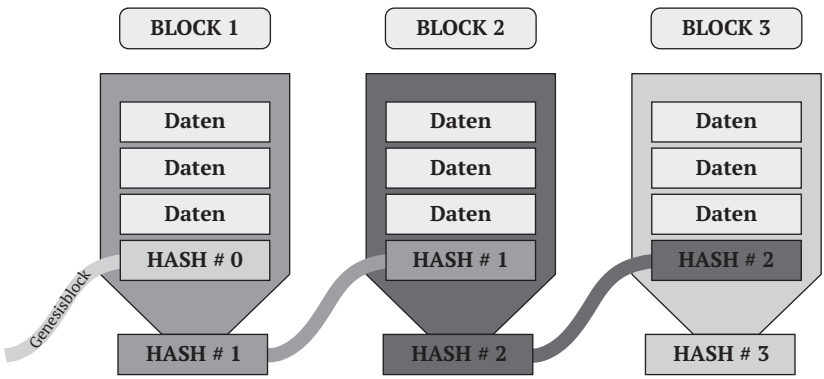
Blockchains sind somit verteilte Datenbanken. Ihre Inhalte werden durch die Nutzer kreiert. Der jeweils folgende Eintrag wird dabei untrennbar mit dem vorherigen verkettet. Das erfolgt, indem die Informationen zu Datenblöcken (***Blocks***) zusammengefasst und durch ihre digitalen Fingerabdrücke (***Hashes***) miteinander **10**

**8** Vgl https://coincierge.de/kryptowaehrungen-kaufen/krypto-winter/ (zuletzt aufgerufen am 16. 2. 2024).

**9** Vgl https://b2broker.com/de/news/what-crypto-winter-means-and-when-it-will-come-to-a-close/ (zuletzt aufgerufen am 16. 2. 2024).

**10** Vgl Kapitel I.D.4. für Details zu Nodes.

verknüpft werden.[11] Durch das Hash-Verfahren erhält jeder einzelne Datenblock eine individuelle und einzigartige Zeichenfolge einer fixen Länge, den Hashwert, zugewiesen.[12] Dieser errechnet sich aus dem konkreten Inhalt der Datensätze. Dieselben Eingabedaten ergeben bei Verwendung desselben Verschlüsselungsverfahrens immer denselben Hashwert, während jede – auch noch so kleine – Abweichung des Inhaltes und damit auch jede nachträgliche Veränderung der Ursprungsdaten zu einem anderen Prüfwert führt. Die Verkettung erfolgt in weiterer Folge dadurch, dass jeder neu generierte Block sowohl den Hash des vorangehenden Datensatzes als auch den Hashwert der im neuen Datenblock enthaltenen Informationen beinhaltet.[13] So verweist jeder einzelne Block auf alle früheren Datensätze. Durch die Aneinanderreihung protokolliert die Blockchain somit alle jemals gespeicherten Informationen in chronologischer Reihenfolge.[14] Nach der Verknüpfung kann der Inhalt der gesamten historischen Datensätze daher – je nach Größe des Blockchain-Netzwerks – praktisch nicht mehr manipuliert werden: Jede noch so minimale **nachträgliche Veränderung eines Blocks** führt zu einem **neuen Hashwert** und damit zu einer **Durchbrechung der Kette**. Kurzum: Die Datenkette kann durch Hinzufügen neuer Blöcke unendlich erweitert, aber nachträglich nicht geändert werden.[15] Zur Veranschaulichung:




11 Jede Blockchain beginnt mit einem sog *Genesisblock*, der vom Programmierer der Anwendung stammt und fest im Source Code verankert ist. Mit welchen Da-

11 *UK Government Chief Scientific Adviser*, Distributed Ledger Technology: beyond block chain (2016) 33.
12 *Fraunhofer Institut*, Blockchain Grundlagen, Anwendungen und Potenziale (2016) 8 ff.
13 *Creusen/Gall/Hackl*, Digital Leadership (2017) 17.
14 *Fraunhofer Institute*, Blockchain Grundlagen, Anwendungen und Potenziale 10.
15 *Böhme/Pesch*, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD 2017, 473.

tensätzen der Initiator seinen Genesisblock befüllt, um dann daraus den Hash #0 zu errechnen, bleibt komplett ihm überlassen.[16] Der Hashwert dieses Ursprungsdatensatzes wird in den Block 1 aufgenommen. Aus der individuellen Kombination der Inhaltsdaten des ersten Datenblocks samt Hash #0 errechnet sich der Hashwert des gesamten Blocks 1 (Hash #1). Der Hash #2 setzt sich, dieser Logik folgend, aus den neuen Einträgen und dem Hash #1 des vorangestellten Blocks zusammen. Dieses Grundprinzip setzt sich bei jedem Hinzufügen eines neuen Blocks fort. Dadurch sind sämtliche alten Einträge über die Berechnung der nachfolgenden Hashwerte unter Mitberücksichtigung des Voreintrages verknüpft und so gesichert. Würde nun nachträglich der Genesisblock oder jeder beliebige andere Eintrag in der Kette verändert werden, stimmen sämtliche nachfolgende Hashwerte nicht mehr überein. Ein solches Durchbrechen der Datenkette fällt im Zuge der automatisch durchgeführten Autorisierungs- und Validierungsprozesse beim Versuch des Hinzufügens des nächsten Blocks sofort auf. Wird eine Abweichung der Hashwerte festgestellt, ist ein Anfügen dieses weiteren Blocks nicht möglich.

## b) Dezentralität

Die in der Blockchain generierte Datenkette wird nicht zentral an einem Ort gespeichert, sondern in einem Netzwerk verteilt: Jeder Teilnehmer an einer Blockchain verfügt über eine vollständige, sich automatisch synchronisierende Kopie der Datenbank und damit aller historischen Transaktionen. Die Blockchain wird somit von einem Netzwerk vieler Teilnehmer dezentral betrieben und verwaltet. Diese dezentrale Struktur bringt ein hohes Maß an Sicherheit mit sich: Der Ausfall eines einzelnen Rechners hat keine Auswirkungen auf die mehrfach abgespeicherte und laufend synchronisierte Datenbank. Alle berechtigten Teilnehmer des Netzwerks können zudem stets auf die aktuelle Version des Protokolls und die gesamte Historie zugreifen. **12**

Die Netzwerkteilnehmer fungieren außerdem als neutrale, kollektive Kontroll- und Sicherheitsinstanzen, die die Integrität und Beständigkeit der Blockchain-Inhalte sicherstellen. Bevor ein Datensatz in das Protokoll der Kette aufgenommen wird, entscheidet das Peer-to-Peer-Netzwerk in den meisten Blockchain-Varianten (vgl Kapitel I.B. für Details) durch eine Übereinkunft (Konsens) gemeinsam über die Aktualisierung der Daten.[17] Dadurch werden abhängig von der Größe des Netzwerks möglichst manipulationssichere Autorisierungs- und Validierungsprozesse **13**

**16** Der Bitcoin-Genesisblock enthält zB eine Headline der Times und den Blockreward von 50 BTC für die Erzeugung des ersten Blocks.

**17** *BSI*, Blockchain sicher gestalten (2019) 9.

verwendet. So wird sichergestellt, dass die betreffenden Informationen korrekt sind (der Hashwert unverändert ist). Dies schafft die Vertrauensbasis für die Blockchain und der darin gespeicherten Daten.

14 Die Blockchain-Technologie erlaubt es den Teilnehmenden somit, **unabhängig von einer zentralen Kontrollinstanz** und dennoch **manipulationssicher** Informationen abzuspeichern und auf dieser Basis etwa Transaktionen durchzuführen.

### c) Fazit

15 Die zentralen Wesensmerkmale einer Blockchain sind somit va die **unveränderbare Verknüpfung der Informationen** miteinander und ihre **dezentrale Speicherung**. Solche dezentralen und fälschungssicheren Datenbanken sind freilich nicht nur für Kryptowährungen, sondern für mannigfaltige andere Anwendungsbereiche und viele Branchen interessant. Tatsächlich werden auf Basis der Blockchain bereits alle möglichen Arten von Transaktionen wie Aktiengeschäfte oder auch Smart Contracts abgewickelt, Grundbücher geführt oder Lieferketten transparent gemacht.[18]

## B. Blockchain-Arten

16 Um möglichst vielen Anwendungsfeldern in diversen Branchen – von sensiblen Geschäftsbereichen über die öffentliche Verwaltung bis hin zu modernen Lieferketten und neu gedachten Marktplätzen – gerecht zu werden (vgl dazu Beispiele in Kapitel I.E.), haben sich in der Praxis auf Basis der dargestellten Grundidee mittlerweile verschiedenste Ausprägungen der Blockchain gebildet. Daher gibt es nicht *die* Blockchain, sondern es existieren vielmehr eine Reihe ähnlicher Systeme, die sich in Details unterscheiden. Die wichtigsten Unterscheidungskriterien und Spielarten verschiedener Blockchain-Typen stellen wir in der Folge kurz vor. Sie unterscheiden sich insb danach, wer Zugang zum Datenprotokoll hat und wer Eintragungen darin vornehmen kann.

### 1. Private permissioned Blockchain

17 Bei einer privaten und zugangsbeschränkten Blockchain ist im Vorhinein festgelegt, welche Teilnehmer eine Kopie des Protokolls erhalten, darin Einsicht nehmen und Eintragungen vornehmen können. Sie steht somit nur einer **geschlossenen Teilnehmergruppe** zur Verfügung und eignet sich daher insb für

18 Vgl https://www.eublockchainforum.eu/initiative-map (zuletzt aufgerufen am 14. 2. 2024).

unternehmens- bzw konzerninterne Anwendungen sowie abgrenzbare unternehmensübergreifende Kooperationen bzw Transaktionen. Solche Blockchains werden bspw eingesetzt, um Lieferketten über mehrere Zwischenakteure hinweg nachvollziehbar zu gestalten, indem jeder Teilnehmer seine Einträge in der Datenkette hinterlässt.

Private Blockchain-Netzwerke nutzen aufgrund des bestehenden Vertrauensverhältnisses regelmäßig einfachere Konsensmechanismen, wie zB Proof of Authority.[19] **18**

## 2. Öffentliche Blockchain

Öffentliche, aber zugangsbeschränkte Blockchains sind demgegenüber für jedermann einsehbar. Hier ist zwar fest vorgegeben, welche Stellen eine Kopie der gesamten Kette halten dürfen und wer Eintragungen darin vornehmen kann, Einsicht in das Protokoll wird jedoch jedermann gewährt. Diese Art der Blockchain eignet sich bspw für staatliche Blockchain-Plattformen zur Aufzeichnung von Eigentumsverhältnissen im Grundbuch. **19**

Öffentliche und zugangsfreie Blockchains stellen die ursprüngliche, liberalste Variante des Systems dar. Hier steht es jedermann frei, am Netzwerk teilzunehmen, in die Chain-Historie einzusehen, sie downzuloaden oder Einträge vorzunehmen. Klassische Beispiele für public permissionless Blockchains sind Bitcoin und Ethereum.[20] **20**

## 3. Konsortiale Blockchain

Die *konsortiale* Blockchain ist eine Hybridlösung aus den oben genannten Spielarten. Sie wird meist von einem Konsortium aus mehreren Organisationen verwaltet. Das Konsortium bestimmt daher, wer validieren und Leserecht erhalten darf. Zugang haben nur zugelassene Teilnehmer. Dadurch sind konsortiale Blockchains deutlich flexibler. **21**

**19** Für Details zu Proof of Authority vgl Kapitel I.C.4.c.

**20** *Scherk/Pöchhacker-Tröscher*, Die Blockchain – Technologiefeld und wirtschaftliche Anwendungsbereiche (2017) 15 ff.

## 4. Übersicht über die verschiedenen Blockchain-Arten

22

| | Öffentlich | Privat | Konsortial |
|---|---|---|---|
| **Zugang** | Offen zugänglich | Nur für zugelassene Teilnehmer | Nur für zugelassene Teilnehmer |
| **Personenbezug** | Pseudonyme Nutzung | Herstellbar | Herstellbar |
| **Bildung neuer Blöcke** | Dezentral durch Ressourceneinsatz der Miner | Zentral durch eine Instanz | Je nach Ausgestaltung |
| **Konsensmechanismus** | idR Proof of Work, zT auch Proof of Stake | idR Proof of Stake oder Proof of Authority | Je nach Ausgestaltung |
| **Sicherheit** | Sehr hoch | Eingriffe durch zentrale Akteure möglich | Je nach Ausgestaltung |
| **Energieverbrauch** | Hoch (beim Proof of Work) | Eher niedrig | Je nach Ausgestaltung |
| **Transparenz** | Hoch | Nur für ausgewählten Teilnehmerkreis | Nur für ausgewählten Teilnehmerkreis |
| **Systemänderungen** | Niedrige Flexibilität | Hohe Flexibilität | idR Konsens im Konsortium |
| **Änderungen an bereits durchgeführten Transaktionen** | Nicht möglich | Möglich durch zentrale Instanz | Möglich (zB durch Mehrheitsbeschluss im Konsortium) |
| **Geschwindigkeit der Transaktionen** | Gering (beim Proof of Work) | Eher schnell | Eher schnell |
| **Kryptowährung** | idR als Anreizmechanismus zur Bildung neuer Blöcke notwendig | Optional | Optional |

**Abbildung:** Quelle: Bundesnetzagentur[21]

**21** *Bundesnetzagentur*, Die Blockchain-Technologie (2021) 15.

# C. Technische Funktionsweise der Blockchain

Um die Funktionsweise einer Blockchain zu verstehen, müssen zunächst die relevantesten Begriffe erklärt und das Verfahren veranschaulicht werden. Angesichts der dargestellten Vielfalt der Ausprägungen gehen wir im Folgenden auf die technischen Basics der gängigsten Blockchain-Typen ein: **23**

## 1. Netzwerk

Die Blockchain beruht auf der *Distributed Ledger Technologie* („DLT"). Dabei können alle Zugriffsberechtigten ständig in die synchronisierte, identische Kopie des Protokolls und somit jederzeit Einsicht in die gesamte Historie aller jemals abgelegten Inhalte nehmen.[22] Die Informationen werden also laufend aktualisiert, synchronisiert und somit alle Teilnehmer stets auf dem neuesten Stand gehalten. Solche Systeme sind folglich mit riesigen Datenbanken vergleichbar, die nicht auf einem Server liegen, sondern auf vielen Servern im gesamten Netzwerk verteilt sind.[23] **24**

Die Blockchain baut auf diesem Ansatz auf und schafft ein **Peer-to-Peer-Netzwerk, dessen Teilnehmer unmittelbar und ohne eine zentrale Instanz miteinander interagieren**. Bei herkömmlichen Anwendungen zur Daten- und Informationsverwaltung (etwa einem Zahlungssystem) existiert dagegen regelmäßig eine zentrale Instanz (etwa eine Bank), die die Hoheit über die gesamten Tätigkeiten hat. Bei einem dezentralen System wird auf diese „*Trusted Third Party*" (den Mittelsmann) verzichtet und diese Instanz durch das gesamte Netzwerk ersetzt. Im dezentralen Netzwerk einer Blockchain gibt es daher **keine einzelne Autorität**, die über die Datenaufzeichnung oder die Richtigkeit der Einträge bzw Transaktionen entscheidet. Stattdessen sind zur kollektiven Entscheidungsfindung innerhalb des Netzwerks dezentrale Konsensmechanismen vorgesehen.[24] **25**

## 2. Kryptografische Funktionen

Die wichtigsten (kryptografischen) Funktionen sind das **Public Key Verschlüsselungsverfahren** und **die Hash-Funktionen**. **26**

---

**22** *Schlund/Pongratz*, Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, DStR 2018, 598.

**23** https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1602_blockchain.html (zuletzt aufgerufen am 14. 2. 2024).

**24** Vgl Kapitel I.C.4. für Details zu Konsensmechanismen.

27 Beim Public Key (asymmetrischen) Verfahren wird durch einen Algorithmus ein mathematisch verbundenes Schlüsselpaar generiert, das aus einem Private- und einem Public Key besteht. Den Private Key hält der jeweilige Nutzer geheim. Mit diesem kann er Datensätze signieren und an die anderen Teilnehmer senden. Der Public Key ist dagegen allen Teilnehmern im Blockchain-Netzwerk bekannt und wird dazu verwendet, um den einzelnen Nutzer im Netzwerk zu identifizieren.[25]

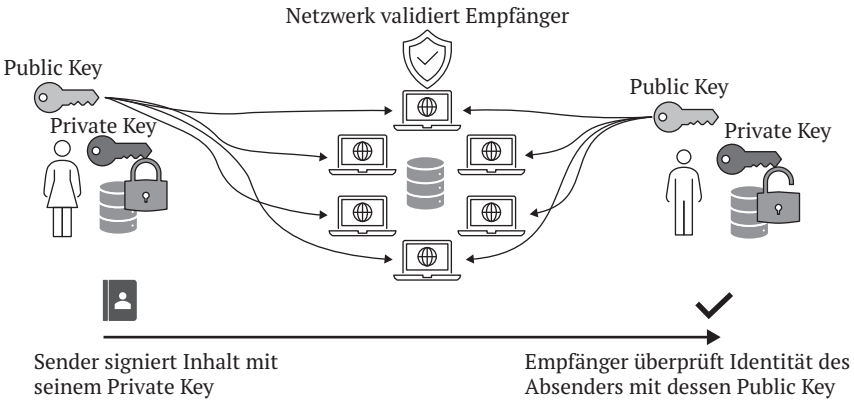



**Abbildung:** *Alexandra Ciarnau*

28 Beim Hashing werden beliebig große Datenmengen auf eine zuvor vom Algorithmus festgelegte kleinere Zeichenfolge reduziert. Der Hash generiert sich aus dem Inhalt eines Datensatzes und stellt somit eine Art Prüfsumme der enthaltenen Information dar. Ein Hash besteht immer aus einer bestimmten Anzahl von Zeichen, unabhängig davon, wie umfangreich die eingegebene Datenmenge ist. Der hinter diesem Verfahren stehende Algorithmus stellt sicher, dass das Hashing eine Einwegfunktion ist. Somit ist es idR nicht möglich, aus der Zeichenabfolge eines Hashs die zugehörigen Ursprungsdaten zu ermitteln. Allerdings ergeben dieselben Ursprungsdaten immer denselben Hash. Ein kryptografischer Hash hat damit die Einmaligkeit eines Fingerabdrucks.[26]

25 *Bundesnetzagentur*, Die Blockchain-Technologie 7.
26 *Freitag*, Die Blockchain-Technologie, CFOaktuell 2018, 59 ff.