Kapitel 2 – Die Blockchain-Technologie

Die Blockchain-Technologie ist eine neue Technologie zur Datenverwaltung, deren wesentliches Merkmal ist, dass Daten dezentral verwaltet werden. Erstmalig trat sie im Zusammenhang mit der virtuellen Kryptowährung Bitcoin in Erscheinung. Sie ist allerdings keinesfalls auf Kryptowährungen beschränkt, sondern kann zur Datenverwaltung insgesamt verwendet werden.

Zur Vereinfachung der komplizierten, technischen Darstellung wird im Folgenden zunächst die Blockchain-Technologie anhand des Bitcoin-Systems dargestellt (hierzu unter A.).

Daran anschließend wird die Blockchain-Technologie mit ihren Funktionen auf einer abstrakteren Ebene als Datenverwaltungsstruktur unabhängig vom Bitcoin-Kontext dargestellt (hierzu unter B.), um abschließend zu erörtern, welche weiteren Anwendungsmöglichkeiten es für die Blockchain-Technologie noch gibt (hierzu unter C.).

A. Die Blockchain-Technologie anhand des Bitcoin-Systems

Die Blockchain-Technologie kann als dezentrale Datenverwaltungsstruktur verstanden werden, die bei Bitcoin eingesetzt wird, um ein Register über die virtuelle Kryptowährung unabhängig von einem zentralen Intermediär dezentral zu führen.

Was das bedeutet, wird im Folgenden zunächst dadurch erläutert, dass der historische Hintergrund von Bitcoin dargestellt wird (hierzu unter I.). Daran anschließend wird dargestellt, wie Nutzer das Bitcoin-System verwenden können (hierzu unter II.). Abschließend wird erörtert, was die Blockchain-Technologie hierfür leisten muss und wie diese Anforderungen technisch erfüllt werden und ablaufen (hierzu unter III.).

I. Historischer Hintergrund von Bitcoin und Blockchain-Technologie

Ende 2008 veröffentlichte eine bisher unbekannte Person unter dem Pseudonym *Satoshi Nakamoto* die technische Abhandlung „Bitcoin: A Peer-to-

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Peer Electronic Cash System"[7]. Diese Abhandlung enthielt die technische Bauanleitung zur ersten praxistauglichen „virtuellen Kryptowährung"[8]. Zwar gab es auch schon vor Bitcoin Konzepte zur Entwicklung virtueller Kryptowährungen, diese konnten aber entweder praktisch gar nicht umgesetzt werden, oder enthielten noch derartige Umsetzungsschwierigkeiten, dass sie sich nicht durchsetzen konnten.[9]

Die Abhandlung von *Nakamoto* erschien im Zusammenhang mit der weltweiten Finanzkrise und kann als Antwort auf den Vertrauensverlust der Menschen in das weltweite Banken- und Finanzsystem verstanden werden.[10] So referenziert Bitcoin im sog. „Genesis-Block"[11] ihrer Blockchain[12] den Artikel einer britischen Tageszeitung mit dem Titel „Chancellor on Brink of Second Bailout for Banks".[13] Vor diesem historischen Hintergrund war es also Ziel von *Nakamoto* ein Zahlungsmittel zu schaffen, das losgelöst von staatlich regulierten Banken funktionieren sollte.[14] Anders als bei staatlich regulierten Finanz- und Währungssystemen soll bei Bitcoin die Integrität des Systems bzw. das Vertrauen in das System nicht durch eine staatliche Regulierung erreicht werden, sondern durch den Algorithmus des Systems selbst.[15] Diese Integrität liefert die Blockchain-Technologie.[16] Deshalb wird Bitcoin häufig als „Trustless Trust"[17] bezeichnet. Denn anders als konventionelle Buch- und E-Geld-Systeme generiert Bitcoin das

7 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 6; *Hofert*, Regulierung der Blockchains, S. 1.

8 Zur Einordnung des Begriffs ausführlich: *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 25ff.

9 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 7; Grzywotz, Virtuelle Kryptowährungen und Geldwäsche, S. 28 m.w.N. zu vorherigen Versuchen von virtuellen Währungen.

10 *Simmchen*, MMR 2017, 162 (162).

11 Der Genesis-Block ist der erste berechnete Datensatz im Bitcoin-Netzwerk, vgl. *Hofert*, Regulierung der Blockchains, S. 1.

12 Zur Vereinfachung kann der Begriff „Blockchain" zunächst als Datenbank verstanden werden. Ausführlich werden Inhalte und Funktionsweise der Blockchain unter A.II.7, III. dargestellt.

13 *Hofert*, Regulierung der Blockchains, S. 1 m.w.N.

14 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 1; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 6f.; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 28f.

15 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 1; *Hofert*, Regulierung der Blockchains, S. 2.

16 *Hofert*, Regulierung der Blockchains, S. 2.

17 *Hofert*, Regulierung der Blockchains, S. 2 m.w.N.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Vertrauen der Nutzer lediglich durch seine technische Funktionsweise – ein Vertrauensverhältnis zwischen Kunden und Bank bzw. Bürger und Staat ist gerade nicht mehr erforderlich.[18] Dementsprechend ist der technische Ablauf der Blockchain besonders wichtig dafür, dass das Konzept von Bitcoin funktioniert.

II. Funktionsweise und Anwendung von Bitcoin für Nutzer – wie verwendet ein Nutzer Bitcoin?

Bitcoin soll als alternatives Zahlungsmittel fungieren, das für jeden Interessierten zugänglich ist (hierzu unter 1.). Die Nutzer agieren unter den Pseudonymen der *public keys* (hierzu unter 2.) bzw. den *Bitcoin-Adressen* (hierzu unter 3.).[19] Hierbei sind die *Bitcoin-Adressen* die Ergebnisse von Hashfunktionen der *public keys* (hierzu unter 4.).[20]

Anders als bei herkömmlichen Zahlungssystemen bestehen bei Bitcoin keine „Konten" als solches (hierzu unter 5.)[21], denn Bitcoin sind keine digitalen Geldmünzen, sondern lediglich Einträge von Wertzuweisungen in ein Register (hierzu unter 6.)[22]. Diese Wertzuweisungen können „übertragen" werden, indem die Wertzuweisung durch eine Transaktion verändert wird (hierzu unter 7.)[23]. Derartige Transaktionen werden in das Register des Systems, also in die Blockchain, eingetragen (hierzu unter 8.).[24]

18 So insbesondere *Hofert*, Regulierung der Blockchains, S. 2.
19 *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754); *Pesch/Böhme*, DuD 2017, 93 (93).
20 *Pesch/Böhme*, DuD 2017, 93 (93f.); *Börner*, NZWiSt 2018, 48 (48). Im Folgenden werden die Begriffe public key und Bitcoin-Adresse synonym verwendet, da die Differenzierung nur eine technische Besonderheit ist, die unter A.II.2. dargestellt wird.
21 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33f.
22 *Kütük/Sorge*, MMR 2014, 643 (643).
23 *Safferling/Rückert*, MMR 2015, 788 (790); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754); *Kaulartz*, CR 2016, 474 (474ff.); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31.
24 *Pesch/Böhme*, DuD 2017, 93 (94).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

1. Keine Zugangsbeschränkung

Das Bitcoin-System ist als offenes Netzwerk[25] ausgestaltet, an dem sich jeder Interessierte beteiligen kann – unabhängig von Standort, Bankkonto oder Herkunft, erforderlich ist nur ein Internetzugang.[26] Um sich am Netzwerk zu beteiligen ist außerdem keinerlei Angabe von personenbezogenen Daten erforderlich.[27]

2. Private Key und Public Key

Zur Beteiligung muss sich der Interessierte ein Schlüsselpaar aus sog. *private key* und *public key* generieren lassen.[28] Hiermit können die Nutzer im Bitcoin-Netzwerk aktiv werden. Dabei dient der *public key* als eine Art Adresse bzw. Kontonummer[29] und der *private key* als eine Art Signatur und Authentifizierung von Transaktionen – vergleichbar mit der PIN einer EC- bzw. Kreditkarte oder der Unterschrift auf einem (Bar-) Scheck. [30]

Hintergrund von *private key* und *public key* ist das sog. asymmetrische Verschlüsselungsverfahren. Verständlich wird dieses Verschlüsselungsverfahren durch einen Vergleich zur symmetrischen Verschlüsselung. Bei der symmetrischen Verschlüsselung existiert nur ein einziger Schlüssel zum Verschlüsseln einer Nachricht – Absender und Empfänger müssen beide diesen Schlüssel kennen.[31] Hierdurch kann aber nicht gewährleistet werden, dass keine andere Person den Schlüssel kennt, bzw. der Empfänger kann nicht mit Sicherheit wissen, dass die Nachricht auch tatsächlich vom genannten Absender stammt.[32]

---

25 Im Folgenden meint der Begriff des (Bitcoin-)Netzwerkes das *Peer-to-Peer*-Netzwerk, in dem alle Nutzer des Bitcoin-Systems zusammengeschlossen sind. Siehe hierzu insbesondere die Ausführungen zum *Peer-to-Peer*-Netzwerk unter A.III.1.b).

26 *Boehm/Pesch*, MMR 2014, 75 (75); *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 1f.; *Safferling/Rückert*, MMR 2015, 788 (793); *Kaulartz*, CR 2016, 474 (475).

27 *Boehm/Pesch*, MMR 2014, 75 (76).

28 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.

29 Der Vergleich mit einer Kontonummer ist ungenau (hierzu unter A.II.5), er soll hier nur zur Veranschaulichung dienen.

30 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 61; *Hofert*, Regulierung der Blockchains, S. 18. Auch dieser Vergleich ist stark vereinfacht und dient lediglich der Veranschaulichung.

31 *Kaulartz/Matzke*, NJW 2018, 3278 (3282).

32 *Kaulartz*, CR 2016, 474 (475); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (31f).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Im Fall von asymmetrischer Verschlüsselung gibt es dagegen zwei Schlüssel – bei Bitcoin den sog. *private key* und den sog. *public key*.[33]

Im Fall von Bitcoin wird zunächst der *private key* als eine zufällige alphanummerische Zahlenfolge erzeugt.[34] *Grzywotz* vergleicht die Funktion des *private keys* mit einem Schlüssel zu einem öffentlichen Briefkasten, in den jeder Nachrichten einwerfen, aber nur derjenige mit dem *private key* sie auch lesen kann.[35] Über diese Funktion des öffentlichen Briefkastens, den nur der Inhaber des *private keys* lesen kann, hinaus, dient der *private key* allerdings auch zum Verschlüsseln von Nachrichten bzw. wird durch die Verschlüsselung mit dem *private key* die Nachricht „signiert" (hierzu sogleich).[36]

Aus dem *private key* wird über eine rechnerische Funktion der *public key* erzeugt.[37] Der *public key* ist jedem Netzwerkteilnehmer bekannt. Er ist, wie der Name schon sagt, öffentlich.[38] Im oben dargestellten bildlichen Vergleich des öffentlichen Briefkastens, kann er als der Standort des Briefkastens verstanden werden, den der Absender von Nachrichten kennen muss, um sie an den Empfänger zu übermitteln.

Außerdem dient er zur Überprüfung der soeben erwähnten Signatur.[39] Wird eine Nachricht mit dem *private key* verschlüsselt, kann durch den dazugehörigen *public key* überprüft werden, ob sie auch tatsächlich mit dem zugehörigen *private key* verschlüsselt wurde.[40] Der Empfänger der Nachricht kann also überprüfen, ob der genannte Absender auch tatsächlich die Nachricht versendet hat – so kann der Absender seine Nachricht signieren.[41]

Das Schlüsselpaar aus *private key* und *public key* ist dabei zufällig generiert und lässt insgesamt keinerlei Rückschlüsse auf die Identität des dahinterstehenden Nutzers zu, insbesondere auch, da die Teilnahme am Netzwerk keinerlei Angabe von personenbezogenen Daten erfordert.[42]

---

33 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 2; *Kaulartz*, CR 2016, 474 (475); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.

34 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 64f.

35 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.

36 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32.

37 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32 m.w.N.

38 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31f.

39 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32f.

40 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32f.

41 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 32f.

42 *Boehm/Pesch*, MMR 2014, 75 (76).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

3. Bitcoin Adresse – als Ergebnis einer Hashfunktion

Die *Bitcoin-Adresse* ist der sog. *Hashwert* des *public keys*. Er wird verwendet, um die Datenmenge im Bitcoin-System zu verringern.[43] Ein solcher *Hashwert* entsteht, wenn eine Ziffern- und Zahlenfolge (im Folgenden als „Zeichenfolge" bezeichnet) durch eine sog. *Hashfunktion* abgebildet wird.[44]

4. Hashfunktionen

Einfachstes Beispiel einer solchen *Hashfunktion* ist die Quersumme – die Quersumme von 17 ist 8, die Quersumme von 23 ist 5.[45] Ziel solcher Funktionen ist es, eine beliebig lange Zeichenfolge „durch eine kurze Zeichenfolge fester Länge"[46] darzustellen, um schnell abgleichen zu können, ob mehrere lange Zeichenfolgen gleich sind, denn wird auch nur ein Zeichen beim Eingabewert verändert[47], verändert sich der gesamte *Hashwert*.[48] Im Fall von langen Nachrichten[49] bzw. großen Datensätzen ermöglichen die *Hashfunktionen* also den schnellen Vergleich, ob etwas an der Nachricht verändert wurde.[50] Aus diesem Grund wird der *Hashwert* eines Datensatzes häufig auch als sein digitaler Fingerabdruck bezeichnet.[51]

Damit die Nachrichten im Bitcoin-System nicht zu lang werden, werden an verschiedenen Stellen *Hashfunktionen* eingesetzt, u.a. beim *public key* – konkret wird die Funktion SHA-256 verwendet, bei der eine Zeichenfolge

43 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33. Denn dadurch, dass mit jedem Weiterleiten einer Transaktion jeweils der *public key* des neuen Empfängers der Transaktion angehängt wird, verlängert sich die Datenmenge einer Transaktionsnachricht mit jeder Transaktion.

44 Im Bitcoin-System wird die Hashfunktion SHA-256 verwendet, *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 3. Die Zeichenfolge, die in die Hashfunktion eingegeben wird und aus der der Hashwert ermittelt wird, wird im Folgenden als „Eingabewert" bezeichnet.

45 *Kaulartz*, CR 2016, 474 (475).

46 *Kaulartz*, CR 2016, 474 (475).

47 Bzw. sogar die Veränderung von Groß- und Kleinschreibung im Eingabewert wirkt sich aus.

48 *Kaulartz*, CR 2016, 474 (475).

49 Gemeint sind hiermit die Transaktionsnachrichten, die die Nutzer an das Netzwerk aussenden.

50 *Kaulartz*, CR 2016, 474 (475).

51 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193; *Kaulartz*, CR 2016, 474 (475).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

mit einer Länge von 64 Zeichen erzeugt wird.[52] Entsprechend wird aus dem *public key* eine 64 Zeichen lange Zeichenfolge erzeugt – die *Bitcoin Adresse*. Sie kann am ehesten mit einer Kontonummer im herkömmlichen Banken- und Finanzsystem verglichen werden, denn an sie adressieren Nutzer ihre Zahlungen.[53]

Die SHA-256 *Hashfunktion* wird insbesondere auch bei der Verkettung der Datenblöcke der Blockchain eingesetzt und ermöglicht damit insbesondere ihre Fälschungssicherheit (hierzu im Einzelnen unter A.III.2.).

5. Konten

Anders als der Vergleich des *public keys* bzw. der *Bitcoin-Adresse* mit einer Kontonummer vermuten lässt, bestehen im Bitcoin-System keine „Konten" im Sinne des herkömmlichen Banken- und Finanzsystems.[54] Anbieter von sog. *Wallets* und anderen Diensten im Zusammenhang mit Bitcoin stellen für ihre Nutzer zwar eine derartige Saldenansicht bereit, diese beruht allerdings nur auf der eigenen Darstellung der Anbieter.[55] Im Bitcoin-System bzw. konkret in der *Blockchain* – gibt es dagegen keine Saldenansichten von Konten.

Denn bei Bitcoin gibt es lediglich sog. *unspent transaction outputs (=UTXO),* wörtlich übersetzt „nicht ausgegebene Transaktionen" bzw. „nicht weitergeleitete Transaktionen".[56] Denn das Bitcoin-Netzwerk lebt von sog. Transaktionen – vergleichbar mit herkömmlichen Überweisungen.[57] Der „Kontostand" eines Pseudonyms ergibt sich aus allen Transaktionen, die er empfangen, aber nicht ausgegeben hat – über die er also noch verfügen kann.[58]

52 *Kaulartz*, CR 2016, 474 (475); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33.
53 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33.
54 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114; *Kaulartz*, CR 2016, 474 (475f.); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 33f.
55 Auch andere Anbieter wie etwa blockchain.org stellen eine derartige Saldenansicht für alle Bitcoin-Adressen bereit.
56 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114; *Kaulartz*, CR 2016, 474 (475).
57 *Kaulartz*, CR 2016, 474 (475).
58 *Kaulartz*, CR 2016, 474 (475f).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Dies können einerseits Transaktionen sein, die darauf beruhen, dass das Pseudonym sie von einem anderen Pseudonym empfangen hat, oder auf dem sog. *Bitcoin-Mining* (vereinfacht = Bereitstellen von Rechenleistung zur Funktionsweise des Netzwerks)[59]. All diese Transaktionen des gesamten Netzwerks werden in chronologischer Reihenfolge in der Blockchain gespeichert.[60] Die Transaktionen eines bestimmten, einzelnen Pseudonyms können also über den gesamten Datenbestand der Blockchain verteilt sein.[61] Entsprechend kann eine Salden-Ansicht der „Konten" von einzelnen *public keys* nur abgeleitet werden, indem alle vorherigen Transaktionen ausgewertet werden.[62]

Da es also kein Konto als solches bzw. keine Saldenansicht gibt, wird bei einer Transaktion im Bitcoin-Netzwerk lediglich eine bereits empfangene Transaktion „weitergeleitet".[63]

Zu berücksichtigen ist in diesem Kontext, dass eine empfangene Transaktion nur als Ganzes weitergeleitet werden kann – ähnlich wie beim Bargeld, bei dem eine Münze bzw. ein Schein nur als Ganzes übergeben wird und der zu viel gezahlte Betrag als Wechselgeld herausgegeben wird.[64] In jeder Transaktionsnachricht muss deshalb bereits enthalten sein, an welche *Bitcoin-Adresse* das „Wechselgeld" transferiert werden soll, da es sonst als Transaktionsgebühr eingezogen wird.[65]

6. Bitcoin

Anders als der Begriff „Bitcoin" suggeriert, gibt es keine derartige „digitale Geldmünze".[66] Denn bei digitalen Gütern besteht immer das Problem, dass sie nicht rivalisierend sind.[67] Das bedeutet, dass digitale Güter, anders als materielle Güter, gleichzeitig von verschiedenen Nutzern ge- und

59 Das *Bitcoin-Mining* wird ausführlich unter A.III.1.c) beschrieben.
60 *Martini/Weinzierl*, NVwZ 2017, 1251 (1251); *Schrey/Thalhofer*, NJW 2017, 1431 (1431).
61 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114.
62 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114.
63 *Kaulartz*, CR 2016, 474 (475f).
64 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
65 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
66 *Kütük/Sorge*, MMR 2014, 643 (643).
67 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz*, Kap. 4.1 Rn. 8; *Kütük/Sorge*, MMR 2014, 643 (643); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754). Der Begriff „rivalisierend" wird hier nicht im ökonomischen Sinne verwendet, sondern bedeutet lediglich, dass die Nutzung eines Gutes die Nutzungsmöglichkeit eines anderen nicht ausschließt.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

verbraucht werden können, ohne, dass dadurch die Nutzungsmöglichkeit Anderer eingeschränkt wird.[68]

Was bereits seit Jahren ein Problem der Film- und Musikindustrie ist, würde genauso bei virtuellem Geld auftreten, wenn die virtuellen Geldmünzen einfach kopiert werden könnten.[69] Deshalb ist ein Bitcoin kein bestimmtes, digital kopierbares „Datum", sondern ein Bitcoin ist die Zuschreibung eines Wertes zu einem Pseudonym.[70] Diese Zuweisung erfolgt durch Transaktion an einen *public key*. Ein Bitcoin wird also transferiert bzw. überwiesen, indem die Zuweisung einer Transaktion zu einem Pseudonym verändert wird.[71]

Zu beachten ist, dass ein Bitcoin bis zu acht Nachkommastellen geteilt werden kann – ähnlich einem Euro, der auch bis zu zwei Nachkommastellen geteilt werden kann (Cents).[72] Die kleinste Einheit von Bitcoin heißt *Satoshi*.[73]

7. Transaktionen

Um eine Transaktion im Bitcoin-System auszuführen, muss also die Zuweisung einer noch nicht weitergeleiteten Transaktion verändert werden.[74]

a) „Transaktion 01"

Hierzu erstellt der Bitcoin-Nutzer die Nachricht an das Netzwerk, dass eine ursprünglich seinem *public key* zugewiesene Transaktion an einen anderen *public key* weitergeleitet werden soll.[75] Diese Nachricht verschlüsselt der Absender mit seinem *private key*.[76]

68 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 8f.
69 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 8.
70 *Safferling/Rückert*, MMR 2015, 788 (790); *Grzywotz/Köhler/Rückert*, StV 2016, 753 (754); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31.
71 So bezeichnen bereits *Safferling/Rückert*, MMR 2015, 788 (789)„Bitcoin als Kette digitaler Signaturen".
72 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 114; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
73 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
74 *Kaulartz*, CR 2016, 474 (476); *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 31.
75 *Kaulartz*, CR 2016, 474 (475f.).
76 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Hiermit signiert er sie und weist gegenüber dem Netzwerk nach, dass er dazu berechtigt ist, Transaktionen weiterzuleiten, die dem zugehörigen *public key* zugewiesen ist[77] – vereinfacht: er weist nach, dass er über den *public key* verfügen kann.[78] In der Nachricht enthalten ist auch der *public key* des Empfängers.[79]

Das Netzwerk nimmt diese Nachricht zur Kenntnis, überprüft sie und bestätigt sie, sodass nun die Transaktion dem *public key* des Empfängers zugewiesen ist.[80]

b) „Transaktion 02"

Will nun der Empfänger der Transaktion 01, die Transkation weiterleiten, muss auch er eine derartige Nachricht an das Netzwerk versenden und einen neuen Empfänger als *public key* definieren.[81] Ebenfalls muss er nun die Nachricht mit seinem *private key* signieren. Das Netzwerk kann so überprüfen, ob Absender der Transkation 02 auch tatsächlich der Empfänger der Transkation 01 ist.[82]

c) Gültigkeit einer Transaktion

Eine Transaktion gilt allerdings erst als erfolgt, wenn sie in die Blockchain aufgenommen wurde – vereinfacht bedeutet das, dass sie als gültig von den anderen Nutzern bestätigt wurde.[83]

8. Blockchain

Um die Gültigkeit einer Transaktion zu überprüfen, muss das Bitcoin-Netzwerk einerseits die Berechtigung mittels *public key* und *private key* überprüfen und andererseits überprüfen, ob die gegenständliche Transaktion

77 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 34.
78 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 63.
79 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.
80 Zum Ablauf dieser Bestätigung innerhalb des Netzwerkes unter A.III.1.c).
81 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.
82 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 113f.
83 Im Einzelnen hierzu unter A.III.1.c).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nicht bereits zuvor anderweitig ausgegeben bzw. weitergeleitet wurde (sog. *double spending*).[84]

Hierzu dient die Blockchain (wörtlich übersetzt als „Blockkette") als „zentrales"[85], chronologisches Transaktionsregister, in das alle Transaktionen aller Nutzer fortlaufend eingetragen werden.[86] Die Blockchain ist insoweit vergleichbar mit einem Kontobuch, das alle Transaktionen aller Kunden einer Bank aufzeichnet.[87] Da der Begriff des „Kontobuchs" allerdings widersprüchlich zu den fehlenden Konten[88] ist, wird im Folgenden der von *Grzywotz* verwendete Begriff des „Hauptbuchs" verwendet.[89]

Anhand dieses vom Netzwerk erzeugten Hauptbuchs können die Nutzer abgleichen, ob die Transaktion, die weitergeleitet werden soll, nicht bereits zuvor ausgegeben bzw. weitergeleitet wurde.[90]

III. Funktionsweise der Blockchain-Technologie – wie wird die Blockchain fortgeschrieben?

Der besondere technologische Fortschritt der Blockchain-Technologie liegt darin, wie dieses Hauptbuch erzeugt wird. Denn das Hauptbuch wird – anders als im herkömmlichen Bankensystem – von allen Nutzern gemeinsam fortgeschrieben, anstatt von einer zentralen Verwaltungsinstanz.[91]

Im herkömmlichen Banken- und Finanzsystem führt jede Bank ein solches Hauptbuch für ihre Nutzer[92] – also ein zentraler Intermediär.[93]

---

84 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1f.; *Safferling/Rückert*, MMR 2015, 788 (790); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 25ff.

85 „Zentral" meint in diesem Kontext, nicht die Form der Datenverwaltung, sondern stellt darauf ab, dass die Blockchain als Transaktionsregister die Grundlage der Überprüfung von Transaktionen ist.

86 *Martini/Weinzierl*, NVwZ 2017, 1251 (1251); *Schrey/Thalhofer*, NJW 2017, 1431 (1432).

87 *Börner*, NZWiSt 2018, 48 (49).

88 Siehe oben unter B.II.3.

89 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 41.

90 *Safferling/Rückert*, MMR 2015, 788 (790); *Kaulartz*, CR 2016, 474 (476).

91 *Safferling/Rückert*, MMR 2015, 788 (789f.).

92 *Kaulartz*, CR 2016, 474 (476). Im Folgenden wird der Begriff „Nutzer" synonym zum Begriff „Kunde" verwendet, auch um den Vergleich zwischen Bitcoin und herkömmlichen Zahlungsverkehr zu unterstreichen.

93 *Hofert*, Regulierung der Blockchains, S. 18; Breidenbach-Glatz RhdB-Legal-Tech/*Sandner/Voigt/Fries,* Kap. 5.4 Rn. 15f. S. 150f.; *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2254f.).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Die Bank überprüft vor einer Überweisung, ob der Überweisende bzw. Absender[94] das überwiesene Vermögen überhaupt hat und führt nach der Überweisung sein Konto mit einem entsprechenden Eintrag fort.[95]

Ziel von Bitcoin war es aber gerade, die zentrale Verwaltung von „Konten" zu vermeiden und die Verwaltung dezentral zu ermöglichen.[96] Allerdings müssen die (Verwaltungs-)Aufgaben, die sonst Banken bzw. zentrale Intermediäre übernehmen, auch bei einer dezentralen Verwaltungsstruktur gewährleistet werden.[97] Dies ermöglicht die Blockchain-Technologie. Mit diesem Instrument schreiben alle Nutzer das gemeinsame Hauptbuch fort.[98]

Dazu muss die Blockchain-Technologie folgende zwei Funktionen erfüllen:

1. Alle Nutzer des Bitcoin-Systems müssen einen Konsens über den Inhalt des Hauptbuchs bzw. seine Fortschreibung erreichen (hierzu unter 1.).
2. Das Hauptbuch bzw. die Blockchain muss fälschungssicher sein – darf also nicht durch einen Angriff von außen verändert werden können (hierzu unter 2.).

1. Konsensmechanismus – Governance

a) Konnektivität durch Internet und Peer-to-Peer-Netzwerk

Um einen Konsens der Nutzer zu erreichen, müssen die Nutzer zunächst miteinander kommunizieren. Die Kommunikation der Bitcoin-Nutzer erfolgt über das Internet. Das Internet stellt als Netzwerkprotokoll die Konnektivität aller Nutzer sicher.[99]

---

94 Im Folgenden wird der Begriff „Absender" synonym zum Begriff des „Überweisenden" verwendet, auch um den Vergleich zwischen Bitcoin und herkömmlichem Zahlungsverkehr zu unterstreichen.

95 *Kaulartz*, CR 2016, 474 (476).

96 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1f.; *Kaulartz*, CR 2016, 474 (476).

97 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 40f.

98 *Hofert*, Regulierung der Blockchains, S. 21.

99 *Böhme/Pesch*, DuD 2017, 473 (475); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Durch das Internet werden alle Nutzer, die die Bitcoin-Software[100] nutzen, zu einem sog. *Peer-to-Peer-Netzwerk* zusammengeschlossen.[101] Das *Peer-to-Peer-Netzwerk* ist ein Netzwerkprotokoll, das ein dezentrales Kommunikationsnetzwerk erzeugt.[102] Die Kommunikation der Netzwerkteilnehmer findet hier unmittelbar – also direkt – zwischen den einzelnen Nutzern, ohne den Umweg über einen zentralen Knotenpunkt statt – deshalb werden die Nutzer auch als *nodes* (=Knoten) bezeichnet.[103] Regelmäßig findet Kommunikation im Internet nämlich über zentrale Diensteanbieter und deren Server statt – wie etwa bei Facebook, WhatsApp oder auch beim E-Mail-Postfach bei einem E-Mail-Diensteanbieter. Bei einem *Peer-to-Peer*-Netzwerk werden die Nutzer unmittelbar, ohne den Umweg über den Server eines Dritten, zusammengeschlossen – deshalb ist auch jeder Beteiligte Rechner selbst Server.[104]

Bildlich ausgedrückt gleicht das *Peer-to-Peer*-Netzwerk also einem persönlichen Gespräch in Abgrenzung zu einem Telefonat – die Kommunikation findet beim persönlichen Gespräch unmittelbar zwischen den Teilnehmern des Gesprächs statt, beim Telefonat dagegen wird die Kommunikation zwischen den Gesprächsteilnehmern vom Telefonanbieter vermittelt.

Wichtig ist in diesem Zusammenhang, dass die Teilnehmer eines *Peer-to-Peer*-Netzwerks gleichberechtigte Nutzer des Netzwerks sind, also alle den gleichen Einfluss auf das Netzwerk haben.[105]

b) Nodes im Peer-to-Peer Netzwerk – wer schreibt die Blockchain fort?

Jeder dieser *nodes* hält fortlaufend die gesamte Blockchain auf seinem lokalen Rechner vor und hält sie auf dem aktuellen Stand.[106] Hierzu steht

100 Zur Differenzierung der verschiedenen Bitcoin-Software sogleich unter A.III.1.b).
101 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 1; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12.
102 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 12; *Hofert*, Regulierung der Blockchains, S. 17.
103 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 17; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Hofert*, Regulierung der Blockchains, S. 17.
104 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 139.
105 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 139; *Hofert*, Regulierung der Blockchains, S. 17.
106 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 17ff.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

er im ständigen Austausch mit den anderen *nodes* im Netzwerk, um den aktuellen Stand abzugleichen.[107]

Bei Bitcoin ist zwischen drei verschiedene Varianten von *nodes* zu differenzieren[108]:

i. Sog. *Full-Node* als umfassendstes Endnutzerprogramm. Der Full-Node speichert fortlaufend die gesamte Blockchain, kann selbst im Netzwerk mit einer *Bitcoin-Adresse* bzw. *public key* agieren und schreibt die Blockchain fort.[109]
ii. Sog. *Solo-Miner*, die die Blockchain fortschreiben und sie fortlaufend lokal speichern, aber selbst nicht im Netzwerk mit einer *Bitcoin-Adresse* aktiv werden können.[110]
iii. Sog. *Full-Blockchain-Nodes,* die die gesamte Blockchain zwar fortlaufend lokal vorhalten, sie aber weder selbst fortschreiben oder mit einer *Bitcoin-Adresse* aktiv werden können, sondern lediglich „gültige Blöcke an andere Knoten weiterleiten".[111]

Die ersten beiden Varianten schreiben selbst die Blockchain fort, sie sind sog. *miner.*[112] Begrifflich wird deshalb zwischen *minern* und *nodes* differenziert. *Nodes* sind diejenigen Netzwerkteilnehmer, die sich an der Kommunikation im Netzwerk beteiligen – also alle der drei genannten. *Miner* sind dagegen nur solche *nodes* die selbst die Blockchain fortschreiben.

c) Fortschreiben der Blockchain bzw. Bitcoin-Mining – wie wird die Blockchain fortgeschrieben?

Wenn eine Transaktion erfolgen soll, erstellt der Nutzer eine entsprechende Nachricht und sendet diese an die *nodes.*[113] Die *miner* überprüfen diese

107 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 17ff.
108 Hierzu ausführlich *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
109 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 140f.
110 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 140f.
111 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche; ausführlich hierzu *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 149ff.
112 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 4; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
113 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43. Siehe auch oben unter A.II.7.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Nachricht und leiten sie an weitere *nodes* weiter.[114] Die Transaktionsnachricht gelangt durch ständiges Weiterleiten der *nodes* an andere *nodes* ins Netzwerk.

Daraufhin gelangt die Nachricht in den sog. *memory-pool*.[115] Im *memory-pool* befinden sich alle Transaktionsnachrichten aller Nutzer, die noch nicht in die Blockchain aufgenommen wurden und aus denen sich die *miner* beim Erstellen eines neuen Blocks bedienen können.

Die *miner* entnehmen diesem *memory-pool* geeignete[116] Transaktionsnachrichten und berechnen hieraus einen neuen sog. *candidate-block*.[117]

(1) Überprüfung der Transaktionen – Verhinderung von „Double Spending“

Geeignet sind dabei nur solche Transaktionsnachrichten, die spezifische Kriterien einer Checkliste erfüllen.[118] Zu diesen Kriterien gehört u.a. auch, dass die Transaktion sich nicht bereits mit einem anderen Empfänger im *memory-pool* befindet (*double spending*) – dann wird sie nicht in den *candidate-block* aufgenommen.[119] Außerdem darf sie nicht der bisherigen Transaktionshistorie widersprechen – konkret: die weitergeleitete Transaktion darf nicht bereits zuvor vom gleichen Absender an einen anderen Empfänger weitergeleitet worden sein.[120]

Hierdurch wird gewährleistet, dass nur „gültige“ Transaktionen in die Blockchain aufgenommen werden und das Problem des *double spending* wird hierdurch gelöst.[121]

114 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
115 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
116 Die miner können aus den Transaktionsnachrichten auswählen, abhängig von der Höhe der Transaktion, der Höhe der Transaktionsgebühr und der Länge der Wartezeit, *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43f.
117 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 43.
118 Siehe zur genauen Darstellung dieser Checkliste *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 182f.
119 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 182.
120 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 183.
121 Siehe ausführlich hierzu: *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 49f.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

(2) Proof-of-Work

Der *miner* muss dem *candidate-block* außerdem noch den sog. *Proof-of-Work*[122] beifügen – ein Nachweis darüber, dass er Rechenleistung für die Berechnung des Blocks aufgewendet hat.[123] Dies erfolgt wiederum durch eine *Hashfunktion*[124]. Allerdings muss diesmal nicht der *Hashwert* eines Eingabewertes durch die *Hashfunktion* berechnet werden, sondern der *miner* muss den *Hashwert* des *candidate-blocks* berechnen und dabei zu einem bestimmten, vom System vorgegebenen Ergebnis gelangen – bspw. muss die erste Ziffer des *Hashwerts* des *candidate-blocks* 0 sein.[125] Da sich aber bei *Hashfunktionen* der *Hashwert* vollständig verändert, wenn sich der Eingabewert nur um ein Zeichen verändert, kann dieses Ziel nur durch ausprobieren erreicht werden.[126] Der *miner* muss also den Inhalt des *candidate-blocks* anpassen – regelmäßig wird er immer eine weitere Transaktion hinzufügen. Dabei muss er jedes Mal den *Hashwert* neuberechnen, bis er den vorgegebenen Zielwert erreicht – je nachdem, wie genau das zu erzielende Ergebnis vorgegeben ist, ist diese Rechenoperation sehr aufwändig.[127] Findet der *miner* einen *candidate-block*, der den vorgegebenen *Hashwert* erreicht, kann das Netzwerk einfach überprüfen, ob die Berechnung richtig ist, denn hierfür muss nur berechnet werden, ob der vom *miner* gefundene Block tatsächlich den vorgegebenen *Hashwert* ergibt.

Insoweit ist der Rechenprozess, um einen *Proof-of-Work* zu finden, für den *miner* sehr aufwändig, kann aber vom Netzwerk durch eine einzige Rechenoperation überprüft werden.[128] So können die anderen *nodes* sicher-

122 Das sog. *Proof-of-Work*-Verfahren wird bei Bitcoin verwendet, ein anderes Verfahren ist das sog. *Proof-of-Stake*-Verfahren, hierzu sogleich.

123 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 3; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 44.

124 Zur Funktionsweise einer Hashfunktion siehe oben unter A.II.4.

125 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Hofert*, Regulierung der Blockchains, S. 20f.

126 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Kaulartz*, CR 2016, 474 (475); *Hofert*, Regulierung der Blockchains, S. 20f.

127 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 195; *Hofert*, Regulierung der Blockchains, S. 20f.

128 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

stellen, dass der *miner*, der den Block gefunden hat, auch entsprechende Rechenleistung aufgewendet hat.[129]

d) Konsens über Gültigkeit der längsten Kette

Der so gefundene Block wird im Anschluss mit dem entsprechend berechneten *Hashwert* an die anderen *nodes* im Netzwerk verteilt und hierdurch an die Blockchain angehängt. Dabei beinhaltet ein neuer Block auch immer den *Hashwert* des vorhergehenden Blocks. So entsteht eine Kette aus Datenblöcken (= „Blockchain").

Da aber die *miner* die Blockchain gleichzeitig fortschreiben, besteht das Problem, dass sie sich einigen müssen, wer nun die „richtige" bzw. gültige Kette berechnet hat. Von den anderen *minern* wird deshalb nur die längste Kette als die gültige Kette anerkannt.[130] Dass eine Kette als die gültige anerkannt wird, kommuniziert nun der weitere *miner* dadurch, dass er sie als Ausgangspunkt für seine weitere Kette annimmt und diese dann wiederum an das Netzwerk kommuniziert.[131]

e) Exkurs – Andere Konsensmechanismen

Problematisch ist das *Proof-of-Work*-Verfahren u.a., weil es sehr rechenintensiv ist und damit auch einen sehr hohen Energieverbrauch hat – insbesondere da der Rechenaufwand immer höher wird.[132] Aus diesen Gründen werden verschiedene alternative Konsensverfahren diskutiert – insbesondere der sog. „*Proof-of-Stake*" und der sog. „*Proof-of-Authority*".[133]

Bei dem *Proof-of-Stake*-Verfahren wird im Wesentlichen die erforderliche Rechenkraft durch die Währung der jeweiligen Blockchain-Netzwerke

129 *Kütük/Sorge*, MMR 2014, 643 (643).
130 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 45; *Hofert*, Regulierung der Blockchains, S. 19.
131 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 45; *Hofert*, Regulierung der Blockchains, S. 17f.
132 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 33; *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2100f.).
133 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 34; *Janicki/Saive*, ZD 2019, 251 (251f.).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

selbst ersetzt.[134] Die *miner* müssen ihre jeweiligen Werteinheiten einsetzen, um einen neuen Block zu finden, je höher dabei der Einsatz, desto höher ist auch die Wahrscheinlichkeit, dass sie einen neuen Block finden.[135]

Eine andere Alternative ist das sog. *Proof-of-Authority*, bei dem die *miner* vom System auf Grund eines überprüften Vertrauens dazu autorisiert werden, die Blockchain fortzuschreiben.[136]

Beide Alternativen sehen sich allerdings der Kritik ausgesetzt, dass hierdurch der ursprüngliche Gedanke einer dezentralisierten Währung verfehlt wird.[137]

2. Unveränderlichkeit der Blockchain

Damit die *miner* die zu validierende Transaktion verifizieren können – insbesondere abgleichen können, ob die zu bestätigende Transaktion bereits vormals an einen anderen Absender transferiert wurde (*double spending*) – muss die Blockchain eine vollständige Historie aller bisher getätigten Transaktionen enthalten und diese Transaktionshistorie muss fälschungssicher bzw. unveränderlich sein.[138]

Dabei wird die erforderliche Unveränderlichkeit durch eine „Verkettung" der Datenblöcke erreicht.[139] Die Verkettung wird – wie oben bereits kurz beschrieben – dadurch gewährleistet, dass jeder neue Block den *Hashwert* des vorhergehenden Blocks referenziert.[140] Insoweit wird die Verkettung der Blockchain als Weiterentwicklung verketteter Listen beschrieben.[141]

Denn von einer einfach verketteten Liste spricht man, wenn in einer Datenstruktur jeder neue Block auf „die Adresse der ersten Speicherzelle des vorhergehenden Elements" verweist.[142] In diesem Fall können Elemente

134 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 34.
135 *King/Nadal*, PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, S. 2; *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2102).
136 *Janicki/Saive*, ZD 2019, 251 (251f).
137 *Schlund/Pongratz*, DStR 2018, 598 (599).
138 *Schrey/Thalhofer*, NJW 2017, 1431 (1432); *Martini/Weinzierl*, NVwZ 2017, 1251 (1255); *Hofert*, Regulierung der Blockchains, S. 21.
139 *Hofert*, Regulierung der Blockchains, S. 21.
140 *Hofert*, Regulierung der Blockchains, S. 19f; *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2257).
141 *Böhme/Pesch*, DuD 2017, 473 (474).
142 *Böhme/Pesch*, DuD 2017, 473 (474).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

der Speicherkette aber einfach ausgetauscht werden und durch Änderung lediglich eines Elements verändert bzw. eingefügt oder gelöscht werden.[143]

Eine schwieriger zu verändernde Datenstruktur erhält man, wenn der neue Block in einer Datenstruktur auf den *Hashwert* eines vorhergehenden Speicherelements verweist.[144] In diesem Fall müssen die gesamten *Hashwerte* neu berechnet werde, die dem veränderten Element nachfolgen.[145] Entsprechend aufwändiger ist die Veränderung der Datenstruktur.

Die Technologie der Blockchain geht hierüber noch hinaus. Denn, wenn ein Element eines Blocks verändert werden soll, müssen nicht nur die *Hashwerte* neu berechnet werden, sondern es muss jeweils ein bestimmter neuer *Hashwert* eines nachfolgenden Blocks, entsprechend dem oben[146] beschriebenen Verfahren, gefunden werden.[147] Möchte ein Angreifer also den Inhalt der Blockchain nachträglich verändern, müsste er mehr Rechenkapazität aufwenden als alle Rechner, die die Blockchain zuvor berechnet haben – sog. 51%-Angriff.[148]

Dass ein solcher Angriff äußerst unwahrscheinlich ist, beruht auf dem Grundgedanken, dass mit der so aufgewendeten Rechenkapazität wirtschaftlich sinnvoller neue Blocks berechnet werden könnten und damit auf dem von *John F. Nash* entwickelten spieltheoretischen Prinzip des sog. *Nashgleichgewichts*.[149] Denn den *minern* des Bitcoin-Systems wird ein „pekuniärer Anreiz" geboten.[150] Sie erhalten für die Berechnung neuer Blöcke einerseits die Transaktionsgebühren der neuberechneten Blöcke und andererseits werden mit jedem neuen, gültigen Block, der an die Blockchain angehängt wird, neue Bitcoin geschaffen, die demjenigen, der den neuen Block berechnet hat, gutgeschrieben werden.[151]

143 *Böhme/Pesch*, DuD 2017, 473 (474).
144 *Böhme/Pesch*, DuD 2017, 473 (474).
145 *Böhme/Pesch*, DuD 2017, 473 (474).
146 Siehe hierzu unter A.III.1.c)(2).
147 *Hofert*, Regulierung der Blockchains, S. 21.
148 *Nakamoto*, Bitcoin : Ein elektronisches Peer-to-Peer- Cash-System, S. 2; *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 193, 195; *Böhme/Pesch*, DuD 2017, 473 (95); *Hofert*, Regulierung der Blockchains, S. 21.
149 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 27.
150 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46f.; *Hofert*, Regulierung der Blockchains, S. 22.
151 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 47; *Hofert*, Regulierung der Blockchains, S. 22.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

So gewährleistet das Bitcoin-System, dass es wirtschaftlich sinnlos ist, die Blockchain nachträglich zu verändern, sodass es eine fälschungssichere Transaktionshistorie gibt.[152]

IV. Öffentliche Verfügbarkeit der Blockchain-Daten als Folge dieser Funktionsweise der Blockchain-Technologie

Aus diesem Verfahren der Konsensfindung zwischen allen Beteiligten Nutzern ergibt sich mittelbar, dass alle Transaktionsdaten öffentlich verfügbar sein müssen, soweit ein öffentliches Blockchain-Netzwerk verwendet wird.[153]

Denn Kerngedanke der Blockchain-Technologie ist eine Datenverwaltungsstruktur, für die kein Vertrauen in eine zentrale Instanz notwendig ist. Stattdessen soll die Funktion der Währung dadurch gewährleistet werden, dass alle Beteiligten gleichberechtigt die Verwaltungsaufgaben des Systems übernehmen.[154] Entsprechend kontrolliert nicht eine zentrale Verwaltungsinstanz die Gültigkeit der Transaktionen, sondern das Kollektiv der Nutzer selbst überprüft dies.[155] Das setzt allerdings auch voraus, dass alle Nutzer die notwendigen Informationen haben müssen, um die Transaktionen zu kontrollieren. Entsprechend muss die Transaktionshistorie, anhand derer der Abgleich vorgenommen wird, allen Nutzern zur Verfügung stehen.[156]

Da bisher die virtuellen Kryptowährungen gerade nicht zugangsbeschränkt sind und sich jeder Interessierte sowohl am Handel wie auch am *mining* beteiligen kann, sind die Daten der Transaktionshistorie entsprechend transparent und damit auch öffentlich verfügbar.[157]

V. Zwischenergebnis

Vorstehend wurde dargestellt, wie Bitcoin und die dahinterstehende Blockchain-Technologie funktionieren. Hieraus ist Folgendes festzuhalten:

---

152 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 27.
153 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6; *Safferling/Rückert*, MMR 2015, 788 (793); *Pesch/Böhme*, DuD 2017, 93 (94).
154 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 20ff.
155 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 20f.
156 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 40f.
157 *Safferling/Rückert*, MMR 2015, 788 (793); *Pesch/Böhme*, DuD 2017, 93 (93).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Nutzer des Bitcoin-Systems können im Netzwerk mit sog. *private* und *public key* aktiv werden und sog. Bitcoin transferieren. Eine Transaktion bedeutet, dass die Zuweisung eines Wertes zu einem *public key* verändert wird. Solche Veränderungen der Wertzuweisungen werden in die sog. Blockchain eingetragen – das Hauptbuch des Bitcoin-Systems. Der Eintragungsprozess erfolgt dabei durch alle Nutzer gemeinsam und setzt insoweit voraus, dass sich alle Nutzer auf einen entsprechenden Konsens einigen. Dieser Konsens wird dadurch erreicht, dass nur die längste Blockchain fortgeschrieben wird, denn für sie wurde bisher am meisten Rechenleistung aufgewendet. Eingetragen werden außerdem nur Transaktionen, die der vorhergehenden Transaktionshistorie nicht widersprechen bzw. die einer noch einzutragenden Transaktion nicht widersprechen. Da die Bitcoin-Blockchain als offenes Netzwerk ausgestaltet ist, an dem sich jeder beteiligen kann, sind die Transaktionsdaten in der Blockchain auch für jeden Nutzer verfügbar und damit insgesamt öffentlich verfügbar.

B. Die Blockchain-Technologie außerhalb des Bitcoin- und Kryptowährungskontextes

Auch wenn die Blockchain-Technologie am Anwendungsbeispiel von Bitcoin erklärt wurde, ist sie gerade nicht auf die Verwaltung von Kryptowährungen beschränkt – ihr Anwendungsbereich ist sehr viel umfassender.[158]

I. Nicht die „eine" Blockchain

So ist für das Verständnis zunächst wichtig, dass es nicht die „eine" Blockchain gibt, sondern die oben im Zusammenhang mit Bitcoin dargestellte Technologie kann auf beliebige andere Vorgänge angewendet werden.[159] Hierzu muss der Programmcode der Blockchain natürlich entsprechend angepasst werden. Das „Grundkonzept" bleibt aber gleich. Denn die Blockchain-Technologie zeichnet sich durch:

158 *Kaulartz*, CR 2016, 474 (474); *Schrey/Thalhofer*, NJW 2017, 1431 (1431); *Simmchen*, MMR 2017, 162 (162f.).

159 *Kaulartz*, CR 2016, 474 (474); *Glatz*, DGRI Jahrbuch 2016, Rn. 1ff.; *Schrey/Thalhofer*, NJW 2017, 1431 (1431); *Hoffer/Mirtchev*, NZKart 2019, 239 (239ff.).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

- einen Zusammenschluss gleichberechtigter Rechner zu einem Netzwerk aus,
- die auf der Grundlage eines vorher festgelegten Netzwerkprotokolls
- eine gemeinsame, verteilte Datenbank (die Blockchain) fortschreiben,
- indem sie sich in einem vorher festgelegten Verfahren auf einen Konsens der fortzuschreibenden Daten einigen.[160]

II. Transaktions- und Dokumentationsfunktion

Aus dem Bitcoin-Kontext werden aber bereits die beiden wesentlichen Funktionen der Blockchain-Technologie ersichtlich: einerseits eine Transaktionsfunktion und andererseits eine Dokumentationsfunktion.[161]

1. Transaktionsfunktion

Im Bitcoin-System dient die Blockchain-Technologie zur Führung des dezentral geführten Transaktionsregisters.[162] Dabei führt sie selbst Transaktionen aus, indem sie die Zuweisung von Werten dadurch verändert, dass das Transaktionsregister entsprechend fortgeschrieben wird.[163] Bei Bitcoin und anderen virtuellen Kryptowährungen werden hierdurch die jeweiligen Werteinheiten transferiert.[164]

Anders als im Fall von Bitcoin und anderen virtuellen Kryptowährungen, muss sich die Transaktionsfunktion der Blockchain-Technologie aber nicht auf die Transaktion der jeweiligen Werteinheiten beschränken, sondern die Transaktionsfunktion kann umfassend dahingehend verstanden werden, dass die transferierten Werteinheiten alles repräsentieren können, worauf Menschen sich einigen können.[165] Die Transaktionsfunktion kann

160 *Kaulartz*, CR 2016, 474 (476f.); *Hoffer/Mirtchev*, NZKart 2019, 239 (239ff). So auch Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 15ff.
161 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255).
162 *Börner*, NZWiSt 2018, 48 (48).
163 Siehe hierzu oben unter A.II.7., III.1.c). Hierzu insbesondere auch *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255).
164 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 8f.
165 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 41.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

sich also gerade auch auf Umstände erstrecken, die außerhalb der Blockchain liegen.[166]

So könnte die Blockchain-Technologie etwa für das Grundbuchamt, das Handelsregister[167], sog. *Smart Contracts*[168], Musiklizensierung, Versicherungen und gesellschaftsrechtliche Organisationen[169] dienen (zu diesen Anwendungsmöglichkeiten im Einzelnen sogleich unter C.).

2. Dokumentationsfunktion

Daneben bietet die Blockchain-Technologie auch eine Dokumentationsfunktion, da sie auf Grund ihrer Unveränderlichkeit[170] in besonderem Maße fälschungssicher ist.[171] Deshalb kann sie gerade auch zur Dokumentation von (Transaktions-)Vorgängen verwendet werden.[172] Sie dokumentiert insoweit die soeben beschriebene Transaktionsfunktion. Insoweit ist sie Integritätssicherung von Daten.[173]

III. Blockchain-Technologie ist dezentrale Datenverwaltungsstruktur

Daraus ergibt sich, dass die Blockchain-Technologie nicht einmal auf die Anwendung zur Transaktion von Werteinheiten beschränkt ist. Sie kann deshalb allgemein im technischen Sinne als Protokoll zur dezentralen Datenverwaltung verstanden werden.[174]

166 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2255f.); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 43f.
167 Siehe hierzu etwa *Knaier/Wolf*, Betriebs-Berater 2018, 2253.
168 Siehe hierzu etwa *Kaulartz/Heckmann*, CR 2016, 618.
169 Siehe hierzu etwa *Mann*, NZG 2017, 1014.
170 Siehe hierzu oben unter Kap. 2, A.III.2. m.w.N.
171 *Schrey/Thalhofer*, NJW 2017, 1431 (1431); *Martini/Weinzierl*, NVwZ 2017, 1251 (1252); *Kaulartz/Matzke*, NJW 2018, 3278 (3282); *Spindler*, ZGR 2018, 17 (49).
172 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2256).
173 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2256); *Sattler*, Betriebs-Berater 2018, 2243 (2245).
174 *Glatz*, DGRI Jahrbuch 2016, Rn. 1ff.; *Böhme/Pesch*, DuD 2017, 473 (474); Breidenbach-Glatz RhdB-Legal-Tech/*Krall,* Kap. 5.7 Rn. 11; *Hoffer/Mirtchev*, NZKart 2019, 239 (239ff.).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

IV. Differenzierung von Blockchain-Technologien und thematische Beschränkung

Diese Datenverwaltung kann in unterschiedlicher Weise erfolgen. So ist zwischen verschiedenen Ausprägungen der Blockchain-Technologien zu differenzieren.

1. Ausgangspunkt: Offene, genehmigungsfreie, pseudonymisierte Blockchain

Ausgangspunkt ist die von *Satoshi Nakamoto* entwickelte Blockchain-Technologie. Sie wurde als Netzwerk, das für jeden zugänglich ist (=offen)[175] und in dem jeder Teilnehmer gleichzeitig auch *miner* bzw. *nodes* sein kann (=genehmigungsfrei) und die Blockchain fortschreiben kann, angelegt. Außerdem handeln die Nutzer im Netzwerk nur unter den Pseudonymen der *public keys* bzw. den *Bitcoin-Adressen* (=Pseudonymität).[176]

2. Abweichung 1: geschlossene Blockchain

Mittlerweile haben insbesondere Finanzdienstleister, aber auch andere Unternehmen[177] das Potenzial der Blockchain-Technologie entdeckt.[178] Allerdings insbesondere wegen ihrer Datenverwaltungsstruktur.[179] Sie haben Blockchain-Technologien entwickelt, auf die nur bestimmte Beteiligte – wie etwa die Unternehmen[180] – Zugriff haben.[181] Hier dient die Blockchain-

175 *Kaulartz*, CR 2016, 474 (475); *Schlund/Pongratz*, DStR 2018, 598 (599).
176 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 1.
177 Wie zum Beispiel die AXA-Versicherung.
178 So beschreibt Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 51ff. ausführlich, für welche Wirtschaftsbereiche und Anwendungsfälle die Blockchain-Technologie angewendet werden könnte.
179 So etwa Breidenbach-Glatz RhdB-Legal-Tech/*Regierer,* Kap. 5.2 Rn. 3, der darstellt, dass die dezentrale Verwaltungsstruktur besondere Vorteile für die Abwicklung von Lieferketten hat. Außerdem ist die Blockchain-Technologie gerade auch mit Blick auf die Integrität der in ihre enthaltenen Daten für Unternehmen interessant.
180 Oder etwa Unternehmenskonsortien, wie etwa das sogleich genannte R3-Bankenkonsortium.
181 So etwa das R3-Bankenkonsortium, das sich zu einem weltumspannenden Transaktionsnetzwerk zusammengeschlossen hat, vgl. *Glatz*, DGRI Jahrbuch 2016, Rn. 7.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Technologie nur als interne Datenverwaltungsstruktur.[182] Weiteren Nutzern steht diese Blockchain nicht zur Verfügung (= geschlossene Blockchain).

3. Abweichung 2: genehmigungsbedürftige Blockchain

Wie oben bereits erwähnt hat das beschriebene *Proof-of-Work*-Konsensverfahren insbesondere den Nachteil, dass es sehr viel Rechenleistung benötigt.[183] Eine oben kurz angedeutete Alternative ist das sog. *Proof-of-Authority*-Verfahren, bei dem nur diejenigen Netzwerkteilnehmer die Blockchain fortschreiben, die vom Algorithmus hierzu autorisiert wurden.[184] Das Fortschreiben der Blockchain setzt also eine Genehmigung voraus (= genehmigungsbedürftige Blockchain).[185]

4. Abweichung 3: Blockchain mit unmittelbarem Personenbezug

Soweit die Blockchain-Technologie lediglich für interne Datenverwaltungsstrukturen verwendet wird, ist die durch den *public key* gewährleistete Pseudonymität bzw. Anonymität nicht mehr erforderlich. Eine Blockchain, die mit „Klarnamen" funktioniert erscheint insoweit möglich.[186]

5. Beschränkung der Untersuchung auf offene Blockchains

Die nachfolgende Untersuchung der rechtlichen Zulässigkeit von Blockchain-Auswertungen zu Strafverfolgungszwecken beschränkt sich auf die Inhalte in offenen Blockchains. Denn soweit die Blockchain-Technologie lediglich zur internen Datenverwaltung im Unternehmen bzw. in der internen öffentlichen Verwaltung verwendet wird und die Blockchain-Daten nicht öffentlich zugänglich sind, ergibt sich aus der Verwendung der Blockchain-Technologie für strafprozessuale Ermittlungen keine Besonderheit.

---

182 *Glatz*, DGRI Jahrbuch 2016, Rn. 7f.; *Hofert*, Regulierung der Blockchains, S. 14, 22; *Janicki/Saive*, ZD 2019, 251 (254).

183 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 30.

184 *Janicki/Saive*, ZD 2019, 251 (251f.).

185 *Janicki/Saive*, ZD 2019, 251 (251f.); siehe hierzu auch die Differenzierung von *Martini/Weinzierl*, NVwZ 2017, 1251 (1253f.), die zwischen zulassungsfreien und zulassungsbeschränkten Blockchains differenzieren. So etwa die im Folgenden dargestellte virtuelle Kryptowährung "Libra".

186 So etwa eine von *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2257) dargestellte Möglichkeit zur Führung des Handelsregisters.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Da auch genehmigungsbedürftige Blockchains als offenes Netzwerk ausgestaltet sein können[187], werden auch sie Gegenstand der nachfolgenden Untersuchung sein. Außerdem können sich in der rechtlichen Bewertung Unterschiede dadurch ergeben, dass die Inhaltsdaten in der Blockchain pseudonymisiert bzw. anonymisiert sind, sodass auch diese Abweichung Gegenstand der Untersuchung sein wird.

C. Weitere blockchain-basierte Anwendungen

Welche Daten dann durch die Blockchain-Technologie verwaltet werden, hängt davon ab, wie sie konkret eingesetzt und ausgestaltet wird. Hierzu gibt es sowohl von Seiten der Bundesregierung wie auch von privaten Unternehmen verschiedene Ideen, die teilweise bereits umgesetzt wurden.[188] Da die Anwendungsfälle der Blockchain-Technologie fast täglich wächst[189], kann eine vollumfassende Darstellung der Anwendungsfälle von Blockchain-Technologien im Folgenden nicht geleistet werden. Um aber einen Überblick zu geben, wie weitreichend die Anwendungsfälle sein können, werden nachfolgend verschiedene Beispielsanwendungen dargestellt.

Zu differenzieren ist hier zwischen den klassischen virtuellen Kryptowährungen (hierzu unter I.), den sog. *Smart Contract*-Anwendungen (hierzu unter II.) und Anwendungen im Bereich der öffentlichen Verwaltung (hierzu unter III.).

I. Virtuelle Kryptowährungen

Bereits vor dem rasanten Bekanntheitsgrad und dem Kursgewinn von Bitcoin in den vergangenen Jahren hatten sich bereits weitere virtuelle Kryptowährungen herausgebildet – im Dezember 2021 wurden auf der

187 Vgl. insoweit etwa die nachfolgend dargestellte virtuelle Kryptowährung „Libra".

188 Siehe hierzu u.a. die Antwort der Bundesregierung auf die kleine Anfrage, welche Anwendungsmöglichkeiten es für sog. *Distributed-Ledger-Technologien* gibt, BT-Drs. 19/3817. Einen Überblick über mögliche Anwendungsfelder geben auch: *Glatz*, DGRI Jahrbuch 2016, Rn. 1ff.; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 51ff.

189 Siehe hierzu etwa die Offenlegungsschriften des Deutschen Patentamtes, die nach dem Stichwort „Blockchain" gefiltert werden können; so auch *Glatz*, DGRI Jahrbuch 2016, Rn. 7ff.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Website „coinmarktecap“ 15.838 virtuelle Kryptowährungen gelistet.[190] Im Folgenden werden nur drei Beispiele weiterer virtueller Kryptowährungen in ihren technischen Abweichungen dargestellt.

1. Bitcoin-Cash

Bitcoin-Cash ist eine Abspaltung aus dem ursprünglichen Bitcoin-Netzwerk, die am 01. August 2017 stattfand.[191] Hintergrund war, dass die Datenmenge der Blöcke im Bitcoin-System begrenzt war und deshalb nur etwa 7 Transaktionen pro Sekunde durchgeführt werden konnten.[192] Bitcoin-Cash erweiterte die Datenmenge der Blöcke, sodass im Bitcoin-Cash-System etwa 8-mal so viel Transaktionen pro Sekunde möglich sind.[193]

2. Litecoin

Litecoin wurde im Oktober 2011 als Open-Source-Software veröffentlicht und wird, wie Bitcoin, dezentral über ein *Peer-to-Peer-Netzwerk* verwaltet.[194] Die virtuelle Kryptowährung unterscheidet sich zu Bitcoin technisch darin, dass die Blöcke etwa alle 2,5 Minuten erzeugt werden[195] und auch in diesem kürzeren Zeitabstand jeweils neue Litecoin durch das *mining* erzeugt werden. Dementsprechend ist auch die verfügbare Gesamtmenge der Litecoin ca. 84 Millionen.[196] Außerdem verwendet Litecoin eine andere *Hashfunktion* in ihrem *Proof-of-Work* Algorithmus, der das *mining* gleichmäßig auf die beteiligten Nutzer verteilen soll.[197]

---

190 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 27f.; https://coinmarketcap.com/currencies/views/all/ (letzter Abruf: 20. Dezember 2021).

191 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46. Siehe hierzu auch: https://www.bitcoincash.org (letzter Abruf: 20. Dezember 2021).

192 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46. Hierzu insbesondere auch: https://bchfaq.com/faq/whats-the-difference-between-bitcoin-cash-and-bitcoin/ (letzter Abruf: 20. Dezember 2021).

193 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 46.

194 Siehe hierzu: https://litecoin.org/de/ (letzter Abruf: 20. Dezember 2021).

195 Statt wie bei Bitcoin etwa alle 10 Minuten, *Kaulartz*, CR 2016, 474 (474); *Hofert*, Regulierung der Blockchains.

196 Vgl. hierzu https://litecoin.info/index.php/Main_Page und https://litecoin.org (letzter Abruf jeweils: 20. Dezember 2021).

197 *Grzywotz*, Virtuelle Kryptowährungen und Geldwäsche, S. 28; Hierzu ebenfalls https://litecoin.info/index.php/Main_Page und https://litecoin.org (letzter Abruf jeweils: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

3. Libra / Diem – FacebookCoin

Im Juni 2019 veröffentlichte die LibraAssociation das Whitepaper der Kryptowährung „Libra" – eine virtuelle Kryptowährung in Kooperation mit Facebook.[198] Mittlerweile hat sich das Projekt in „Diem" umbenannt.[199] Das vordergründig gemeinnützige Ziel, den 1,7 Milliarden Menschen auf der Welt, die bisher noch keinen Zugang zu einem Konto haben, aber ein Smartphone besitzen, Zahlungen über ein alternatives Finanzsystem zu ermöglichen, soll ab 2020 durch ein blockchain-basiertes alternatives Zahlungssystem erreicht werden.[200] Grundlage soll zwar auch hier die Blockchain-Technologie sein, in diesem Fall aber in der modifizierten Form, dass die Transaktionen von sog. *validator-nodes* (= Mitglieder der LibraAssociation) bestätigt werden.[201] *Miner*[202] und damit diejenigen, die die Blockchain fortschreiben, sind zum Zeitpunkt des Starts des Systems nur diejenigen, die von der LibraAssociation eine entsprechende Genehmigung erhalten haben (= genehmigungsbedürftige Blockchain).[203] Obwohl die Verwaltung insoweit nicht von allen Nutzern gleichberechtigt vorgenommen wird, sollen alle Nutzer Zugriff auf die Inhaltsdaten der Blockchain haben mit dem vordergründigen Ziel eine offene, transparente und verlässliche virtuelle Kryptowährung zu schaffen.[204]

198 Siehe hierzu etwa: https://www.tagesschau.de/wirtschaft/facebook-digitale-weltwaehrung-101.html (letzter Abruf: 20. Dezember 2021)

199 Vgl. https://www.diem.com/en-us/white-paper/#cover-letter (letzter Abruf: 20. Dezember 2021)

200 So das erklärte Ziel im Whitepaper der *LibraAssociation*, Cover Letter, White Paper v2.0, S. 4.

201 *LibraAssociation*, Cover Letter, White Paper v2.0, S. 8.

202 Die LibraAssociation spricht in ihrem White-Paper zwar von *validator-nodes,* hier wird allerdings an der oben angegebenen Differenzierung zwischen *nodes,* die lediglich Kommunikationsknoten sind, und *minern,* die die Blockchain selbst aktiv fortschreiben, festgehalten.

203 *LibraAssociation*, Cover Letter, White Paper v2.0, S. 8. Allerdings soll die Libra Blockchain im weiteren Verlauf als genehmigungsfreie Blockchain ausgestaltet werden. Siehe zur Differenzierung der Blockchain-Technologien oben unter B.IV.2.

204 *LibraAssociation*, Cover Letter, White Paper v2.0, S. 22f. Deshalb wird Libra in der öffentlichen Debatte aktuell scharf kritisiert, vgl. hierzu etwa *Menges*, Datenschützer äußern Bedenken zu Facebooks Libra.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

II. Smart Contracts

Ähnlich wie die virtuellen Währungen, ist auch der Begriff der sog. *Smart Contracts* bereits aus den 90er Jahren bekannt.[205] *Nick Szabo* veröffentlichte 1997 erstmals seine Theorie von Verträgen, die sich selbst ausführen.[206] Zentrales Problem zu dieser Zeit war allerdings, dass ein zentraler Intermediär weiterhin erforderlich war um die Verträge abzuwickeln.[207] Deshalb konnten sich die *Smart Contracts* zu diesem Zeitpunkt noch nicht durchsetzen.[208] Die Idee gewann deshalb mit Einführung der Blockchain-Technologie wieder an Interesse, da diese gerade ohne eine zentrale Verwaltungsinstanz auskommt.[209]

1. Was ist ein Smart Contract und wie funktioniert er?

a) Ziel und Funktion eines Smart Contracts

Smart Contracts sollen Vertragsbeziehungen programmieren und automatisieren.[210] Das bedeutet, dass das synallagmatische Verhältnis von Verträgen automatisch ausgeführt wird, indem es in die Programmlogik eines Computers implementiert wird.[211]

Vielfach zitiertes Beispiel ist der Leasingvertrag eines Autos.[212] In den *Smart Contracts* werden die Vertragsbedingungen wie die Höhe der Leasingraten und die Fälligkeit der Raten und der Leasinggegenstand implementiert.[213] Der Bordcomputer des Autos ist mit dem *Smart Contract*

205 *Kaulartz/Heckmann*, CR 2016, 618 (618); *Glatz*, DGRI Jahrbuch 2016, Rn. 19; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 13.

206 *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2092); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3, Rn. 13; *Heckelmann*, NJW 2018, 504 (504).

207 *Kaulartz/Heckmann*, CR 2016, 618 (618).

208 *Kaulartz/Heckmann*, CR 2016, 618 (618); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 17ff.

209 *Kaulartz/Heckmann*, CR 2016, 618 (618f.); Vgl. insoweit auch *Tschorsch/Scheuermann*, IEEE CST 2016, 2084 (2092).

210 *Kaulartz/Heckmann*, CR 2016, 618 (618f); *Mann*, NZG 2017, 1014 (1015); *Heckelmann*, NJW 2018, 504 (504).

211 *Kaulartz/Heckmann*, CR 2016, 618 (618f.); *Mann*, NZG 2017, 1014 (1015); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 14f.; *Heckelmann*, NJW 2018, 504 (504).

212 Hierzu ausführlich *Kaulartz/Heckmann*, CR 2016, 618 (618).

213 *Kaulartz/Heckmann*, CR 2016, 618 (618).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

verknüpft und kann so selbständig überprüfen, ob die Leasingraten zum vereinbarten Zeitpunkt gezahlt wurden, und kann davon abhängig machen, ob die Zündung des Autos funktioniert.[214]

In diesem Kontext ist eine Instanz notwendig, die das Vorliegen der Vertragsbedingungen überprüft und der beide Vertragspartner vertrauen – durch die Blockchain-Technologie kann diese Funktion nun das Netzwerk der Blockchain-Teilnehmer übernehmen.[215]

b) (Versuch einer) Definition eines Smart Contracts

Den ersten Versuch einer Definition von *Smart Contracts* nehmen *Kaulartz/Heckmann* vor und arbeiten die folgenden wesentlichen Merkmale von *Smart Contracts* anhand des Beispiels eines Leasingvertrags über ein Auto heraus:[216]

- „ein digital überprüfbares Ereignis
- ein Programmcode, welcher das Ereignis verarbeitet
- eine rechtlich relevante Handlung, welche auf Grundlage des Ereignisses ausgeführt wird“[217]

Dementsprechend soll ein *Smart Contract* eine Software sein, „die rechtlich relevante Handlungen […] in Abhängigkeit von digital überprüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert“[218].

c) Die Blockchain-Technologie bei Smart Contracts

Im Kontext der *Smart Contracts* übernimmt die Blockchain-Technologie die Funktion der Überprüfung der Transaktionen.[219]

---

214 *Kaulartz/Heckmann*, CR 2016, 618 (618).

215 *Kaulartz/Heckmann*, CR 2016, 618 (618); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 18f.

216 *Kaulartz/Heckmann*, CR 2016, 618 (618).

217 *Kaulartz/Heckmann*, CR 2016, 618 (618), der auf die von *Nick Szabo* verwendete Definition „*A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.*“ verweist. Ähnlich auch: *Heckelmann*, NJW 2018, 504 (504).

218 *Kaulartz/Heckmann*, CR 2016, 618 (618).

219 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 19. Siehe zur Transaktionsüberprüfung ausführlich oben unter A.III.1.c).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Denn im Bitcoin-System überprüfen die *miner* die Transaktionen des *memory-pools* anhand einer Checkliste, bevor sie sie in den *candidate-block* aufnehmen.[220] Bei Bitcoin umfasst die Überprüfung der Transaktionen insbesondere das Kriterium, dass die zu verifizierende Transaktion der bisherigen Blockchain nicht widerspricht und auch keine weitere widersprechende Transaktion im *memory-pool* enthalten ist.[221] Bei der Transaktionsprüfung können aber beliebig viele weitere Kriterien enthalten sein.[222] Hierzu ist aber eine Modifizierung der oben beschriebenen Funktionsweise der Blockchain-Technologie erforderlich, und zwar dahingehend, dass in der Blockchain die zu überprüfenden Bedingungen abgelegt werden müssen.[223]

2. Die „Ethereum"-Blockchain als Grundlage von Smart Contracts

Eine Plattform, die dies ermöglicht, bietet die bislang in diesem Bereich erfolgreichste Blockchain „Ethereum".[224] Genauso wie die Bitcoin-Blockchain erfolgt ein Zusammenschluss der Rechner über das Internet zu einem *Peer-to-Peer-Netzwerk,* das gemeinsam die zugrundeliegende Blockchain fortschreibt.[225]

Anders als bei Bitcoin ist es im Etherum-Netzwerk möglich, nicht nur sog. *Ether* (= die von Etherum verwendete virtuelle Kryptowährung) zu transferieren, sondern die *nodes* können auf der Blockchain eigene *Smart Contracts* ablegen, nach deren Bedingungen Transaktionen ablaufen.[226] Die Ethereum-Blockchain ist insoweit entwicklungsoffen und kann deshalb als Weiterentwicklung der Bitcoin-Blockchain verstanden werden.[227]

Ein *Smart Contract* ist in diesem Zusammenhang ein automatisierter Agent, der im Ethereum-Netzwerk lebt, eine eigene Ethereum-Adresse und

220 *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, S. 182f.
221 Siehe hierzu bereits oben unter A.III.1.c). *Antonopoulos*, Mastering Bitcoin: Unlocking Digital Cryptocurrencies.
222 *Kaulartz/Heckmann*, CR 2016, 618 (619).
223 *Kaulartz/Heckmann*, CR 2016, 618 (619).
224 *Kaulartz/Heckmann*, CR 2016, 618; *Heckelmann*, NJW 2018, 504 (505); Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 5.3 Rn. 21.
225 *Buterin*, Ethereum White Paper, S. 1; *Kaulartz/Matzke*, NJW 2018, 3278 (3278).
226 *Hoffer/Mirtchev*, NZKart 2019, 239 (241). Siehe hierzu insbesondere auch die Darstellung auf https://www.ethereum.org/beginners/ (letzter Abruf: 20. Dezember 2021).
227 *Mann*, NZG 2017, 1014 (1015).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

-Guthaben hat und selbst Transaktionen senden und empfangen kann.[228] Dieser Agent wird jedes Mal „aktiviert", wenn jemand eine Transaktion an ihn richtet, dann führt er seinen Code aus. So ist es möglich, dass in einer Blockchain die Bedingungen eines Vertrages abgelegt werden können, der sich selbst automatisch ausführt.[229]

So könnte das oben angesprochene Beispiel des Leasingvertrages in die Ethereum-Blockchain abgelegt werden.[230] Eine Transaktion an den *Smart Contract* wäre dann etwa das Drehen des Zündschlüssels, bei dem der Code des *Smart Contracts* ausgelöst würde und überprüfen könnte, ob eine Zahlung auf einem bestimmten Konto eingegangen ist und im Anschluss die Nachricht an den Bordcomputer des Autos sendet, dass der Motor gestartet werden darf.[231]

Werden mehrere dieser sich selbst ausführenden Verträge miteinander verbunden, spricht das Netzwerk von sog. *DApps* – Decentralized Apps.[232] Solche DApps können sehr komplex gestaltet werden, sodass sie etwa

228 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 48, der insoweit auf *Buterin*, Ethereum White Paper verweist.

229 *Glatz*, DGRI Jahrbuch 2016, Rn. 17ff.; Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 48.

230 Ähnlich auch *Glatz*, DGRI Jahrbuch 2016, Rn. 17ff., der als Beispiel einen Kauf im Internet erläutert, bei dem der Kaufpreis an einen dritten public key gesendet wird, von dem der Kaufpreis erst an den Verkäufer überwiesen werden kann, wenn sowohl Käufer wie auch Verkäufer die Transaktion mit ihren private keys signiert haben.

231 *Kaulartz/Heckmann*, CR 2016, 618 (618). Das bedeutet jedoch nicht, dass jeder blockchain-basierte Smart Contract auch jede Transaktion in der Blockchain ablegt, denn – wie bereits dargestellt – sind für die Datenverwaltung von Blockchains große Rechenkapazitäten erforderlich. Bei kommerziellen Anbietern wird deshalb wohl die Blockchain praktisch nicht zu Verwaltung aller Daten eingesetzt werden, sondern lediglich zur Verfügung über Berechtigungen. Im Fall des Leasingvertrages könnte entsprechend auch nur die Verfügung über die Berechtigung an den Leasingnehmer in die Blockchain eingetragen werden – alle weiteren Daten könnten in einer „herkömmlichen" Datenverwaltungsstruktur erfasst werden. Allerdings sind auch durchaus Anwendungsfälle denkbar, in denen es erforderlich ist, sämtliche Daten in die Blockchain einzutragen – namentlich dann, wenn es keinen zentralen Diensteanbieter gibt. Ein Beispiel könnte etwa ein dezentraler Carsharing Smart Contract sein, bei dem jeder Interessierte sein Auto zur Verfügung stellen kann und selbst auch die Autos aller anderer Nutzer mieten kann. Soweit hier wiederum auf einen zentralen Diensteanbieter verzichtet werden soll, wäre es erforderlich, alle notwendigen Daten (wie Zeitpunkt der Anmietung, Ort der Anmietung, Zeitpunkt der Rückgabe und Ort der Rückgabe, sowie die „Vertragsparteien") in die Blockchain einzutragen.

232 *Buterin*, Ethereum White Paper, S. 1, 33; *Hoffer/Mirtchev*, NZKart 2019, 239 (241).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Gesellschaftsverträge, Shareholder-Agreements und verschiedene Finanzinstrumente abbilden können.[233]

Die Blockchain-Technologie liefert dabei wiederum die Funktion der Verifikationsstelle. Die Teilnehmer des *Peer-to-Peer-Netzwerkes* überprüfen, ob die Bedingungen eingetreten sind, die Voraussetzungen für die Ausführungen bzw. Verifikation der Transaktion sind.[234]

3. Was sind ICOs – „Initial Coin Offerings"?

Über die Ethereum-Blockchain werden mittlerweile vermehrt sog. *ICOs (= „Initial Coin Offerings")* abgewickelt, die eine bestimmte Form des Crowdfundings darstellen.[235] Hierbei veröffentlichen Entwickler ihre Ideen und verkaufen sog. *tokens* über *Smart Contracts* an Kapitalgeber.[236] Mit dem eingenommenen Kapital wird dann die Idee des Entwicklers ausgearbeitet.[237] Den *token* kommt insoweit eine mit Unternehmensanteilen vergleichbare Funktion zu.[238]

4. Smart-Contract-Beispiele

a) The DAO

Das wohl wichtigste Beispiel der *Smart Contracts* dürfte die im Jahr 2016 auf der Etherum-Blockchain abgelegte sog. *„The DAO"* – The Decentralized Autonomus Organisation – sein, die innerhalb kürzester Zeit Kapital in

233 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 49; *Sattler*, Betriebs-Berater 2018, 2243 (2249).

234 *Kaulartz/Heckmann*, CR 2016, 618 (619); *Mann*, NZG 2017, 1014 (1015).

235 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.2 Rn. 24ff.; *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (90).

236 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.2 Rn. 25f.

237 Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.2 Rn. 27ff.

238 Dieser Vergleich dient lediglich zum Verständnis und ist vereinfacht. Lediglich die sog. *Investment Tokens* haben tatsächlich mit Unternehmensanteilen vergleichbare Funktionen, vgl. *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (92). Hierzu sogleich am Beispiel der „The DAO". Diese gesellschaftsrechtliche Differenzierung ist allerdings für die Frage nach den Auswertungsmöglichkeiten von Strafverfolgungsbehörden irrelevant.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Höhe von ca. 160 Mio. $ aufnahm und damit das damals größte Crowdfunding Projekt aller Zeiten war.[239]

Die *DAO* besteht aus mehreren *Smart Contracts,* die *Christopher Jentzsch* 2016 in seinem White Paper als Programmcode veröffentlichte.[240] Die DAO soll nach Ablage auf der *Ethereum-Blockchain* Kapital aufnehmen, indem Nutzer *Ether* an ihre *Ethereum-Adresse* senden.[241] Im Gegenzug erhalten die kapitalgebenden Nutzer frei weiterveräußerliche Eigentümer- und Stimmrechte (sog. *token*), mit denen sie im Anschluss Vorschläge über die Verwendung des Kapitals machen könnten.[242] Sobald sich eine bestimmte Mehrheit aus den *token* gebildet hätte, sollte die entsprechend gewählte Verwendung ausgeführt werden.[243]

Mann beschreibt die *DAO* als „eine auf Dauer angelegte Organisation, die aus einem Programmcode besteht, der dezentralisiert in der digitalen Welt verwahrt und ausgeführt wird; ihr wird eigenes Kapital überwiesen, das die Gesamtheit der Kapitalgeber gemäß den selbstausführenden Regeln des Programmcodes unmittelbar verwaltet."[244]

Auch wenn die juristische Einordnung dieses Programmcodes bisher nicht eindeutig geklärt ist[245], gleicht sie einer gesellschaftsrechtlichen Organisation und verdeutlicht dadurch insbesondere, welches Ausmaß *Smart Contracts* haben können.[246]

b) Lition

Das 2018 an den Markt gegangene Start-Up „Lition", das mittlerweile im Oktober 2021 Insolvenz anmelden musste[247], bezeichnete sich selbst als ers-

239 *Mann*, NZG 2017, 1014 (1014, 1016); *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (91).
240 *Mann*, NZG 2017, 1014 (1015); *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (91); *Sattler*, Betriebs-Berater 2018, 2243 (2250).
241 *Mann*, NZG 2017, 1014 (1015); *Klöhn/Parhofer/Resas*, ZBB 2018, 89 (91); *Sattler*, Betriebs-Berater 2018, 2243 (22250).
242 *Mann*, NZG 2017, 1014 (1015); *Sattler*, Betriebs-Berater 2018, 2243 (2250).
243 *Mann*, NZG 2017, 1014 (1015); *Sattler*, Betriebs-Berater 2018, 2243 (2250).
244 *Mann*, NZG 2017, 1014 (1015).
245 Vgl. insoweit zur Diskussion der rechtlichen Einordnung ausführlich *Mann*, NZG 2017, 1014 (1019f.).
246 *Sattler*, Betriebs-Berater 2018, 2243 (2250f.).
247 Vgl. https://lition.de/goodbye-lition (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ter blockchain-basierter Energieversorger.[248] Sein Ziel war es, dass Kunden am Strommarkt selbst agieren können und den Strom von Produzenten direkt beziehen können.[249]

Auf der von Lition angebotenen Plattform konnten Kunden einen Stromerzeuger auswählen und dann bilanziell von diesem Erzeuger ihren Strom erwerben. Die Abwicklung übernahm dabei die Plattform Lition, die selbst am Strommarkt auftrat und den jeweils von Kunden abgenommenen Strom am Markt kaufte. Eine direkte Vertragsbeziehung zwischen Produzent und Konsument war laut Unternehmensangaben auf Grund gesetzlicher Vorgaben noch nicht möglich.

Dabei verwendete das Unternehmen die Ethereum-Blockchain zur Abwicklung der Verträge. Gemeint waren hiermit wohl die konkreten Verträge zwischen Lition und den Stromerzeugern, da Lition angab, den Strom für seine Kunden entweder als Beauftragte des Kunden am Markt zu beschaffen oder den Kunden die Aktivität am Markt selbst über die Ethereum-Blockchain zu ermöglichen.

c) Fizzy – Flugverspätungsversicherung

Ein ähnliches Projekt war die von der AXA entwickelte Flugverspätungsversicherung, die im Versicherungsfall (eine Flugverspätung von mehr als 2 Stunden) eine automatische Auskehrung der Versicherungssumme versprach. Hierzu wurde wiederum die Ethereum-Blockchain verwendet, in der der *Smart Contract* über die Flugversicherung niedergelegt wurde.[250] Wenn das Flugzeug nun landete, glich der *Smart Contract* die Zeitdaten ab und zahlte im Fall einer Verspätung automatisch die Versicherungssumme

248 Vgl. hierzu ein Interview mit dem Unternehmensgründer, abrufbar unter: https://www.energate-messenger.de/news/190680/ha-erloes-ist-etwa-zehn-prozent-hoeher-als-ueblich- (letzter Abruf: 20. Dezember 2021).

249 So das erklärte Ziel des Unternehmens, abrufbar unter. Vgl. auch die Podiumsdiskussion mit dem CEO von Lition im Fachgespräch „#leben2030“ der Unionsfraktion vom 03. April 2019, abrufbar unter: https://www.cducsu.de/veranstaltungen/leben2030-blockchain-chancen-nutzen (letzter Abruf: 20. Dezember 2021).

250 So die Unternehmensangabe, abrufbar unter: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

an den Versicherungsnehmer aus.[251] Dabei wurden allerdings die persönlichen Daten des Kunden nicht in der Ethereum-Blockchain niedergelegt.[252]

d) „Bitsong“ und „KodakOne“ – Musik- und Fotoindustrie

Auch im Bereich der Musik- und Fotoindustrie gibt es mittlerweile erste blockchain-basierte Anwendungen.

So gibt es mittlerweile mit „Bitsong“ einen ersten blockchain-basierten Musik-Streaming-Anbieter, bei dem Künstler ihre Musik in einer Blockchain veröffentlichen können und diese von Kunden dann mittels *Smart Contract* gehört werden kann.[253]

Für den Bereich der Fotoindustrie hat Kodak mit „KodakOne“ eine ähnliche Anwendung geschaffen. Über die „blockchain-basierte Foto-Rechte-Management Plattform“[254] können Fotografen Lizenzen ihrer Fotos anbieten.[255]

e) Zwischenergebnis

Die vorstehenden Beispiele für blockchain-basierte *Smart Contracts* verdeutlichen wie weit der mögliche Anwendungsbereich der Blockchain-Technologien ist. Kernpunkt aller Anwendungen ist dabei, dass durch die Blockchain-Technologie hohe Verwaltungskosten wegfallen sollen, da sich die Anwendungen durch die Technologie selbst abwickeln sollen. Dabei sind die Inhaltsdaten der Blockchains überwiegend öffentlich einsehbar. Uneinheitlich bleibt in diesem Zusammenhang die tatsächliche konkrete Ausgestaltung der Anwendungen – insbesondere, welche Daten in die jeweiligen Blockchains geschrieben werden.

---

251 So die Unternehmensangabe, abrufbar unter: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy (letzter Abruf: 20. Dezember 2021).

252 So die Unternehmensangabe, abrufbar unter: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy (letzter Abruf: 20. Dezember 2021).

253 Vgl. hierzu das White-Paper des Streaming-Anbieters, *Recca/Ricli/Anghelin/Farruggio*, The first decentralized music streaming platform a new era in music streaming.

254 So die wörtliche Übersetzung der Unternehmensangabe, abrufbar unter: https://www.kodakone.com (letzter Abruf: 28. August 2019).

255 Vgl. https://vkool.com/kodakone/ (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

III. Öffentliche Verwaltung

Auch im Bereich der öffentlichen Verwaltung bzw. der öffentlichen Registerführung wird mittlerweile intensiv diskutiert, ob und inwieweit die Blockchain-Technologie hier zum Einsatz kommen kann[256] – teilweise gibt es in anderen Ländern bereits blockchain-basierte Bereiche der öffentlichen Verwaltung.[257] Diskutiert wird in Deutschland aktuell vor allem der Einsatz beim Handelsregister und Grundbuchamt.[258] In anderen Europäischen Ländern – wie etwa Estland – kommt die Blockchain-Technologie bereits für verschiedene Register – wie etwa das „Healthcare Registry" und das „Property Registry" – zum Einsatz, allerdings nur zur Absicherung der Daten.[259]

D. Zwischenergebnis

Die Blockchain-Technologie geht zurück auf die virtuelle Kryptowährung Bitcoin aus dem Jahr 2008 und fungiert in diesem Zusammenhang als dezentral geführtes Transaktionsregister. Ihr Ziel besteht darin, ein Register zu führen, das losgelöst von zentralen Intermediären funktioniert und für das kein Vertrauen mehr in eine zentrale Instanz notwendig ist.

Wesentlicher technologischer Fortschritt der Blockchain-Technologie ist ihre dezentrale Verwaltungsstruktur, die davon geprägt ist, dass sich alle Nutzer bzw. Teilnehmer des Netzwerks auf einen Konsens einigen und diesen in ihrer zentralen Datenbank fortschreiben. Dies ist deshalb ein wesentlicher Fortschritt, weil auch im Zeitalter des World Wide Web die meisten Online-Anwendungen von einer jeweils zentralen Instanz verwal-

256 Vgl. insoweit die intensive Diskussion von *Knaier/Wolf*, Betriebs-Berater 2018, 2253., der sich ausführlich mit der Frage auseinandersetzt, wie die Blockchain-Technologie für das Handelsregister und das Grundbuch eingesetzt werden können.

257 Vgl. insoweit die Einführung der sog. *E-ID* in der Schweiz und das darauf aufbauende blockchain-basierte Wahlsystem, abrufbar unter: https://www.heise.de/newsticker/meldung/Schweiz-Blockchain-Identitaet-fuer-Zug-E-ID-fuers-ganze-Land-3892220.html; https://www.heise.de/newsticker/meldung/Schweizer-Crypto-Valley-E-Voting-auf-Blockchain-Basis-in-Zug-4092661.html (letzter Abruf jeweils: 20. Dezember 2021).

258 *Martini/Weinzierl*, NVwZ 2017, 1251 (1252); *Schrey/Thalhofer*, NJW 2017, 1431 (1432); *Knaier/Wolf*, Betriebs-Berater 2018, 2253.

259 *Knaier/Wolf*, Betriebs-Berater 2018, 2253 (2256). Vgl. auch: https://e-estonia.com/blockchain-healthcare-estonian-experience/ (letzter Abruf: 20. Dezember 2021).

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

tet werden. So verwalten Facebook, Google, Amazon und andere Online-Dienstanbieter die Daten ihrer Nutzer in zentralen Rechenzentren. Im Fall der Blockchain-Technologie sind dagegen die Nutzer des Netzwerks bzw. des Online-Angebotes selbst diejenigen, die die Daten des Netzwerks verwalten – hier existieren keine zentralen Knoten, über die die Kommunikation abgewickelt wird, sondern alle Nutzer sind selbst die Knoten.[260]

Der Anwendungsbereich der Blockchain ist allerdings nicht auf das Register von Kryptowährungen beschränkt, sondern die Technologie kann insgesamt als eine dezentral verwaltete Datenverwaltungsstruktur verstanden werden, in der Daten unabhängig von ihrem Inhalt dokumentiert und verwaltet werden können.

So können durch die Blockchain *Smart Contracts* abgebildet und ausgeführt werden, über die etwa Stromhandel, Musikstreaming, Fotolizensierung und auch gesellschaftsrechtliche Strukturen abgewickelt werden können. Dementsprechend weit können auch die Inhaltsdaten der verschiedenen Blockchains sein.

Als mittelbare Folge dieser technologischen Architektur sind jegliche Inhaltsdaten der Blockchain öffentlich verfügbar, soweit die jeweilige Blockchain als offenes Netzwerk ausgestaltet ist, da jeder Teilnehmer des Netzwerkes die Transaktionen der anderen Teilnehmer des Netzwerkes überprüfen können muss.

260 Dieser Architektur-Unterschied wird besonders deutlich anhand der Abbildung in Breidenbach-Glatz RhdB-Legal-Tech/*Glatz,* Kap. 4.1 Rn. 13.

https://doi.org/10.5771/9783748941248-33, am 19.11.2024, 12:45:13
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb