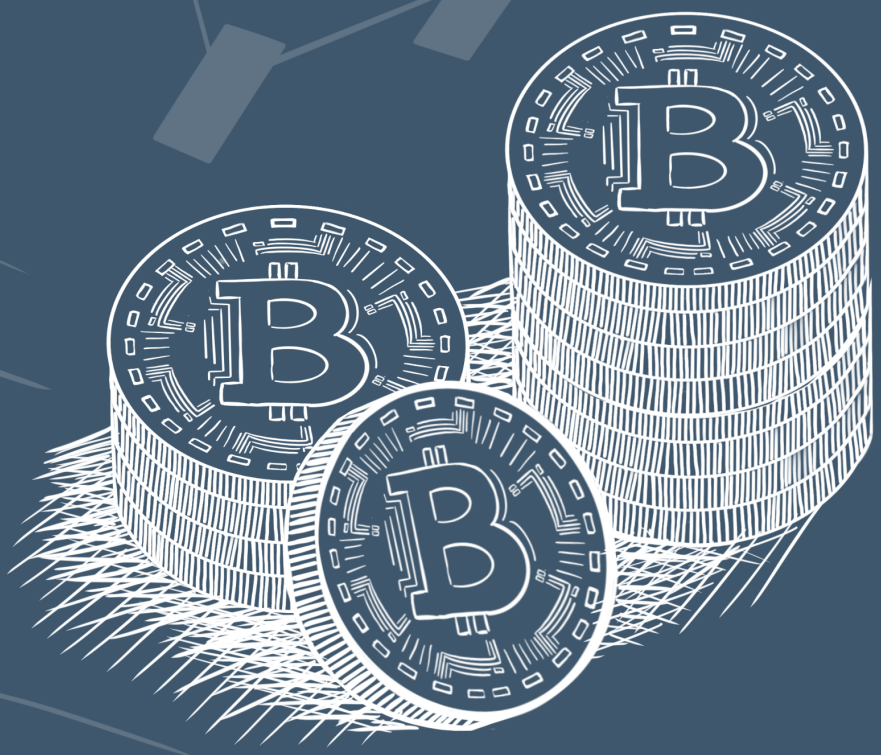
ODDO BHF

INSIDE *BLOCKCHAIN*

Die Bitcoin-Blockchain – ein Überblick



April 2021
Sandra Sohn

Inhalt

Einleitung 05

Distributed Ledger Technology
– das Fundament 07

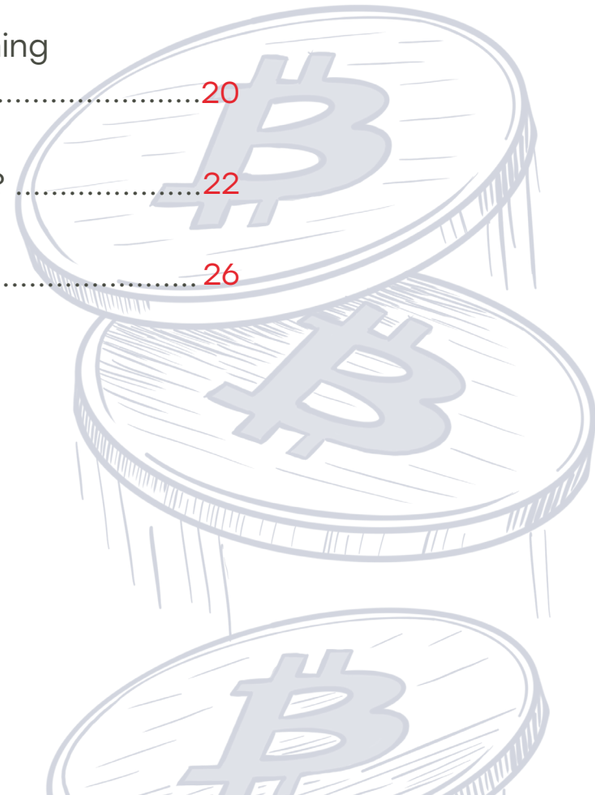
Wallet, Private Key & Public Key
im Zusammenhang 11

Die Bitcoin-Blockchain
– Funktionsweise 15

Kritikpunkt – Bitcoin-Mining
und Stromverbrauch 20

Bitcoin oder Blockchain? 22

Quellen 26



Einleitung

Der Bitcoin und die Blockchain – eine Technologie, die bereits seit zwölf Jahren existiert, und vor gut drei Jahren das erste Mal weltweite Aufmerksamkeit erhalten hat. Der rasante Kursanstieg des Bitcoins war Ende 2017 der Auslöser, gefolgt von enormer Schwankungsintensität.

Durch die Kursentwicklungen zu Beginn des Jahres 2021 hat der Bitcoin wieder eine hohe mediale Präsenz erhalten – insbesondere getrieben durch große Investitionen des Softwareunternehmens Microstrategy oder des Elektroautoherstellers Tesla, die mehrere Milliarden US-Dollar in Bitcoin investiert haben.[1]

Auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nahm die Kursentwicklung in den ersten Monaten im Jahr 2021 auf den Märkten für Kryptowerte zum Anlass, Verbraucherinnen und Verbraucher erneut vor den Risiken solcher Investments zu warnen („Hype um Kryptowährungen“, 13.01.2021). Der Handel mit Bitcoin und anderen Kryptowährungen bzw. darauf bezogenen Finanzinstrumenten ist insbesondere aufgrund der hohen Volatilität **mit erheblichen Risiken verbunden und kann bis hin zum Totalverlust** des eingesetzten Kapitals führen.

Die Beweggründe für Investitionen in Bitcoin sind genauso vielfältig wie die Sichtweisen auf den Bitcoin. Ob als Spekulationsinstrument, alternative Anlageklasse, Zahlungsmittel oder „Digitales Gold“ – der Wert des Bitcoins scheint reine Definitionssache zu sein. Es findet sich ein ganzer Blumenstrauß an Definitionen und Marktmeinungen zum Bitcoin, die teilweise sehr weit auseinandergehen: Während der CEO von Microstrategy, Michael Saylor, den Bitcoin als „sicheren Wertspeicher“ sieht, betrachtet Nouriel Roubini ihn als „die Mutter aller Betrügerei“.[2]

Welche Meinung nun die richtige ist und welchen „intrinsischen“ Wert der Bitcoin nun tatsächlich hat, lässt sich nur schwer beurteilen. Der Bitcoin ist kein Unternehmen, welches anhand von Strategie, Produkt, Bilanz oder Management beurteilt und bewertet werden könnte.

Der Bitcoin ist lediglich ein „Produkt“ der Blockchain-Technologie. Wer also verstehen will, wie der Bitcoin funktioniert, der muss auch verstehen, wie die Bitcoin-Blockchain funktioniert. Die Technologie birgt jedoch ein hohes Maß an Komplexität, weshalb es häufig schwierig ist, die Funktionsweise nachzuvollziehen. Häufig wird im Zusammenhang mit dem Bitcoin auch von „DLT“ oder „Mining“ geredet, doch nur selten wird dazu eine ausreichende Erklärung geliefert.

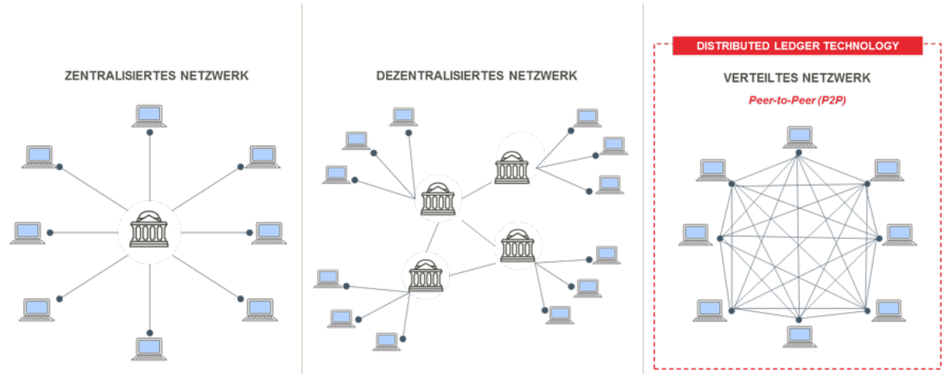
Um diese Schlagwörter und den Bitcoin richtig einordnen zu können, wird nachfolgend die Technologie und die grundlegende Funktionsweise der Bitcoin-Blockchain erläutert, jedoch ohne die komplexen technischen Zusammenhänge im Detail auszuführen. Dadurch ist das Paper auch für interessierte LeserInnen ohne informationstechnische Vorkenntnisse geeignet.

ZAHLUNGSMITTEL,
ALTERNATIVE ANLAGEKLASSE,
DIGITALES GOLD,
SPEKULATIONSINSTRUMENT

[1] Vgl. Microstrategy (Hrsg.) (2021); CNBC (Hrsg.) (2021)
[2] Vgl. Bloomberg (Hrsg.) (2021); Handelsblatt (Hrsg.) (2021)

Distributed Ledger Technology – das Fundament

Das Konzept der Blockchain-Technologie wurde erstmals im November 2008 als Teil des Whitepapers „Bitcoin: A Peer-To-Peer Electronic Cash System“ bekannt. Das ursprüngliche Ziel der in dem Whitepaper vorgestellten blockchainbasierten Kryptowährung Bitcoin war es, ein Peer-to-Peer(P2P)-Geld als demokratisches Zahlungssystem zu schaffen, welches nicht von Zentral- und Geschäftsbanken gesteuert wird. Unter P2P versteht man ein verteiltes Netzwerk, welches ausschließlich aus gleichberechtigten Teilnehmern besteht und von keiner zentralen Kontrollinstanz kontrolliert oder dominiert wird.[3]



Die Blockchain-Technologie gehört zu der sogenannten „Distributed Ledger Technology“ (DLT). Ein Distributed Ledger ist eine verteilte Datenbank, welche von verschiedenen, gleichberechtigten Teilnehmern (P2P) betrieben wird, um die Notwendigkeit einer zentralen Kontrollinstanz zur Verarbeitung, Validierung oder Authentifizierung von Transaktionen zu eliminieren. Alle Teilnehmer, die die Distributed-Ledger-Datenbank betreiben, müssen allen Änderungen der Datenbank zustimmen, z.B. wenn neue Datensätze gespeichert werden sollen. Alle neuen Datensätze werden kryptografisch verschlüsselt und können von allen Teilnehmern jederzeit eingesehen werden – ein verteiltes Netzwerk wird folglich von allen Teilnehmern zu gleichen Teilen kontrolliert. Bei zentralisierten Netzwerken liegt die Kontrolle hingegen immer bei einer Organisation bzw. einer Partei und bei dezentralisierten Netzwerken bei mehreren Teilnehmern bzw. mehreren Parteien. [4]

Die Blockchain kann sowohl als verteiltes Netzwerk als auch als dezentralisiertes Netzwerk ausgestaltet werden, wobei sie grundsätzlich als verteiltes Netzwerk geschaffen wurde.

[3] Vgl. Nakamoto, Satoshi (Hrsg.) (2008)
[4] Vgl. Attaran, M./Gunasekaran, A. (2019), S.1

Beispiel: Ökosystem Café

Das Prinzip eines verteilten Netzwerks lässt sich in dem folgendem Beispiel veranschaulichen. Der Kontext: Sie sitzen in einem Café und trinken mit ihrem Kollegen Timo einen Milchkaffee. Die Café-Betreiberin steht hinter der Theke und bereitet die nächsten Kaffee-Bestellungen vor. Nach ein paar Stunden möchten Sie gerne zahlen und die Rechnung für Ihren Kollegen Timo übernehmen, der eilig das Café verlassen musste.

Zentrales System:

Sie sagen der Café-Betreiberin, dass Sie gerne zahlen möchten und diese legt Ihnen die Rechnung vor. Angenommen, auf der Rechnung steht, dass Timo zwei Milchkaffee und ein Wasser getrunken hat, was Sie in Summe 11,50€ kosten würde. Die Café-Betreiberin gibt Ihnen den zu zahlenden Betrag vor, ohne dass Sie nachvollziehen können, ob es tatsächlich die richtige Summe ist. Sie müssen in diesem Fall darauf vertrauen, dass die Café-Betreiberin die Getränke richtig gebucht hat und Ihnen die richtige Summe nennt, denn Sie haben keine Möglichkeit, diesen Vorgang zu überprüfen. Die Café-Betreiberin ist in diesem Sinne die „zentrale Kontrollinstanz“ in dem „Ökosystem Café“.

Verteiltes System:

Ein verteiltes System im Ökosystem Café könnte wie folgt aussehen: Sie sitzen mit Ihrem Kollegen Timo im Café und dieses Mal liegt vor jedem Gast ein Notizblock, auf dem die Café-Betreiberin bei jeder Bestellung die Getränke notiert. Das besondere an diesem Notizblock ist, dass nicht nur Ihre Getränke notiert werden, sondern auch die von allen anderen Gästen. Wenn Sie nun zwei Espresso trinken und ihr Kollege Timo zwei Milchkaffee, dann würde beides auf dem Notizblock von jedem Gast im Café stehen. Wenn Sie jetzt die Rechnung für Timo übernehmen möchten, dann könnten Sie einfach den zu zahlenden Betrag Ihrem Notizblock entnehmen, ohne die Café-Betreiberin fragen zu müssen bzw. darauf zu vertrauen, dass diese Ihnen die richtige Summe nennt. Die Notizblöcke dienen als Protokoll bzw. als „verteilte“ Datenbank, über die jeder Gast jederzeit nachvollziehen kann, wer welche Getränke bestellt, erhalten und bezahlt hat. Natürlich möchten wir in einem Café nicht, dass jeder Gast weiß, wie viel und was man getrunken hat. Aus diesem Grund sind die Namen sowie jede Bestellung (kryptografisch) verschlüsselt und jeder sieht zwar die entsprechenden Beträge, kann sie aber nicht direkt einer Person zuordnen. So würde ein verteiltes System im Ökosystem Café funktionieren – ohne zentrale Kontrollinstanz.

NOTIZBLOCK

Gast	Bestellung	Betrag
Anna	*2 Espresso*	*5 EUR*
Louisa	*3 Kaffee*	*7,30 EUR*
Timo	*2 Milchkaffee 1 Wasser*	*11,50 EUR*

NOTIZBLOCK
(verschlüsselt)

Gast	Bestellung	Betrag
1e800a5c324b81f61cc107b8eefab2	*2 Espresso*	*5 EUR*
18f61cc107b8eefab2f1eda32e00a5	*3 Kaffee*	*7,30 EUR*
1a516b32d952d8eefab2f120f52b43	*2 Milchkaffee 1 Wasser*	*11,50 EUR*

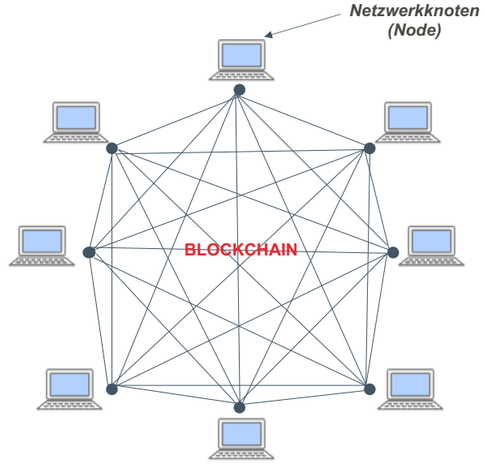
Der Grundgedanke der Distributed Ledger Technology ist es also, zentrale Kontrollinstanzen, die wir in der traditionellen Welt als vermittelnde und vertrauenswürdige Dritte wie Banken oder Makler (oder eben eine Café-Betreiberin) kennen, in diversen Transaktionsprozessen auszuschalten.[5]

Die Blockchain ist eine bestimmte Art der Distributed Ledger Technology. Im weiteren Sinne ist eine Blockchain eine Datenbank, die die Historie aller Transaktionen zwischen ihren BenutzerInnen seit ihrer Entstehung enthält und in Datenblöcken zusammenfasst.[6]

Diese Datenblöcke werden auf sogenannten Netzwerkknoten gespeichert. Als Netzwerkknoten (auch „Nodes“ genannt) werden die Teilnehmer in einem Blockchain-Netzwerk bezeichnet, die sich via Download der Open-Source-Software mit der entsprechenden Blockchain verbunden haben. Ein Netzwerkknoten ist also jeder Computer, Laptop oder größere Server, der die entsprechende, frei zugängige Software heruntergeladen hat.[7] Die Bitcoin-Blockchain wird von ca. 10.000 Netzwerkknoten betrieben, die das gesamte Bitcoin-Blockchain-Protokoll heruntergeladen haben.

Netzwerkknoten bilden die Infrastruktur einer Blockchain. Alle Netzwerkknoten sind miteinander verbunden und tauschen ständig die neuesten Datensätze untereinander aus, sodass diese immer auf dem aktuellen Stand sind. Jeder einzelne Teilnehmer speichert, verbreitet und bewahrt die in der Blockchain gespeicherten Daten.

In unserem Ökosystem Café wären die Netzwerkknoten die Gäste mit dem entsprechenden Protokoll in Form des Notizblocks, über den jeder Gast verfügt.



[5] Vgl. Schacht, S./Lanquillon, C. (2019), S. 13
[6] Vgl. Brühl, V./Dorschel, J. (2018), S.10
[7] Vgl. Rutz, V. (2020), S.17

UM BITCOIN
KAUFEN ZU KÖNNEN,
MUSS EIN *WALLET*
ANGELEGT WERDEN.

Wallet, Private Key & Public Key im Zusammenhang

Mit der wachsenden Popularität von Bitcoin und anderen Kryptowährungen ist auch die Anzahl an Plattformen und Anbietern für den Handel ebendieser rasant gestiegen. Mittlerweile haben Interessierte eine große Auswahl an Möglichkeiten, um Kryptowährungen zu kaufen und zu verkaufen – häufig reicht eine Google-Suche aus, um verschiedene Rankings und Auflistungen zu erhalten. Denn um Kryptowährungen wie Bitcoin kaufen zu können, muss ein sogenanntes „Wallet“ angelegt werden, welches als „Schnittstelle“ zur Blockchain gesehen werden kann.

Ein Wallet ist eine Art elektronische Geldbörse bzw. ein Online-Konto zur Speicherung von Kryptowährungsbeständen. Ein Wallet kann mittlerweile sehr schnell über verschiedene Plattformen angelegt werden. Beim Anlegen eines Wallets erhalten die InhaberInnen grundsätzlich einen „Private Key“ (privaten Schlüssel) und einen „Public Key“ (öffentlichen Schlüssel).

Der Public Key ist die „Wallet-Adresse“ und kann als eine Art Kontonummer gesehen werden. Diese könnte folgendermaßen aussehen: „1P82rBjJMDFSay2RqKx1bydDRVh5QnGkkZ“. Jede Person, die eine Wallet-Adresse kennt, kann Transaktionen dorthin senden und außerdem einsehen wie viele (und in welcher Höhe) Transaktionen von dem Wallet getätigt und erhalten wurden und wie die aktuelle Bilanz aussieht. Wallet-Adressen können jedoch nicht direkt realen Personen zugeordnet werden, denn sie sind lediglich ein Pseudonym, unter dem Wallet-InhaberInnen in der Blockchain agieren. Wichtig ist hier, dass der Handel mit Bitcoin bzw. Kryptowährungen nicht ohne Weiteres vollständig anonym ist. Grundsätzlich findet beim Anlegen des Wallets eine Identitätsüberprüfung von der entsprechenden Plattform statt, welche die persönlichen Nutzerdaten hinterlegt und auch dann wieder benötigt, wenn die Bitcoins bzw. Kryptowährungen wieder in Fiatwährung umgewandelt werden sollen. Diese Identitätsüberprüfungsverfahren variieren jedoch sehr stark von Plattform zu Plattform, da es noch keine klare globale Regulierung dafür gibt.

Neben der Wallet-Adresse wird bei der Wallet-Erstellung auch ein Private Key generiert. Der Private Key ist ein geheimes Passwort, welches Zugang zum Wallet gewährt und das gleichzeitig auch benutzt wird, um Transaktionen auszuführen. Nur der bzw. die Wallet-InhaberIn sollte den Private Key kennen und ihn sicher aufbewahren, denn wenn dieser verloren geht, ist der Zugang zum Wallet gesperrt und kann i. d. R. durch keine Instanz wieder freigegeben werden. Die Person, die den Private Key hat, kann mit diesem uneingeschränkt auf das Wallet zugreifen und Transaktionen tätigen (z. B. Kryptowährungen versenden und erhalten). Deshalb ist eine sichere Verwahrung der Private Keys enorm wichtig, denn das Blockchain-Netzwerk erkennt immer die Person als rechtmäßigen Besitzer des Wallets an, die den Private Key zum zugehörigen Wallet besitzt. Falls das niemand ist, gibt es kaum eine Möglichkeit, wieder Zugriff auf das Wallet zu erhalten.

Häufig wird in den Medien über Szenarien berichtet, in denen Personen ihren Private Key verloren haben und keinen Zugriff mehr auf ihre Bitcoins in Millionenhöhe haben. Um genau diese Situationen zu vermeiden, gibt es mittlerweile verschiedene Verfahren, um den Zugang zu Wallets und die Absicherung ebendieser zu gewährleisten. Viele Plattformen, die die Erstellung von Wallets anbieten, bieten auch häufig die Verwahrung der Private Keys an. Hier gibt es verschiedene Mechanismen, die dafür sorgen, dass der Private Key nicht abhandenkommt oder in die falschen Hände gerät. Manche Plattformen übernehmen die vollständige Verwahrung der Private Keys, d. h. der bzw. die Wallet-InhaberIn erhält gar keinen Zugang zum Private Key, sondern der Zugang zum Wallet erfolgt durch ein einfaches Passwort, welches im Zweifelsfall zurückgesetzt werden könnte, während die Plattform im Hintergrund die Private Keys verwahrt und verwendet, um Transaktionen zu autorisieren.

Wie im Beispiel am Ökosystem Café erwähnt, wären die Namen der Gäste auf dem Notizblock, der als Protokoll dient und über den jeder Gast verfügt, kryptografisch verschlüsselt. Das bedeutet eben, dass jeder Gast in dem Café nicht über seinen Klarnamen im Notizblock-Protokoll agiert, sondern unter einem Pseudonym – dem jeweiligen Public Key.

NOTIZBLOCK

Gast	Bestellung	Betrag
Anna	*2 Espresso*	*5 EUR*
Louisa	*3 Kaffee*	*7,30 EUR*
Timo	*2 Milchkaffee 1 Wasser*	*11,50 EUR*

NOTIZBLOCK
(verschlüsselt)

Public Key der Gäste	Bestellung	Betrag
1e800a5c324b81f61cc107b8eefab2	*2 Espresso*	*5 EUR*
18f61cc107b8eefab2f1eda32e00a5	*3 Kaffee*	*7,30 EUR*
1a516b32d952d8eefab2f120f52b43	*2 Milchkaffee 1 Wasser*	*11,50 EUR*

Kurze Zusammenfassung der wichtigsten Begrifflichkeiten:

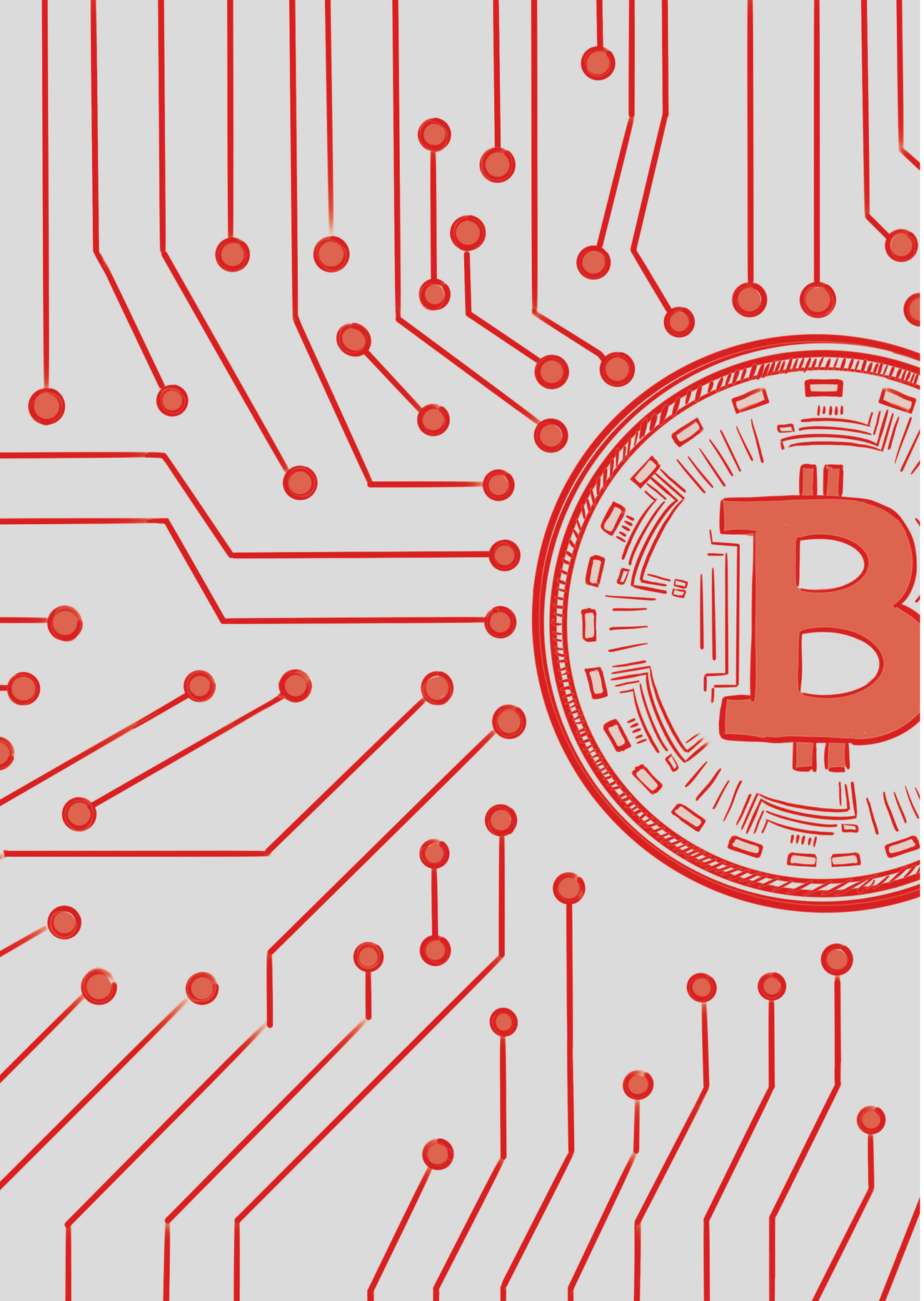
Blockchain: Dezentrale oder verteilte Datenbank, welche von vielen gleichberechtigten Netzwerkknoten (Teilnehmer, die die entsprechende Software auf ihrem Computer heruntergeladen haben) verwaltet und durch keine zentrale Kontrollinstanz gesteuert wird.

Netzwerkknoten: Bilden die Infrastruktur einer Blockchain. Alle Netzwerkknoten sind miteinander verbunden und tauschen ständig die neuesten Datensätze untereinander aus, sodass diese immer auf dem aktuellen Stand sind. Jeder einzelne Teilnehmer speichert, verbreitet und bewahrt die in der Blockchain gespeicherten Daten.

Wallet: Digitales Konto, das benötigt wird, um auf der Blockchain zu agieren, z. B. um Bitcoins oder andere Kryptowährungen zu kaufen/verkaufen. Kann auf einer beliebigen Online-Plattform eröffnet werden und setzt eine Identitätsprüfung voraus.

Public Key: „Wallet-Adresse“ bzw. „Kontonummer“ des Wallets. Der Public Key ist eine alphanumerische Zeichenkette bestehend aus 27–34 Zeichen, mit der ein Wallet eindeutig identifiziert werden kann.

Private Key: Ein geheimes Passwort, welches Zugang zum Wallet gewährt und gleichzeitig auch benutzt wird, um Transaktionen auszuführen. Nur der bzw. die Wallet-InhaberIn sollte den Private Key kennen und ihn sicher aufbewahren, denn wenn dieser verloren geht, ist der Zugang zum Wallet gesperrt und kann i. d. R. durch keine Instanz wieder freigegeben werden.



Die Bitcoin-Blockchain – Funktionsweise

Der tatsächliche Kauf oder Verkauf von Kryptowährungen wie dem Bitcoin ist von den meisten Plattformen bereits so gestaltet, dass sich die Ausführung einer Transaktion nur unerheblich von einer normalen Überweisung oder dem Kauf einer Aktie über eine Online-Plattform unterscheidet.

Wichtig ist aber, zu verstehen, was in der Blockchain passiert, wenn eben solche „normalen“ Transaktionen stattfinden. Die verschiedenen Mechanismen und Funktionsweisen werden im Folgenden anhand eines einfachen Transaktionsbeispiels erläutert, in dem Anna für drei Bitcoins einen Tesla kauft.

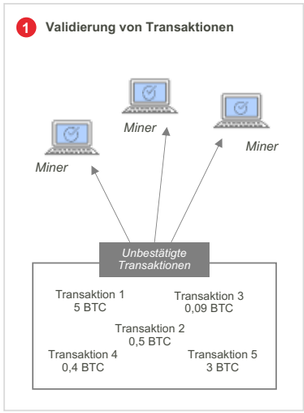
Beispiel:

Anna verfügt schon seit längerem über diverse Kryptowährungen, die sie in ihrem Wallet auf einer Plattform hält. Anna möchte sich einen neuen Tesla kaufen und sie hat gelesen, dass man die Autos nun auch mit Bitcoins erwerben kann. Sie beschließt ihren neuen Tesla mit Bitcoins zu bezahlen, schließt den Kaufvertrag ab und erhält die Wallet-Adresse von Tesla, an die sie nun drei Bitcoins überweisen muss. Anna loggt sich über ihre Plattform in ihr Wallet ein und fordert eine Transaktion an. Dazu gibt Anna die Wallet-Adresse von Telsa und den Betrag (3 BTC) in eine Transaktionsmaske ein und bestätigt die Transaktion.[8] Dieser Prozess unterscheidet sich nur gering von dem einer normalen Onlineüberweisung über das Onlinebanking der Hausbank. Sobald die Transaktion abgeschickt wurde, übernimmt die Blockchain die Arbeit, während Senderin (Anna) und Empfänger (Tesla) nur noch die Bestätigung der erfolgreichen Transaktion erhalten.

Nachdem Anna die Transaktion über ihre Plattform ausgeführt hat, wird die gesendete Transaktion kryptografisch verschlüsselt. Hier greifen verschiedene Sicherheitsmechanismen der Blockchain, denn jede Transaktion wird in der Blockchain so verschlüsselt, dass sie im Nachhinein nicht mehr unbefugt verändert oder eingesehen werden kann.

Annas Transaktion wird nun verschlüsselt an das Netzwerk gesendet und dort in einem „Pool“ mit anderen Transaktionen gesammelt.

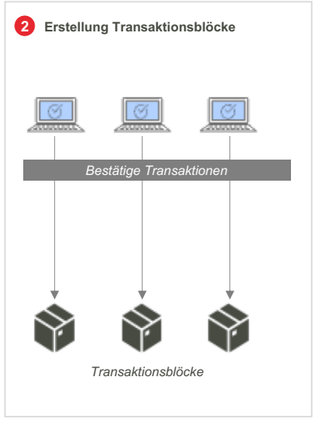
Sogenannte „Miner“ validieren die eingehenden Transaktionen nach einem bestimmten Regelwerk, das vorgibt, welche Anforderungen Transaktionen erfüllen müssen, um validiert zu werden. Bei der Bitcoin-Blockchain müssen Miner u. a. prüfen, ob der Sender über die entsprechende Anzahl an Bitcoin in seinem Wallet verfügt, um die Transaktion zu tätigen.



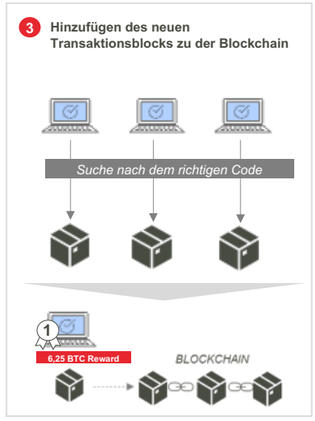
[8] Vgl. Bajpai, P. (2019); Elrom, E. (2019), S.29

In unserem Beispiel könnte Anna also nur drei Bitcoins an Tesla senden, wenn diese auch tatsächlich in ihrem Wallet angezeigt werden.[9]

In einem Blockchain-Netzwerk gibt es mehrere Miner, die gleichzeitig Transaktionen validieren und in Transaktionsblöcken sammeln. Jeder Miner erstellt also parallel seinen eigenen Transaktionsblock.[10]



In einen Transaktionsblock passen im Durchschnitt ca. 2000 Transaktionen. Wenn diese Anzahl erreicht ist, müssen die Miner ihren Transaktionsblock verschlüsseln, wofür sie einen bestimmten Code finden müssen. Dieser Prozess heißt „Proof-of-Work“ und kostet die Miner viel Rechenleistung und Energie.[11] Der Miner, der zuerst den richtigen Code gefunden und den Transaktionsblock verschlüsselt hat, darf seinen Transaktionsblock in die Blockchain hinzufügen und erhält dafür eine „Belohnung“ über 6,25 Bitcoins.



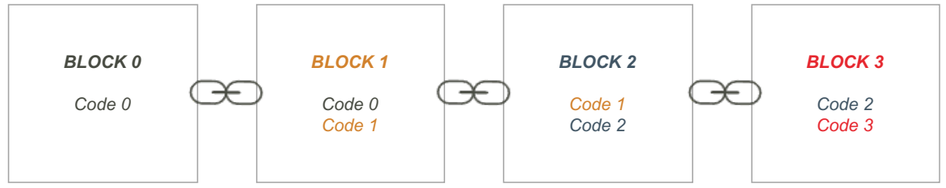
Die Belohnung für den Miner (6,25 BTC) werden neu vom Netzwerk ausgegeben; das bedeutet, dass diese Bitcoins sich noch nicht im Umlauf befunden haben, sondern neu erschaffen wurden. Durch diesen sogenannten „Mining“-Prozess werden einerseits die Sicherheit des Netzwerks gewährleistet und gleichzeitig neue Bitcoins geschaffen. Analog zum traditionellen System würden wir hier von „Geldschöpfung“ in Form von neu geschaffenem Giralgeld sprechen, mit dem Unterschied, dass die Menge neu ausgegebener Bitcoins immer auf einen festgelegten Betrag (momentan 6,25 BTC) beschränkt ist.

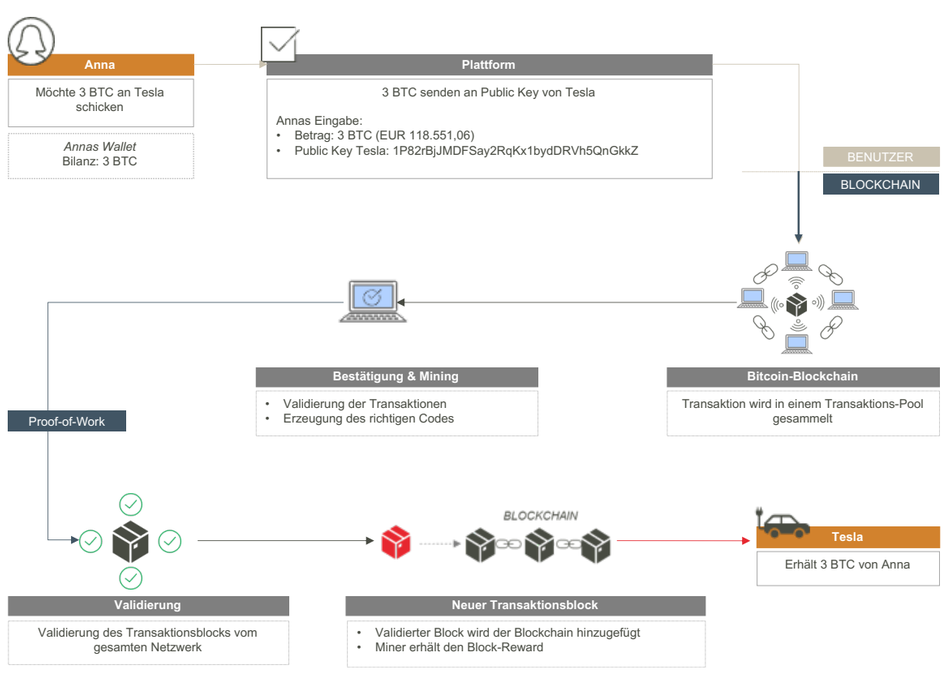
Alle Netzwerkknoten, die die Bitcoin-Blockchain betreiben, validieren nun die Gültigkeit des neuen Transaktionsblocks und wenn mindestens 51 % Übereinstimmung herrscht, kann der Transaktionsblock der Blockchain hinzugefügt werden.[12]

Sobald der Transaktionsblock zur Blockchain hinzugefügt wurde, erhält Tesla die drei Bitcoins von Anna.

[9] Vgl. Schacht, S./Lanquillon, C. (2019), S. 39
[10] Vgl. Dhillon, V./Metcalf, D./Hooper, M. (2017), S. 8
[11] Vgl. Brühl, V./Dorschel, J. (2018), S. 279f.
[12] Vgl. Himmer, K. (2019), S. 8f.

Alle Transaktionsblöcke sind in der Blockchain über den Code, den die Miner erzeugen, miteinander verbunden. Dadurch entsteht eben eine „Block-Kette“. Falls nun jemand versuchen würde, eine Transaktion in der Blockchain zu verändern, würden sich auch die Codes der Transaktionsblöcke verändern und die Netzwerkknoten würden dieser Veränderung nicht zustimmen.[13] Es ist demnach zum heutigen Zeitpunkt nicht möglich, Daten in einer Blockchain zu manipulieren oder ohne die entsprechende Berechtigung Daten in der Blockchain abzurufen.





[13] Vgl. Palladino, S. (2019), S.4

Kurze Zusammenfassung der wichtigsten Begrifflichkeiten:

Miner: Miner sind Netzwerkknoten, die Transaktionen nach einem bestimmten Regelwerk validieren, das vorgibt, welche Anforderungen diese erfüllen müssen. Es gibt mehrere Miner in einem Netzwerk und jeder erstellt seinen eigenen „Transaktionsblock“. Nur der, der am schnellsten den richtigen Code findet, darf seinen Transaktionsblock hinzufügen und wird dafür belohnt.

Block Reward: Der Miner, der zuerst den richtigen Code gefunden hat, darf seinen Transaktionsblock der Blockchain hinzufügen. Der Miner erhält dafür die Transaktionsgebühr, die bei einer Bitcoin-Transaktion fällig wird, plus eine festgesetzte Belohnung, den „Block Reward“, der aus einer bestimmten Anzahl von Bitcoins besteht (aktuell 6,25 BTC).

Proof-of-Work: Proof-of-Work ist ein Konsensalgorithmus, bei dem den Miner einen bestimmten Code finden müssen (mithilfe ihrer Hardware). Wer es zuerst schafft, den richtigen Code für einen neuen Block zu finden, darf diesen an die Blockchain anhängen und wird entsprechend belohnt.

ALLE TRANSAKTIONSBLÖCKE SIND IN DER BLOCKCHAIN MITEINANDER VERBUNDEN.

Kritikpunkt – Bitcoin-Mining und Stromverbrauch

Die Bitcoin-Blockchain reguliert sich u. a. durch den Proof-of-Work-Algorithmus selbst. Je schwieriger es für die Miner ist, den richtigen Code zu finden, desto mehr Rechenleistung und Elektrizität benötigen sie, um Transaktionsblöcke zur Blockchain nach dem Proof-of-Work-Konsens hinzuzufügen. Das führte dazu, dass die Mining-Aktivitäten in den letzten Jahren mehr Energie verbrauchten als die Niederlande, Argentinien oder die Schweiz.

Damit das Bitcoin-Mining effizient und profitabel bleibt, haben sich viele große „Mining-Pools“ (große Rechenzentren, die Bitcoin-Mining betreiben) in Regionen niedergelassen, in denen Strom relativ günstig bezogen werden kann. So finden die meisten Bitcoin-Mining-Aktivitäten nach dem „Cambridge Bitcoin Electricity Consumption Index“ in China, den USA und Russland statt.[14]

Jedoch benutzen nicht alle Mining-Pools billigen Strom aus Kohlekraftwerken. Im Oktober 2020 schätzte ein Bericht des „Cambridge Centre for Alternative Finance“, dass im Durchschnitt 39 % der gesamten Energie, die für das Mining verwendet wird, aus erneuerbaren Quellen stammt. 76 % aller Miner nutzten erneuerbare Energien als Teil ihrer Stromversorgung, wobei Wasserkraft mit 62 % eine der häufigsten Energiequellen für Mining-Pools ist.[15] Darüber hinaus gibt es bereits einige Blockchain-Netzwerke neben der Bitcoin-Blockchain, die auf andere Konsens-Algorithmen zurückgreifen, welche keine Elektrizität in diesem Ausmaß benötigen.

[14] Vgl. Cambridge Centre for Alternative Finance (Hrsg.) (2021)
[15] Vgl. Cambridge (Hrsg.) (2020), S. 26

BITCOIN-MINING
BEREITS JETZT MIT
ERNEUERBAREN ENERGIEN

Bitcoin oder Blockchain?

Die Blockchain-Technologie ist alles andere als trivial und die ursprüngliche Idee, den Bitcoin als dezentralisiertes P2P-Zahlungsmittel zu verwenden, hat sich bis heute aufgrund der hohen Wertschwankungen noch nicht durchgesetzt. Ein beliebtes Beispiel hierfür ist der Kauf von zwei Pizzen des Programmierers Laszlo Hanyecz. Hanyecz hatte im Mai 2010 zwei Pizzen bei einem Lieferservice für 10.000 Bitcoins erworben. Beim aktuellen Bitcoin-Kurs (Stand 27. Februar 2021) wären diese beiden Pizzen heute ca. 390 Millionen Euro wert. Ein ähnliches Szenario wurde in einem Bericht der Nachrichtenagentur Reuters geschildert. In diesem hatte 2016 ein Mann für einen Tesla 130.000 US-Dollar in Bitcoins bezahlt, die heute über 14 Millionen US-Dollar wert wären.[16]

Die Fragen, ob sich der Bitcoin jemals als legitimes P2P-Zahlungsmittel durchsetzen kann und was genau den „intrinsischen" Wert des Bitcoins ausmacht, sind also mehr als berechtigt. Basierend auf den veröffentlichten Meinungen und Einschätzungen verschiedener Institute lässt sich lediglich festhalten, dass die Sichtweisen auf den Bitcoin stark unterschiedlich zu sein scheinen: Für den einen ist der Bitcoin ein Spekulationsinstrument, für den anderen eine alternative Anlageklasse, für andere wieder einfach nur Humbug. Sehr häufig wird der Bitcoin auch als „digitales Äquivalent zu Gold" oder „Gold des 21. Jahrhunderts" beschrieben.

Diese Parallelen beziehen sich auf die begrenzte Verfügbarkeit des Bitcoins, denn anders als bei den traditionellen (unlimitierten) Fiatwährungen können nicht beliebig viele Bitcoins erstellt werden. Im Code der Bitcoin-Blockchain wurde bei der Erstellung eine maximale Gesamtmenge von 21.000.000 Bitcoins festgelegt, die nicht überschritten werden kann. Anders als bei Gold ist die Limitierung des Bitcoins jedoch klar ersichtlich. Um zu verhindern, dass die maximal verfügbare Anzahl von Bitcoins zu schnell erreicht wird, wurde im Code der Bitcoin-Blockchain der „Halving"-Mechanismus implementiert. „Halving" bedeutet die Halbierung des Block Rewards, also der Belohnung, die die Miner erhalten, wenn sie einen neuen Block zu der Blockchain hinzugefügt haben.

Das Halving findet alle 210.000 Blöcke statt, und da ca. alle 10 Minuten ein neuer Block erstellt und damit neue Bitcoins erzeugt werden, passiert das Halving ca. alle 4 Jahre. Das erste Halving fand am 28. November 2012 statt. Zu diesem Zeitpunkt wurde der Block Reward von 50 BTC auf 25 BTC gekürzt, am 09. Juli 2016 wiederum auf 12,5 BTC und am 11. Mai 2020 auf 6,25 BTC Belohnung pro erstelltem Block. Durch das Halving wird die Menge an neuerzeugten Bitcoins reduziert, wodurch es bei erhöhter Nachfrage auch zu einem Preisanstieg kommen kann. Dies konnte in den Monaten vor und nach den vergangenen Halvings beobachtet werden, wo es zu teils starken Preisanstiegen gekommen ist. Jedoch waren die Situationen rund um die jeweiligen Halvings immer sehr unterschiedlich, weshalb sich basierend auf diesen Ereignissen keine Schlussfolgerung für zukünftige Verläufe treffen lassen. Beispielsweise haben in den Jahren 2016/2017 noch kaum institutionelle Investoren große Beträge in Bitcoin investiert. Das hat sich im Jahr 2020 stark geändert, u.a. durch große Investitionen von Kryptowährungs-Fondsmanagern wie Grayscale Investments, die mittlerweile über 500.000 Bitcoins in ihrem Bitcoin-Trust-Fonds hält oder eben durch die anfänglich erwähnten Investitionen von Unternehmen wie Microstrategy und Tesla.[17]

Wichtig ist hier zwischen dem Bitcoin und der Blockchain-Technologie zu differenzieren. Der Bitcoin ist auf seinen vermeintlichen Nutzen als P2P-Zahlungsmittel beschränkt – völlig gleich, welcher Wert ihm zugerechnet wird –, während die zugrundeliegende Blockchain-Technologie als verteilte, programmierbare und hochsichere Datenbank viel mehr Anwendungsfälle zulässt. So wird momentan der Einsatz der Blockchain-Technologie im Hinblick auf die Entwicklung von digitalem Zentralbankgeld u. a. von der Europäischen Zentralbank geprüft. Auch in der Finanzindustrie könnte die Blockchain-Technologie Mehrwert liefern, insbesondere im Hinblick auf die Infrastruktur für digitale Wertpapiere. Es gibt mindestens genauso viele Anwendungsmöglichkeiten für die Technologie wie es Meinungen zum Bitcoin gibt – und auch hier gilt es, die zu identifizieren, die langfristig Mehrwert schaffen können.

Vergangene Wertentwicklungen, Simulationen oder Prognosen sind kein zuverlässiger Indikator für die Zukunft. Bitte beachten Sie, dass Kryptowährungen – wie gezeigt – insbesondere hoch komplex sind und starken Kursschwankungen unterliegen. Der Handel mit Bitcoin und anderen Kryptowährungen bzw. darauf bezogenen Finanzinstrumenten ist daher mit erheblichen Risiken verbunden und kann bis hin zum Totalverlust des eingesetzten Kapitals führen. Auch sind etwa Totalverluste durch Hackerangriffe auf Wallets möglich.

[16] Vgl. Reuters (Hrsg.) (2021)

[17] Vgl. Grayscale Investments (Hrsg.) (2021)

Wichtige Hinweise

Diese Publikation ist eine Kundeninformation der ODDO BHF Aktiengesellschaft, Bockenheimer Landstraße 10, 60323 Frankfurt am Main (nachfolgend „ODDO BHF“). Sie enthält Informationen, die aus öffentlichen Quellen stammen, die wir für verlässlich halten, für deren Verlässlichkeit wir jedoch keine Gewähr übernehmen können. Die ODDO BHF übernimmt weder eine rechtliche Verbindlichkeit, noch garantiert sie die Aktualität, Vollständigkeit und Fehlerfreiheit etwaiger in dieser Unterlage enthaltener Meinungen, Vorhersagen, Schätzungen und Prognosen. Zusätzlich ist die ODDO BHF nicht verpflichtet, den jeweiligen Inhalt zu aktualisieren, an Änderungen anzupassen oder zu vervollständigen, oder den Empfänger in anderer Weise zu informieren, falls sich eine dieser Aussagen verändert hat oder unrichtig, unvollständig oder irreführend wird.

Weder dieses Dokument noch irgendeine in Verbindung hiermit gemachte Aussage stellt ein Angebot, eine Aufforderung oder eine Empfehlung zum Erwerb oder zur Veräußerung von Finanzinstrumenten im Sinne des Wertpapierhandelsgesetzes bzw. des Kreditwesengesetzes (einschließlich etwa Bitcoins) dar. Insbesondere berücksichtigt dieses Dokument nicht Ihre persönlichen Umstände und Verhältnisse und ist somit für sich allein genommen weder dazu geeignet noch dazu bestimmt, eine individuelle anleger- und anlagegerechte Beratung zu ersetzen.

Redaktionell verantwortlich: Sandra Sohn und Alexander Eimermacher. Etwaige Meinungsäußerungen in dieser Publikation geben die Einschätzung der Autoren zum Zeitpunkt der Erstellung wieder, die sich insbesondere von der Hausmeinung innerhalb der ODDO BHF Gruppe unterscheiden und ohne vorherige Ankündigung ändern kann.

Die ODDO BHF untersteht der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Straße 108, 53117 Bonn und Marie-Curie-Straße 24-28, 60439 Frankfurt am Main sowie der Europäischen Zentralbank, Sonnemannstraße 20, 60314 Frankfurt am Main.

Ohne vorherige schriftliche Zustimmung von ODDO BHF darf/dürfen diese Unterlage, davon gefertigte Kopien oder Teile davon nicht verändert, kopiert, vervielfältigt oder verteilt werden. Mit Entgegennahme der Unterlage erklärt sich der Empfänger mit den vorangegangen Bestimmungen einverstanden.

Quellen

Attaran, Mohsen/Gunasekaran, Angappa (2019): Applications of Blockchain Technology in Business, Challenges and Opportunities, Cham.

Bajpai, Prableen (2019): How to Buy Bitcoin. Online unter https://www.investopedia.com/tech/how-to-buy-bitcoin/, Abruf am 09.03.2021.

Bloomberg (Hrsg.) (2021): Bitcoin Is the Scarcest Asset, MicroStrategy CEO Saylor Says. Online unter: https://www.bloomberg.com/news/articles/2021-02-08/bitcoin-is-the-scarcest-asset-microstrategy-ceo-saylor-says, Abruf am 09.03.2021.

Brühl, Volker/Dorschel, Joachim (2018): Praxishandbuch Digital Banking, Wiesbaden.

Cambridge Center for Alternative Finance (Hrsg.) (2021): Cambridge Bitcoin Electricity Consumption Index. Online unter: https://cbeci.org/, Abruf am 09.03.2021.

CNBC (Hrsg.) (2021): Tesla buys $1.5 billion in bitcoin, plans to accept it as payment. Online unter: https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html, Abruf am 09.03.2021.

Dannen, Chris (2017): Introducing Ethereum and Solidity Foundations of Cryptocurrency and Blockchain Programming for Beginners.

Dhillon, Vikram/Hooper, Max/Metcalf, David (2017): Blockchain Enabled Applications, New York.

Drescher, Daniel (2017): Blockchain basics, a non-technical introduction in 25 steps, New York.

Elrom, Elad (2019): The Blockchain Developer, A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects. New York.

Fill, Hans-Georg/Meier, Andreas (2020): Blockchain kompakt, Grundlagen, Anwendungsoptionen und kritische Bewertung. Wiesbaden.

Grayscale (Hrsg.) (2021): Grayscale Bitcoin Trust. Online unter: https://grayscale.co/bitcoin-trust/, Abruf am 03.09.2021.

Handelsblatt (Hrsg.) (2018): Starökonom Roubini schießt gegen Kryptowährungen – „Die Mutter aller Betrügereien“. Online unter: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/bitcoin-und-co-staroekonom-roubini-schiesst-gegen-kryptowaehrungen-die-mutter-aller-betruegereien/23178166.html, Abruf am 09.03.2021.

Himmer, Klaus (2019): Blockchain-basiertes Fundraising als innovative Alternative der Unternehmensfinanzierung, Eine steuer- und aufsichtsrechtliche Analyse, Wiesbaden.

Kohn, Wolfgang/Tamm, Ulrich (2019): Mathematik für Wirtschaftsinformatiker, Berlin.

Microstrategy (Hrsg.) (2021): MicroStrategy Acquires Additional 19,452 Bitcoins for $1.026 Billion. Online unter: https://www.microstrategy.com/content/dam/website-assets/collateral/financial-documents/press-release-archive/microstrategy-acquires-additional-19452-bitcoins-for-1-026-billion_02-24-2021.pdf, Abruf am 09.03.2021.

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. Online unter https://bitcoin.org/bitcoin.pdf, Abruf am 09.03.2021.

Palladino, Santiago (2019): Ethereum for Web Developers.

Paypal (Hrsg.) (2021): PayPal Launches New Service Enabling Users to Buy, Hold and Sell Cryptocurrency. Online unter: https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency, Abruf: 09.03.2021.

Reuters (Hrsg.) (2021): Analysis: Can you buy a Tesla with bitcoin? How the payments might work. Online unter: https://www.reuters.com/article/us-crypto-currency-tesla-payments-idUSKBN2A82O0, Abruf am 09.03.2021.

Rutz, Victor (2020): Blockchain quo vadis, Eine Stärken-Schwächen-Analyse des Private- und des Public-Blockchain Ansatzes. Wiesbaden.

Schacht, Sigurd/Lanquillon, Carsten (2019): Blockchain und maschinelles Lernen, Wie das maschinelle Lernen und die Distributed-Ledger-Technologie voneinander profitieren. Berlin.

University of Cambridge (Hrsg.) (2020): 3rd Global Cryptoasset Benchmarking Study. Online unter: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/, Abruf am 09.03.2021.

www.oddo-bhf.com