Julia Fohrer

KRYPTO WIKI

Diese Begriffe solltest Du kennen!

Krypto- und Blockchain

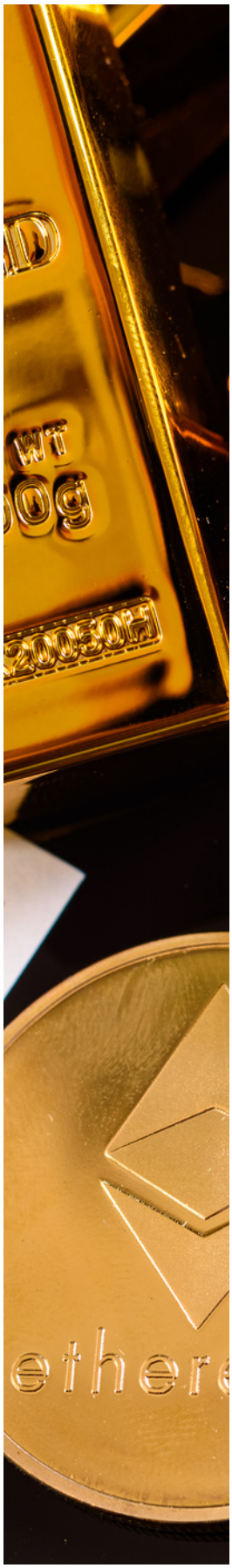
Englische Wörter und Abkürzungen kommen bei dem Thema Kryptowährungen häufig über den Weg. Was erstmal kompliziert klingt, erklären wir dir ganz einfach. Blockchain ist ein relativ neuer Begriff. Drum herum sind auch viele Begriffe entstanden, die vielen Menschen noch nicht so geläufig sind. Mit diesem kleinen und feinen Nachschlagewerk bieten wir jedem die Möglichkeit, sich einzulesen und auf den neuesten Stand zu bringen.

51%-Angriff

Ein 51%-Angriff liegt vor, wenn ein oder mehrere Validierungsknoten mehr als die Hälfte der Rechenleistung des Netzwerks kontrollieren und damit die Kontrolle über den Transaktionsfluss der Blockchain übernehmen können. Sobald sie dies erreicht haben, können diese Knoten manipulieren, welche Transaktionen validiert werden, während andere Transaktionen nicht aufgezeichnet werden. Bei einem 51%-Angriff sind die kontrollierenden Knoten in der Lage, alle Transaktionen rückgängig zu machen, die in der Zeit, in der sie die Kontrolle hatten, hinzugefügt wurden. Sie können auch Token doppelt ausgeben - wenn eine digitale Währung zweimal ausgegeben wird. Dadurch wird die Integrität des Netzwerks beeinträchtigt und der Wert des Tokens sinkt.

Adresse

Die Adresse ist ein öffentlicher Teil jeder Transaktion. Will man eine Krypto-Zahlung empfangen, gibt man für diese Transaktion seine Adresse heraus. Zudem ist sie Bestandteil des Public Key, also der Signierung von einzelnen Transaktionen. Die Adresse ist ein sogenannter Hash-Wert und besteht aus alphanumerischen Zeichen, welche als QR-Code dargestellt werden können. Diese Form der Darstellung erleichtert gerade das Erfassen des Bitcoin-Adresse per Smartphone.



Airdrop

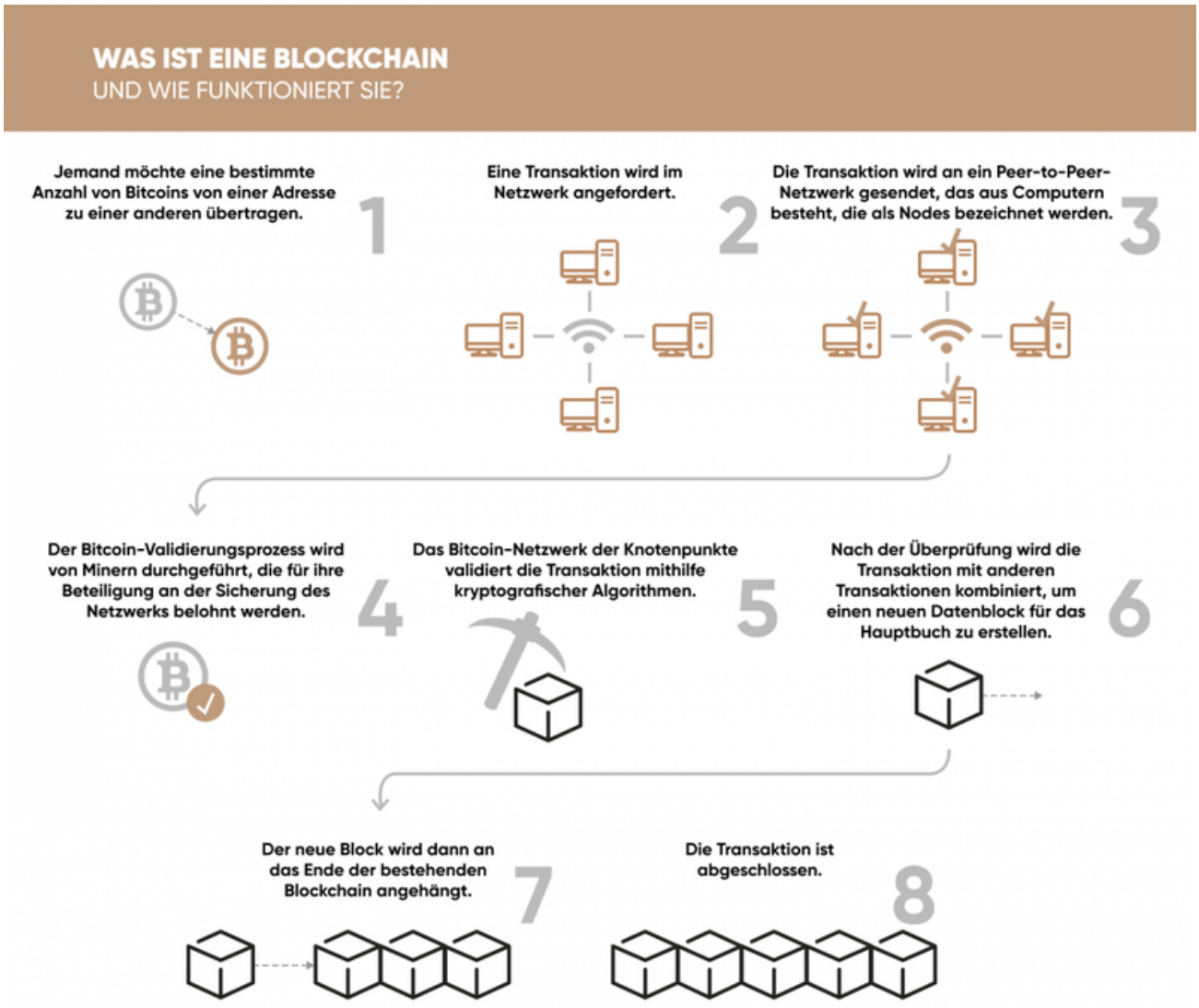
Als Airdrop ("aus der Luft fallend") wird eine Marketingstrategie im Bereich der Kryptowährungen bezeichnet, bei welcher Coins oder Token kostenlos entweder gezielt an einzelne Investoren oder per Zufall an verschiedene Wallet-Adressen verteilt werden. Die Initiatoren erhoffen sich dadurch meistens eine größere Bekanntheit ihrer eigenen Kryptowährung.

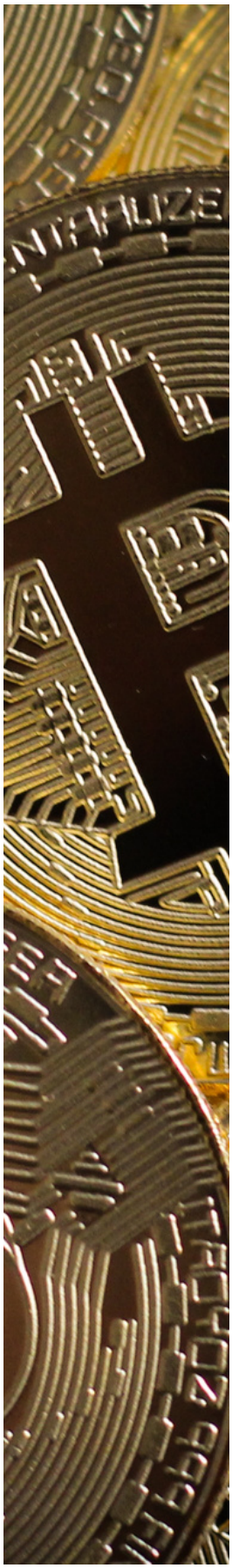
Altcoin

Altcoin, die Abkürzung für Alternative Coin, bezieht sich auf jeden Token, der kein Bitcoin ist. Da Bitcoin der Pionier des Kryptowährungsökosystems war, werden alle Token, die nach BTC eingeführt wurden, von einigen als Alternativen zu Bitcoin betrachtet. Allerdings sind nicht alle Token gleich. Der Ethereum (ETH)-Token beispielsweise wird heutzutage als Utility-Token betrachtet, da die Ethereum-Blockchain Hunderte von dezentralen Anwendungen antreibt. Uniswap (UNI) ist eines der beliebtesten dezentralen Handelsprotokolle, das den automatisierten Handel mit dezentralen Finanz-Token (DeFi) ermöglichen soll. Ende Juli 2021 waren die fünf größten Altcoins nach Marktkapitalisierung laut CoinMarketCap folgende: Ethereum (ETH), Tether (USDT), Binance Coin (BNB), Cardano (ADA) und Ripple (XRP).

Blockchain

Eine Blockchain ist ein virtuelles Hauptbuch, in dem Transaktionen sicher aufgezeichnet werden können. Sie ist „dezentralisiert“, was bedeutet, dass es keine zentrale Behörde gibt, die die Dinge steuert. Stattdessen muss jeder neue Datensatz von einem mit dem Netzwerk verbundenen Computer, einem „Knoten“, validiert werden, bevor er registriert werden kann.
Der Name Blockchain kommt von der Struktur des Netzwerks, in dem jeder Datensatz als „Block“ bezeichnet wird. Neue Blöcke, die in fortlaufender Reihenfolge hinzugefügt werden, bilden eine „Kette“.
In einer Blockchain gespeicherte Datensätze können nicht geändert oder gelöscht werden. Stattdessen muss eine neue Transaktion durchgeführt werden, um Fehler oder Irrtümer aus früheren Transaktionen zu korrigieren. Dadurch wird verhindert, dass sie manipuliert werden.





BTC = Bitcoin

BTC ist eine geläufige Abkürzung für eine Bitcoin-Einheit. Es ist ebenfalls das Kürzel für Bitcoin an der Börse.

Client

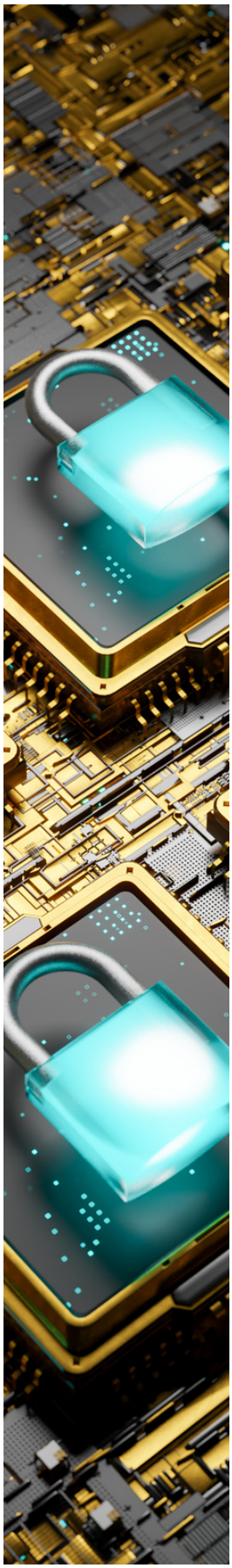
Bei einem Client handelt es sich um eine Software. Ein Client kann sowohl auf einem mobilen Endgerät, einem Computer oder auch einem Laptop installiert werden. Über den Client wird das Gerät und sein Nutzer mit dem Bitcoin-Netzwerk verbunden. Über ihn werden die verschiedenen Transaktionen des Users abgewickelt und er enthält in einigen Fällen bereits ein Wallet.

CEX

s. "DEX/CEX"

Cloud Mining

Will man Bitcoins – oder eine andere Kryptowährung – erzeugen, muss man über Rechenleistung verfügen. Hier hat man als User zwei Möglichkeiten: sich sogenannte Mining-Hardware anzuschaffen oder aber die benötigte Rechenleistung in einer Cloud zu mieten oder zu kaufen. Gängige Methode ist dabei für die meisten Nutzer das Mieten in der Cloud. Hier wird ihnen von den Anbietern die benötigte Infrastruktur geliefert. Der Anbieter betreibt zudem die Mining-Hardware, so dass der User ohne großen Aufwand loslegen kann mit dem Mining.



Dezentrales System

Eine zentrale Eigenschaft der Blockchain ist ihre Funktion als dezentrales System. Das bedeutet, dass es statt einem zentralen Netzwerk ein sogenanntes Peer-to-Peer-Netzwerk ist. Die gesamten Daten werden gleichberechtigt zwischen allen Usern geteilt. Das Transaktionsregister, auch als distributed ledger bezeichnet, ist dabei auf alle Knoten oder Noldes des gesamten Netzwerks verteilt. Alle Nutzer verfügen über die gleichen Rechte und einen gleichberechtigten Zugriff auf die Informationen. Bei jeder Transaktion werden die dazugehörigen Informationen in jedem Knoten gespeichert. Das dezentrale System schützt sich auf diese Weise gegen Manipulationen. Durch seine selbstverwaltende Funktion ist es zudem deutlich geschützter gegenüber Machtmissbrauch als herkömmliche Systeme.

Dezentralisierte Anwendungen (dApps)

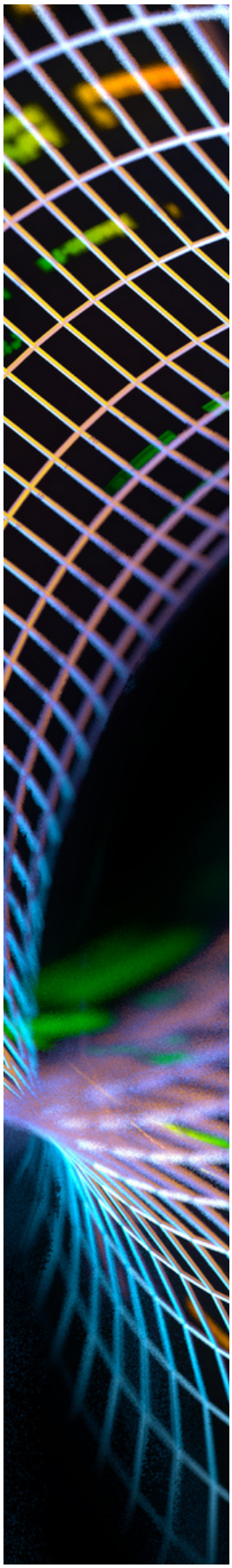
Das Akronym dApp bezieht sich auf eine „dezentrale Anwendung“ - ein Programm, das auf einer bestehenden Blockchain aufbaut. Der Unterschied zwischen einer normalen Anwendung und einer dApp besteht darin, dass Transaktionen über die Infrastruktur der Blockchain validiert werden, ohne dass ein Vermittler erforderlich ist.

DEX/CEX

Eine dezentrale Börse (DEX) ist eine Börse, über die Krypto-Transaktionen ohne die Beteiligung eines Mittelsmannes abgewickelt werden. Sie gelten als echte Peer-to-Peer-Plattformen. Sie funktionieren über eine Reihe von intelligenten Verträgen, die bei jeder Transaktion generiert werden, während alle Transaktionsdatensätze in der Blockchain aufgezeichnet werden.
Eine zentralisierte Börse (CEX) nimmt im Namen Dritter Aufträge zum Kauf, Verkauf, Umtausch und Transfer von Kryptowährungen entgegen und führt diese aus.

Difficulty

Der Begriff Difficulty oder auch Mining Difficulty fällt im Zusammenhang mit dem Hashen eines neuen Blocks. Dabei steigt die Difficulty mit der Rechenleistung des Kryptowährungsnetzwerkes. Sprich: Umso höher die Rechenleistung des Kryptowährungsnetzwerks, desto höher die Mining Difficulty. Da das Netzwerk lebendig ist, bleibt auch der Wert der Difficulty in Bewegung.
Die Schwierigkeit beim Hashen eines Blocks hängt damit zusammen, wie viele Hashes maximal in einem Transaktionsblock erlaubt sind. Wenn die Anzahl an Hashes geringer ist, wird das Erzeugen eines Hashes schwieriger. Durch den Popularitätsgewinn von Bitcoin steigt die Netzwerkleistung durch mehr Miner und damit steigt zugleich die Schwierigkeit.

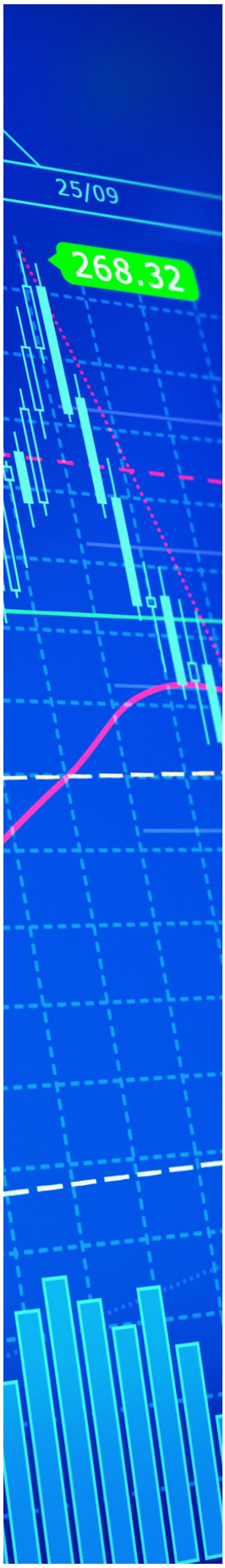


Distributed Ledger Technology (DLT)

Jegliches dezentrale und digital geführte Kontenbuch wird unter dem Oberbegriff Distributed Ledger Technology zusammengefasst. Den Begriff gibt es dementsprechend bereits länger als die Blockchain Technologie. Eine Blockchain ist so nur eine von unterschiedlichen DLT. Allerdings unterscheidet sich die Blockchain durch ihre Komplexität von anderen DLT, die einen anderen Rahmen benötigen, um funktionieren zu können. Die Blockchain hingegen ist so komplex gebaut, dass sie autonom und in sich geschlossen agieren kann. Dieser Umstand hebt sie bei den DLT hervor.

Doppelausgabe / Double Spending

Bei vielen Nutzern besteht die Angst vor einer Manipulation der Blockchain, beispielsweise durch das sogenannte Double Spending. Dabei wird vom User versucht, die gleichen Bitcoins parallel an unterschiedliche Empfänger zu verteilen. Diese Doppelausgabe von Bitcoins werden jedoch durch unterschiedliche Sicherheitsmechanismen erschwert. Zum einen wäre dabei das Bitcoin Mining und zugleich auch die Beschaffenheit der Blockchain mit ihren Rückversicherungen. An diesen Kontrollen scheitern die Versuche von Double Spending in der Regel.



Exchange

Proof of Work, zu deutsch: Arbeitsnachweis. Nach vollbrachter Arbeit bekommt man seine Entlohnung. Dieses Prinzip nutzt auch die Blockchain. Jede Transaktion muss vom Netzwerk überprüft und genehmigt werden. Damit werden Betrug und Hackerangriffe ausgeschlossen. Die Überprüfung wird durch Arbeiter, so genannte Miner, im Blockchain Netzwerk sichergestellt. Die Miner stellen Rechenleistung zur Verfügung, welche Rechenaufgaben lösen muss. Für die bereitgestellte Rechenleistung sowie den damit verbunden Zeit- und Stromkosten wird der Miner entlohnt.

Fungible und nicht-fungible Token

Der Begriff fungibel bezieht sich auf eine der wichtigsten Eigenschaften von Blockchains und den Token, die sie antreiben. Ein fungibler Vermögenswert bezieht sich in wirtschaftlicher Hinsicht auf seine Austauschbarkeit mit einem anderen Vermögenswert oder einer Ware desselben Wertes. Ein Beispiel für einen fungiblen Vermögenswert ist Fiatgeld, da man Dollarscheine gegen Waren und Dienstleistungen eintauschen kann.
In der Blockchain-Welt kann ein fungibler Token gegen einen anderen Vermögenswert oder Token getauscht werden. Auf der anderen Seite unterscheiden sich nicht-fungible Token von fungiblen Token, da sie keinen inhärenten Wert besitzen und nicht mit anderen Token ausgetauscht werden können.

FUNGIBLE TOKEN	NICHT-FUNGIBLE TOKEN
Auswechselbar Ein Token kann gegen jeden anderen Token desselben Typs ausgetauscht werden.	**Nicht austauschbar** Eine NFT kann nicht gegen eine andere NFT desselben Typs ausgetauscht werden.
Uniform Alle Spielsteine desselben Typs sind identisch.	**Einzigartig** Jeder Token ist einzigartig und unterscheidet sich von allen anderen Token desselben Typs.
Teilbar Funbigle-Münzen können in kleinere Teile aufgeteilt werden.	**Nicht teilbar** NFTs können nicht geteilt werden und haben ihren Wert als Ganzes.
ERC-20-Standard Fungible-Token basieren auf dem Ethereum-Standard ERC-20.	**ERC-721-Norm** Nicht-fungible Token verwenden einen neuen ERC-721-Ethereum-Standard.

Fork

s. "Hard Fork und Soft Fork"

Gas und Gasgebühren

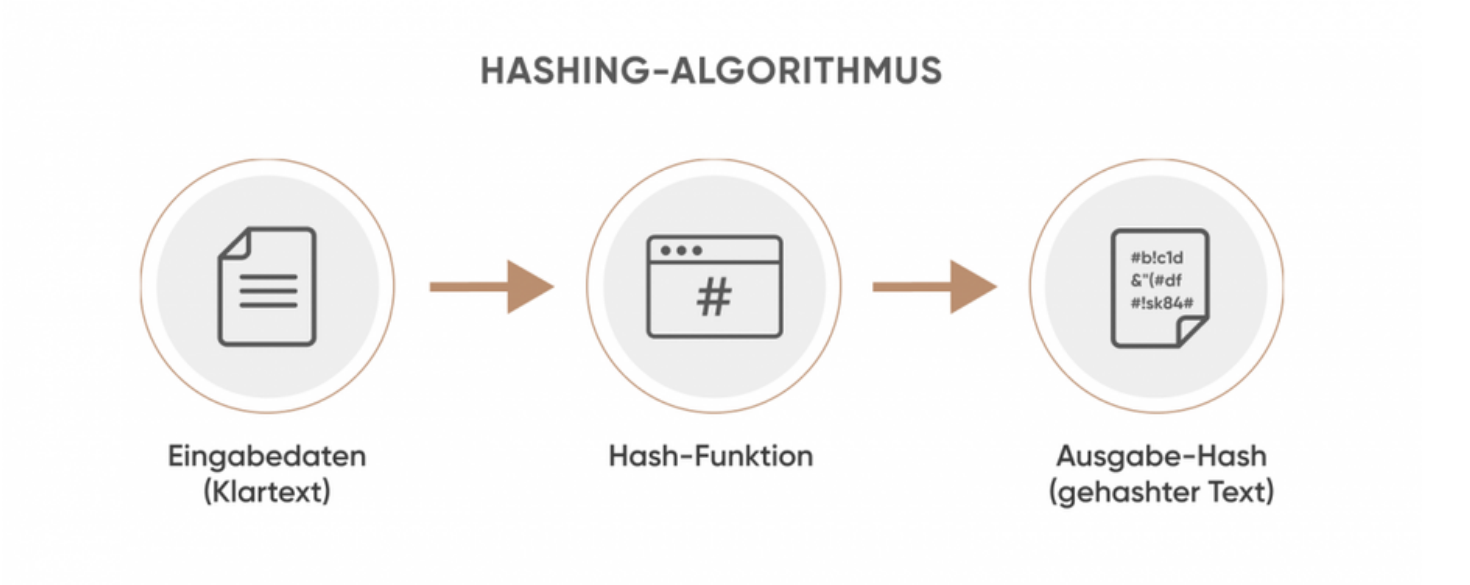
Gas bezieht sich auf den Rechenaufwand, der erforderlich ist, um das spezifische Rätsel zu lösen, das dem Abbau eines Blocks oder der Aufzeichnung einer einzelnen Transaktion zugeordnet ist. Die Menge an Gas, die zur Durchführung dieser Operationen erforderlich ist, bestimmt die Höhe der zu zahlenden Gasgebühren.
Bei den Gasgebühren handelt es sich um die Kosten für die Aufzeichnung einer Transaktion auf einer bestimmten Blockchain, die üblicherweise als Dezimalwert des Tokens, mit dem das Netzwerk betrieben wird, oder in einer Fiat-Währung wie US-Dollar ausgedrückt werden. Je höher das von Ihnen festgelegte Gaslimit ist, desto schneller wird Ihre Transaktion verifiziert und zur Blockchain hinzugefügt.

Hash

Ein Hash ist eine Funktion, die eine beliebige Eingabe in eine verschlüsselte Sprache umwandelt. In der Blockchain-Welt wird ein Hash erzeugt, nachdem die Daten einer Transaktion validiert und im Netzwerk aufgezeichnet wurden.

Hashes haben eine feste Länge. Dies erhöht die Sicherheit, da niemand den Inhalt eines Hashes ohne die spezifische Referenztabelle entschlüsseln kann, die zur Erstellung des Hashes verwendet wurde.

Die Arbeit der Miner besteht darin, jede Art von Aufzeichnung, die in die Blockchain aufgenommen wird, zu verschlüsseln, indem sie einer bestimmten Hash-Struktur folgen, die mehrere Abschnitte umfasst. Diese Abschnitte enthalten u. a. Informationen über den Zeitstempel des vorherigen Hash, den vom vorherigen Block erzeugten Hash und den Ziel-Hash. Die Hash-Strukturen variieren von Blockchain zu Blockchain, je nachdem, was der Entwickler bevorzugt.



Hard Fork und Soft Fork

Eine Abspaltung (Fork) liegt vor, wenn eine neue Blockchain als Ergebnis einer Änderung des Quellcodes des ursprünglichen Projekts erstellt wird. Die ursprüngliche Blockchain und die Abspaltung arbeiten jeweils nach anderen Regeln.

Bei einer harten Abspaltung (Hard Fork) werden von einer Gruppe von Knoten neue Regeln vorgeschlagen, die mit den vom Konsens (dem Protokoll, das die Integrität der Plattform aufrechterhält) festgelegten Regeln unvereinbar sind. Dies führt zur Schaffung einer neuen Blockchain, die nach den neuen Regeln funktioniert.

Ein Soft Fork tritt auf, wenn andere, aber mit dem Konsens kompatible Regeln eingeführt werden, was zur Schaffung einer neuen Blockchain führt, die noch mit der ursprünglichen kommunizieren kann, aber unabhängig arbeitet.

KRYPTOWÄHRUNG FORK

Hard fork	Soft fork
Eine radikale Änderung des Protokolls eines	Eine Aktualisierung der Software eines Kryptowährungsprotokolls
Größere Software-Aktualisierung, die mit älteren Versionen nicht kompatibel ist	Kleines Software-Update, das mit älteren Versionen kompatibel ist
Kann die Erstellung einer neuen Blockchain auslösen	Bringt neue Regeln in das Netzwerk, ist aber abwärtskompatibel

ICO/IEO

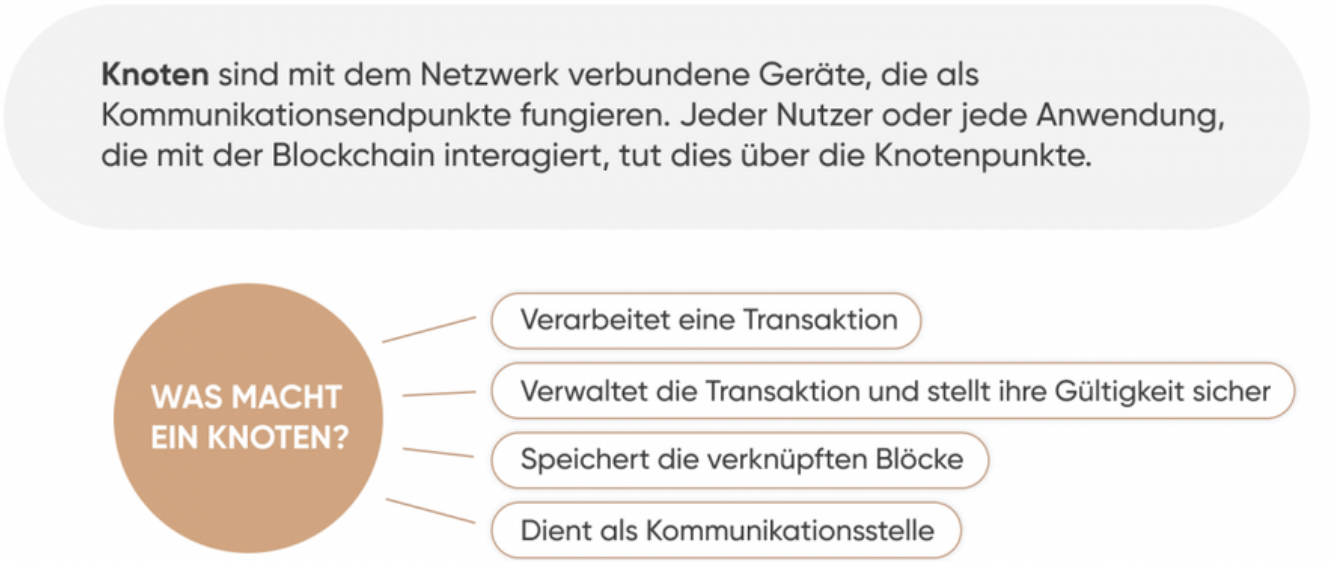
Sowohl bei Initial Coin Offerings (ICOs) als auch bei Initial Exchange Offerings (IEOs) handelt es sich um Verfahren, mit denen ein Blockchain-Projekt durch den Verkauf einer bestimmten Anzahl von Token an die Investorengemeinschaft Mittel aufbringen kann.
Bei einem ICO ist kein Mittelsmann erforderlich, da das Projekt Geld von jedem aufnehmen kann, der bereit ist, Fiat-Geld oder andere Token im Austausch gegen das projekteigene Token zu tauschen.
In der Zwischenzeit müssen IEOs von der Börse zugelassen werden, über die die Münzen den Anlegern angeboten und verkauft werden sollen. In den meisten Fällen werden IEOs nur über eine einzige exklusive Börse angeboten, was die Zahl der Anleger, die sich beteiligen können, einschränkt.

Initial Coin Offering (ICO)

ICO – Initial Coin Offering, zu deutsch: Erstangebot von Coins ist eine Form einer Gruppenfinanzierung oder auch bekannt als Crowdfunding. Neue Krypto-Unternehmen möchten mit dieser Methode Kapital sammeln, indem erste Coins der neuen Kryptowährung an Investoren verkauft werden. Durch dieses Vorgehen erhalten Jungunternehmen Liquidität, ohne dafür einen Kredit aufnehmen zu müssen. Vergleich kann man das auch mit einem Börsengang (Verkauf von Firmenanteilen).

Knoten

Ein Knoten ist ein Terminal, das mit der Blockchain verbunden ist. Er dient der Aufrechterhaltung der Integrität des Netzwerks durch die konsistente Validierung neuer Blöcke, die hinzugefügt werden.
Ein aktiver Knoten speichert zu jeder Zeit die aktuellste Version der Blockchain. Er kommuniziert ständig mit anderen Knoten, um sie über alle Änderungen an der Kette zu informieren.



Know Your Customer (KYC)

KYC bedeutet „Kenne deinen Kunden“. Es beschreibt den Prozess der Überprüfung der Identität von (neuen) Kunden. Der KYC-Prozess wird durchgeführt, um illegale Aktivitäten wie Geldwäsche oder Betrug zu verhindern und damit sowohl das Unternehmen als auch den Kunden zu schützen.

Krypto-Geldbörsen

Eine Wallet ist eine Anwendung, in der Krypto-Token sicher aufbewahrt werden können. Da es sich bei Krypto-Token im Wesentlichen um Code handelt, fungiert eine Wallet als Ort, an dem diese Codes geparkt werden. Eine Wallet verhindert, dass Dritte ohne die Erlaubnis des Besitzers auf die Codes zugreifen können.

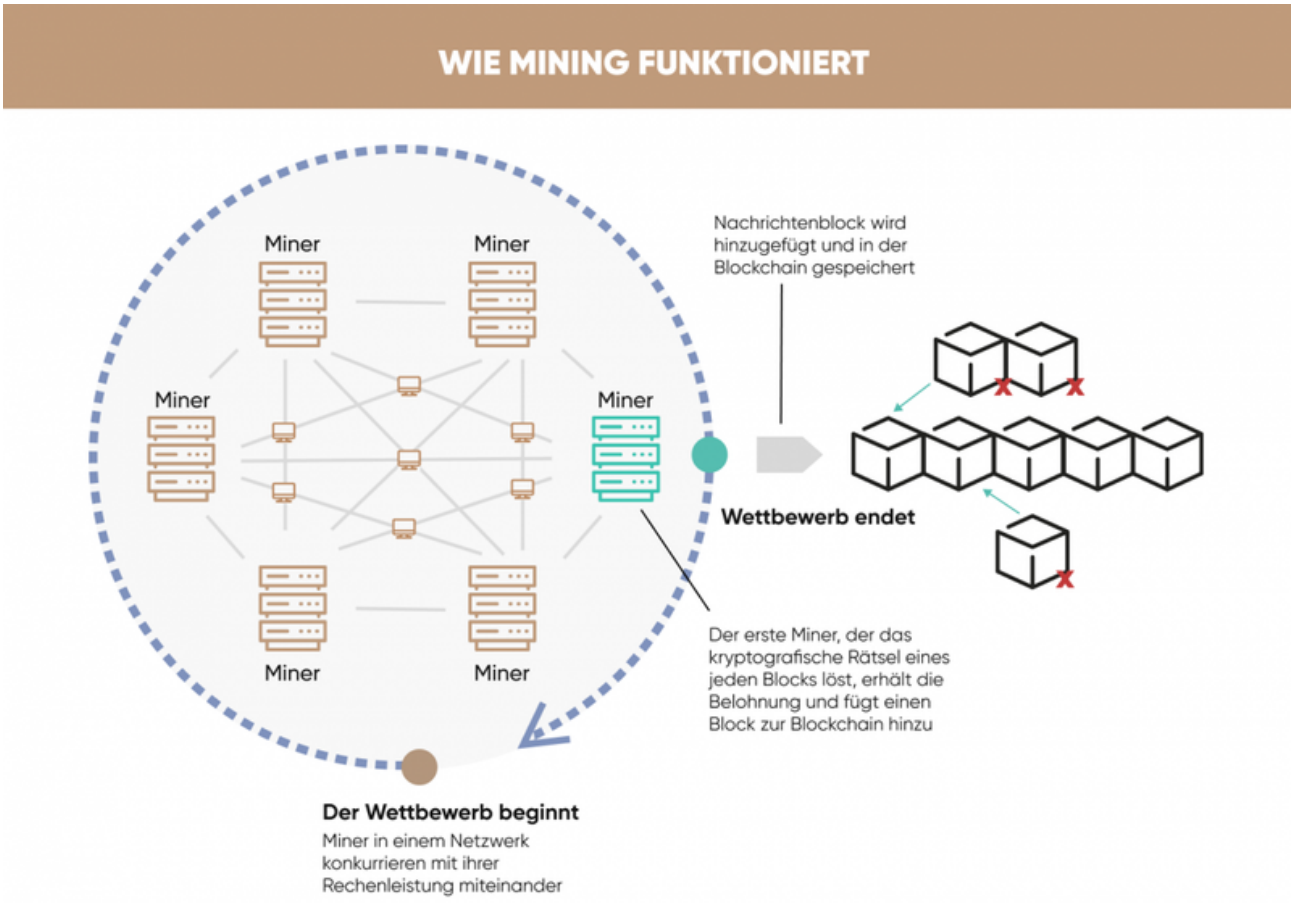
Es gibt verschiedene Arten von Wallets, darunter Cold Wallets (ohne Internetverbindung) und Hot Wallets (mit Zugriff über das Internet). Es gibt Hardware-Geldbörsen, bei denen es sich um physische Geräte wie eine Festplatte handelt. Auf mobile und Desktop-Geldbörsen kann nur über ein Smartphone bzw. einen PC zugegriffen werden.

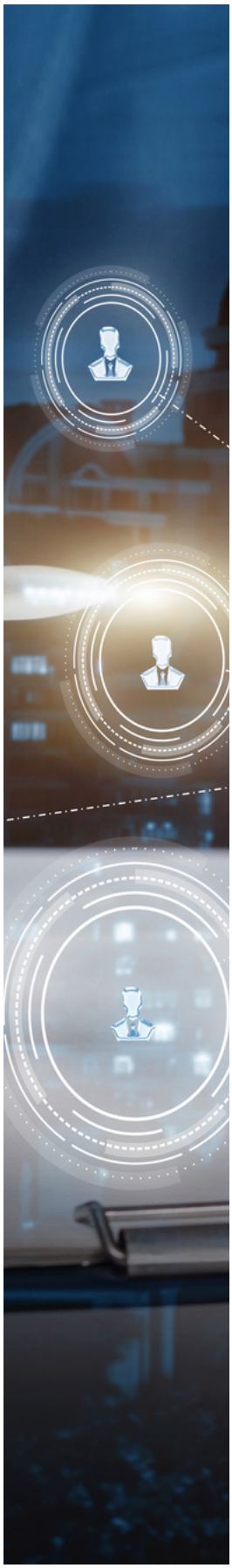
5 ARTEN VON CRYPTOCURRENCY-WALLETS

Typ	Beschreibung	Vorteile	Nachteile
Online-Geldbörse	Zugriff auf Krypto-Vermögenswerte über das Internet ermöglicht. Nutzer können Kryptowährungen erreichen, speichern und Zahlungen vornehmen. Der Anbieter der Online-Geldbörse speichert den privaten Schlüssel der Kryptowährung auf seinem Server.	• Ermöglicht schnelle Transaktionen • Kann mehrere Kryptowährungen verwalten • Geeignet für aktiven Handel	• Risiko von Online-Hacks • Risiko von Computerviren • Beteiligung eines Dritten an der Aufbewahrung Ihres Vermögens
Mobile Geldbörse	Über eine App auf Ihrem Mobiltelefon verfügbar.	• Überzeugend für den Einsatz unterwegs • Bietet zusätzliche Funktionen wie das Scannen von QR-Codes	• Risk of losing your crypto assets if your phone is lost or damaged • Risiko von Handy-Viren
Desktop-Brieftasche	Eine Desktop-Geldbörse wird auf Ihrem Computer installiert. Kann als kalte Geldbörse verwendet werden, wenn Sie nicht mit dem Internet verbunden sind.	• Bequeme Nutzung vom Desktop aus • Private Schlüssel werden nicht auf einem Server eines Dritten gespeichert • Könnte sicherer sein als Online-Geldbörsen, wenn keine Verbindung zum Internet besteht	• Unterwegs schwieriger zu benutzen • Weniger sicher, wenn sie mit dem Internet verbunden sind • Wenn Ihr Computer ausfällt und Sie keine Sicherungskopie erstellt haben, können Sie Ihre Daten verlieren
Hardware-Geldbörse	Speichert Ihre privaten Schlüssel auf einem Gerät wie einem USB-Treiber. Sie können immer noch Online-Transaktionen durchführen, aber da es die meiste Zeit offline ist, können Sie es als kalte Brieftasche betrachten.	• Schützt private Verschlüsselungen der Nutzer, die auf dem Gerät gespeichert sind • Geeignet für die Speicherung großer Mengen von Kryptowährungen, die Sie nicht täglich verwenden	• Ziemlich teuer • Nicht sehr praktisch für den aktiven Handel
Papier Geldbörse	Die 'kälteste' Krypto-Geldbörse. Sie drucken Ihre privaten und öffentlichen Schlüssel aus und können Transaktionen durch Scannen eines QR-Codes auf der Papiergeldbörse durchführen.	• Hacksicher • Nicht auf einem beweglichen Gerät oder Computer gespeichert • Nicht auf einem Server eines Drittanbieters gespeichert	• Schwerer zu handhaben bei alltäglichen Transaktionen • Sie müssen sich um das Stück Papier kümmern!

Mining (Proof-of-Work)

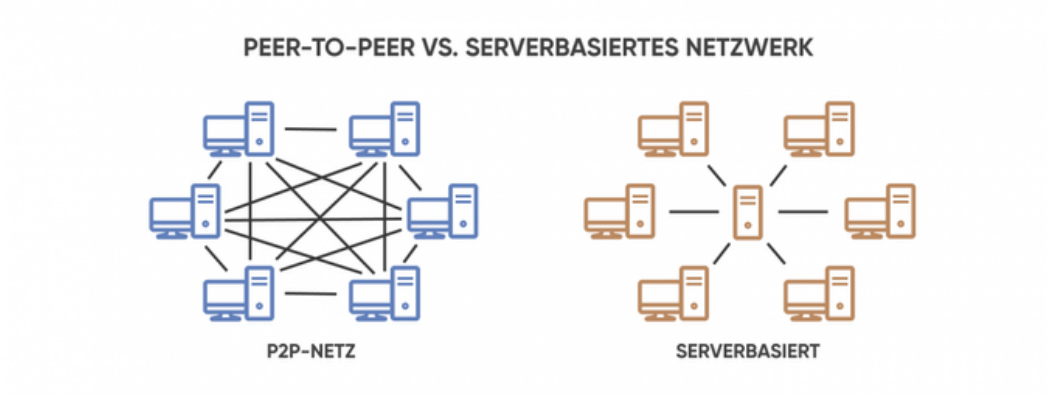
Das Protokoll, das das Bitcoin-Netzwerk antreibt, ist als Proof-of-Work (PoW) bekannt. Es ist ein Konsensmechanismus, der verwendet wird, um neue Transaktionen zu validieren, die in die Blockchain aufgenommen werden sollen. Obwohl theoretisch jede Person ein „Miner“ werden kann, ist dieser Prozess in der Praxis sehr energieaufwändig und erfordert eine Menge Rechenleistung, Spezialausrüstung und Platz für Hochgeschwindigkeitsserver. Damit eine Transaktion validiert werden kann, muss ein Miner oder ein Knotenpunkt, der aus mehreren leistungsstarken Computern besteht, ein zufälliges mathematisches Rätsel lösen, um den „Hash“ zu erzeugen, der den neuen Datensatz identifiziert. Im Falle von Bitcoin wird für jeden Datensatz ein SHA-256-Hash erzeugt. Ein Hash ist eine eindeutige Nummer zur Identifizierung des Datensatzes. Das verteilte Hauptbuch wird dann entsprechend aktualisiert, so dass jeder die Integrität der neuen und aktualisierten Datensätze überprüfen kann.
In einem Proof-of-Work-Ökosystem werden die Miner entschädigt, indem sie eine bestimmte Anzahl von Token für die Validierung der in der Blockchain enthaltenen Transaktionen erhalten.





Peer-to-Peer

Peer-to-Peer bezieht sich auf die Interaktion zwischen zwei Parteien direkt, ohne die Notwendigkeit eines Vermittlers. Im Wesentlichen sind alle Blockchains als Peer-to-Peer-Plattformen konzipiert, über die alles ausgetauscht werden kann, ohne dass eine dritte Partei zur Validierung des Vorgangs hinzugezogen wird, da diese Funktion von der Blockchain selbst übernommen wird.

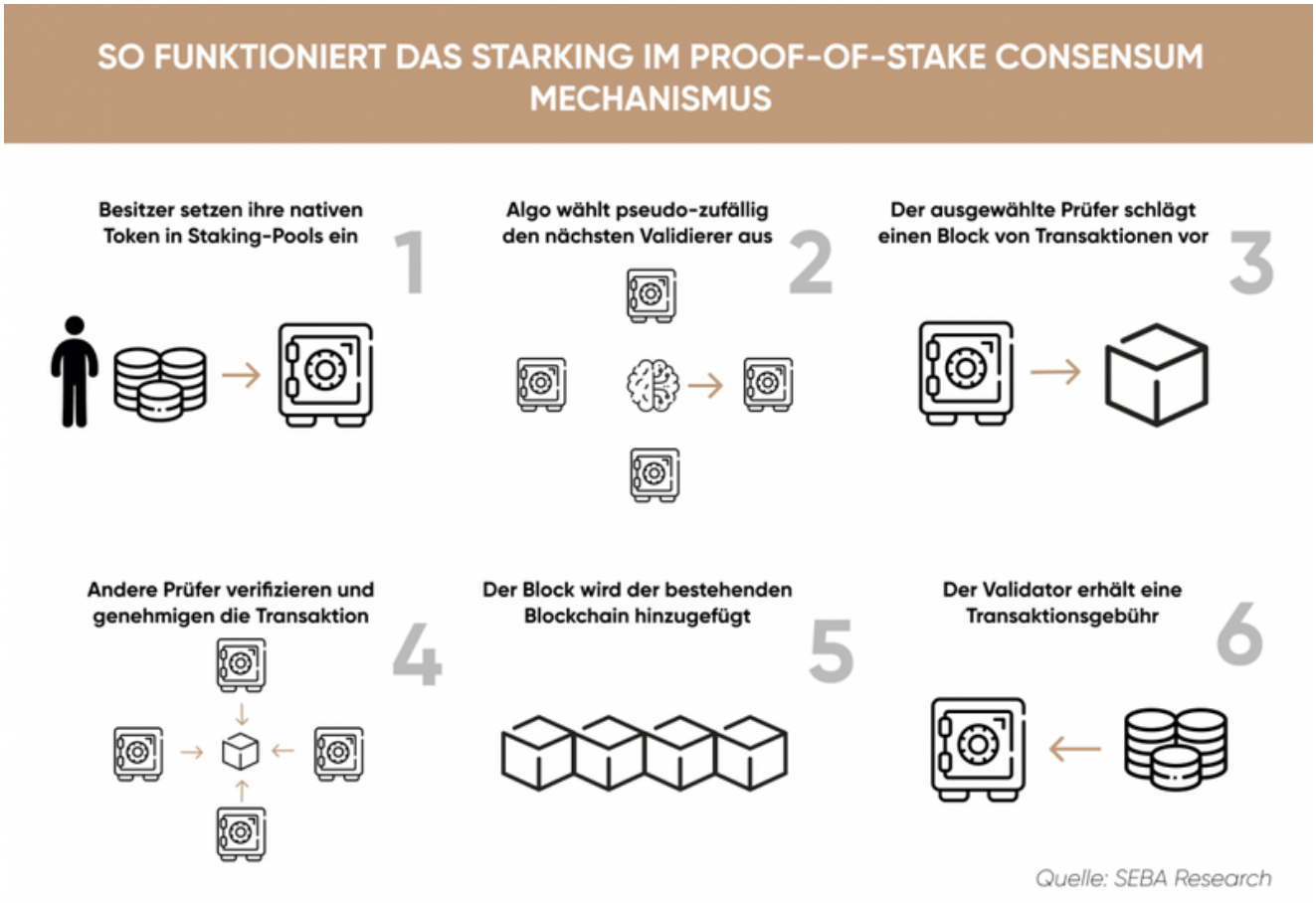


Proof of Work (POW) --> s. "Mining"

Proof of Work, zu deutsch: Arbeitsnachweis. Nach vollbrachter Arbeit bekommt man seine Entlohnung. Dieses Prinzip nutzt auch die Blockchain. Jede Transaktion muss vom Netzwerk überprüft und genehmigt werden. Damit werden Betrug und Hackerangriffe ausgeschlossen. Die Überprüfung wird durch Arbeiter, so genannte Miner, im Blockchain Netzwerk sichergestellt. Die Miner stellen Rechenleistung zur Verfügung, welche Rechenaufgaben lösen muss. Für die bereitgestellte Rechenleistung sowie den damit verbunden Zeit- und Stromkosten wird der Miner entlohnt.

Proof of Stake (POS)

Die Aufgabe des Poof of Stake ist die gleiche des Proof of Work, jedoch wird hier die Überprüfung anders gelöst. Beim POS wird keine Rechenleistung und Strom benötigt, denn hier müssen ausschließlich bereits erschaffene Coins bereitgestellt werden. Die Kryptowährungen werden entweder in der eigenen Wallet oder auf spezielle Plattform zurückgehalten. Durch das Bereitstellen der Coins wird das Netzwerk unterstützt und schüttet an den Coin-Inhaber als Belohnung neu entstandene Coins aus. Abhängig von Coin und Einsatz liegt die jährliche Rendite bei 3% bis zu 100%.



Satoshi

Da der Bitcoin-Preis immer weiter steigt, werden viele Transaktionen in Dezimalbeträgen von einem Bitcoin und nicht in ganzen Zahlen durchgeführt. Um die „Fungibilität“ von Bitcoin-Token als geeignetes Tauschmittel zu fördern, haben die Entwickler von Kryptowährungen den kleinsten Bitcoin-Betrag, der getauscht werden kann, als 1 Satoshi oder 1 Sat bezeichnet.

Der Name dieses dezimalen Ausdrucks stammt vom Erfinder von Bitcoin, Satoshi Nakamoto, der anonymen Figur, die als erste das Whitepaper veröffentlichte, in dem die Funktionsweise der Bitcoin-Blockchain erklärt wurde. Ein Satoshi entspricht dem 100sten Millionstel eines Bitcoins.

Smart Contract

Ein Smart Contract heißt übersetzt "intelligenter Vertrag" und ist ein Algorithmus, der dazu dient, eine bestimmte Transaktion auf der Grundlage einer Reihe von zuvor festgelegten Parametern auszuführen. Diese Verträge werden von der Blockchain automatisch ausgeführt, sobald die Parameter, die sie regeln, erfüllt sind. Es gibt keine Möglichkeit, einen Vertrag zu ändern, sobald er in die Blockchain aufgenommen wurde.

Stablecoin

Stablecoins sind Token oder Coins, die sich zum Ziel gesetzt haben den Wert einer FIAT-Währung (z.B. US-Dollar) nachzubilden.
Es gibt unterschiedliche Typen von Stablecoins. Die bekanntesten sind Stablecoins, die 1-zu-1 mit der jeweiligen Fiat-Währung gedeckt sind (z.B. USDT, USDC) oder Stablecoins, die mit Hilfe eines Algorithmus den Referenzwert nachbilden (z.B. DAI, USDN).

Token und ihre Klassifizierungen

Ein Token ist die Kryptowährung, die verwendet wird, um Miner und Nodes zu belohnen, wenn sie in der Blockchain aufgezeichnete Transaktionen validieren. Diese Token werden als digitale Vermögenswerte betrachtet. Sie können über eine zentralisierte oder dezentralisierte Börse gehandelt werden.
Token werden üblicherweise unterschieden in Utility-Token, die für einen bestimmten praktischen Zweck entwickelt und verwendet werden, Payment-Token (oder Währungs-Token), die als Zahlungsmittel geschaffen wurden, und Asset-Token (Sicherheits-Token), die in Bezug auf ihren wirtschaftlichen Wert Aktien, Anleihen und Derivaten ähneln. Auch wenn es noch andere Klassifizierungen für die verschiedenen Token gibt, sind dies laut der Eidgenössischen Finanzmarktaufsicht FINMA die gängigsten Arten.

Validator

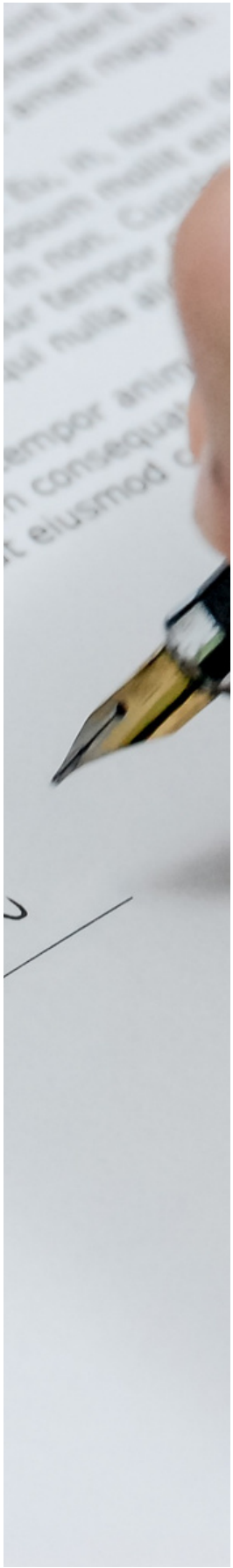
Ein Validator ("Prüfer") ist ein Computer oder eine Person, der/die die Aufgabe hat, die Integrität jedes neuen Datensatzes, der der Blockchain hinzugefügt wird, zu überprüfen und zu bestätigen, unabhängig davon, ob sie dem Proof-of-Work-, dem Proof-of-Stake- oder einem anderen Protokoll folgen.
In PoW-Systemen wie Bitcoin werden die Validierer auch „Miner“ genannt. Sie werden für ihre Bemühungen entschädigt, indem sie eine bestimmte Menge an Token erhalten, sobald ein Block oder eine Gruppe von Blöcken gemined wurde. In PoS-Blockchains werden die Validierer dafür belohnt, dass sie neue Blöcke vorschlagen und den Token des Netzwerks einsetzen.

Wallets

Wallets (deutsch: digitale Brieftaschen) verwalten Adressen. Wallets enthalten einen öffentlichen und einen privaten kryptografischen Schlüssel, um Zahlungen zu genehmigen.
Der öffentliche Schlüssel wird dabei durch die Adresse repräsentiert. Vereinfacht ausgedrückt verfügt eine Wallet somit über öffentliche Konten und dazugehörige Passwörter. Wallets autorisieren das Durchführen von Transaktionen im Netzwerk.

Wei

Wei ist die kleinste Einheit im Ethereum-Netzwerk. Ein Ether entsprechen 1.000.000.000.000.000.000 Wei



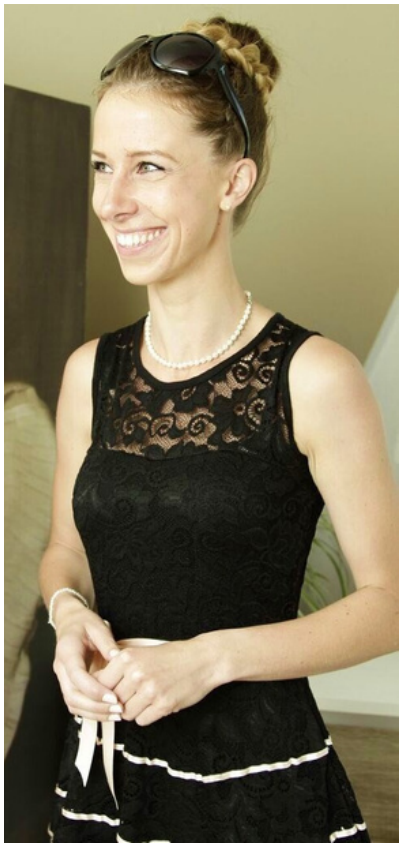
Whitepaper

Das Whitepaper beschreibt die initiale Problemstellung und geplante Lösungsansätze von Blockchain-Projekten. Whitepaper kommen aus der Wissenschaft, daher sind Whitepaper im Kryptobereich häufig aber nicht immer unter wissenschaftlichen Aspekte verfasst. Satoshi Nakamoto verfasste das erste Whitepaper zu Bitcoin

Wrapped Token

Ein Wrapped Token ist ein Token, der an den Wert eines anderen Kryptoassets 1 zu 1 gekoppelt ist. Beispiel: Der ERC20-Token WBTC (Wrapped Bitcoin) entspricht genau dem Wert von einem BTC auf der Bitcoin Blockchain.

Na, raucht nun Dein Kopf? :)



Das war keine Absicht! Ich freue mich, wenn ich Dir mit diesem Nachschlagwerk, die am häufigsten verwendeten Begriffe in der Krypto- und Blockchainwelt, etwas näher bringen konnte.

Schreibe mir gerne eine E-Mail an **info@juliafohrer.de** und teile mir mit, wie dir das Kryptowiki gefallen hat.

Du möchtest mehr?

Vereinbare hier ein Gespräch

SCAN ME

Julia Fohrer

https://juliafohrer.de