

Glossar

- **Altcoin:** Steht für alternative Coins. Damit sind alle Coins außer dem Bitcoin gemeint.
- **Binance:** ein Krypto-Börse, die auch einen eigenen Binance-Coin herausgibt. Dieser war als Incentive für die Kunden der Börse gedacht, um die Transaktionsmenge anzureizen. Sie betreiben auch ein Innovation Lab und haben umfangreiche Incentivierungsmechanismen noch über den Coin hinaus auf der Börse aufgebaut. Die Börse hat sehr gute Konditionen, ist aber zB deutlich jünger als Kraken
- **Bitcoin:** Kürzel: BTC. Hier sieht man die Visualisierung von BTC und ETH: <https://txstreet.com/> Es verdeutlicht, aus welchen Transaktionen sich die Blöcke zusammensetzen
- **Bitcoin Cash:** ist aus einem Hardfork mit Bitcoin entstanden mit dem Ansatz, eine schnelle Lösung für die Abwicklung von Zahlungsverkehr zu erzeugen. Der UseCase ist analog zum Litecoin, den es bereits länger als Bitcoin Cash gibt.
- **Cardano:** Die Cardano-Blockchain ermöglicht eine Inter-Operabilität zwischen verschiedenen, ansonsten voneinander getrennten Blockchainlösungen und verbindet somit verschiedene Technologien
- **Chainlink:** Chainlink ist ein sog. Oracle. Wenn zB ein bestimmtes, externes Event passiert, dann löst dies eine bestimmte Handlung aus. Chainlink ist eine Verbindung zwischen der realen Welt und des Krypto-Universums
- **Coin:** Bezeichnung für ein Einheit einer Kryptowährung
- **Consensus:** Übereinstimmung innerhalb des Netzwerks, ob eine Transaktion stattgefunden hat. Gilt sie als validiert, wird sie in den Block geschrieben und gilt als nicht mehr veränderbare Wahrheit
- **Decentralized Finance (DeFi):** beschreibt dezentralisierte Applikationen, bei denen wir innerhalb des Krypto-Universums bleiben und keinen Kontakt zur Außenwelt benötigen. Hier sieht man die Unterschiede zwischen DeFi und Cenztralized Exchanges:
<https://medium.com/totle/the-great-divide-in-cryptocurrency-cefi-vs-defi-72a676c51dfc>
- **Dogecoin:** Communitycoin, der entstanden ist, weil eine Community einen eigenen Coin erstellen wollte. Es liegt kein Usecase dahinter, die Community ist gewachsen und Elon Musk hat immer wieder über diesen Coin getwittert, so dass der Preis gestiegen ist - auch ohne UseCase.

- **Ethereum:** 2. größte Kryptowährung, die nicht als Währung, sondern als weltweites Netzwerk konzipiert wurde, auf dem sog. Smart Contracts laufen
- **Exchange:** Börse, an der man Fiatwährungen (Euro, Dollar etc) in Kryptos tauschen kann
- **halvening:** die Anzahl an Bitcoins, die alle 10 Minuten gemined werden, halbiert sich alle 4 Jahre. Aktuell (Februar 2021) sind wir bei 6,25 Bitcoins alle 10 Minuten
- **hashrate:** Bezeichnet die Power, die einem Netzwerk zur Verfügung steht um einen Mining-Algorithmus zu lösen
- **hodlen:** bezeichnet das langfristige Halten von Cryptowährungen
- **Lending:** Beim Lending überlässt der Darlehensgeber anderen Nutzern der jeweiligen Plattform einen Teil seiner Kryptowährung für eine begrenzte Zeit zur Nutzung. Im Gegenzug erhält der Darlehensgeber Zinsen in der hingebenen oder einer anderen Kryptowährung.
- **LiteCoin:** eine Art kleinerer Bruder von Bitcoins, der deutlich schnellere Transaktionen zu geringeren Kosten ermöglicht und zB für Händlernetze interessant ist, die Kryptowährungen einführen möchten.
-
- **Masternodes:** Masternodes sind Server im Netzwerk einer Kryptowährung. Sie speichern Blockchains in Echtzeit ab und synchronisieren die Daten mit anderen Masternodes.
- **Mining:** ja nach Coin ist das Verfahren zur Consensus-Herstellung unterschiedlich. Vor jeder Transaktion muss geprüft werden, ob die Voraussetzungen dafür bestehen. Wenn dies so ist, muss die Transaktion im Fall von Bitcoin durch die Lösung eines Algorithmus bestätigt werden. Derjenige, der den Algorithmus löst, bekommt einen sog. Block-Reward (dieser besteht aus den Transaktionsgebühren und aus neuen Bitcoins, die dadurch erzeugt werden). Der Lösende wird somit über den Proof of Work dafür entlohnt, eine Verifikation der durchgeführten Transaktion durch die Bereitstellung von Rechenleistungen getätigten zu haben.
- **Oracle:** Oracle ist ein Agent, der reale Ereignisse aus der Welt außerhalb der Blockchains findet und bestätigt und diese Daten an eine Blockchain zur Verwendung Smart Contracts sendet. Blockchains selbst können nicht auf Daten außerhalb ihres Netzwerks zugreifen – deshalb bedarf es dieser speziellen technischen Komponente, um externe Daten zu integrieren. Denn Smart Contracts geben in der Regel nichts Anderes vor als Ablauffolgen: "Wenn Bedingung A eingetreten ist, wird Operation B ausgeführt".
- **Polka Dot:** Kryptocoins dessen Anwendungsgebiet (use case) darauf beruht, eine Vernetzung (Interoperabilität) zwischen verschiedenen Blockchains zu ermöglichen. Dies war vorher nicht möglich, die unterschiedlichen Technologien liefen voneinander

getrennt ohne Schnittstellen. Eine Anwendung ist <https://shopping.io>, wo man mit über 100 Kryptowährungen in verschiedenen Shops einkaufen kann.

- **Privatekey:** Ein Private Key (privater Schlüssel) ist eine Form der Kryptographie, die es einem Benutzer ermöglicht, auf seine Kryptowährung zuzugreifen. Ein Private Key ist ein integraler Bestandteil von Bitcoin und Altcoins. Seine Sicherheitsstruktur hilft, einen Benutzer vor Diebstahl und unbefugtem Zugriff zu schützen
- **Proof of work:** zur Verfügungstellung von Rechenleistung für die Lösung eines Mining-Algorithmus
- **Proof of stake:** wie viele Coins hat eine Person? Je mehr Coins man hält, desto höher die Wahrscheinlichkeit, dass man den nächsten Block lösen darf. Die Auswahl geschieht zufällig, ist jedoch abhängig davon, wie viele Coins man hält. So wird gewährleistet, dass nur diejenigen die Blocks lösen, die selber ein hohes Interesse daran haben, dass dem Coin bzw dem Netzwerk nicht geschadet wird. Proof of stake ist deutlich weniger kostenintensiv
- **Public Key:** Der Public Key, also der öffentliche Schlüssel, ist sehr gut mit der IBAN Ihres Bankkontos vergleichbar. Es handelt dabei um die öffentliche Adresse Ihres Wallets, die Sie beispielsweise einem Zahlungspflichtigen mitteilen können, der Ihnen gerne eine Kryptowährung übersenden möchte.
- **Ripple:** eine der ältesten Währungen, die zentral gehalten wird und bei der bereits alle verfügbaren Coins existieren (es wird nicht mehr gemined). RXP
- **Smart Contract:** Smart Contracts (intelligente Verträge) laufen auf der Ethereum Blockchain und funktionieren ähnlich wie Verkaufsautomaten. Man wirft einfach eine erforderliche Menge einer Kryptowährung (Ether) in den Smart Contract, und ein smarter contract wird ausgeführt. Z.B. die Übertragung von Eigentumsrechten
- **Staking:** Staking bedeutet Kryptowährungen zurückzuhalten, um Belohnungen (Rewards) zu erhalten. In den meisten Fällen kann man Coins direkt in den Krypto-Wallets staken. Auf der anderen Seite bieten viele Börsen ihren Benutzern Staking-Dienste an
- **Tether:** Tether ist ein sog. Stable Coin, dessen Wert sich 1:1 am Wert des Dollar orientiert und somit eine Art feste Verrechnungsgröße im Krypto-Universum darstellt
- **Token:** Im Gegensatz zu einem Coin nutzt ein Token eine bereits bestehende Plattform, wie etwa das Ethereum-Netzwerk, als Basis. Ein Token wie zum Beispiel OmiseGo (OMG) nutzt die funktionierende Infrastruktur von Ethereum aus, besitzt also keine eigene Blockchain, keine eigenen Nodes und keine eigenen Miner..

- **app.Uniswap.org:** Tauscht ETH in andere Coins
- **Wallet:** Krypto-Geldbörse. Es gibt Hardware-Wallets (z.B. den Ledger), Software-Wallets (zB Jaxx), Cold-Storage-Wallets (zB ein Blatt Papier, auf dem ich meinen Privatekey notiere) oder auch Börsen, über die man seine Coins halten kann (zB Bitpanda und Kraken)
- **Yield Farming:** Mit <https://apy.finance> wird das Netz automatisch nach Arbitrage-Möglichkeiten durchsucht

Wichtige Websites:

Steuerliche Erfassung unserer Krypto-Transaktionen:

- <https://cointracking.info/?language=de>
- <https://cryptotax.io>

Blockchains, die sehr effizient viele Transaktionen bewältigen:

- <https://blocktivity.info>