Endlich verständlich: So funktionieren Kryptowährungen

Es war der 18. Dezember 2017 – der Bitcoinkurs liegt bei sagenhaften 18.737,60 US-Dollar! Nie zuvor ist eine Kryptowährung so hoch gehandelt worden. Seitdem ist der Bitcoin wieder abgestürzt (zuletzt auf 9.700 US-Dollar, Stand Mai 2018), aber inzwischen hat jeder mitbekommen, dass es ihn gibt. Staaten und Banken wollen ihn regulieren, manche mutige Investoren ihr Vermögen einsetzen, und Programmierer sehen in ihm und anderen digitalen Währungen die Zukunft.

Die wenigsten aber haben wirklich verstanden, was eine Kryptowährung überhaupt ist und wie sie funktioniert. Denn versucht man das herauszufinden, landet man schnell bei Wörtern wie Blockchain, FinTech, Hashing und so fort. Wir haben uns für Sie durch die komplizierte Computersprache und das Finanzkauderwelsch gegraben, um Licht ins Dunkle zu bringen.

Die Serie

Teil 1: Das Krypto-Ein-mal-Eins
Teil 2: Die Gefahren
Teil 3: Der Bitcoin
Teil 4: Ethereum
Teil 5: Ripple

> *Kryptowährungen: Alles, was Sie an Geld nicht verstehen, kombiniert mit allem, was Sie an Computern nicht verstehen!*
>
> *John Oliver – TV-Moderator der Late-Night-Show „Last Week Tonight“*

Bank vs. Kryptowährungen

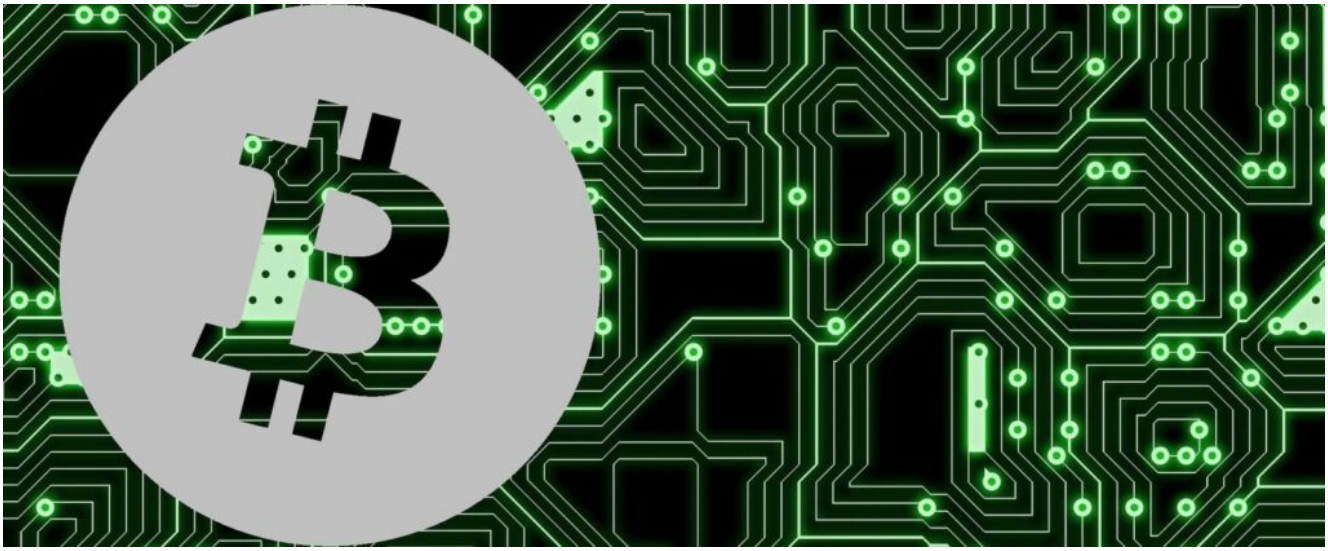
Worin besteht der Unterschied zwischen einer digitalen Währung und „echten“ Währungen? Das folgende Beispiel soll den Unterschied erklären:

- Alex (Köln) – Zasterbank
- Sabine (Sydney) – DownUnderBank
- Südkorea – Olympiabank.

Alex wohnt in Köln. Seine Freundin ist gerade für ein Jahr nach Australien gereist. Dafür hat sie ihrem Freund vorher ihre Ersparnisse überwiesen. Die soll er ihr immer wieder auf ihr neues Konto in Australien überweisen. Alex ist bei der **„Zasterbank“.** In Australien angekommen, eröffnet Sabine ein Konto bei einer lokalen Bank. Wir nennen die Bank einfach **„DownUnderBank“.** Sabine ruft ihren Freund Alex an und bittet ihn, erstmal 2000 Euro für den ersten Monat zu überweisen.Alex beauftragt jetzt die „Zasterbank“ damit, die 2000 Euro auf das neue Konto von Sabine zu überweisen. Die „Zasterbank“ kann das Geld aber nicht direkt nach Australien überweisen, da sie mit der „DownUnderBank“ von Sabine leider nicht in Kontakt steht und dort auch kein ausländisches Konto hat. Aber dafür hat die Zasterbank eine Partnerbank in Südkorea. Die **„Olympiabank“.** Und die Olympiabank macht glücklicherweise Geschäfte mit der „DownUnderBank“. Also bildet sich ein Kette.
Bei der „Olympiabank“ hat die Zasterbank nämlich ein sogenanntes **Nostrokonto**. Ein Nostrokonto ist ein Bankkonto, das Banken bei anderen Banken im Ausland haben, um darauf Geld zu überweisen. Darauf überweist die „Zasterbank“ die 2000 Euro von Alex. Bei der Überweisung nach Südkorea fallen natürlich Wechselkurse und Gebühren an. Die „Olympiabank“ sendet das Geld dann an ihr Nostrokonto bei der „DownUnderBank“ von Sabine. Von diesem Konto wird das Geld dann an Sabines Konto überwiesen. Die „DownUnderBank“ nimmt natürlich auch nochmal Gebühren und Wechselkurse. Inzwischen sind 9 Tage vergangen,

und zu den 2000 Euro sind ein Haufen von Gebühren hinzugekommen.
So in etwa sieht es aus, wenn wir internationale Überweisungen außerhalb der Europäischen Union machen – ganz schön kompliziert. Manchmal scheitern Überweisungen sogar komplett, oder es müssen sich drei oder vier Banken dazwischen schalten. Dieses „Wirrwarr“ ist nicht nur anstregend und kompliziert, sondern auch teuer. Vor allem aber für Unternehmen, die täglich viele Überweisungen tätigen. Die brauchen ganze Buchhaltungsabteilungen, die sich nur damit beschäftigen, das Geld, was sie durch die Welt senden, zu verfolgen.

Auch deshalb hat eine Person oder eine Gruppe unter dem Pseudonym **Satoshi Nakamoto** die erste digitale Währung erfunden, den Bitcoin. Dieser Bitcoin existiert nur virtuell. Das heißt, es gibt keine Münzen oder Scheine von ihm. Sondern nur Zahlen in einem Netzwerk. Der Vorteil: Sie können Bitcoins direkt international versenden, sie brauchen keine Bank, werden nicht reguliert, und das Ganze verläuft dezentral. Mit Kryptowährungen können Sie in unglaublicher Geschwindigkeit digitales Geld direkt ans andere Ende der Welt schicken, ohne hohe Transaktionsgebühren der Bank zu bezahlen und ohne tagelang zu warten. Aber wie funktioniert das?



Das Krypto-1×1

Damit man das System von Kryptowährungen versteht, muss man wie beim Mathematikunterricht im Kleinen beginnen. Bei Kryptowährungen sind das die **Begriffe**. Kryptowährungen benutzen eine besondere Sprache.

FinTech: Der Begriff FinTech bedeutet nichts anderes als Finanztechnologie. Er steht für die ganzen neuen Firmen, die digitale Währungen erstellen und auf diesem Gebiet Innovation fördern.

Coins: Coin ist das englische Wort für Münze und steht für den Wert einer digitalen Währung. Das heißt: Man kann eine beliebig hohe Anzahl an Coins haben, also eine beliebig hohe Anzahl an Werten. In der Menge der Coins wird das Guthaben gemessen.

Shared Memory/Geteilte Erinnerung: Geteilte Erinnerung ist dass erste und gleichzeitig wichtigste Prinzip von digitalen Währungen. Bei Kryptowährungen wird jede einzelne, jemals getätigte Transaktion gespeichert und in einen großen Datensatz eingespeist. Bei herkömmlichen Banken werden Transaktionen auf den Servern der Bank gespeichert. Bei Kryptowährungen ist dieser Datensatz nicht auf einem einzelnen Server, sondern auf immens vielen Knotenpunkten im Netzwerk gespeichert. Auf dieses Netzwerk hat jeder Zugriff. Damit hat im Gegensatz zur Bank niemand die Herrschaft über die Daten.

Dezentralität: Was heißt, jeder hat auf dieses Netzwerk Zugriff? – Mit der *Blockchain* tritt man über das Internet dem Netzwerk bei. Sobald man Teil dieses Netzwerkes ist, wird eine Kopie der Blockchain, also aller jemals getätigten Transaktionen, auf den eigenen Rechner übertragen. Das bedeutet, jeder hat zu jeder Zeit alle Daten. Jeder weiß zu jeder Zeit, was im Netzwerk passiert ist und wer wem etwas überwiesen hat.

Anonymität: Diese ganzen Daten sind aber anonym. Im Datensatz ist jede einzelne Transaktion gespeichert, aber es ist nicht sichtbar, wer hinter der Transaktion steht. Denn jeder Nutzer hat ein Pseudonym. Es ist also sichtbar, welcher Account welches Guthaben hat und welcher Account an wen wieviel Guthaben überwiesen hat. Es ist aber niemals sichtbar, wer hinter dem Account steckt.

Block: Überweisen Sie einige Coins an einen Freund, wird diese Transaktion aufgezeichnet und gespeichert. Und zwar in dem eben erklärten Datensatz. Die ganzen gespeicherten Transaktionen, werden aber nicht durcheinander abgespeichert sondern nach einem logischen Prinzip: Es werden immer mehrere Transaktion in ein „Paket“ zusammengefasst. Dieses Paket nennt man Block. Das kann man sich bildlich vorstellen. Jede Transaktion kommt in eine Kiste. Ist die Kiste voll, hat man ein Datenpaket, den Block. Dieser Block kommt an seinen Platz und es wird eine neue Kiste befüllt.

Blockchain: Blockchain bedeutet übersetzt Blockkette. Denn das Prinzip dieser digitalen Währungen ist es, das alle Blocks aneinander gereiht werden. So entsteht eine riesige lange Kette, in der alle jemals getätigten Transaktionen gespeichert sind. Im Beispiel von vorher bedeutet das, dass alle Kisten hintereinander aufgereiht werden.

Kommen wir nun zum genauen Abspeichern der Daten:

Hashing: Die Daten einer Transaktion, die in dem Block gespeichert werden, werden auf besondere Weise gespeichert. Und zwar wird die Transaktion verschlüsselt, mit Hilfe einer sogenannten Hashfunktion. Diese Hashfunktion versieht die Transaktion mit einem Code. Den Code nennt man Hash. Vereinfacht dargestellt, sieht das ungefähr so aus:

0101001110110101 (Transaktion) –> efghtuvnbemf (Hash)

Die Nullen und Einsen verkörpern jede Transaktion in

„Computersprache“. Jede Transaktion wird nun in den „Buchstabensalat“ übersetzt, den Hash. Kommt jetzt eine neue Transaktion in unsere „Kiste“, wird dieser Hash in die Transaktion übernommen. Das ist wie mit einer Matheaufgabe. Stellen sie sich ein lange Kettenaufgabe vor. Sie brauchen das Ergebnis der vorherigen Aufgabe um die nächste zu lösen. Das heißt, der Hash der einen Transaktion, ist das Startergebnis der nächsten Transaktion.

Ist jetzt eine Kiste gefüllt und es steht ein „Endergebnis“ fest, ist der Block fertig. Das Endergebnis aus dem Block ist das Startergebnis für den nächsten Block. So ist alles mit einander verbunden wie eine riesige Matheaufgabe. Jedes Ergebnis ist der Anfang der nächsten Aufgabe.

Fälschungssicher: Warum der ganze Aufwand mit der Blockchain und den Codes? – Weil jede Transaktion mit der nächsten und jeder Block mit dem nächsten durch Codes verbunden ist, kann **niemand** die Kette manipulieren. Denn wenn irgendeiner, irgendwo in einer langen Matheaufgabe etwas verändert, geht das Gesamtergebnis nicht mehr auf. Die gesamte Kette würde theoretisch zerstört. Da aber wie oben gesagt die Daten nicht auf einem Zentralserver sind, auf welchen nur wenige Zugriff haben, sondern jeder eine Kopie der Kette hat, kann niemand behaupten, er habe Geld überwiesen oder keines bekommen, da sonst der Datensatz anders aussehen würde. Das ist ein riesiger Vorteil der Blockchain. Wenn jemand die Daten ihrer Bank hackt, kann ein großer Schaden entstehen. Wenn jemand die Blockchain manipuliert, können alle zeigen, dass das Ergebnis nicht stimmt, und die Transaktion funktioniert nicht.

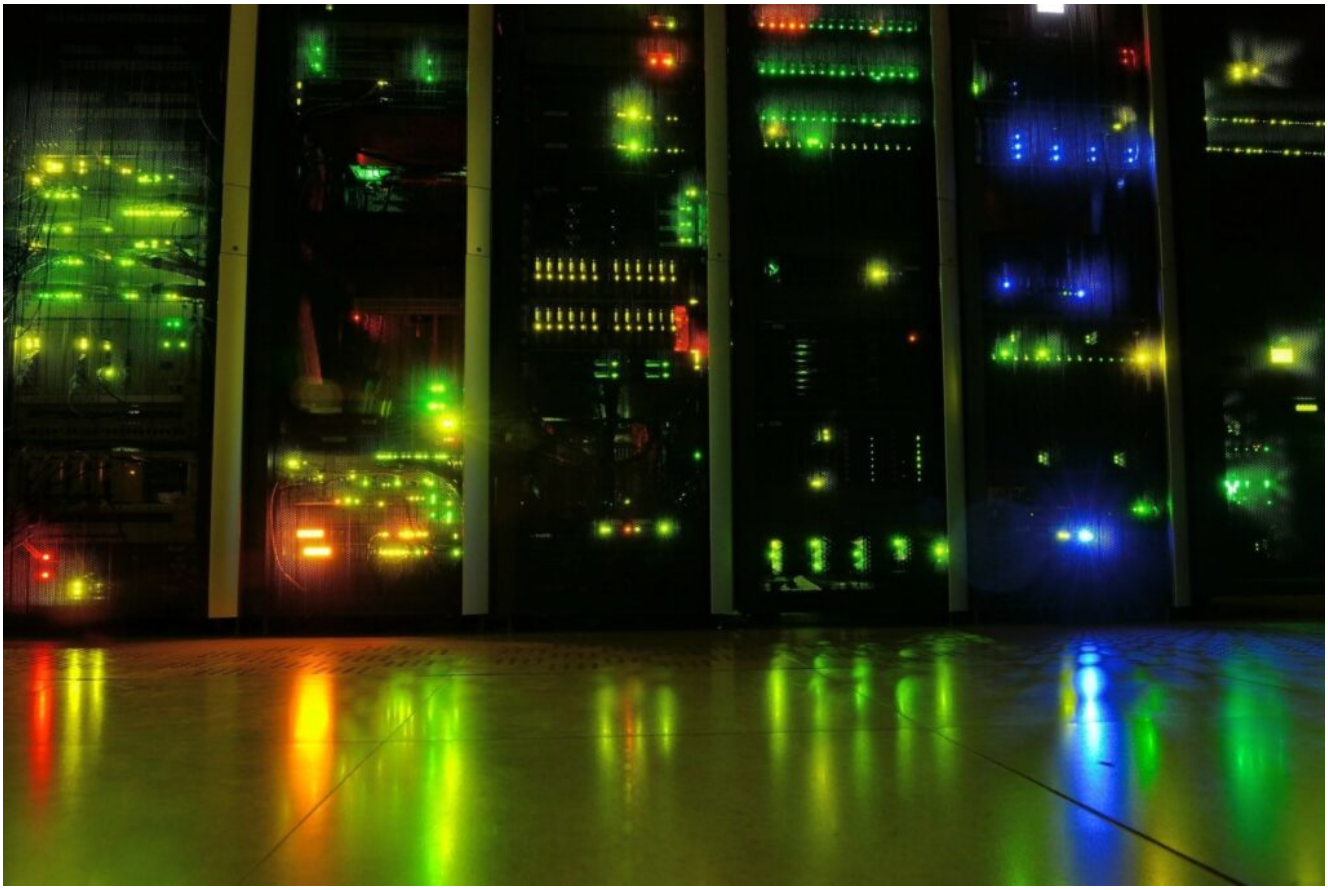
Bitcoin-Blockchain vereinfacht

The Bitcoin Foundation

Mining: Woher kommen eigentlich die Bitcoins? – Da diese Coins nicht real existieren, sondern aus dem Nichts erschaffen werden, müssen die ja irgendwie entstehen. Den Entstehungsprozess nennt man Mining, was englisch für Schürfen steht. Das heißt: Die Münzen werden geschürft. Um einen Bitcoin zu schürfen, müssen Sie ihren Computer Rechenaufgaben lösen lassen. Was sind das für Rechenaufgaben? – Die Aufgabe des Miners ist es, den Hash für die Transaktionen zu erzeugen, denn irgendwer muss ja die Arbeit in dem Netzwerk übernehmen. Da das aber zu einfach wäre, gibt es immer neue Vorgaben für die Hashes, zum Beispiel nach Aussehen. Diese Rechenaufgaben sind deshalb unglaublich kompliziert, und ein Computer alleine braucht eine Ewigkeit dafür. Die Aufgaben sind so schwierig, damit keine Inflation entsteht. So entstehen sehr langsam neue Coins.

Miningpools: Natürlich haben sich die Menschen sofort gedacht, dass es viel besser wäre, wenn man die Computer zusammen Aufgaben lösen lässt, als jeder alleine mit seinem Laptop. So sind riesige Datenzentren entstanden, die ununterbrochen laufen und Bitcoins schürfen.

Zeuge: Das Prinzip von Kryptowährungen ist es ja, dass die Datensätze nicht manipulierbar sind. Dadurch, dass jeder eine Kopie der Blockchain hat, kann man beweisen, welche Transaktionen stattgefunden haben und welche nicht. Dadurch wird das Ganze aber langsam, und Transaktionen brauchen mehrere Stunden. Es gibt nun auch Blockchains, die nach dem Prinzip funktionieren, dass nur eine bestimmte Anzahl an Personen die Blockchain speichert und damit als Zeuge die Transaktion bestätigt. Das heutige Banksystem zum Beispiel kennt nur einen Zeugen, nämlich die eigene Bank. Die EOS-Kryptowährung kennt nur eine bestimmte Anzahl, die von allen gewählt werden. Beim Ethereum-Netzwerk ist jeder einzelne Teilnehmer Inhaber und Zeuge der Blockchain.



Geschafft! Jetzt wissen sie wie Kryptowährungen grundsätzlich funktionieren. In den nächsten Teilen, stellen wir Ihnen einzelne Währungen vor und erklären Ihnen, was Sie genau mit denen machen können – angefangen mit dem Bitcoin. Nächste Woche berichten wir in Teil 2 der großen Serie über die Gefahren der Kryptowährungen.