Blockchain, Crypto, Bitcoin

Was ist eine Blockchain? Kryptowährungen wie Bitcoin und Ethereum beruhen auf einer Technologie namens Blockchain. Im Grunde genommen ist eine Blockchain eine Liste mit Transaktionen, die jeder einsehen und überprüfen kann. Die Bitcoin-Blockchain beispielsweise erfasst jede Transaktion, bei der Bitcoin verschickt oder empfangen werden.

Bitcoin ist eine sogenannten Kryptowährung, also eine virtuelle Währung, die Kryptographie (Verschlüsselung) zur Sicherung von Transaktionen benutzt. Sie soll die Probleme, die etwa durch die heutigen Bank-Systeme entstehen, aus der Welt schaffen: Wenn wir heute Geld zum Bezahlen im Internet benutzen, brauchen wir einen Mittelsmann wie eine Bank, die garantiert, dass das Geld real vorhanden ist und auch beim Empfänger ankommt.

Das setzt voraus, dass wir der Bank vertrauen und hat zur Folge, dass alle Transaktionen an dieser Stelle gebündelt sind. Dort liegt jedoch auch die Schwachstelle: Die Bank ist die einzige, die sicherstellen kann, dass Zahlungen getätigt werden und keine Doppelbuchungen entstehen. Fällt die Bank einem Hack zum Opfer, ist das gesamte System in Gefahr.

Mit einer dezentralisierten Kryptowährung hingegen braucht man keine Bank mehr. Jeder einzelne Teilnehmer des Bitcoin-Netzwerks bekommt nämlich eine verschlüsselte Kopie eines kompletten Transaktionsverlaufs, also quasi eine Datei mit den Infos, welche Summe von A nach B überwiesen wurde. Konkrete Namen oder andere sensible Details sind natürlich nicht für alle einsehbar. Da jeder Nutzer das System automatisch mitüberwacht, wird auch jeder Versuch, das Netzwerk zu manipulieren schnell entdeckt und verhindert. Ein weiterer Vorteil ist, dass keine einzelne Person, Bank oder Regierung Kontrolle über den Geldfluss übernehmen kann. Dadurch wird es einfacher, schnellerer und günstiger, Geld zu überweisen, sogar über nationale Grenzen hinweg.

Das Zusammenspiel von Bitcoin und Blockchain

Die Blockchain ist der grundlegende Baustein, der die Sicherheit der Bitcoin-Währung garantiert. Im Prinzip handelt es sich dabei um eine komplette und chronologische Liste aller Transaktionen, die in Bitcoin getätigt wurden. Neue Überweisungen kommen immer in Blöcken zur Liste hinzu, wobei jeder Transaktionsblock ein Protokoll über vorhergehende Blöcke enthält. Dadurch bilden die Blöcke eine Kette, daher auch der Begriff Blockchain (dt. Blockkette). Da in jedem Block immer Verweise auf frühere Blöcke in der Kette enthalten sind, ist es extrem schwer für Betrüger, einen falschen Block, der keine oder nur wenige Verweise auf vorangehende Transaktionen enthält, in das Netzwerk einzuschleusen.

Man kann sich die Blockchain als Anreihung von Blöcken vorstellen. Die blauen Blöcke sind vom Netzwerk verifizierte Transaktionen. Nicht verifizierte graue Blöcke werden nicht in die Kette eingefügt

Die Verweise sind in einem Block gebündelt, bis der Block die vorgesehene Größe von 1 Megabyte erreicht. Der neue Block kommt jedoch nicht einfach zur Kette hinzu, das Netzwerk muss ihn erst „beglaubigen“. Um ihn zu überprüfen, müssen die Netzwerkmitglieder eine Art Ratespiel lösen, das nur mit sehr viel Rechenpower lösbar ist.