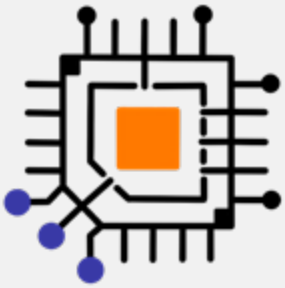
TECHNOLOGISCHE PERSPEKTIVE



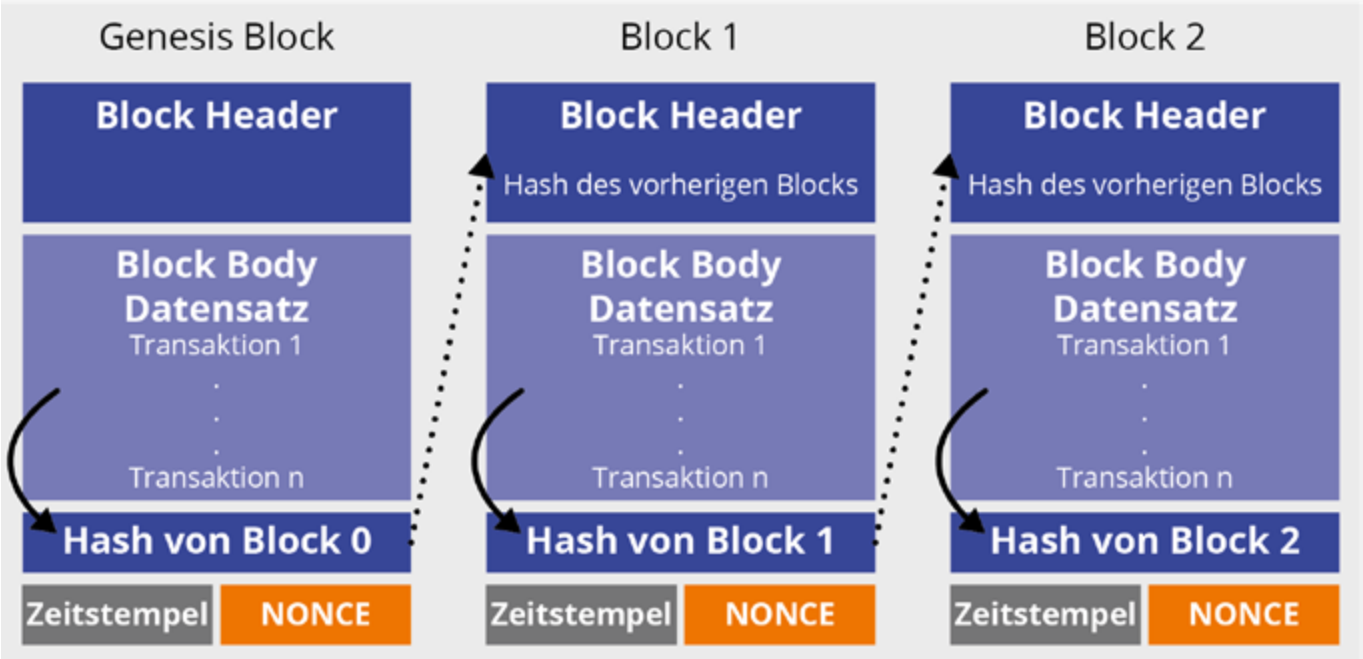
Die Blockchain-Technologie: Sie ist die zukunftsweisende Technologie, die hinter NFTs und Kryptowährungen steckt. Doch wie funktioniert sie eigentlich? Komplex, wie man auf den ersten Blick meinen könnte, doch keine Sorge, wir zeigen euch, was hinter der Blockchain steckt, wie sie funktioniert und wie die Technologie mit NFTs zusammenhängt.

Um die Funktion der Blockchain zu verstehen, schauen wir uns zunächst an, wie die Blockchain aufgebaut ist. Die Blockchain lässt sich als dezentrale Datenbank darstellen, welche Transaktionen ohne das Eingreifen Dritter ermöglicht. Diese Datenbank ist aber nicht zentral auf einem Server oder bei einem Unternehmen abgespeichert, sondern auf jedem teilnehmenden Rechner der Blockchain. Dies wird auch als Peer-to-Peer-Netzwerk bezeichnet, d.h. ein Netzwerk von gleichberechtigten Computern, die alle über eine vollständige Kopie der Blockchain verfügen. Alle Computer im Netzwerk erhalten die Informationen zu einem neuen Informationsblock, sprich einer Transaktion, gleichen sie ab und bestätigen dann die Aufnahme. Die einzelnen Transaktionen befinden sich in einer Kette von Informationsblöcken – daher der Name Blockchain.

Anhand der folgenden Abbildung ist zu sehen, dass jeder Informationsblock aus einem Block Header (kryptografisch gesicherter Hash des vorangehenden Blockes), den Transaktionsdaten, einem Zeitstempel sowie der Number Only Used Once (NONCE) besteht. Der Hash-Wert kann als einzigartiger elektronischer Fingerabdruck betrachtet werden, der zur Identifizierung des jeweiligen Blocks dient und berechnet wird, sobald ein Block kreiert wurde.

In der Abbildung wird der erste Informationsblock der Blockchain durch den „Genesis Block" dargestellt. Wird ein neuer Block angehängt, in diesem Fall Block 1, bildet der Hash aus dem Genesis Block den Block Header für den Block 1. Demnach bildet der Hash des vorherigen Blocks immer den Block Header für den nächsten Block. Der nächste Block – Block 2 – enthält dann die Transaktionsdaten aus dem Genesis Block und Block 1. So lässt sich immer im jeweiligen Block die bisherige Transaktionshistorie nachvollziehen.

Dadurch, dass sämtliche Blöcke miteinander durch die Hashcodes verbunden sind, ist es nur schwer möglich, diese Kette zu manipulieren. Wenn jemand versuchen



würde, einen Block mit falschen Informationen in die Blockchain zu integrieren, müsste er oder sie diesen in alle Kopien derselben einspeisen. Geschieht dies nicht, werden die folgenden Blöcke ungültig, weil der Hash nicht mehr übereinstimmt. Da dies nahezu unmöglich ist, stellt die Blockchain eine extrem sichere Variante der Datenspeicherung dar.

Wie findet eine Transaktion statt? Stellen wir uns hierfür vor, dass Person A einen bestimmten Geldbetrag in Form von Kryptowährung an Person B übertragen möchte. Um eine Transaktion stattfinden zu lassen, benötigen beide Parteien ein sog. Wallet, in welchem die Kryptowährungen, der private Schlüssel und der öffentliche Schlüssel hinterlegt werden. Den öffentlichen Schlüssel können wir mit einer Kontonummer vergleichen. Person B teilt Person A seinen öffentlichen Schlüssel mit. Nun sendet Person A die Transaktion über die öffentlichen Schlüssel an Person B. Person B kann diese nun mit seinem privaten Schlüssel öffnen. Die Transaktion ist dann bestätigt, wenn sie für alle Teilnehmer:innen einsichtig in einem Block hinterlegt ist. Sie ist damit in der Blockchain gespeichert, für jeden einsehbar und unveränderbar.

Doch wie wird eine Transaktion validiert? Dafür werden sog. „Miner" eingesetzt. Sie sind die Buchprüfer der Blockchain. Miner erstellen mithilfe von mathematischen Funktionen einen Block, bzw. schließen diesen ab, um ihn unveränderbar in der Blockchain abzulegen. Um einen Block abzuschließen, muss eine Zufallszahl ermittelt werden, die sog. NONCE. Die Miner müssen mit Hilfe eines algorithmischen Suchprozesses eine Zufallszahl für das NONCE-Feld suchen, dies geschieht nach dem Try-and-Error-Verfahren. Dabei kann nur ein Miner die richtige Zufallszahl finden und die aufgebrachte Energie der anderen Computer ist somit umsonst. Diesen Vorgang bezeichnet man als Proof-of-Work, welche für die erfolgreiche Generierung eines zielkonformen Hashwertes sehr viel Rechnerarbeit verwendet, um einen neuen Block zu generieren. Für diesen hohen Aufwand erhält der Miner, der den Block abschließt, eine systeminterne Belohnung, in den meisten Fällen sind es hier Kryptowährungen wie Bitcoins. Anschließend wird der neu generierte Block zusammen mit den darin befindlichen Transaktionen an sämtliche Netzwerkknoten gesendet. Diese Netzwerkknoten können als nächstes kontrollieren, ob die Transaktionen in dem Block korrekt validiert wurden und diese Abwandlung der Blockchain übernehmen oder, sofern sie Fehler beinhaltet, ablehnen.

Eine Alternative zum Proof-of-Work ist der Proof-of-Stake. Hier werden keine Miner benötigt. Nutzer:innen hinterlegen Teile ihres Vermögens auf die Blockchain, dieses Vermögen wird so lange einbehalten, bis die Transaktion abgeschlossen ist. Unter all denen, die Vermögen hinterlegt haben, entscheidet ein Algorithmus, wer den nächsten Block erzeugen darf. Je höher die Anzahl der gegebenen Coins, desto höher die Wahrscheinlichkeit, vom Algorithmus ausgewählt zu werden.

Wie hängt die Blockchain-Technologie mit NFTs zusammen? NFTs werden in der Blockchain gespeichert. Die Einträge und Transaktionen in einer Blockchain sind unveränderbar. Somit kann der Besitz eines NFTs eindeutig nachgewiesen und übertragen werden. Die Herkunft sowie die komplette Besitzhistorie ist für immer in der Blockchain gespeichert. Ein NFT hat jeweils eine eigene Blockchain-Adresse, in der die Daten aufgezeichnet werden. Ein Datensatz enthält Informationen wie die Identität des Eigentümers, die Anzahl der gesammelten NFTs und Informationen zu den Transaktionen des jeweiligen NFTs. Die Käufer:innen eines solchen NFTs bekommt einen Link, mit dem sie direkt zum auf der Blockchain vorhandenen Vermögenswert gelangt.

GOOD TO KNOW

Der jährliche Stromverbrauch des **Bitcoin-Netzwerks** wird auf rund **94 Terrawattstunden** geschätzt — Zum Vergleich: Schweden liegt jährlich bei einem Verbrauch von etwa **130 Terrawattstunden**.