HINTERGRUNDINFORMATION

WIE FUNKTIONIERT BITCOIN – MINING?

Der Prozess, bei dem neue Bitcoins geschaffen werden, wird als Mining (von engl. „to mine", schürfen) bezeichnet. Der Begriff ist absichtlich in Anlehnung an das Schürfen von Gold so gewählt. Je mehr Gold geschürft wird, desto weniger ist noch in der Erde vorhanden. Dieser Prozess wird durch den Algorithmus, der Rechenvorschrift des Bitcoins, nachempfunden. Ungefähr im Jahr 2100 werden dann alle 21 Millionen Bitcoins gemint sein. Der Begriff „Miner" kann dabei unterschiedliche Bedeutungen haben. Zum einen bezeichnet er die Person oder Organisation, die neue Bitcoins mint. So ist zum Beispiel Northern Bitcoin auch ein Bitcoin-Miner. Zum anderen steht Miner auch für die Computerhardware, die darauf spezialisiert ist, den Algorithmus des Bitcoins auszuführen.

Heute erfüllt das Bitcoin-Mining insbesondere drei Aufgaben:

- Es bestätigt die Richtigkeit von Bitcoin-Transaktionen und führt sie durch.
- Es garantiert die Fälschungssicherheit des Bitcoins.
- Es bringt neue Bitcoins in Umlauf.

Die Arbeit der Bitcoin-Miner umfasst verschiedenen Phasen:

Phase 1: Transaktionen werden registriert und verifiziert
Wenn eine Bitcoin-Transaktion, also zum Beispiel die Zahlung für eine Ware im Internet, stattfinden soll, erscheint diese mit Absender- und Empfängeradresse sowie dem zu überweisenden Betrag im Bitcoin-Netzwerk. So sind ständig Transaktionen offen und neue kommen dazu. Ein Miner sucht sich aus allen Bitcoin-Transaktionen, die weltweit durchgeführt werden sollen, eine bestimmte Anzahl aus und prüft jede einzelne. Dazu gleicht er sie mit der Blockchain ab. Die Blockchain ist vergleichbar mit einem Hauptkassenbuch („public ledger"), das jede jemals getätigte Transaktion dokumentiert und

in das jeder hineinschauen kann. Er prüft anhand der Historie der Adressen, ob eine neue Transaktion gültig ist: Verfügt der Käufer über genügend Bitcoins für die Transaktion? Ist er der Eigentümer der Bitcoins, die transferiert werden sollen? Nach der Prüfung fasst der Miner gültige Transaktionen in einer Liste, dem sogenannten Block, zusammen.

Phase 2: Ein neuer Block mit Transaktionen wird vorbereitet

Der Miner fügt nun zu diesem Block den Hash des vorhergehenden Blocks, also des letzten gültigen Blocks, der an der Blockchain hängt, hinzu. Ein Hash ist ein Code, eine individuelle Folge von Buchstaben und Zahlen, der jede beliebige Datei, in diesem Fall den betreffenden Block, eindeutig codiert. Wird in der Datei auch nur ein Zeichen geändert, ändert sich der Hash komplett. Es ist sozusagen der Fingerabdruck der Datei. Neben dem Hash fügt der Miner dem Block eine Nonce hinzu. Die Abkürzung Nonce steht für „Number only used once", das ist zunächst eine beliebige Zahl.

Phase 3: Der neue Block wird verifiziert – das eigentliche Mining

Im nächsten Schritt errechnet der Miner nun einen Hash für den Block, den er gerade zusammengestellt hat. Normalerweise ist ein Hash sehr schnell, in Sekundenbruchteilen, zu errechnen. Für den Bitcoin wurde allerdings festgelegt, dass nur alle zehn Minuten ein neuer Block geschaffen werden soll. Deshalb wurden Kriterien festgelegt, die ein gültiger Hash erfüllen muss. Es reicht also nicht, irgendeinen beliebigen Hash zu finden. Ein gültiger Hash der Bitcoin-Blockchain muss immer mit einer bestimmten Zahl von Nullen beginnen. Also muss der Miner für seinen Block ständig neue Hashes ausprobieren, um einen Hash zu finden, der diese Bedingung erfüllt. Damit sich der Hash ändert, muss er auch den Block jedes Mal leicht ändern, und dafür hat er die Nonce eingebaut. Es wird also immer wieder die Nonce geändert, bevor ein Hash errechnet und gecheckt wird, ob er mit der richtigen Anzahl von Nullen beginnt. Da der gesuchte Hash schwer zu berechnen ist, müssen viele Hashs berechnet werden. So entsteht die enorme Rechenleistung, verbunden mit dem hohen Energiebedarf des Bitcoins.

Phase 4: Der neue Block ist gültig, Transaktionen werden bestätigt

Hat der Miner einen gültigen Hash gefunden, stellt er den verifizierten Block samt seinem Hash ins Netzwerk. Alle anderen Miner beziehen diesen nun in ihre Berechnungen ein. Nur, wenn alle Transaktionen in dem Block korrekt sind, wird er ein verifizierter Teil der Blockchain und weitere Blöcke werden angehängt. Dafür, dass er einen neuen gültigen Block verifiziert hat, bekommt der Miner eine Belohnung von 12,5 Bitcoins. Dazu kommen in der Regel noch Transaktionsgebühren für die einzelnen Transaktionen im Block.

Proof-of-Work garantiert Fälschungssicherheit des Bitcoins

Der Vorgang vom Erstellen eines neuen Blocks mit Hash des vorhergehenden Blocks über das Errechnen eines neuen Hashs und Verifizieren des Blocks wird als Proof-of-Work

bezeichnet. Der Proof-of-Work stellt sicher, dass es sehr aufwendig ist, einen neuen Block für die Blockchain zu finden. Die neuen Bitcoins und die Transaktionsgebühren erhält der Miner erst, wenn an seinen Block mindestens 100 weitere Blocks angehängt wurden. Das ist der Nachweis dafür, dass alle Transaktionen in seinem Block gültig sind. Wäre auch nur eine Transaktion ungültig, würde das bemerkt werden und mit seinem Block würde nicht mehr weitergearbeitet werden. Es ist dieser Umstand, der den Bitcoin fälschungssicher macht, denn für einen Block, der falsche Transaktionen enthält, bekommt der Miner keine Bitcoins. Seine komplette Rechenleistung, um den Hash zu errechnen, wäre umsonst gewesen. Die im weltweiten Bitcoinetzwerk errechneten Hashes werden in der Einheit Terahash pro Sekunde (TH/s) angegeben. Ein Terahash entspricht 10^{12} Hashes. Das lässt erahnen, welche immense Rechenleistung den Bitcoin sichert.

Transaktionsgebühren beschleunigen Transaktionen
Wenn sehr viele Bitcoin-Transaktionen anstehen, spielt der Faktor Zeit eine Rolle für deren Umsetzung. Es kann deshalb manchmal länger dauern, bis eine Transaktion umgesetzt wird. Wer ganz sicher gehen will, dass seine Transaktion schnell durchgeführt wird, kann zu seiner Transaktion eine Gebühr beistellen. Diese Gebühr geht an den Miner. Die Miner werden die Transaktionen immer nach Höhe der Transaktionsgebühr abarbeiten

Die Miner werden mit neuen Bitcoins vergütet
Die Miner werden für ihre Arbeit mit Bitcoins entlohnt. Auf diesem Weg werden gleichzeitig neue Bitcoins in Verkehr gebracht. Zurzeit werden pro Block 12,5 Bitcoins ausgeschüttet.