

# Rabbit fragt #7



## Was sind Hashes und was bedeutet Hashrate?



Hashes sind Ausgabewerte die bestimmte Eigenschaften erfüllen. Eine SHA 256 Hashfunktion erzeugt aus einem Eingabewert (einer Nachricht oder anderen Daten) einen festen Ausgabewert (den Hashwert). SHA bedeutet „sicherer Hash-Algorithmus“. Die Zahl 256 gibt die Länge des Hashes an, in dem Fall 256 Bit. Ich benutze einen SHA 256 Generator und gebe z.B. das Wort **Bitcoin** ein, der Hash der entsteht sieht dann für diese Eingabe immer so aus. `b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4`

Jetzt gebe ich das Wort **bitcoin** ein und es entsteht dieser Hash.

`6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b`

Das bedeutet, wenn man nur eine Kleinigkeit verändert, verändert sich der komplette Hash. Nun errechnen die Miner einen passenden Hash, der eine gewisse Anzahl vorstehender Nullen haben muss (Difficulty), um einen Block an die Blockchain zu hängen. Die Miner nehmen die wartenden Transaktionen aus dem Mempool, die Nonce und den Hash des vorherigen Blocks und suchen einen neuen Hash für den aktuellen Block. Jeder Block ist dadurch in sich miteinander verkettet. Wenn jemand die Kette manipulieren wollte, müsste er auch die anderen Blöcke ändern. Das würde unendlich viel Zeit und Energie (Strom) kosten. Die speziell verbauten Microchips, die nur zum errechnen dieser Hashes sind, können z.B. beim Aintminer s17, 73TH/s finden das sind 73.000.000.000.000 Billionen Hashes in der Sekunde. Eine unfassbar große Menge. Im Vergleich hat ein NerdMiner 73KH/s auf dem Schreibtisch, das sind 73.000 Tausend Hashes in der Sekunde. Einen gültigen Block zu finden ist also eine Sache der Power/Geschwindigkeit. Die Hashrate stellt die Hashpower aller Miner auf der Welt da, die im Bitcoin-Netzwerk minen. Umso höher die Hashrate um so sicherer ist das Netzwerk.

Ähnhm, Moment mal, Rabbit fragt: Was ist das Bitcoin-Netzwerk?

Das erfahren wir im nächsten Hole, bis dann...

