Wie funktionieren Bitcoins?

von Gerhard Dorn

Referat am 5.11.2018 (Graz)

Bitcoin – ein digitales dezentrales Währungssystem (Idee)
In diesem kurzen Beitrag möchte ich die Technologie hinter Bitcoin, einer neuen Art digitaler und dezentraler Währung, vorstellen.
Im November 2008 wurde die Idee von Bitcoin geboren, indem unter dem Pseudonym Satoschi Nakamoto ein Whitepaper mit der Idee und ein Programmpaket veröffentlicht wurde.
Die Hauptidee bestand darin, eine digitale, dezentrale Währung zu schaffen, bei der also nicht alle Kontostände zentral bei einer Leitstelle (Bank) gespeichert sind, sondern bei der die Kontostände transparent, aber anonym überall gespeichert werden. Um zu gewährleisten, dass kein Geld aus dem Nichts entsteht oder verschwindet, werden gleich auch alle Überweisungen in dieser Liste gespeichert, aus denen ersichtlich ist, wie die Bitcoins auf das jeweilige Konto gewandert sind.
Es gibt also ca 10000 [1] dieser sogenannten Nodes, die die gesamte Liste an Überweisungen speichern und aktualisieren.

Wie werden Überweisungen in dieser Liste gespeichert?
Dies wird durch die sogenannte **Blockchain** Idee umgesetzt. Alle Überweisungen sind chronologisch im zehn Minuten Takt in sogenannte Blöcken geordnet. Also alle Überweisungen, die in zehn Minuten dem Bitcoin Netzwerk mitgeteilt werden, werden zu einem Block zusammengefasst und sollen an den letzten Block angehängt werden. Wenn man so Blöcke aneinander anhängt, entsteht eine Kette, daher der Name Blockchain.

Was steht in einem Block?
Ein Block besteht aus einem Header und einer Auflistung aller Überweisungen:

- Header:
  - Nummer des Blocks
  - Hash des vorherigen Blocks (fälschungssicherer Verweis auf den vorherigen Block)
  - Schwellwert, der maßgeblich für die Schwierigkeit der Blockberechnung ist
  - Nonce: variables Feld für die Rechenaufgabe zur Berechnung des Blocks
  - Merkle Root: verweist auf das ganze Bündle an Überweisungen
- Überweisungen

Siehe Abb. 1.

Wie funktioniert das Anhängen von einem Block an einen anderen?
Das Aneinanderhängen funktioniert mit einem sogenannten Hashwert, einer Zahl, die aus dem alten Block berechnet (soetwas wie eine Prüfsumme) und im neuen Block gespeichert wird.
Sobald auch nur ein Zeichen im alten Block gefälscht wird, ändert sich diese Prüfzahl (Hashwert) und somit kann man überprüfen, ob etwas nicht stimmt.

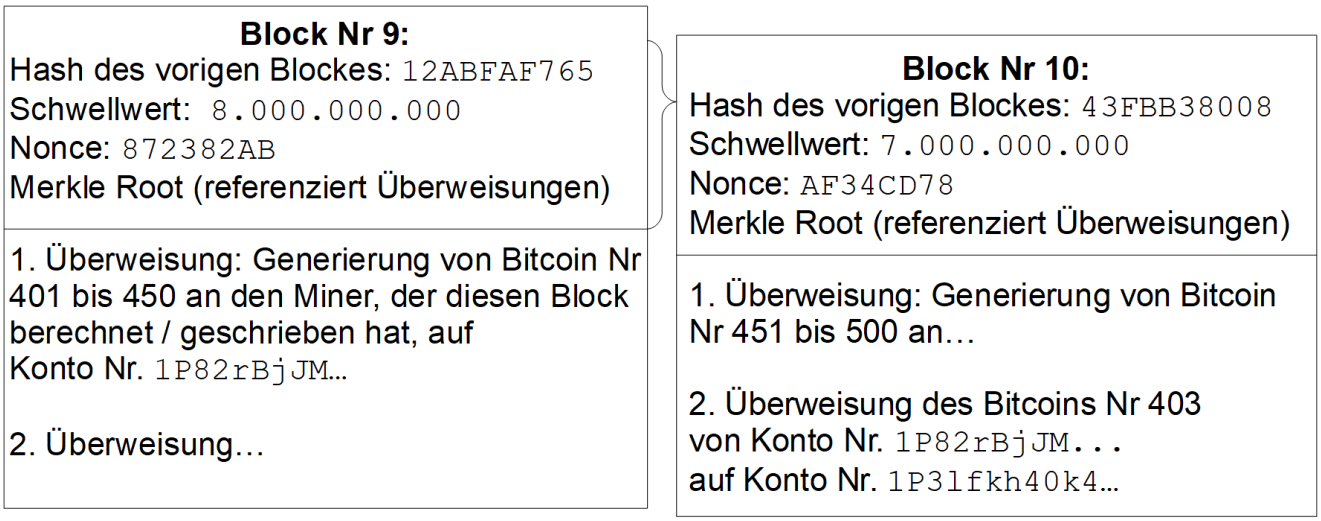

Abbildung 1: Aufbau zweier Blockchain Blöcke. Der Hashwert (Prüfzahl) des Blockheaders muss kleiner als der Schwellwert sein um einen gültigen Block darzustellen und vom Bitcoin Netzwerk akzeptiert zu werden. Der Hashwert kann mit der Nonce Zahl beeinflusst werden. Das Finden der Nonce Zahl um unter den Schwellwert zu kommen stellt die immens schwierige Rechenaufgabe dar.

Wie wird gewährleistet, dass die Liste überall immer am gleichen Stand ist und es keine unterschiedlichen Varianten gibt?
Die 10000 Nodes tauschen ständig ihre Blöcke aus und bei Unstimmigkeiten wird mit einer Mehrheitsentscheidung entschieden. Das heißt man müsste 5001 der 10000 Nodes übernehmen um die Blockchain, damit die Überweisungen und damit die aktuellen Kontostände zu fälschen.
Kann man eine Blockchain fälschen?
Um die Blockchain fälschungssicher zu machen, wurde ein sehr arbeitsintensiver Mechanismus eingebaut (ähnlich einem Wasserzeichen, das schwer zu reproduzieren, aber leicht zu kontrollieren ist): **Das Minen**
Jeder Block, der an die Blockchain hinzugefügt werden soll, muss eine Rechenaufgabe lösen, deren Schwierigkeit gerade so eingestellt ist, dass die gesamte Rechenkapazität, die derzeit an dem Problem arbeitet (Summe aller Miner), im Durchschnitt alle zehn Minuten eine Lösung errechnet.
Das Errechnen eines Blocks benötigt also sehr sehr viel Rechenleistung, wodurch das Fälschen einer Blockchain erschwert wird, müsste man doch alle Blöcke der Vergangenheit nachrechnen.
Wieso sollte man seine Rechenkapazität als Miner zur Verfügung stellen?
Derjenige, der es schafft einen neuen Block zu errechnen, erhält eine Belohnung in Form von Bitcoins. Mit dem Erzeugen eines jeden neuen Blockes werden Bitcoins ausgegeben (geschürft). Die Anzahl der ausgegebenen Bitcoins pro Block halbiert sich alle 210.000 Blöcke (im Moment 12.5 Bitcoins pro Block). Der Miner kann in den Block sein Konto schreiben, dem dann diese geschürften Bitcoins gutgeschrieben werden (siehe erste Überweisung in Abbildung 1).

Wer entscheidet, welche Überweisungen in den Block aufgenommen werden?
Jeder Miner sammelt Überweisungen um einen neuen Block zu füllen, für das Aufnehmen einer Überweisung in einen neuen Block erhält der Miner eine Überweisungsgebühr.
Der erste Miner, der einen gültigen Block (nach Lösen der Rechenaufgabe) an das Bitcoin Netzwerk schickt und von mehr als 50 % der Nodes bestätigt wird, wird in die Blockchain übernommen.

Ist das Netzwerk getrennt und entstehen auf diese Weise zwei unterschiedliche Blockstränge wird jener Strang weiter akzeptiert, der die größte Zustimmung (>50%) aufweist.

Welche Rechenaufgabe wird von den Minern gelöst um einen gültigen neuen Block zu erzeugen?

Die Rechenaufgabe, die es zu lösen gilt, besteht darin eine Zahl (Nonce) im Blockheader so zu wählen, dass der Hashwert (Prüfzimmer) des Blockheaders kleiner als der vorgegebene Schwellwert ist, der die Schwierigkeit beschreibt. Die Hashfunktion hat dabei die schöne Eigenschaft, dass man nicht vorhersehen kann wie man diese Nonce Zahl ändern muss, und man fast alle Zahlen durchprobieren muss.

Was ist ein Hash?

Ein Hash ist eine Prüfzahl, die sich aus einem Text mit der sogenannten Hashfunktion berrechnet lässt. Anhand dieser Zahl kann man einen Text eindeutig identifizieren. Die Hashfunktion hat ein chaotisches Verhalten, das heißt, der Hashwert ändert sich völlig unvorhersehbar, auch wenn man im Eingabetext nur ein einziges Zeichen ändert. Einen Text so zu ändern, dass ein bestimmter Hashwert herauskommt ist daher eine sehr schwierige Aufgabe, die nur durch Probieren aller Textänderungen bewerkstelligt werden kann. Dies ist die Rechenaufgabe, die beim Minen (Schürfen) von Bitcoins bei der Blockerstellung, gelöst werden muss.

Wie entstehen Bitcoins?

Bitcoins entstehen als Belohnung für das Herstellen eines schwierig zu fälschenden Blocks (Minen). Diese können dann überwiesen werden. Siehe oben.

Wann besitze ich ein Bitcoin?

Um ein Bitcoin zu besitzen muss man (als einziger) in der Lage sein, es zu überweisen. Dies wird über eine asynchrone Verschlüsselung bewerkstelligt, bei der es einen öffentlichen und einen privaten Schlüssel gibt. Bei einer Verschlüsselung wird dabei mit dem einen ver- und mit dem anderen entschlüsselt.

Man kann sich das vorstellen wie ein Nummernbogenschloss, das zwei Zahlen kennt, eine öffentliche und eine geheime (private). Wenn mit einer der beiden Zahlen zugesperrt wird, kann man nur mit der anderen Zahl wieder aufsperren.

Wie wird also ein Bitcoin von dem Besitzer überwiesen?

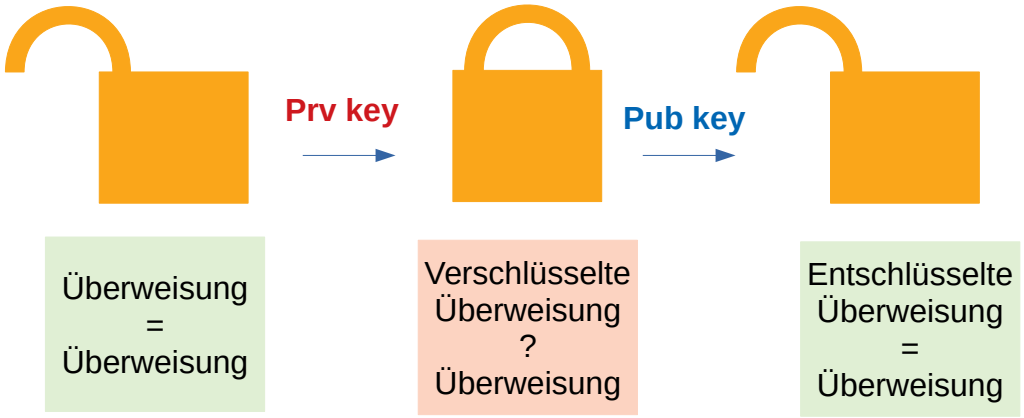

Abbildung 2: Darstellung einer Überweisung. Nur mit dem privaten Schlüssel (Prv key) kann eine gültige Überweisung angeordnet (signiert) werden. Die Überprüfung der Überweisung kann von jedem mit der Kontonummer (entspricht dem öffentlichen Schlüssel (Pub key) durchgeführt werden.

Dazu erstellt man die Überweisung, bestehend aus Betrag, Zielkonto, Ausgangskonto und verschlüsselt diese Überweisung dann noch extra mit seinem geheimen Schlüssel. Die Kontonummern entsprechen den öffentlichen Schlüsseln. Mit diesem öffentlichen Schlüssel kann jeder überprüfen, ob diese

Überweisung korrekt ist, indem man den verschlüsselten Text mit der Kontonummer entschlüsselt und mit dem Überweisungtext vergleicht. Stimmen die zwei Texte überein, ist die Überweisung korrekt und kann in einem Blockchain Block aufgenommen werden (Siehe auch Abbildung 2).
Da es ohne den geheimen Schlüssel faktisch unmöglich ist, so eine Überweisung zu fälschen, gelten die Bitcoins als sehr sicher (solange der eigene geheimen Schlüssel nicht gestohlen wird).

Wie funktioniert die Verschlüsselung genau?
Die asynchrone Verschlüsselung die bei Bitcoins verwendet wird heißt ECDSA (Elliptic Curve Digital Signature Algorithm) und benutzt eine spezielle elliptische Kurve (Secp256k1) um asynchrone Schlüssel zu erstellen.
Im Prinzip beruht die Verschlüsselung darauf auf einer elliptischen Kurve (y^2 = x^3 + 7, siehe Abbildung 3) Punkte (über einer Restklasse zu einer sehr großen Primzahl) zu multiplizieren. Die Multiplikation eines Referenzpunktes mit einer ganzen Zahl (privater Schlüssel) ergibt einen neuen Punkt auf dieser Kurve (öffentlicher Schlüssel).
Da es sehr leicht ist, mit dem privaten Schlüssel den öffentlichen Schlüssel auszurechnen (man weiß, wie oft man den Referenzpunkt G multiplizieren muss), es aber irrsinnig schwierig ist, vom öffentlichen Schlüssel auf den privaten Schlüssel zu schließen (Division, die Umkehroperation, ist hier nicht möglich und man muss durchprobieren), ist dieses Zahlenpaar die solide Basis der gesamten Cryptoökonomie.

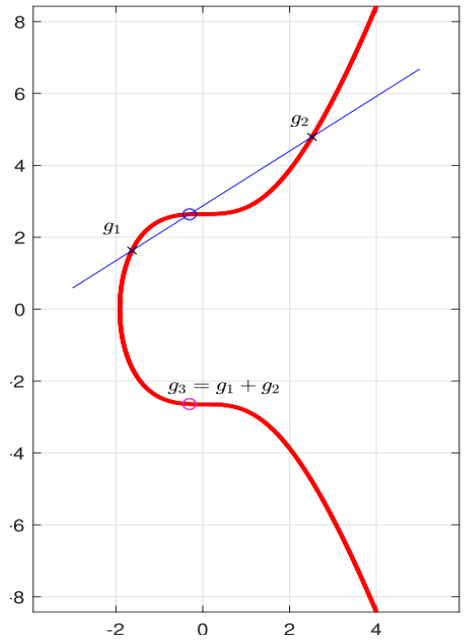

Abbildung 3: Die elliptische Kurve, die bei der Bitcoin Verschlüsselung (und den meisten anderen Kryptowährungen) verwendet wird.

References:
[1] https://bitnodes.earn.com/
[2] Bitcoin, Blockchain und Kryptoassets
Aleksander Berentsen, Fabian Schär, Universität Basel