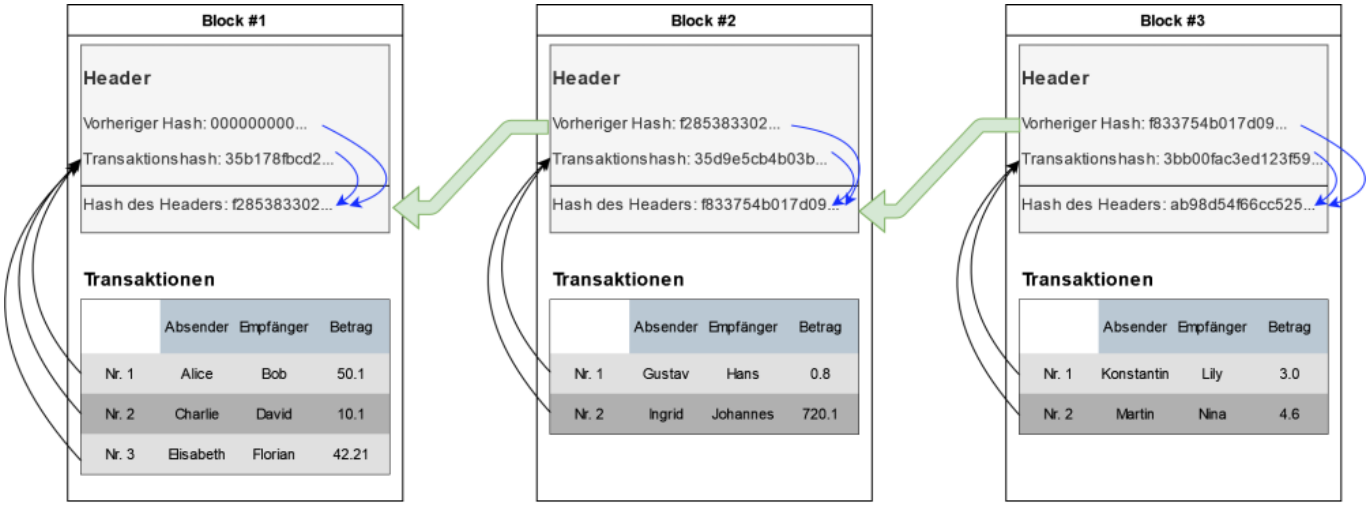
Wie funktioniert die Blockchain? Am Beispiel von Bitcoin!

Die Blockchain kannst du nur verstehen, wenn du zuvor Hashing verstanden hast!

Mit der Veröffentlichung von Bitcoin im Jahr 2009, der ersten und bekanntesten Cryptowährung, wurde gleichzeitig auch die neue Technologie "Blockchain" veröffentlicht[1]. Blockchains können auch für andere Dinge verwendet werden (siehe Ende des Artikels), hier soll die Funktionsweise aber am Beispiel von Bitcoin gezeigt werden.

Wenn es um Finanzsysteme geht, dann geht es in erster Linie um Vertrauen: Man muss Banken vertrauen, dass das eigene Geld dort gut aufgehoben ist und dass Buchungen korrekt vermerkt sind. Mit Blockchain-basierten Cryptowährungen wird dieser Punkt eliminiert. Denn anstatt fremden Menschen zu vertrauen, muss man nur noch den mathematischen, kryptographischen Hashfunktionen trauen!

Aufbau



Alle 10 Minuten entsteht ein neuer Block. In einem Block sind alle Transaktionen ("Überweisungen") der letzten 10 Minuten enthalten. Stand Oktober 2024 sind das etwa 5000 Transaktionen pro Block.

Aus allen Transaktionen wird ein SHA-256 Hash berechnet und im Header des Blocks gespeichert (dünne schwarze Pfeile). Ebenso wird dort der Hash des vorherigen Blocks gespeichert (dazu gleich

mehr!). Aus allen Informationen im Header wird wiederum ein Hash generiert. Dieser wird im jeweils darauffolgenden Block im Header gespeichert.

1)

Whitepaper und Forschung zu Blockchains gab es schon länger, aber erst mit Bitcoin entstand die erste sinnvoll nutzbare Blockchain, die daraufhin große Verbreitung fand.

From:
https://www.info-bw.de/ -

Permanent link:
https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:blockchain:start?rev=1729668204

Last update: **23.10.2024 07:23**