

Wie funktioniert die Blockchain? Am Beispiel von Bitcoin!



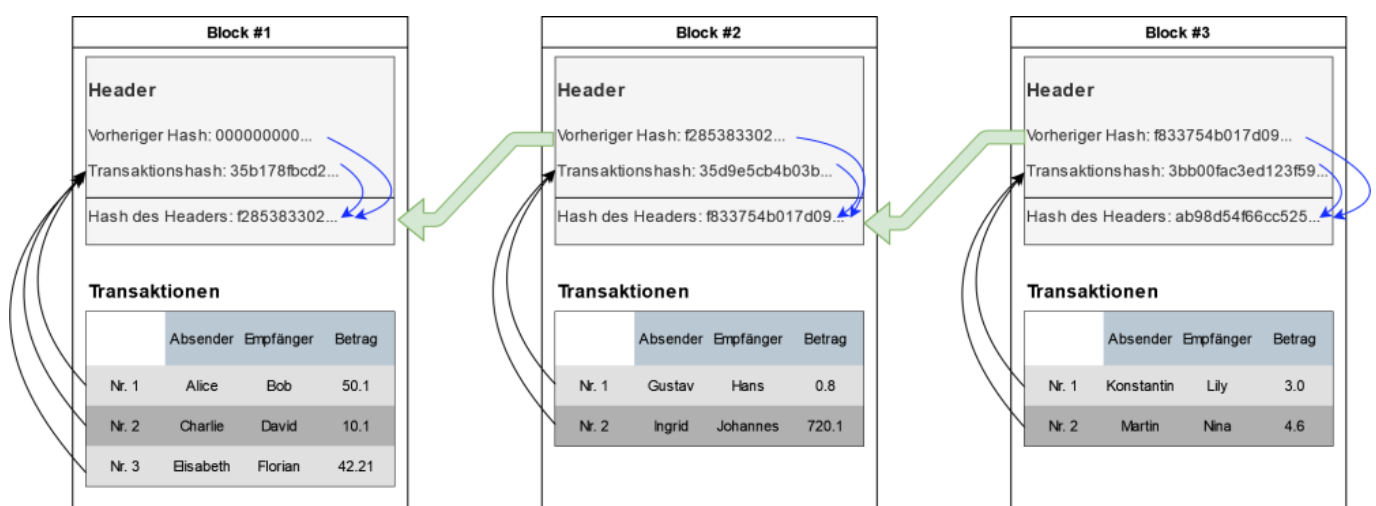
Die Blockchain kannst du nur verstehen, wenn du zuvor [Hashing](#) verstanden hast!

Mit der Veröffentlichung von Bitcoin im Jahr 2009, der ersten und bekanntesten Cryptowährung, wurde gleichzeitig auch die neue Technologie "Blockchain" veröffentlicht¹⁾. 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 (dünne blaue Pfeile). Dieser wird im jeweils darauffolgenden Block im Header gespeichert. Das bedeutet, dass jeder neue Block auf den Vorgänger verweist (grüne Pfeile). Die Blöcke sind also miteinander "verkettet" - daher der Name Blockchain.

Durch die Nutzung der Hashfunktionen bietet dieser simple Aufbau einen unschlagbaren Vorteil: Sollte jemand später in einem alten Block eine Buchung fälschen wollen, so wird daraufhin der bisherige Transaktionshash ungültig und müsste neu berechnet werden. Daraufhin wird auch der Headerhash ungültig und muss ebenso neu berechnet werden. In diesem Moment würde das Netzwerk aller Blockchains weltweit Alarm schlagen, da der Headerhash des veränderten Blocks nicht mehr mit dem verlinkten Hash des nächsten Blocks übereinstimmt. Man könnte genau sehen, in welchem Block eine Manipulation stattgefunden hat.



(A1)

Öffne das interaktive Blockchain-Tool und experimentiere mit den Einträgen. Du kannst neu berechnete Headerhashes auch kopieren und im nächsten Block einfügen. Aktiviere dabei noch nicht das Block-Mining! <https://tools.info-bw.de/blockchain/>

Verteiltes Netzwerk

Jetzt könnte man denken, dass ein Angreifer dann doch einfach alle weiteren Blöcke iterativ korrigieren und alle Hashes bis zum neuesten Block neu berechnen könnte. Ja, im Prinzip kann er das auch. Allerdings stünde er dann mit seiner eigenen, manipulierten Blockchain ganz allein auf weiter Flur. Denn von der Blockchain gibt es zahlreiche Kopien auf tausenden Rechnern weltweit. Auch du kannst eine Kopie der Blockchain hosten ("speichern") und damit zur Stabilität des Netzwerks beitragen.

Stabilität, Vertrauen und das Block-Mining

Prinzipiell kann also jeder eine Kopie der Blockchain speichern und auch neue Blöcke generieren/berechnen und anschließend mithilfe seiner Blockchain behaupten, dass er soeben Millionen an Bitcoins auf sein Konto bekommen habe. Allerdings gibt es im Netzwerk die sogenannte 51%-Hürde²⁾: Die Mehrheit aller weltweiten Blockchains gewinnt bzgl. der Validität der Blockchain. Selbst wenn ein größeres Netzwerk von Angreifern z. B. 50.000 Kopien einer manipulierten Blockchain besitzt, dann genügt das nicht, falls der Rest der Menschheit 60.000 Kopien der nicht-manipulierten Blockchain dagegensetzen kann.

Easy, kann man jetzt denken: Dann müssen die Angreifer also einfach nur 70.000 Kopien der manipulierten Blockchain besitzen? Jein, denn wir haben noch nicht über das **Block-Mining** gesprochen.

Mining

Um genau solche 51%-Angriffe abzuwehren wird bei Bitcoin das **Proof-of-Work**-Verfahren eingesetzt. Ein neuer Block gilt nicht einfach direkt als valide, sobald die Hashes wie oben gezeigt berechnet sind. Vielmehr war das obere Bild noch nicht vollständig, denn im Header versteckt sich noch ein weiterer Wert, der in die Berechnung der Headerhashes einfließt: Die **Nonce** (number used once). Diese ist eine natürliche Zahl, die einen ganz bestimmten Wert besitzen muss.

Sobald ein neuer Block entsteht, machen sich hunderttausende Bitcoin-Mining-Rechner weltweit daran, den Headerhash immer wieder neu zu berechnen. Dabei verändern sie jedes Mal den Wert der Nonce um 1 und probieren damit alle möglichen Nonce-Werte durch. Ziel ist es, einen **Headerhash** zu erhalten, **der mit einer bestimmten Anzahl an 0en beginnt**. Wie viele 0en nötig sind, das wird regelmäßig im weltweiten Blockchain-Netzwerk so angepasst, dass die durchschnittliche Berechnung des korrekten Hashes (**weltweit!**) 10 Minuten benötigt - dies ist auch als *Difficulty* bekannt. Der erste Rechner, der die korrekte Nonce und damit den korrekten Hash gefunden hat, bekommt eine Belohnung in Form von Bitcoin. Erst wenn 51% der Rechner diesen Hash bestätigt haben, gilt er weltweit als fertig berechnet und anerkannt.

Für Angreifer genügt es also nicht, die Werte und Hashes einfach nur neu zu berechnen. Vielmehr müssten sie durchschnittlich mehr als 51% der weltweiten Bitcoin-**Rechenkapazität** aufweisen, um einen eigenen, manipulierten Block vor allen anderen Rechnern korrekt zu berechnen und damit in die weltweite Blockchain einfließen lassen zu können. Dies ist glücklicherweise kaum möglich.



(A2)

Gehe wieder zum [interaktiven Blockchain-Tool](#) und aktiviere nun das Block-Mining. Teste nun, wie lange jeweils die Ermittlung der korrekten Nonce und die Berechnung des Headerhashes dauert.

Andere Einsatzzwecke der Blockchain

Alle Einsatzgebiete nutzen insbesondere die Fähigkeit der Blockchain, dass ältere Einträge nicht mehr (einfach) nachträglich manipuliert werden können.

- Dokumentation der Lieferkette: Automatisierte Techniken ermöglichen das Eintragen aller Zwischenstationen eines Produkts in eine Blockchain. So kann der Endanwender z. B. per QR-Code genau den (Produktions-/Transport-)Weg eines Produkts verfolgen. Dies wird zum Teil bereits eingesetzt.
- Ausstellung und Verwaltung von Zertifikaten: Dokumente, Ausweise, Verschlüsselungszertifikate und ähnliches können mit Signaturverfahren und ähnlichem mithilfe einer Blockchain verifiziert werden.
- Zeitkapsel: Sobald jemand etwas (oder dessen Hash) in einer Blockchain einträgt, ist beweisbar, dass dies zu diesem Zeitpunkt bereits vorhanden war. Forscher können damit z. B. ihre Entdeckungen speichern und man kann auch Jahre später noch nachweisen, wer der erste war, der dies entdeckt hat.
- Bei Wahlen könnte jeder Wähler nachvollziehen, ob seine Stimme korrekt berücksichtigt wurde.

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.

2)

Insb. als 51%-Angriff bekannt

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

Permanent link:
<https://www.info-bw.de/faecher:informatik:oberstufe:kryptographie:blockchain:start?rev=1729671647>

Last update: **23.10.2024 08:20**

