Ausführliche Skripten zum Thema im Ordner von Katharina Spehr

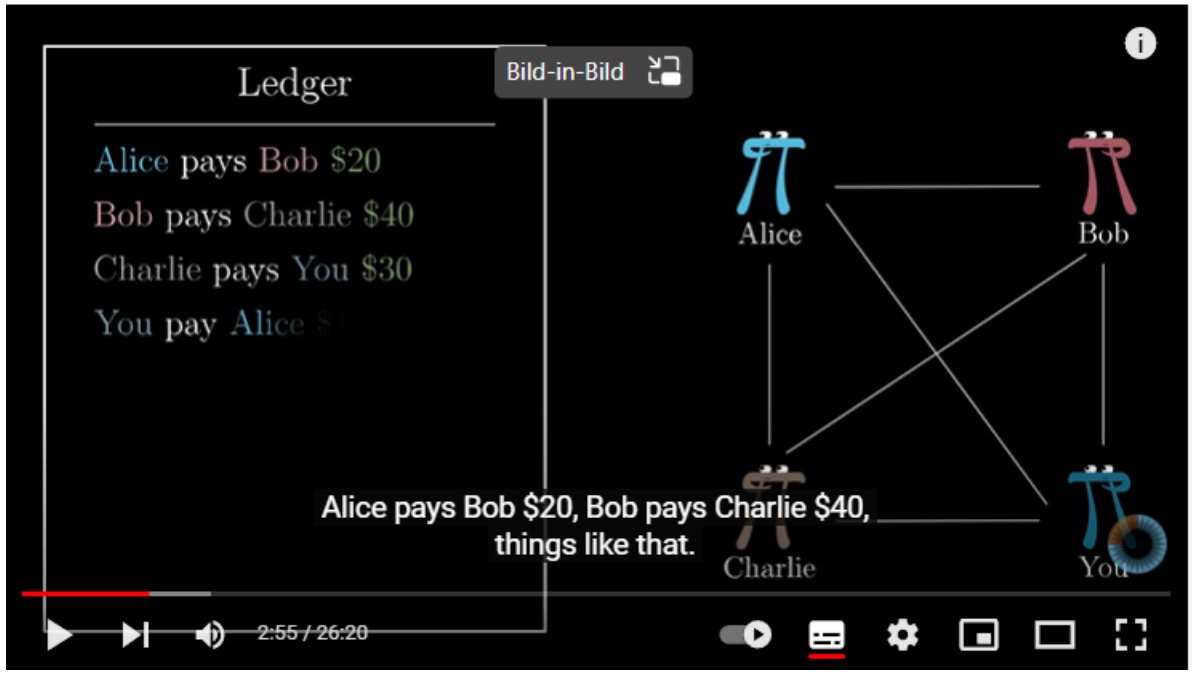
Wie funktioniert Bitcoin?

Am 31. Oktober 2008 veröffentlichte ein Nutzer mit dem **Pseudonym Satoshi Nakamoto** das neunseitige Bitcoin Whitepaper

„Bitcoin: A Peer-to-Peer Electronic Cash System“

– das war gleichzeitig der Startschuss für die Kryptowährung

- Rein digitale Währung
- Keine Regierung gibt sie raus, keine Banken, die Konten verwalten und Überweisungen verifizieren
- Niemand weiß wirklich, wer sie erfunden hat
- System von dezentralisierter Verifikation basierend auf Mathematik, bzw. Kryptographie



Öffentliche Liste, z.B. auf Website, jeder kann Zeilen hinzufügen

Problem: Verifikation

Lösung: Digitale Unterschrift public key /secret key Paar

Signiersystem

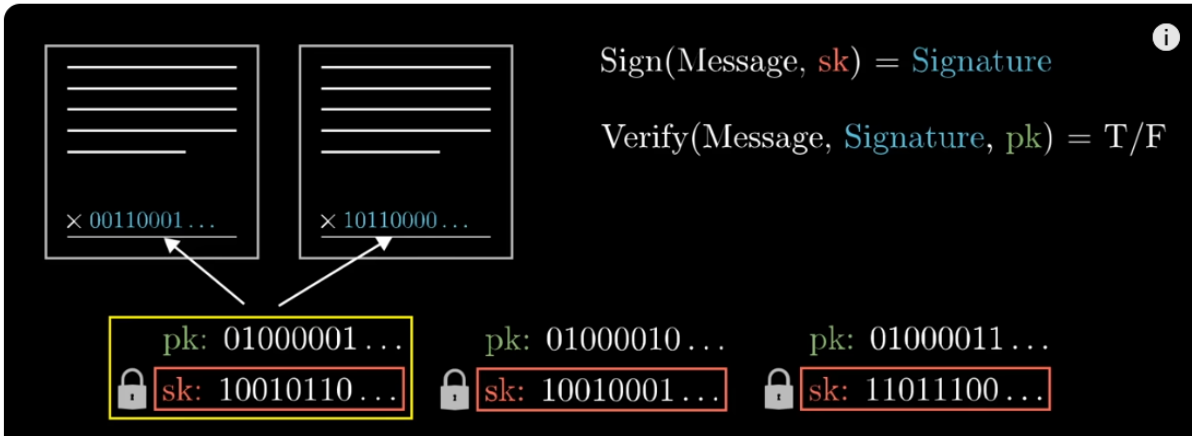
Ein **Signiersystem** wird benutzt, um Integrität, Authentizität und Verbindlichkeit beim elektronischen Nachrichtenaustausch zu gewährleisten.

Integrität: Die Nachricht, die man erhält, ist von keiner dritten Person manipuliert worden.

Authentizität: Die Nachricht, die man erhält, stammt wirklich von der Person, die als Absender angegeben ist.

Verbindlichkeit: Der Urheber kann nachträglich nicht bestreiten, die Nachricht verfasst zu haben.

SignFunktion, die vom Inhalt und dem secret key abhängt, wenn man den Inhalt ändert, ändert sich auch die Funktion



Verify-Funktion, die mit dem public key bestätigt (true/false), dass die Unterschrift mit dem private key erstellt wurde

Um mit dem public key die richtige Unterschrift herzustellen, kann man nur probieren, dafür gibt es aber 2^{256} Möglichkeiten.

Der Public Key wird z.B. mittels SHA256 oder mittels des **Elliptic Curve Digital Signature Algorithm (ECDSA)** vom Private Key abgeleitet.

Wer den Private Key besitzt, hat die Kontrolle über die zugehörige Wallet.

Mathematisch gesehen ist der private Schlüssel eine zufällige Zahl zwischen 1 und 2^{258}

Es ergibt sich eine Zahl mit 51 Stellen und 2^{256} Varianten.

Beispiel für Private Key und Public Key

Public Key (Öffentlicher Schlüssel)
Ein Beispiel für einen Public Key könnte so aussehen:

1a3b5c8d9e1f2g3h4i5j6k7l8m9n0o1p2q3r4s5t6u7v8w9x0y1z2a3b4c

Private Key (Privater Schlüssel)
Ein entsprechendes Beispiel für einen Private Key könnte folgendermaßen aussehen:

5k8x4f2g9d6c3s2v1f0g7h6m5n4b3v2c1x2y3z4a5b6e7d8c9f0e1d2g

Nur unterschriebene Transaktionen sind gültig

Wie verhindert man, dass jemand Schulden anhäuft und nicht mehr zahlen kann?

Keine Überziehungen erlaubt

Dadurch wird der Zusammenhang mit einer echten Währung gekappt.

Die Liste aller Transaktionen ist die Währung!

Jeder hat eine persönliche Liste und teilt allen seine Transaktionen mit

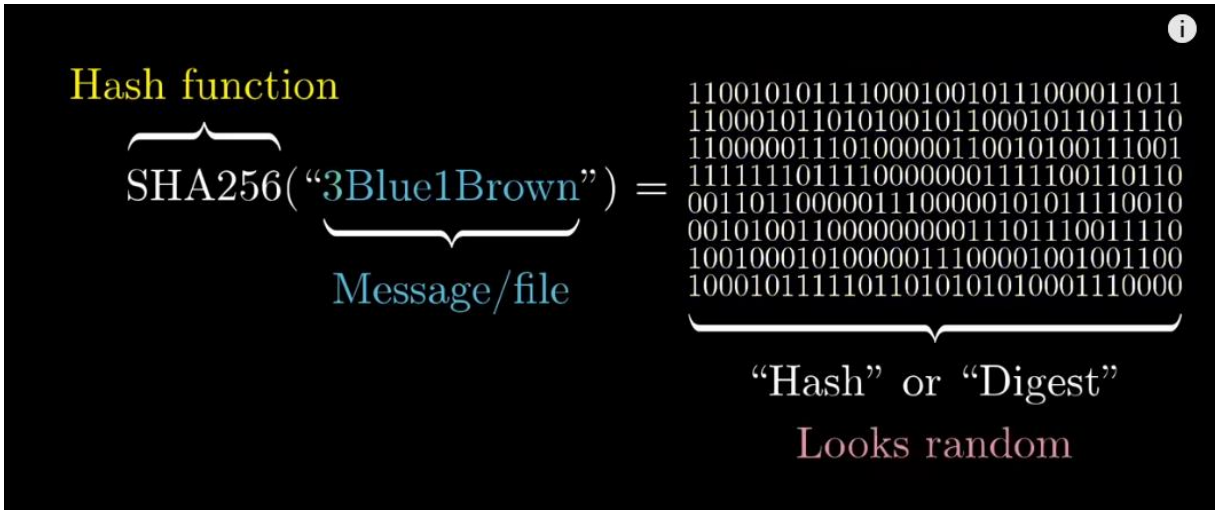
Diese Liste wird Ledger genannt und dient dazu eine genaue und verlässliche Aufzeichnung aller Finanzaktivitäten zu gewährleisten.

Wie gelingt es, dass es ein Protokoll gibt, dass Transaktionen akzeptiert oder ablehnt, und dass jeder die gleiche Liste hat in der die Transaktionen in der gleichen Reihenfolge aufgeschrieben sind? So dass jede Person in der Welt, die diesem Protokoll folgt ein Ledger hat, der wie der eigene aussieht.

Die Lösung steht im originalen Bitcoin-Paper. Man glaubt dem Ledger, in dem die meiste Computerarbeit steckt (proof of work). Dazu verwendet man die kryptographische Hashfunktion. Um ein Ledger zu fälschen braucht es einen unleistbaren Aufwand an Computerarbeit.

Was ist eine Kryptographische Hashfunktion?

Input: irgendein Text, Output 256 Bit Zeichenfolge aus 0 und 1 „Hash“der Nachricht



SHA256, ändert sich komplett sobald sich ein Zeichen im Text ändert. Wie sich die Nachricht ändert ist völlig unvorhersehbar.

Der Weg zurück ist nur durch ausprobieren möglich, 2^{256} Möglichkeiten

Niemand hat bisher einen Weg gefunden, aus dem Hash mit einem Programm den ursprünglichen Text wieder herzustellen.

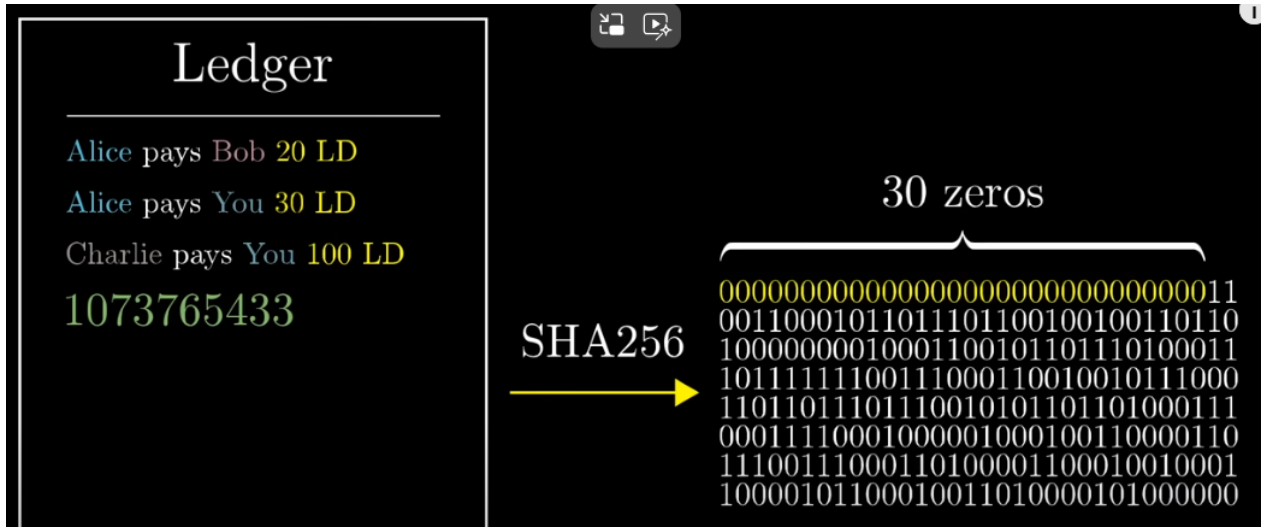
Es gibt keinen richtigen Beweis, dass es nicht geht.

Dennoch basiert unsere Computersicherheit auf dieser Eigenschaft der Hashfunktion.

Proof of Work

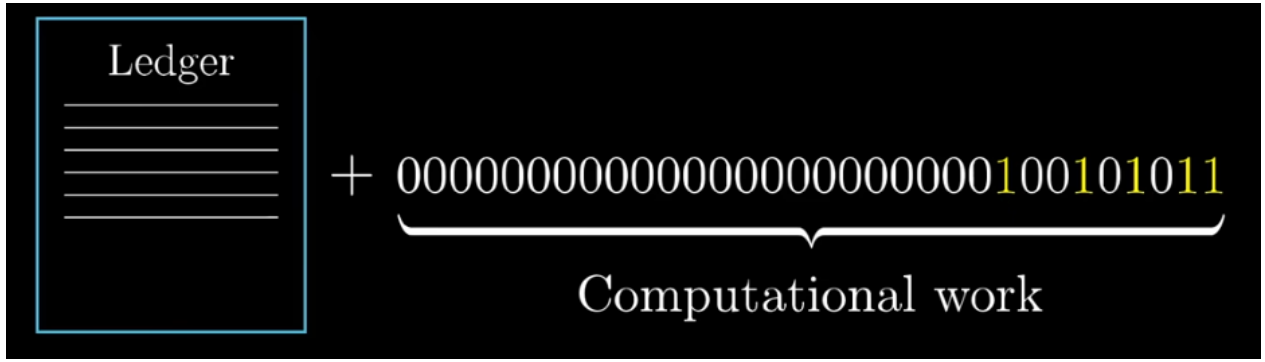
Am Ende jedes Blocks wird eine spezielle Zahl hinzugefügt (Nonce = Number used once), so dass wenn man SHA 256 auf diese Liste anwendet der Hashwert mit einer festgelegten Zahl von Nullen beginnt.

Die Wahrscheinlichkeit, dass das für eine zufällige Zahl klappt ist $\frac{1}{2^{30}}$.



Nachdem wir es mit einer krytographischen Hashfunktion zu tun haben, findet man diese Zahl nur durch Raten und Ausprobieren. Wenn man die Zahl aber einmal gefunden hat und man die Hashfunktion anwendet startet der Hash mit 30 Nullen und man kann verifizieren dass diese Arbeit stattgefunden hat. Das nennt man Proof of Work.

Diese ganze Arbeit ist mit der Liste der Transaktionen verknüpft, sobald man die kleinste Änderung in der Liste vornimmt, verändert sich der Hash komplett und beginnt nicht mehr mit 30 Nullen.



Um sicherzustellen, dass die dezentral gespeicherten Ledger überall die gleichen sind, wird der Liste geglaubt, in der die meiste Computerarbeit steckt.

Dazu wird die Liste in Blöcke aufgeteilt an deren Ende jeweils die Zahl steht, die sicherstellt, dass der Hash mit 30 Nullen beginnt.

eine Transaktion ist nur gültig, wenn sie unterschrieben ist,

ein Block ist nur gültig, wenn er den Proof of Work enthält.

Um eine Reichenfolge festzulegen enthält jeder Block den vorhergehenden Hash als ersten Wert.

Wenn jetzt also im Block etwas verändert wird, oder die Reihenfolge der Blöcke geändert wird, ändert sich der Hash und man müsste alle Rechnungen neu durchführen, damit die geforderte Zahl an Nullen da ist.

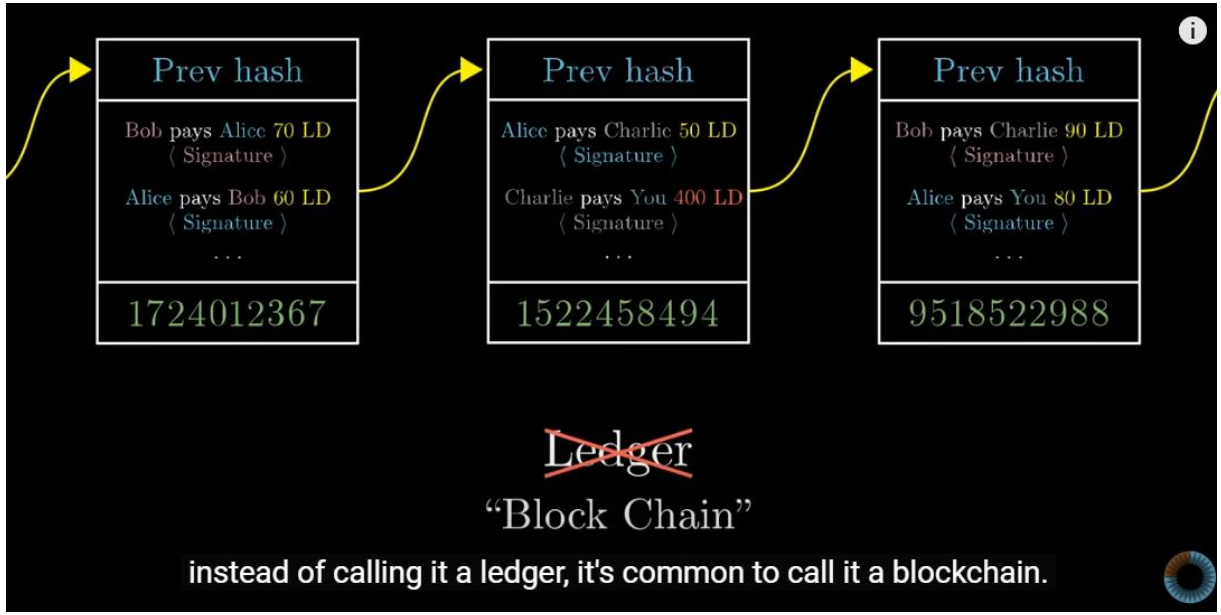
Blockchain

Block mit Liste der Transaktionen, zusammen mit dem Proof of work

Beinhaltet den Hash des vorhergehenden Blocks

Jede Veränderung wirkt sich aus

Deswegen nennt man das nicht Ledger sondern Blockchain

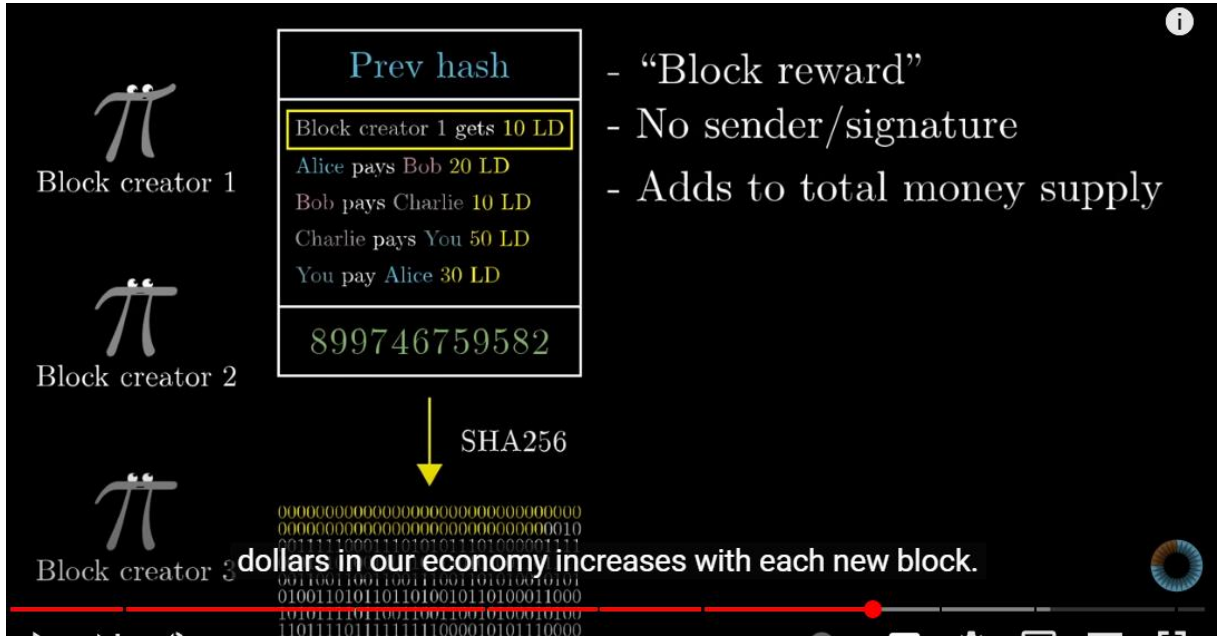


Mining

Jeder kann jetzt die Transaktionen sammeln, die getätigt werden und die Blöcke fertig stellen, d.h. die Zahl finden die die geforderte Anzahl an Nullen generiert. Wenn man sie gefunden hat sendet man den Block an alle.

Um die Person, die den Block erstellt hat zu belohnen, gibt es als erste Transaktion einen Betrag als Belohnung, den Block Reward, der als einzige Transaktion nicht unterschrieben wird, weil er von niemandem kommt.

Der gesamte Betrag an Bitcoins steigt mit jedem Block der fertiggestellt wird.



Blöcke zu kreieren nennt man Mining, da es viel Arbeit ist und den Gesamtbetrag der Währung vermehrt = mining und man bekommt dafür eine Belohnung in Bitcoin (block reward).

Aus Sicht der Miner ist jeder Block eine kleine Lotterie, wo jeder so schnell wie möglich Zahlen ausprobiert, bis er die passende Zahl gefunden hat um den Hash zu erstellen und die Belohnung bekommt.

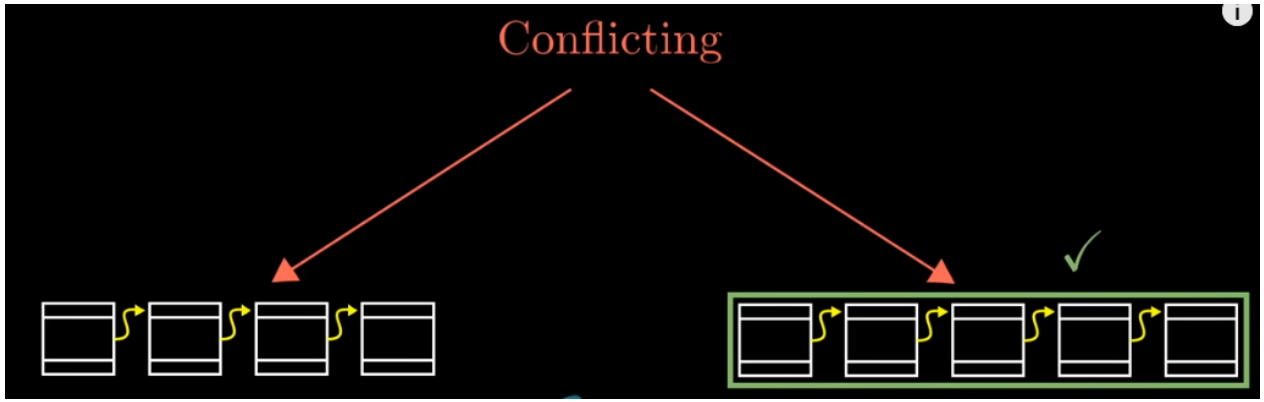
Nachdem es immer mehr Miner gibt wird es immer schwieriger für den Einzelnen die Minilotterie zu gewinnen.

Alle Leute, die Bitcoin nur nutzen um Zahlungen zu tätigen speichern die neuen Blöcke, die die Miner senden in ihrer Blockchain.

Bei zwei unterschiedlichen Lösungen, wartet man bis eine Blockchain länger ist als die andere.

So gibt es eine gültige Liste durch den dezentralen Konsens.

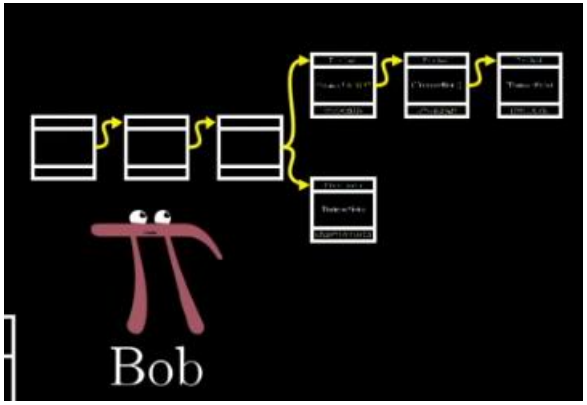
- **System ist vertrauenswürdig.**
- **längste Blockchain ist die geltende**



Was passiert bei Betrug?

Um zu betrügen, also eine falsche Transaktion in einen Block zu schreiben und diesen dann einer Person als richtigen Block zu schicken, muss der Betrüger einen gültigen Proof of Work finden vor allen anderen Minern. Das kann sogar passieren, aber da jeder Nutzer alle Nachrichten empfängt wird die andere Kette früher oder später schneller wachsen. Nur wenn jemand mehr als 50% aller Rechenressourcen im Netz hat, kann es ihm gelingen die längere Kette zu erhalten.

1 extra Block, der immer weiter verlängert werden muss



Das bedeutet, dass man einem neuen Block nicht sofort vertraut, aber sobald ein paar Blocke hinzugefügt wurden und man von keiner längeren Kette gehört hat, dann kann man davon ausgehen, dass dieser Block Teil der Kette ist, den alle nutzen

Zusammenfassung

Nur digital unterschriebene Transaktionen sind gültig

Der Ledger ist die Währung

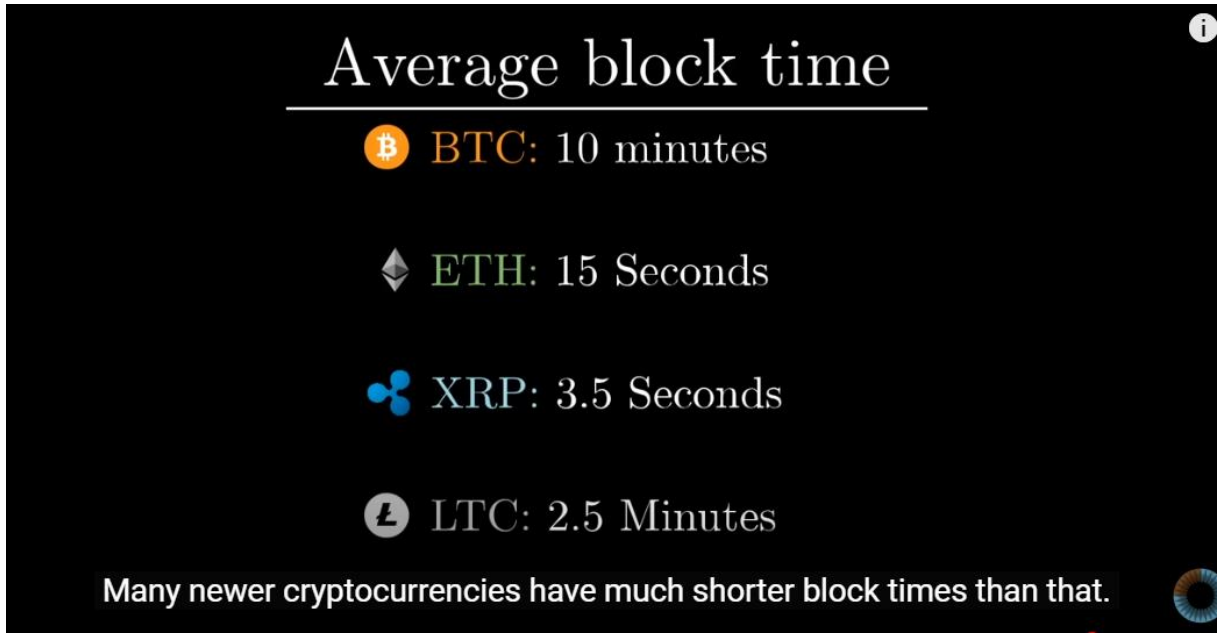
Dezentralisiert

Proof of Work

Block Chain

Durchschnittliche block time

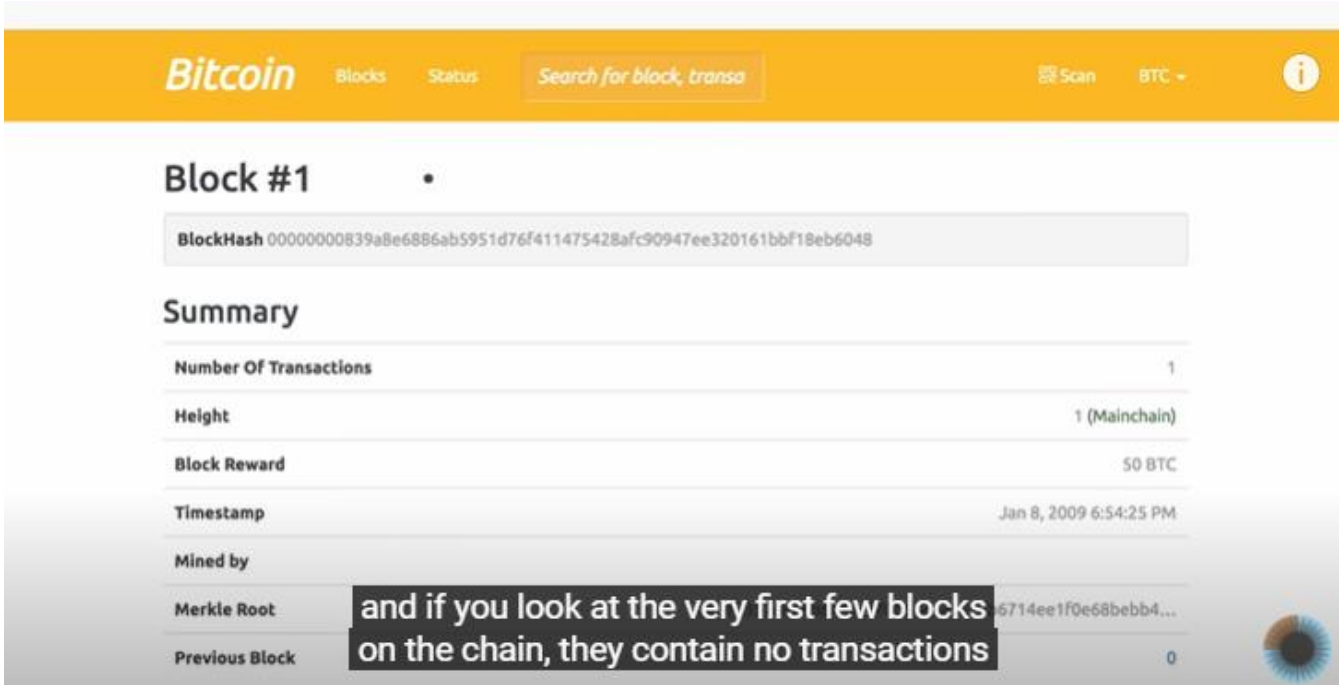
Die Zahl der Nullen ändert sich periodisch, so dass es durchschnittlich 10 Minuten dauert, um einen Block zu kreieren.



Neuere Kryptowährungen haben sehr viel kürzere Zeiten.

Gesamtbetrag an Bitcoins

Alles Geld in Bitcoins kommt von den Block rewards.



Die ersten Rewards waren bei 50 Bitcoins.

Nach **210 000 Blöcken** wird die Belohnung halbiert, ca. alle 4 Jahre

Das jüngste Bitcoin Halving ereignete sich am Samstag, dem 20. April 2024, um 2:10 Uhr Mitteleuropäischer Zeit.

der Blockreward ist derzeit bei 3,125 BTC.

Weil der Betrag sich regelmäßig halbiert, werden maximal 21 Millionen Bitcoin im Umlauf gebracht

210.000 (50 + 25 + 12,5 + 6,25 +…) = 21 000 000

Da die Gesamtzahl der Bitcoins auf 21 Millionen begrenzt ist, wird ein Punkt erreicht werden, an dem kein neuer **Block Reward** in Form neuer Bitcoins ausgegeben wird. Dieses Ereignis wird voraussichtlich um das Jahr 2140 herum eintreten.

Ein häufig diskutiertes Thema innerhalb der Bitcoin-Community ist, wie das Fehlen von neuen Block Rewards das Bitcoin-Ökosystem beeinflussen wird.

Transaktionsgebühren

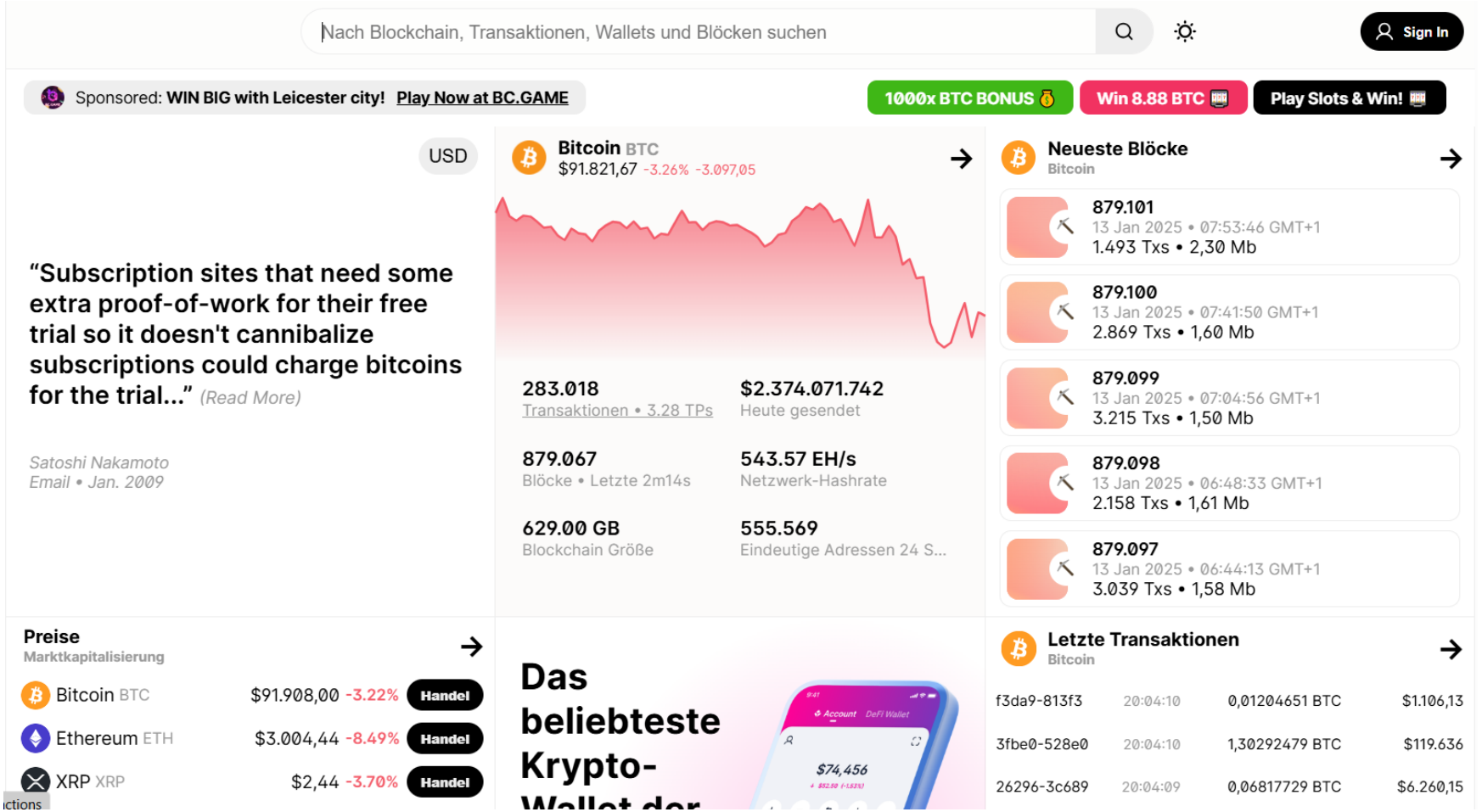
Man geht davon aus, dass zu diesem Zeitpunkt Transaktionsgebühren die Hauptquelle des Einkommens für Miner darstellen werden.

Zusätzlich zu den Block Rewards gibt es nämlich Transaktionsgebühren.

Wenn man eine Transaktion tätigt, kann man optional eine kleine Transaktionsgebühr mitschicken, die der Miner bekommt, dessen Block die Zahlung beinhaltet.

So motiviert man die Miner die Transaktion in den nächsten Block auszunehmen. Bei Bitcoin ist jeder Block auf ca. 2400 Transaktionen limitiert.

Blockchain Explorer - Bitcoin Tracker & More | Blockchain.com



[Blockchain Explorer - Bitcoin Tracker & More | Blockchain.com]

Ausblick

Ethereum

Ethereum (ETH) ist die zweitbeliebteste Kryptowährung und nach Bitcoin

Open-Source-Blockchain-Plattform mit grossartiger „Smart Contract“-Funktionalität (intelligente Verträge

Ethereum ist bekannt für seine kontinuierliche Entwicklung.

Ethereum 2.0 Proof-of-Stake-Konsensmodell das senkt die Transaktionskosten massiv und schont die Umwelt

Dogecoin

ein Experiment in inflationärer Kryptowährung

2013 gestartet wurde

DOGE-Mining unbegrenzt

schönes Experiment zum Begutachten

Originales Bitcoin-Papier: https://bitcoin.org/bitcoin.pdf

Block-Explorer: https://blockexplorer.com/

How the Bitcoin protocol actually works – DDI