Bitcoins und Blockchains

Was es mit Kryptowährungen auf sich hat

Ausarbeitung zum Vortrag im Rotary-Club Frankfurt am Main Friedensbrücke

Dr. Daniel Korn 16.12.2021

1 Einleitung

Bitcoin und seine Konkurrenten sind heutzutage in aller Munde. Der Kurs dieser sogenannten „Kryptowährungen“ schwankt nach anfänglich sehr bescheidenem Start (bis 2011 war ein Bitcoin für einstellige Dollarbeträge zu haben) derzeit zwischen 35.000 und fast 68.000 Dollar und El Salvador hat zum 07. September 2021 Bitcoins sogar als zweite Landeswährung eingeführt.

Was genau sind aber diese ominösen Kryptowährungen? Wir alle haben eine recht genaue Vorstellung von klassischen Währungen, selbst wenn das durch sie bestimmte Geld heutzutage überwiegend auf elektronischem Wege und damit gänzlich immateriell ausgetauscht wird. Von Kryptowährungen hingegen haben viele von uns zwar schon mal was gehört bzw. gelesen, aber die Wenigsten wissen, was sich wirklich dahinter verbirgt.

Der hiesige Vortrag hat sich daher zum Ziel gesetzt, die wesentlichen Aspekte der Kryptowährungen anhand ihres ersten und bekanntesten Vertreters – der Bitcoins – in möglichst einfacher und verständlicher Form zu illustrieren. Dazu soll zunächst der Leitgedanke, der zur Erfindung von Kryptowährungen geführt hat, beleuchtet werden, bevor auf die grundlegenden informationstechnologischen Konzepte sowie die praktische Verwendung dieser Währungen eingegangen werden soll. In einem kurzen geschichtlichen Abriss der Entstehung und Entwicklung von Kryptowährungen soll der Vortrag dann seinen Abschluss finden.

2 Vertrauenswürdigkeit und Unabhängigkeit

2.1 Kritik an klassischen Währungen

Trotz bereits bis in die 1980er Jahre zurückreichender Grundsatzüberlegungen zu digitalen Währungen, die sich unabhängig von zentraler Überwachung auf Basis kryptografischer Verfahren quasi von selbst verwalten, begann die Erfolgsgeschichte der Kryptowährungen mit der expliziten Kritik an den herkömmlichen Währungen, wie sie vom bis heute sagenumwogenen Erfinder der Bitcoins in seinem 2008 unter dem Pseudonym „Satoshi Nakamoto“ veröffentlichten White Paper geäußert wurde. Nakamotos Kritik zielt dabei im Wesentlichen auf die drei folgenden Punkte:

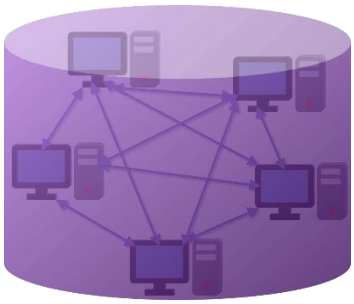
- die alleinige Macht der jeweiligen Zentralbanken über den Wert der von Ihnen kontrollierten Währungen

- die alleinige Macht der Geschäftsbanken über die Aufbewahrung unseres Geldes und die ordnungsgemäße Abwicklung von Geldtransaktionen – vor allem im Angesicht der in 2008 erlebten Immobilienkrise mit den dabei offenbar gewordenen Kreditblasen und mangelnden Kreditdeckungen.

- die alleinige Macht der Geschäftsbanken über die Schutzmechanismen vor unberechtigten Zugriffen auf das Geld ihrer Kunden.

Um diesen Punkten eine funktionsfähige Alternative entgegensetzen zu können, griff Nakamoto die vor allem in den späten 1990er Jahren bereits mehrfach konzipierten Ideen auf, eine Währung zu schaffen, die keiner zentralen Verwaltung unterworfen werden kann, dabei mit kryptografischen Verfahren vor dem Zugriff Unbefugter geschützt ist und deren Transaktionen auf Basis einer technologischen Lösung für jedermann transparent und verifizierbar sowie gelichzeitig fälschungssicher und fehlerresistent sind.

2.2 Nakamotos Idee



Die Grundidee, die Nakamoto zur Umsetzung eines solchen Konzepts entwickelt bzw. weiterentwickelt hat, beruht auf der Schaffung einer global verteilten und vielfach duplizierten Datenbank, in der sämtliche Transaktionen genauso wie die Erzeugung neuen Geldes unabhängig von der Kontrolle staatlicher Instanzen für jedermann einsehbar und steuerbar sind. Um dem Problem der Geldentwertung entgegenzuwirken, sollte die Währung prinzipbedingt so gestaltet sein, dass die zu schöpfende Geldmenge begrenzt ist. Außerdem sollten ausgefeilte kryptografische Konzepte dafür Sorge tragen, dass Wertschöpfungen und Transaktkonen manipulationssicher und transparent sind. Auf diese Weise sollte der Währung ein uneingeschränktes und nicht von konkreten Personen oder Institutionen abhängiges Vertrauen entgegengebracht werden können.

Die dazu von Nakamoto entwickelten Grundkonzepte bestehen aus der „Blockchain“ als Implementierung der global verteilten Transaktions- und Wertschöpfungsdatenbank sowie der Verwendung von Hashwerten und digitalen Signaturen die auf bewährten Verschlüsselungsverfahren beruhen. Im nächsten Abschnitt sollen daher zunächst die Grundkonzepte von Hashfunktionen und digitalen Signaturen sowie anschließend die darauf basierende Funktionsweise der Blockchains erläutern werden.

3 Hashwerte, digitale Signaturen und Blockchains

3.1 Hashwerte

Die Grundidee hinter der Verwendung von Hashwerten beruht auf der allseits bekannten Idee, Daten mit Prüfsummen zu versehen, um Manipulationen an den Daten erkennen zu können. Um dieses Prinzip zu verstehen, stelle man sich als Beispiel eine Folge von zehn Ziffern vor, die unser Datenpaket repräsentieren sollen:

9 5 6 7 2 3 4 1 0 8

Eine naheliegende Möglichkeit, diesem Paket eine Prüfsumme zuzuordnen, besteht darin, alle Ziffern zu addieren und etwa die ersten beiden Ziffern der so entstehenden Summe als Prüfsumme zu verwenden:

$$9 + 5 + 6 + 7 + 2 + 3 + 4 + 1 + 0 + 8 = 45$$

Wird nun eine einzelne Ziffer unseres Datenpakets verändert – z.B. die „0" zu einer „3", so ändert sich gleichzeitig auch die Prüfsumme, die dann 48 lauten müsste. Die mit unserem Datenpaket abgelegte Prüfsumme „45" passt also nicht zu dem veränderten Datenpaket „9 5 6 7 2 3 4 1 **3** 8". Damit kann an der Prüfsumme leicht abgelesen werden, dass eine einzelne Ziffer verändert wurde.

Sicher: wenn zwei oder mehr Ziffern gleichzeitig verändert werden, kann es passieren, dass die Prüfsumme des so manipulierten Datenpakets zufällig wieder der ursprünglichen Prüfsumme entspricht, so dass eine solche Mehrfachmanipulation dann doch wieder unentdeckt bliebe. Der Frage, wie man Prüfdaten so gestaltet, dass Manipulationen bestimmter Schwere mit einer hinreichend großen Wahrscheinlichkeit entdeckt werden, widmet sich das Fachgebiet der Kodierungstheorie, welche im Rahmen dieses Vortrags nicht weiter vertieft werden kann.

Für unsere Zwecke soll hingegen die Erkenntnis genügen, dass es derweil sehr ausgeklügelte Prüfverfahren gibt, um auch erhebliche Manipulationen an großen Datenblöcken aufzudecken – sogenannte „kryptografische Hashfunktionen". Diese erzeugen zu einem gegebenen Datenblock anstelle der einfachen Prüfsumme einen sogenannten „Hashwert", der über die folgenden drei wichtigen Eigenschaften verfügt:

- Zu unterschiedlichen Datenblöcken wird (praktisch) immer ein unterschiedlicher Hashwert erzeugt – und zwar so, dass schon geringste Änderungen am Datenblock vollkommen andere und insofern unvorhersehbare Hashwerte hervorrufen. Dies ist wichtig, um sicherzustellen, dass Manipulationen am Datenblock durch abweichende Hashwerte erkennbar werden.
- Die erzeugten Hashwerte haben unabhängig von Größe und Beschaffenheit des Datenblocks stets feste Längen. Dies ist wichtig, um feste Datenmengen für die Hashwerte vorsehen zu können.
- Es ist (praktisch) unmöglich, den ursprünglichen Datenblock aus dem Hashwert zu rekonstruieren. Insbesondere gibt es keine erkennbare Ähnlichkeit zwischen den Hashwerten ähnlicher Datenblöcke. Dies ist vor allem wichtig, um den Rechenaufwand weiter unten erläuterten „Proof of Work" zu gewährleisten.

Für Hashwerte, die in Bitcoins zum Einsatz kommen, wird das SHA256-Verfahren verwendet, das Hashwerte mit einer festen Länge von 256 Binärstellen (Bits) erzeugt.

$$\boxed{1}\boxed{0}\boxed{1}\boxed{0} = SHA256\left(\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0}\right)$$

3.2 Digitale Signaturen

Um die Urheberschaft einer Transaktion fälschungssicher feststellen zu können, werden die Transaktionen bei Bitcoin mit Hilfe sogenannter „asymmetrischer Kryptosysteme“ verschlüsselt. Diese zeichnen sich durch ein Paar, bestehend aus einem privaten und einem öffentlichen Schlüssel aus. Dabei ist der private Schlüssel fest an die Bitcoin-Adresse des konkreten Absenders einer Transaktion geknüpft, während die (öffentlich bekannte) Bitcoin-Adresse selbst den zum privaten Schlüssel passenden öffentlichen Schlüssel enthält.

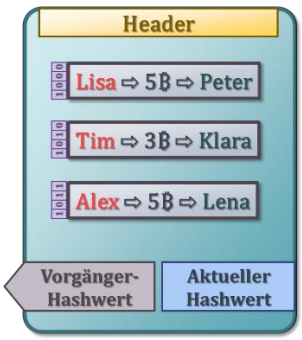
Beim Versenden einer Transaktion bildet der Absender zunächst den oben beschriebenen SHA256-Hashwert der betreffenden Transaktionsdaten und verschlüsselt diesen anschließend mit seinem (nur ihm bekannten) privaten Schlüssel und erzeugt damit eine digitale Signatur der Transaktion. Dieser Schlüssel hat bei dem für Bitcoin verwendeten Secp256k1-Verfahren ebenfalls eine Länge von 256 Binärstellen.

Der Empfänger der Transaktion (ebenso wie jeder andere Bitcoin-Nutzer) verwendet dagegen den aus der Bitcoin-Adresse des Absenders generierten öffentlichen Schlüssel, um die Signatur des Absenders wieder zu entschlüsseln. Das Ergebnis dieser Entschlüsselung vergleicht er dann mit dem selbst berechneten SHA256-Hashwert zu den Transaktionsdaten. Stimmen beide Werte überein, so ist zweifelsfrei sichergestellt, dass die Transaktion vom Absender mit der betreffenden Bitcoin-Adresse stammt.

Wie bei allen Verfahren mit privaten und öffentlichen Schlüsseln, kann der öffentliche Schlüssel jederzeit leicht aus dem privaten Schlüssel berechnet werden, während es (praktisch) unmöglich ist, den privaten Schlüssel aus dem öffentlichen zu rekonstruieren. Damit ist sichergestellt, dass niemand außer dem rechtmäßigen Besitzer des privaten Schlüssels Transaktionen mit diesem Schlüssel signieren kann.

3.3 Blockchains

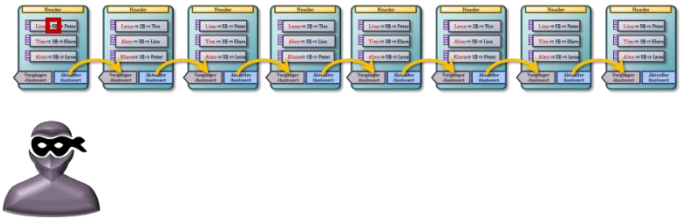
Die eigentliche Abwicklung und Speicherung von Transaktionen mit Bitcoins erfolgt mit Hilfe einer sogenannten „Blockchain“. Dabei handelt es sich um eine Verkettung einzelner Datenblöcke, welche ihrerseits eine oder mehrere Bitcoin-Transaktionen enthalten. Außer den eigentlichen Transaktionsdaten enthält ein solcher Block jedoch noch drei weitere Elemente:



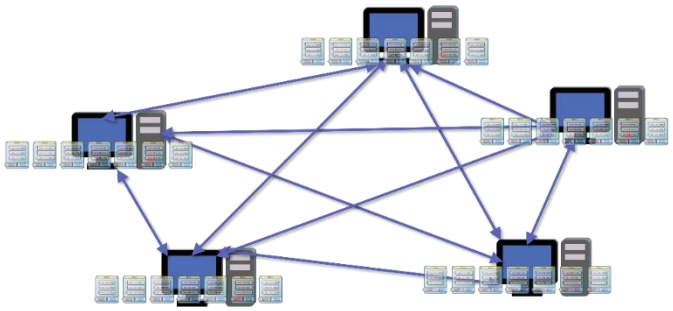
1. Den Hashwert desjenigen Blocks, der ihm in der chronologischen Verkettung aller Blöcke unmittelbar vorausgeht.
2. Eine sogenannter „Block Header“, dessen Zweck im nachfolgenden Unterabschnitt (3.4) beschrieben wird.
3. Einen Hashwert, der mit Hilfe des SHA256-Verfahrens aus den im Blick enthaltenen Transaktionsdaten, dem oben erwähnten Hashwert des Vorgängerblocks und dem oben erwähnten Block Header berechnet wird.

Die Tatsache, dass jeder Block den Hashwert des jeweiligen Vorgängerblocks enthält, dient dabei zwei unterschiedlichen Zwecken:

1. Der Schaffung eines eindeutigen Verweises auf den Vorgängerblock und damit einer unveränderlichen chronologischen Reihenfolge aller Blöcke in der Blockchain.
2. Die Integration des Vorgängerhashwerts in den Hashwert des aktuellen Blocks. Dadurch ist es nahezu unmöglich, die Transaktionsdaten eines Blocks nachträglich zu manipulieren, denn man müsste dann zum Verschleiern der Manipulation nicht nur den Hashwert des manipulierten Blocks, sondern zusätzlich dazu auch noch diejenigen aller nachfolgenden Blöcke neu berechnen, was – wie im nächsten Unterabschnitt dargelegt – extrem zeitaufwändig wäre.



Die Blockchain selbst ist an keiner zentralen Stelle dieser Welt gespeichert, sondern findet sich stattdessen in unzähligen Kopien auf weltweit verteilten untereinander vernetzten Rechnern. Will jemand einen neuen Block an die Blockchain anfügen, muss er zunächst den Hashwert des Blocks wie oben beschrieben berechnen und die so verlängerte Blockchain an alle Rechner versenden, die Kopien der Blockchain enthalten – ein Vorgang der als „Flooding“ bezeichnet wird



Dies kann jedoch zu Konflikten mit anderen Nutzern führen, die mehr oder weniger zeitgleich versuchen, einen neuen Block an die Blockchain anzufügen und ihre eigene Version der so verlängerten Blockchain an alle Netzwerkteilnehmer zu versenden. Dadurch konkurrieren ggf. unterschiedliche Fortsetzungen der aktuellen Blockchain auf unterschiedlichen Rechnern des Bitcoin-Netzwerks. Da es aber gerade keine zentrale Instanz geben soll, die entscheiden kann, welche der parallel existierenden Blockchain-Fortsetzungen die „echte“ ist, muss ein Mechanismus geschaffen werden, solche Konflikte dezentral zu lösen.

Dies geschieht bei Bitcoin über die Festlegung, dass die aktuell jeweils längste Version der Blockchain als die gültige Version gewertet wird. Diese Festlegung ist möglich, weil die Bitcoin-Logik so konstruiert ist, dass die Hinzufügung neuer Blöcke nur mit einem erheblichen Maß an Rechenaufwand und damit einem entsprechenden Maß an Zeitaufwand vollzogen werden kann. Es setzt sich also letztlich derjenige Nutzer durch, der die Hinzufügung eines

neuen Blocks am schnellsten durchführen kann, was im Klartext bedeutet, dass er über die meiste Rechenleistung verfügt.

Wie das konkret funktioniert, soll im folgenden Unterabschnitt dargestellt werden. Für die Beständigkeit einer konkreten Transaktion, die als Teil eines neuen Blocks in die Blockchain eingefügt werden soll, bedeutet die oben beschriebene Konkurrenz um die „echte" Blockchain jedenfalls, dass man nach Einfügung eines jeweils erzeugten neuen Blocks eine gewisse Zeit lang abwarten muss, um zu beobachten, ob die nächsten Blöcke in der Blockchain auch wirklich an den eben eingefügten neuen Block angehängt werden. Setzt sich hingegen ein konkurrierender Block durch, verfällt die eigene Transaktion – wird also sozusagen von der „echten" Blockchain überschrieben. Derzeit geht man davon aus, dass eine Blockeinfügung als bestätigt gilt, wenn sechs oder mehr Blöcke daran angefügt wurden. Damit dauert es rund eine Stunde, bis man praktisch sicher feststellen kann, ob der eigene Block und damit die darin enthaltenen Transaktionen Teil der „echten" Blockchain geworden ist.

Zum Zeitpunkt der Erstellung dieses Vortrags hat die aktuelle Bitcoin-Blockchain eine Länge von rund 713.000 Blöcken mit einem Gesamtdatenvolumen von rund 380GB.

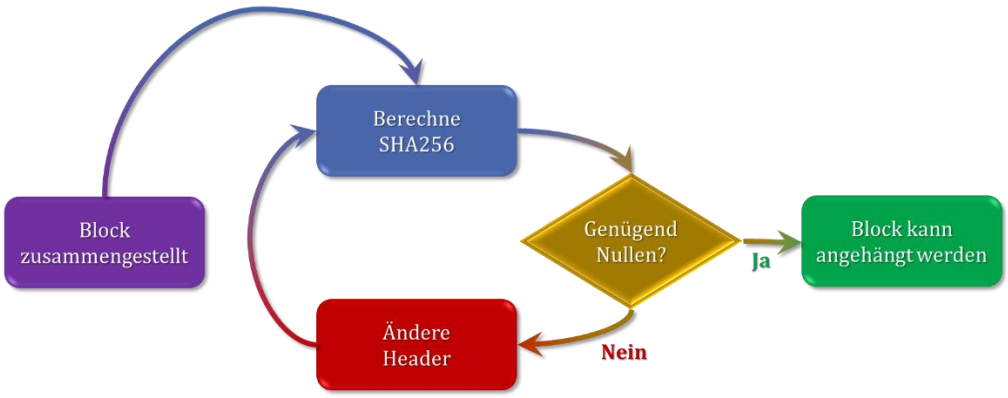
3.4 Proof of Work und Mining

Um sicherzustellen, dass Erzeugung und Anfügung neuer Blöcke an die Blockchain mit einer hinreichend großen Menge an Rechen- und damit Zeitaufwand verbunden sind, verlangt Bitcoin als Voraussetzung für die Anfügung eines neuen Blocks einen sogenannten „Proof of Work". Um zu verstehen, wie dieser Proof of Work zu erbringen ist, erinnern wir uns nochmals an die im vorangegangenen Abschnitt aufgelisteten Bestandteile eines Blocks. Zu diesen gehörte insbesondere ein „Block Header" dessen Zweck später erläutert werden sollte. Dies soll nun im Folgenden geschehen:

Die Grundidee hinter dem „Proof of Work" besteht darin, bestimmte Anforderungen an die Struktur des SHA256-Hashwerts zu stellen, der aus den Blockdaten generiert werden soll.

Konkret bestehen diese Anforderungen darin, dass eine bestimmte Anzahl der führenden Binärstellen im Hashwert den Wert „0" haben muss. Da der Hashwert zu einem konkreten Block aber immer eindeutig durch die Logik der SHA256-Funktion bestimmt ist und seine Struktur insofern nicht einfach nach Belieben vorgewählt werden kann, muss es in jedem Block einen speziellen Bereich geben, dessen Daten man frei verändern kann, um zu erreichen, der Hashwert zum so veränderten Block die geforderte Anzahl führenden Nullen enthält. Genau diesen Zweck erfüllt der Block-Header (genauer gesagt: spezielle darin enthaltene Bereiche – sogenannte „Nonces").

Bisher ist kein Verfahren bekannt, mit dessen Hilfe sich der Ursprungsdatenblock aus seinem zugehörigen SHA256-Hashwert berechnen lässt. Man kann also nicht einfach den gewünschten Hashwert vorgeben und den dafür notwendigen Ursprungsdatenblock berechnen. Stattdessen muss man so lange sukzessive alle möglichen „Nonce"-Werte „ausprobieren" und den daraus resultierenden SHA256-Hashwert des Blocks berechnen, bis irgendwann ein Hashwert mit der geforderten Anzahl an führenden Nullen entsteht:



Dieser Prozess ist in der Praxis extrem rechen- und damit zeitintensiv. Daher erhält jeder, der einen Block mit gültigem Proof of Work anfügt, eine gewisse Anzahl neuer Bitcoins als Gegenleistung für die investierte Rechenleistung. Die Berechnung neuer Blöcke kommt damit also letztlich der Erzeugung bzw. dem Schürfen neuer Bitcoins gleich, weswegen dieser Prozess auch als „Mining" bezeichnet wird.

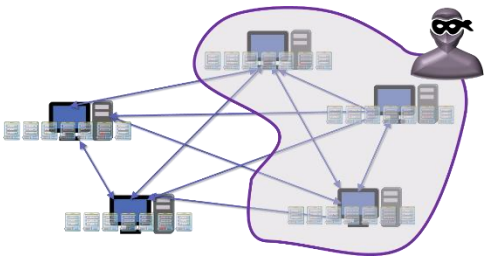
Zum Zeitpunkt der Erstellung dieser Ausarbeitung sind bei Bitcoin 76 führende Nullen in den SHA256-Hashwerten neu einzustellender Blöcke als Proof of Work gefordert. Im Durchschnitt müssen dabei rund $1{,}167 \times 10^{18}$ (also 1.167.000.000.000.000.000 bzw.1,167 Milliarden Milliarden) Hashes pro Block berechnet werden, bis ein Hash mit den geforderten 76 führenden Nullen gefunden ist. Mit den gegenwärtig im Bitcoin-Netzwerk verfügbaren Rechenleistungen benötigt das Mining eines Blocks damit durchschnittlich rund zehn Minuten.

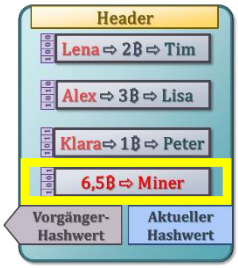
Um der kontinuierlichen Steigerung der verfügbaren Rechenleistung von Computersystemen zu begegnen, wird in regelmäßigen Abständen die geforderte Anzahl an führenden Nullen in den Hashwerten gültiger Bitcoin-Blocks erhöht, so dass der Rechenaufwand umgekehrt proportional an die verfügbare Rechenleistung angepasst wird und das Schürfen neuer Bitcoins damit immer rund zehn Minuten dauert.

Durch diesen Proof of Work werden damit zwei wesentliche Ziele erreicht:

1. Es setzt sich letztlich immer diejenige Blockchain durch (und gewinnt damit das Vertrauen aller Netzknoten), in der die meiste Rechenleistung steckt.

2. Es wird sichergestellt, dass niemand mit vertretbarem Aufwand das Bitcoin-Netzwerk „kapern" – also die alleinige Hoheit über die Verlängerung der Blockchain erlangen kann. Dazu müsste er nämlich über mehr als 50% der für das Netzwerk verfügbaren Rechenleistung verfügen (womit er sicherstellen könnte, dass er bei der Konkurrenz um die Anfügung neuer Blöcke immer der „Gewinner" bleibt). Dies ist aufgrund der weltweit verteilten, dezentralen Struktur des Bitcoin-Netzwerks praktisch ausgeschlossen.





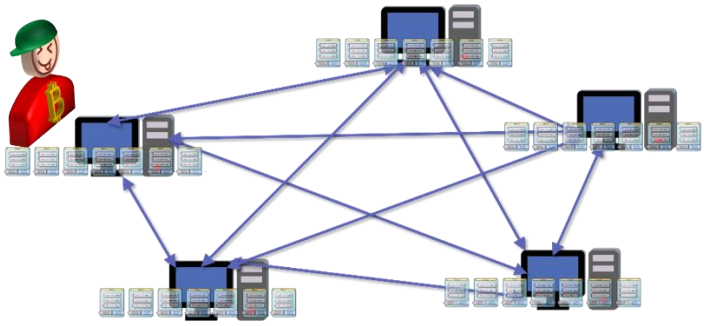
Die oben erwähnte Anzahl an neuen Bitcoins, die einem „Miner“ als „Belohnung“ bzw. Vergütung für das Anfügen neuer Blöcke zugesprochen wird, beläuft sich derzeit auf 6,25 Bitcoins. Alle 210.000 Blöcke (also rund alle vier Jahre) wird die Blockvergütung und damit die Bitcoin-Produktion jedoch halbiert, wodurch sichergestellt ist, dass maximal rund 21 Millionen Bitcoins geschürft werden können, was unter Beibehaltung der eben beschriebenen Anfügungsgeschwindigkeit für Blöcke etwa im Jahre 2140 der Fall sein wird. Damit wird sichergestellt, dass Bitcoins eine endliche Ressource bleiben und insoweit vor unkontrollierter Entwertung geschützt sind.

Nachdem wir uns in diesem Abschnitt mit den Grundkonzepten der Funktionsweise von Bitcoins vertraut gemacht haben, soll der folgende Abschnitt am Beispiel von Bitcoin einen Einblick in die praktische Nutzung von Kryptowährungen gewähren.

4 Nutzung von Kryptowährungen

4.1 Bitcoin-Netzwerk

Wie bereits weiter oben erwähnt, zeichnen sich Kryptowährungen nach Bauart des Bitcoins insbesondere dadurch aus, dass es außer dem Konstruktionsprinzip der Währungen selbst weder eine zentrale Instanz gibt, die wirksam Kontrolle über die Währung ausüben kann, noch einen definierten Ort, an dem die Währung verwaltet und gesteuert wird. Stattdessen besteht zumindest das Bitcoin-Netzwerk aus einer sogenannten „Peer to peer“-Struktur, also einem losen, über das Internet geschaffenen Zusammenschluss weltweit verteilter Rechner, die sich im Eigentum beliebiger Privatleute oder auch Institutionen befinden.



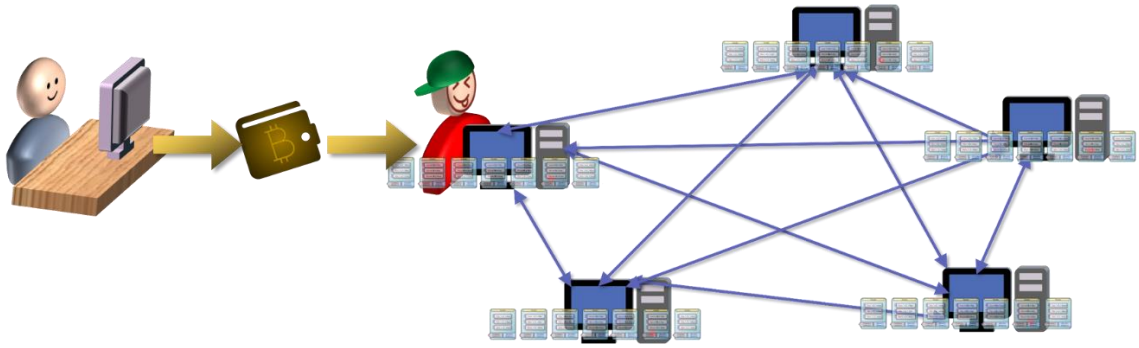
Im Prinzip kann also jeder von uns mit seinem häuslichen Internetanschluss und einer geeigneten Rechenkapazität Teil des Bitcoin-Netzwerks werden. Dazu muss man sich letztlich nur die jeweils aktuelle Software herunterladen, die von diversen Entwicklern angeboten und gepflegt wird. In der Praxis hat jedoch vor allem der sehr rechenintensive Betrieb von Mining-Software dazu geführt, dass ein einfacher Rechner für den Hausgebrauch gegenüber den diversen mittlerweile eigens für Mining geschaffenen „Mining-Pools“ nicht mehr konkurrenzfähig ist. Das eigentliche Mining ist daher gegenwärtig fast ausschließlich in den Händen von Firmen und Institutionen, die sich darauf spezialisiert haben. Daher sieht die Bitcoin-Struktur insbesondere die Möglichkeit vor, dass die Miner Transaktionsgebühren bei den eigentlichen Bitcoin-Nutzern erheben dürfen und so neben der eigentlichen Mining-Vergütung auch noch an den einzelnen in einem erfolgreich geschürften Block enthaltenen Transaktionen verdienen.

Neben dieser Mining-Community, die ja im Wesentlichen eher miteinander konkurriert als kooperiert, sind es ansonsten die Entwickler von Bitcoin-Software, die maßgeblichen Einfluss

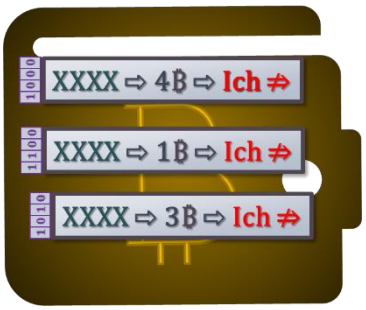
auf die praktische Nutzung des Bitcoin-Konzepts haben. Dabei gibt es nicht den einen Hersteller von Blockchain-Software, sondern vielmehr eine durchaus lebhafte Konkurrenz verschiedener Implementierungen – insbesondere für die im folgenden Unterabschnitt beschriebenen Wallet-Clients. Durch konsequente OpenSource-Lizensierung der einschlägigen Bitcoin-Software ist dabei sichergestellt, dass Software-Fehler vergleichsweise schnell auffliegen und korrigiert werden können. Außerdem ist damit ein kommerzielles Interesse an der Herstellung eigentlichen Software und damit ein etwaiges Streben nach Marktdominanz für die Bitcoin-Software ausgeschlossen. Letztlich wird auf diese Weise die Weiterentwicklung der Bitcoin-Software wiederum überwiegend von der globalen Bitcoin-Community selbst im Dialog zwischen Nutzern und Entwicklern vorangetrieben.

4.2 Zahlungsverkehr

Wie aber kann man praktisch mit Bitcoins bezahlen? Dazu benötigt man letztlich nicht viel mehr als einen Zugang zum Bitcoin-Netzwerk und eine Bitcoin-Adresse. Ersteren erhält man am einfachsten, indem man sich einen sogenannten „Wallet-Client“ herunterlädt, der in der Regel kostenfrei für alle gängigen Plattformen (Windows, MacOS, Linux, Android, iOS) verfügbar ist. Alternativ gibt es aber auch Webdienste, mittels derer man über beliebige Internetbrowser auf sein Wallet zugreifen kann.



Unter Wallet versteht man dabei die Gesamtheit aller in der Blockchain enthaltenen Transaktionen, deren Begünstigter man selbst ist und deren Guthaben man bisher noch nicht ausgegeben hat. Solche Transaktionen bezeichnet man im Bitcoin-Jargon als „unspent transaction outputs“ oder abgekürzt als „UTXOs“. Die Zuordnung der Transaktionen zu einer konkreten Person erfolgt dabei, wie in 3.2 erläutert, über die Bitcoin-Adresse. In der Praxis hat allerdings ein konkreter Nutzer nicht genau eine Bitcoin-Adresse. Aus Sicherheitsgründen wird sogar empfohlen, für jede Transaktion eine neu Bitcoin-Adresse zu verwenden. Damit ist es also entscheidend, die bisher für Transaktionen zu eigenen Gunsten verwendeten Bitcoin-Adressen inklusive der zugehörigen privaten Schlüssel an einer gut geschützten und gesicherten Stelle abzuspeichern.



Genau hier kommen die Wallet-Clients bzw. Online-Dienste zum Tragen. Sie stellen einen online-Zugang mit den üblichen Authentifizierungsmechanismen (E-Mail-Adresse plus Kennwort bzw. oft noch ein zweiter Faktor wie SMS oder TAN) bereit, unter dem dann alle eigenen

Bitcoin-Adressen samt den zugehörigen privaten Schlüsseln abgelegt sind. Man kann sich das in etwa wie einen Banksafe vorstellen, in dem man sein ganzes Geld aufbewahrt. Verliert man

den Schlüssel, ist der Inhalt des Safes nicht mehr zugreifbar. Verliert man seine Zugangsdaten zum Wallet-Client kann man alle Bitcoin-Zuflüsse, die unter den dort abgelegten Bitcoin-Adressen erfolgt sind, nicht mehr zur Bitcoin-Zahlung nutzen. Umgekehrt, kann jeder, der Zugriff auf die eigenen Zugangsdaten erhält, unmittelbar über das darunter gesammelte Bitcoin-Guthaben verfügen. Tatsächlich geschieht es ziemlich oft, dass Nutzer ihre Zugangsdaten verlieren. So lagerten Schätzungen zufolge im Jahre 2021 Bitcoins im Wert von immerhin rund 115 Milliarden Euro ungenutzt in digitalen Geldbörsen, weil der Besitzer keine Zugriffsmöglichkeit mehr darauf hat

Die eigentliche Verfügung läuft dann so ab, dass man die Höhe des Bitcoin-Betrags und den Zahlungsempfänger festlegt und eine entsprechende Transaktion über die Wallet-Software absetzt. Diese wird dann von der Wallet-Software einem willigen Miner zur Einfügung in die Blockchain übergeben. Sobald die Transaktion in die Blockchain eingefügt und bestätigt wurde (siehe 3.3), erhebt der Miner eine vorher bestimmte Transaktionsgebühr, die automatisch vom Zahlbetrag abgezogen wird. Jeder Nutzer kann dabei festlegen, wieviel er maximal an Transaktionsgebühren zu zahlen bereit ist. Je höher dabei diese Obergrenze ist, desto höher ist die Priorität, mit welcher der Miner die betreffende Transaktion vor den Transaktionen anderer Nutzer in den nächsten Block übernimmt, so dass höher vergütete Transaktionen früher ausgeführt und bestätigt werden.

Die Tatsache, dass sich die Bitcoins, über die man verfügen kann, ausschließlich aus der lückenlosen Transaktionshistorie der gesamten Blockchain bestimmen lassen, ist eines der wesentlichen Designprinzipien von Bitcoin. Jeder auf der Welt kann in voller Transparenz nachvollziehen und verifizieren, dass nur über solche Bitcoins verfügt werden kann, die über eine gültige, lückenlose Transaktionskette in den Besitz des jeweiligen Nutzers gelangt und von diesem bisher nicht anderweitig ausgegeben worden sind.

4.3 Mining in der Praxis

Während das Mining in den Anfangsjahren von Bitcoin noch über Software erfolgte, die sich jedermann auf seinem häuslichen PC herunterladen konnte, änderte sich dies schon nach kurzer Zeit, als immer mehr „digitale Goldgräber“ auf das potenziell lukrative Geschäft mit dem Schürfen von Bitcoins aufmerksam wurden. Sie machten sich zunächst die Rechenwerke handelsüblicher Grafikkarten zunutze, die ja speziell für das rasend schnelle Verarbeiten iterativer Berechnungen ausgelegt sind. Grafikkarten sind aber gleichzeitig als regelrechte Stromfresser bekannt, so dass die Vergütung für das Bitcoin-Mining zunehmend von den dafür erforderlichen Energiekosten aufgefressen wurde.

Daher setzte man schon im Jahre 2011 auf programmierbare integrierte Schaltkreise – sogenannte FPGAs („Field Programmable Gate Arrays“) – die mit speziell für Mining optimierten Rechenlogiken programmiert wurden. FPGAs sind zwar teuer in der Herstellung, bieten dafür aber extrem hohe Rechenleistung bei vergleichsweise niedrigen Energiekosten. Seit 2013 kommen jedoch fast nur noch sogenannte ASICs („Application-Specific Integrated Circuits“) für das Mining zum Einsatz, bei denen es sich um eigens für Mining-Berechnungen konstruierte integrierte Schalkreise handelt, die mit möglichst geringem Energieaufwand möglichst viele

Hashwerte pro Sekunde berechnen können. Zur Zeit der Erstellung dieses Vortrags liegt die dabei erzielbare Rate an Hashwerten pro Sekunde bei rund einhundert Billionen.

Da jedoch, wie in 3.4 beschrieben, die Schwierigkeit des Bitcoin-Schürfens über den dafür notwendigen Proof of Work immer so angepasst wird, dass das Schürfen eines Blocks im Durchschnitt rund zehn Minuten in Anspruch nimmt, steigt der für das Erzeugen neuer Blöcke notwendige Rechen- und damit Energieaufwand in entsprechendem Maße. Die extrem schelle Hardware, die derzeit zur Verfügung steht, muss also im Dauerbetrieb auf Hochtouren laufen, um die geforderte Berechnungszeit von rund zehn Minuten pro Block einhalten zu können. Trotz der oben erwähnten stromsparenden Auslegung der Spezialhardware bleibt der dafür erforderliche enorme Rechenaufwand also nicht ohne Folgen für den Energiebedarf, den das weltweite Bitcoin-Mining mittlerweile einfordert.

So kommt eine Schätzung der Universität Cambridge von Februar 2021 auf einen jährlichen Gesamtbedarf von rund 120 Terawattstunden für das weltweite Bitcoin-Mining. Das entspricht etwa 1,2 Megawattstunden pro Bitcoin-Transaktion. Zum Vergleich: eine gewöhnliche Kreditkartenzahlung braucht gerade mal rund 1,5 Wattstunden. Eine Bitcoin-Transaktion verschlingt damit also ungefähr genauso viel Energie wie 800.000 Kreditkartentransaktionen!

Daher verlagert sich das Bitcoin-Mining immer mehr in Regionen mit niedrigen Energiekosten – allen voran nach China, in dem mittlerweile rund 75% des Bitcoin-Minings erfolgt. Nicht zuletzt aufgrund der dort vorhandenen Energiequellenstruktur kommt eine Studie der Universität Cambridge aus dem Jahre 2020 zu dem Schluss, dass zwischen 61% und 71% der weltweit zum Bircoin-Schürfen genutzten Energie aus nicht-regenerativen Quellen stammt. Einer weitern Studie aus dem Jahre 2021 zufolge wird die durch das globale Bitcoin-Mining hervorgerufene jährliche Kohlendioxidemission ab dem Jahr 2025 die Jahresemissionen einer durchschnittlichen europäischen Industrienation wie etwa Italien übertreffen und damit auf Platz 12 der weltweit größten Kohlendioxidemittenten aufsteigen.

Daraus wird ersichtlich, dass Bitcoins trotz ihrer vielen konstruktionsbedingten Vorzüge in der bestehenden Form keine Chance haben, zu einem massentauglichen Zahlungsmittel zu werden. Dafür sind die Transaktionsprozesse viel zu langsam und viel zu energieaufwändig. Inwieweit es gelingen kann, Kryptowährungen mit vergleichbarer Sicherheit und Unabhängigkeit zu schaffen, deren Energiekosten jedoch konkurrenzfähig zu herkömmlichen Zahlungssystemen sind, bleibt abzuwarten und zu beobachten. Viele Bitcoin-Konkurrenten setzen jedenfalls auf Mechanismen, die deutlich schnellere und damit energiesparendere Transaktionen ermöglichen.

Nach der Betrachtung der Funktionsprinzipien und Nutzungspraxis soll die vorliegende Ausarbeitung nun noch in einem kurzen Abriss der Entstehungsgeschichte von Bitcoin ihren Abschluss finden.

5 Vom subversiven Konzept zur Landeswährung

5.1 Idee einer Kryptowährung

Erste Ideen zu rein elektronischen Währungen stammen bereits aus dem Jahre 1983, in dem der US-amerikanische Kryptografie-Wissenschaftler David Chaum ein Papier über eine als „eChash" bezeichnete digitale Währung veröffentlicht hatte. Es folgten in den Jahren 1996 und 1998 weitere Überlegungen der NSA in ihrem Papier „How to Make a Mint: the Cryptography of Anonymous Electronic Cash" bzw. von Wie Dai mit seiner Idee vom „b-money" und Nick Szabo mit seiner Idee vom „bit gold". Wie Dai hatte dabei bereits die Grundidee eines anonymen und verteilten Systems, während Szabo bereits die Idee mit dem „Proof of Work" formuliert hatte. Es sollte allerdings erst bis in das Jahr 2009 dauern, bevor all diese Ideen zu einer real funktionierenden Kryptowährung zusammengefasst wurden.

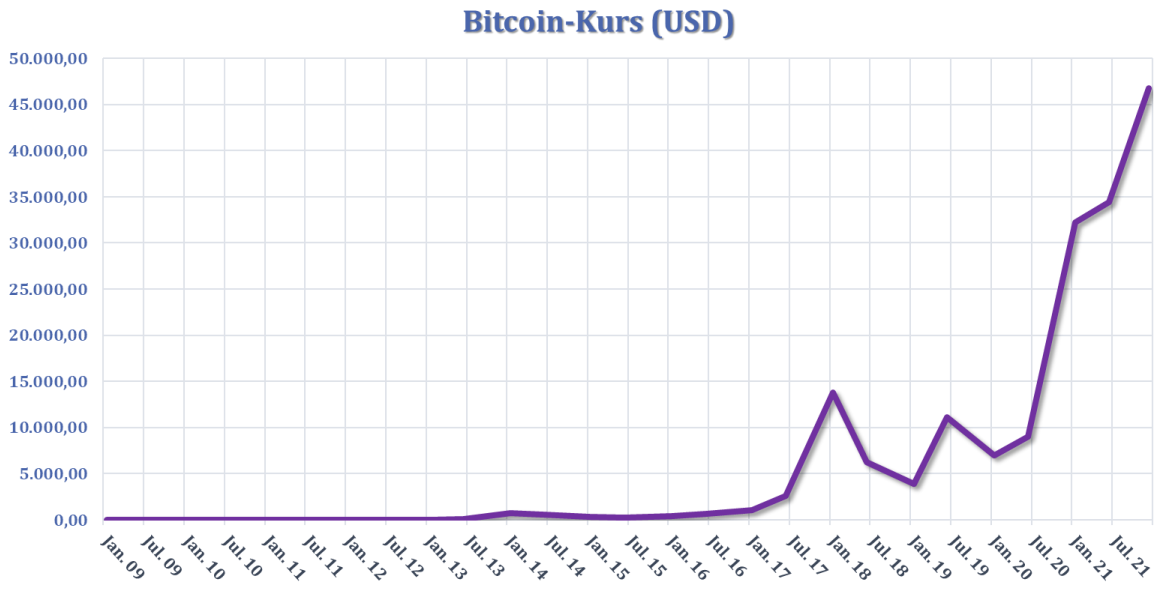
5.2 Nakamotos Papier

Im Jahre 2008 veröffentlichte eine bis heute unbekannte (und insofern sagenumwobene) Person bzw. Gruppe unter dem Pseudonym „Satoshi Nakamoto" ein Papier, in dem zum ersten Mal eine vollständig ausformulierte Methode für ein dezentrales Transaktionssystem zur Zahlung mit digitalem Bargeld unter dem Namen „Bitcoin" präsentiert wurde. Nach Angaben des Autors (bzw. der Autoren) fand die Konzeptionierung der Bitcoins bereits im Jahre 2007 statt. Noch im Jahr Veröffentlichung des Papiers – also im Jahre 2008 – wurde die Domäne „bitcoin.org" registriert, und die erste OpenSource-Referenzimplementierung einer Software für Bitcoins veröffentlichte Nakamoto im Januar 2009. Im selben Monat Schürfte Nakamoto dann gleich auch den ersten Block der Bitcoin-Blockchain – den sogenannten „Genesis-Block". Die erste Bitcoin-Transaktion fand ebenfalls noch im Januar 2009 statt.

Nachdem Nakamoto bis 2010 rund eine Million Bitcoins geschürft hatte (was damals noch mit vergleichsweise geringem Rechenaufwand möglich war), übertrug er die Kontrolle über den Quellcode für die Referenzsoftware an Gavin Andersen, der später zum leitenden Entwickler der Bitcoin Foundation wurde.

In den beiden Folgejahren wurden Bitcoins erstmals für reale Zahlungen verwendet – und zwar überwiegend im Darknet, wo die Anonymität der Bitcoin-Zahlungen aus naheliegenden Gründen besonders geschätzt wurde. Der Preis für ein Bitcoin betrug zum Anfang des Jahres 2011 rund 0,30 US-Dollar, bevor er sich nach heftigen Schwankungen auf rund fünf US-Dollar zum Jahresende einpendelte. Sowohl der Durchschnittskurs von rund fünf Dollar als auch die Volatilität hielten sich über das gesamte Jahr 2012, in dem außerdem die Bitcoin Foundation gegründet wurde. Gleichzeitig wurden in den Jahren 2011 und 2012 erhebliche Verbesserungen an der Bitcoin-Software vorgenommen und veröffentlicht.

5.3 Rasanter Siegeszug



Der eigentliche Siegeszug der Bitcoins begann dann im Jahre 2013, zu dessen Anfang der Kurswert für ein Bitcoin rund 13 US-Dollar betrug. Bis zum Ende desselben Jahres stieg der Kurs dann bereits auf 770 US-Dollar. Der weltweit größte Handel mit Bitcoins wurde damals von einer japanischen Firma namens „Mt. Gox“ betrieben. Bereits im Jahre 2013 gerieten Bitcoins aber wegen ihrer Verwendung im Darknet sowie wegen teils unlizenzierter Geldhandelsgeschäfte in Verruf und waren mehrfach Gegenstand behördlicher Ermittlungen.

Nachdem der Bitcoin-Kurs zum Ende des Jahres 2014 auf etwas über 300 US-Dollar gefallen war, stieg er bis Ende 2015 auf gut 430 Dollar und bis Ende 2016 schon auf fast 1.000 US-Dollar.

Im Jahre 2017 gab es nach Schätzungen der University of Cambridge bereits zwischen 3 und 6 Millionen individueller Nutzer von Kryptowährungen. Nach diversen Software-Verbesserungen in den Jahren 2016 und 2017 stieg der Bitcoin-Kurs zum Ende des Jahres 2017 auf gut 13.400 US-Dollar, fiel aber bis Ende 2018 auf knapp 3.450 US-Dollar – nicht zuletzt, nachdem China den Bitcoinhandel im Jahre 2018 endgültig verboten hatte. Dennoch erholte sich der Bitcoin-Kurs bereits zur Mitte des Jahre 2019 hin wieder auf über 13.000 US-Dollar. Inzwischen wurden Bitcoins zunehmend auch von seriösen Institutionen und Unternehmen wie etwa PayPal als Zahlungsmittel akzeptiert. Auf diese Weise erreichte der Bitcoin-Kurs Ende 2020 zum ersten Mal fast die 20.000 US-Dollar-Marke. Im selben Jahr kündigte der Schweizer Kanton Zug an, dass er ab Anfang 2021 Steuerzahlungen auch in Bitcoins akzeptieren wolle.

Anfang 2021 wurde bekannt, das Tesla über 1,5 Milliarden US-Dollar in Bitcoins investiert hat, was den Bitcoin-Kurs auf über 46.000 US-Dollar ansteigen ließ. Seit dem 7. September 2021 sind Bitcoins offiziell zusätzliche Landeswährung des Staates El Salvador. Der Staat selbst will das Mining von Bitcoins auf Basis geothermisch gewonnener Energie vorantreiben. Anfang November 2021 kletterte der Bitcoin-Kurs erstmals auf über 68.740 US-Dollar und liegt zur Zeit der Abfassung dieses Vortrags bei rund 47.000 US-Dollar.

Quellen

1. https://www.blockchain.com/charts/market-price
2. https://www.coindesk.com/business/2021/03/23/how-paypal-became-a-major-crypto-player/
3. https://de.wikipedia.org/wiki/Anwendungsspezifische_integrierte_Schaltung
4. https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem
5. https://de.wikipedia.org/wiki/Bitcoin
6. https://en.wikipedia.org/wiki/Bitcoin
7. https://de.wikipedia.org/wiki/Bitcoin_Core
8. https://en.wikipedia.org/wiki/Bitcoin_Foundation
9. https://en.wikipedia.org/wiki/Cryptocurrency
10. https://en.wikipedia.org/wiki/Ecash
11. https://de.wikipedia.org/wiki/Field_Programmable_Gate_Array
12. https://en.wikipedia.org/wiki/History_of_bitcoin
13. https://de.wikipedia.org/wiki/Kryptow%C3%A4hrung
14. https://en.wikipedia.org/wiki/Mt._Gox
15. https://en.wikipedia.org/wiki/Wei_Dai
16. https://quantaloop.io/how-many-hashes-create-one-bitcoin/
17. https://www.youtube.com/watch?v=bBC-nXj3Ng4&t=280s