Mi Primer Bitcoin

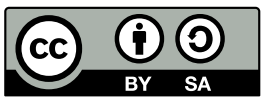
Das Bitcoin-Diplom

FINANZIELLE BILDUNG BASIEREND AUF BITCOIN

Arbeitsbuch für Lernwillige

In deutscher Übersetzung vom spanischen Original (3. Edition, September 2022).

VERSION 1.01| AUGUST 2023



Das Bitcoin-Diplom

FINANZIELLE BILDUNG BASIEREND AUF BITCOIN

Arbeitsbuch für Lernwillige
Version 1.01 | August 2023

Die deutsche Übersetzung des Bitcoin Diploms von ***Mi Primer Bitcoin*** erfolgte durch das Übersetzungskollektiv der Aprycot Content Plebs. Wir möchten uns an dieser Stelle ausdrücklich bei ihnen bedanken, allen voran den hierbei Mitwirkenden, ohne die dies nicht möglich gewesen wäre:

• Stefan Gerber, Twitter: @w4ttSoLdAt, Spende: w4tt5old4t@getalby.com;

• Thomas Geier, Twitter: @DerGeier21, Spende: dergeier@getalby.com;

• Bitboxer, Twitter: @GhostofBitboxer, Spende: BitBoxer75@getalby.com.

Spenden:

Mi Primer Bitcoin
EL SALVADOR

bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf

APRYCOT

slightsock95@walletofsatoshi.com

Danksagung

Das ***Bitcoin-Diplom*** war ein durchschlagender Erfolg und ist schneller gewachsen, als wir es uns je hätten vorstellen können. Wir möchten all den wunderbaren Menschen, die uns so weit gebracht haben, unsere Anerkennung aussprechen.

Das Kernteam des Lehrplans, die treibende Kraft hinter diesem Inhalt, besteht aus Dalia Platt, Gloriana Solano, Raúl Guirola und Robert Malka. Sie haben monatelang unermüdlich hinter den Kulissen gearbeitet, um dieses Projekt unter großem Zeitdruck auf die Beine zu stellen und immer weiter zu lernen und zu verbessern. Ohne diese vier wäre dies alles nicht möglich gewesen. Diese Kerngruppe wurde auf ihrem Weg von Giacomo Zucco, Pedro Solimano, María Andrée Maegli, Alejandro Machado, Gerson Martínez und Vriti Saraf unterstützt. Gerardo Apóstolo und Enrique Jubis, die Designer von ACTIVA, haben ebenfalls hervorragende Arbeit geleistet.

Die Geschichte des ***Bitcoin-Diploms*** beginnt im Februar 2022 bei einem Treffen in La Pacheco, einer öffentlichen Schule in San Marcos, in El Salvador. Wir haben uns beeilt, über 400 Einzelspender zu gewinnen, den Unterricht im April begonnen und die erste Klasse hat im Juni ihren Abschluss gemacht.

Die Urheber dieses Treffens im Februar sind auch die Hauptfiguren in dieser Geschichte. Der Direktor von La Pacheco, Asael Rodríguez, war bestrebt, seine Schüler auf eine Welt im Wandel vorzubereiten. Der Kongressabgeordnete Rodrigo Ayala, der La Pacheco bereits unterstützte, erkannte ebenfalls die Notwendigkeit der Bitcoin-Ausbildung an. Carlos Toriello, Community Builder bei IBEX Mercado, lud andere Bitcoiner, darunter auch mich, ein, die Schule zu besuchen und sich über den Lehrplan zu informieren.

Carlos von IBEX verdient hier eine eigene Rubrik. Sie haben die Mittel für den Bau eines neuen Cafés für La Pacheco aufgebracht, sich für die Sache eingesetzt, uns bei der Finanzierung der restlichen Kosten geholfen und Menschen aus der ganzen Welt organisiert, um an der ersten Aktion teilzunehmen und dabei zu sein. Das Bitcoin-Diplom gibt es inzwischen auch an anderen Orten und mit anderen Sponsoren, aber es baut auf dem Erfolg des Pilotprogramms in La Pacheco auf und wäre ohne sie einfach nicht zustande gekommen.

Mi Primer Bitcoin ist eine gemeinnützige Organisation mit einer einzigartigen Mission: *hochwertige, unvoreingenommene Bitcoin-Ausbildung zu jedem in El Salvador und dann zu jedem in der Welt zu bringen.* Als erstes Land, das Bitcoin eingeführt hat, glauben wir, dass El Salvador ein Beispiel für die Basis sein kann und dass die Grundlage für den Erfolg eine qualitativ hochwertige, unparteiische Ausbildung sein wird. Unsere Vision ist es, eine Nation zu unterrichten und die Welt zu verändern. Ich weiß, es klingt verrückt, aber ich glaube, wir sind auf dem Weg dorthin und das ***Bitcoin-Diplom*** ist ein großer Teil davon.

Für eine bessere Welt,

John Dennehy

Gründer
Mi Primer Bitcoin

Danksagung der Übersetzer

Wir wollen uns herzlich bei dem Team von ***Mi Primer Bitcoin*** für ihren Beitrag zur internationalen Bitcoin-Bildung sowie für die Inspiration bedanken. Kurz nach der Veröffentlichung der ersten Version vom ***Diplomado en Bitcoin*** war für uns klar, dass wir das Werk übersetzen werden.

Die beteiligten Content Plebs haben Anfang 2023 begonnen, ehrenamtlich eine deutsche Version zu erstellen. Dazu wurde das Arbeitsbuch gründlich übersetzt, lektoriert und teilweise überarbeitet, indem einige Fehler beseitigt, Erläuterungen erweitert und einige Links zu Videos in spanischer Sprache wurden ausgetauscht. Dabei wurde stets auf das passende Format und Design geachtet. Die deutsche Übersetzung der zweiten Version in Englisch (März 2023) wird auch zeitnah folgen. Es war uns eine Ehre!

Für die weitere Verbreitung haben wir die zugrunde liegenden Quell- und PDF-Dateien zum kostenfreien Download auf unserer Webseite aprycot.media, sowie auf den Seiten von MiPrimerBitcoin, siehe QR-Codes weiter unten, hinterlegt.

Zum Schluss wollen wir in tiefster Dankbarkeit denjenigen Respekt zollen, ohne die wir alle wohl niemals die Möglichkeit bekommen hätten, bei der Entstehung und Entwicklung einer der bedeutendsten Entdeckungen der Menschheitsgeschichte beteiligt zu sein:
den Cypherpunks,
Satoshi Nakamoto und
allen Bitcoin-Core-Entwicklern.

Einundzwanzig Millionen Mal Danke!

Für eine bessere Welt,

Stefan Gerber, Thomas Geier und BitBoxer

Aprycot Media Content Plebs

www.Aprycot.Media

https://miprimerbitcoin.io/en/my-first-bitcoin/

https://github.com/MiPrimerBitcoin

Inhaltsverzeichnis

Lektion 6

Lektion 7

Lektion 8

Lektion 9

Lektion 10

Zusatzlektion

Warum Bitcoin?

Praxisübung. Schreibe hier auf, warum du denkst, dass es wichtig ist, etwas über Bitcoin zu erfahren. Es gibt keine falsche Antwort.

Lektion 1

Einleitung: Das Geldsystem

1.1 Übung: Einführung in das Thema Geld
1.2 Was sind die Probleme mit dem heutigen Geld?
- Folgen der Entwicklung des Geldes
  - Bedürfnisse versus Ressourcen
- Die Modernisierung

1.3 Definition von Geld
- Funktionen des Geldes
- Eigenschaften des Geldes
- Konventionelles Geld und Geldvermögenswerte
  - Arten von Geld
  - Übung: Sind Rosinen gutes Geld?

Einleitung: Das Geldsystem

1.1 Übung: Einführung in das Thema Geld

Gemeinschaftsübung: Warte auf die Anweisungen der Lehrkraft, um diese Übung durchzuführen!

1.2 Was sind die Probleme mit dem heutigen Geld?

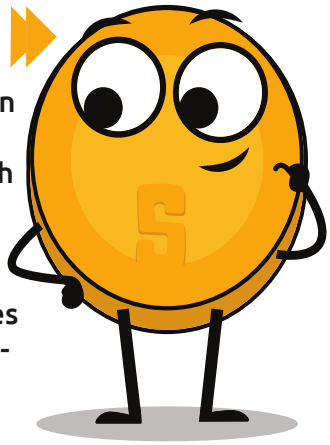
Wir sind so programmiert, uns den Herausforderungen des Lebens zu stellen und uns weiterzuentwickeln. Der Wille, sich zu verbessern und ein noch produktiveres, kreativeres und wertvolleres Leben zu führen, ist ein natürlicher menschlicher Prozess. Aber:

- Wir leben in einer Welt, in der es für einige wenige sehr viel und für die meisten sehr wenig gibt.
    - Individuen mit geringeren ökonomischen Ressourcen haben nicht die gleichen Chancen. Warum?
        - Sie haben keinen Zugang zur gleichen Bildung.
        - Sie haben keinen Zugang zu den erforderlichen Krediten, um ein Unternehmen zu gründen.
- Um die Armut zu verringern und das soziale Wohlergehen zu fördern, ist es wichtig:
    - den Zugang zu finanzieller Bildung für alle zu verbessern.
    - die Fähigkeit zu entwickeln, mit Geld umzugehen.
    - einen verantwortungsvollen Umgang mit neuen Technologien zu erlernen.
    - zu wissen, wie man für die Zukunft plant.

Wir werden sehen, dass **Bitcoin** ein Werkzeug und eine Art von Geld ist, das:

- transparent, dezentralisiert, global, digital, kostengünstig, privat, programmierbar sowie leicht und schnell zugänglich ist und dadurch helfen kann, diese Probleme zu beheben.

SATOSHI



Das ist *SATOSHI*, ein interaktiver Assistent, der dich durch das *Bitcoin-Diplom* begleiten wird. *SATOSHI* wird dir während des Kurses Daten und Empfehlungen geben.

Die Folgen der Entwicklung des Geldes

- Die Menschen mussten schon immer mit irgendwas ihre Zukunftswünsche finanzieren.
    - Sie tun dies, indem sie ihren Arbeitslohn, ihre Zeit und Energie gegen Wertaufbewahrungsmittel eintauschen.
- Hätten wir das Geld nicht erfunden, würden wir uns noch immer an die *Tauschwirtschaft* halten.
    - Alles, was jemand kaufen möchte, müsste gegen etwas getauscht werden, das diese Person bereitstellen könnte.
- Die kontinuierliche Entwicklung von Geldsystemen hat die Gesellschaft und die globale Interaktion revolutioniert. Im Allgemeinen hat es das gemeinsame Interesse gefördert, die Lebensqualität zukünftiger Zivilisationen zu verbessern.
    - Mit dem technologischen Fortschritt und der zunehmenden Produktivität sollten wir eigentlich Folgendes sehen:
        - *immer niedrigere Preise.*
        - *eine stärkere Währung.*
        - *die Möglichkeit, mehr für weniger Geld zu kaufen.*
    - Doch das Gegenteil ist der Fall:
        - *Die Preise steigen, die Währungen werden schwächer und wir müssen mehr ausgeben, um weniger zu kaufen.*

— Wie ist es dazu gekommen?
— Wie, warum und zu welchem Zweck wird mehr Geld geschaffen und was sind die Folgen?
— Was verbirgt sich hinter den heutigen Finanzsystemen?
— Worin besteht die unsichtbare Gefahr des Wertverlusts unseres Geldes?
— Wie können wir den Wert unserer Ersparnisse erhöhen?

● Heute haben nur Banken und Regierungen die Befugnis, in einer Volkswirtschaft Geld zu emittieren.

Das Geld geht einfach nicht aus. Die Regierungen drucken die für die Finanzierung ihrer öffentlichen Ausgaben erforderliche Geldmenge, führen der Wirtschaft Mittel zu und ziehen sie später in Form von Steuern wieder ab.

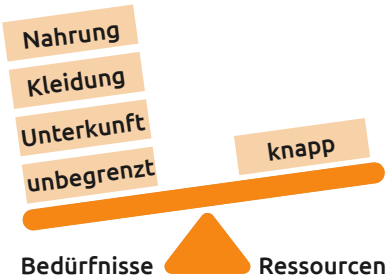
● Das Problem ist, dass die Menschheit mehr ausgibt als sie einnimmt. Die Folgen davon sind:

• ein Vertrauensverlust in den Wert des Geldes und in das moderne Bankensystem.
• globale, wirtschaftliche und politische Instabilität – sogar Kriege.

- Warum?

Bedürfnisse versus Ressourcen

Unsere Bedürfnisse sind unendlich, aber unsere Ressourcen sind knapp.



Die Modernisierung

„Man muss den Banken vertrauen, dass sie unser Geld aufbewahren und elektronisch überweisen, aber sie verleihen es in Zeiten von Kreditblasen, ohne auch nur einen Bruchteil davon in Reserve zu haben." – **Satoshi Nakamoto**

Öffentliche Verwaltungen, Unternehmen und Familien brauchen Geld und bitten die Bank darum.
Für diese Schulden zahlen sie Zinsen an die Bank.

Die Bank ist ein Mittelsmann. Das heißt, sie kauft Geld von Sparern und verkauft es zu einem höheren Zinsatz an diejenigen, die es brauchen.

Viele Familien sparen. Sie legen ihr Geld bei der Bank an und verlangen eine kleine Zinsgebühr.

Einleitung: Das Geldsystem

Das Bankgeschäft besteht aus:

- Dem Ankauf von Geld in Form von Einlagen von Sparern und dem anschließenden Verkauf in Form von Krediten an diejenigen, die es brauchen.

- Der Gewinn der Banken entsteht, wie in jedem anderen Geschäft auch, durch:
  - einen Verkaufspreis, der höher ist als der Einkaufspreis – der Zinssatz für das von den Banken verliehene Geld ist höher als das, was die Banken den Kreditgebern zahlen.
  - Aber der Schlüssel zur Macht im Bankenwesen liegt in der Möglichkeit, etwas zu verkaufen, das nicht der Bank, sondern dem Sparer gehört.

- Regierungen kontrollieren die Emission ihrer Währungen – sie versuchen, dadurch problematische Wirtschaftszyklen zu lösen.

- In Zeiten der Rezession drucken die Regierungen mehr Geld, um:
  - kurzfristig das Wachstum anzukurbeln.
  - die kurzfristige Arbeitslosigkeit zu verringern.

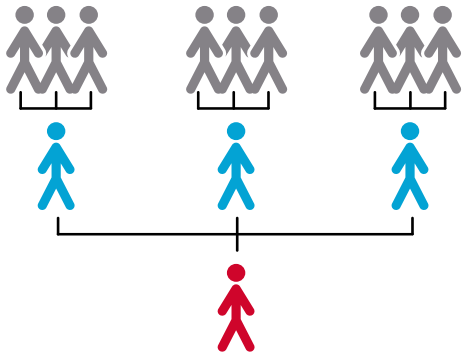
- Die Notwendigkeit von physischem Papiergeld hat an Bedeutung verloren.
  - Online-Banking hat die Nutzung von Krediten erleichtert.

Die Vorteile

— Banken erleichtern sofortige Transaktionen und das Planen für die Zukunft.
— Sie erfassen den gesamten Zahlungsverkehr von Gläubigern und Schuldnern in zentralisierten Datenbanken.
— Sie aktualisieren ständig die Zahlungsein- und -ausgänge ihrer Nutzer.
— Sie überprüfen die Rechtmäßigkeit der Konten.
— Wenn das Geld auf einem Konto aus diversen Gründen verschwindet, ist es ersetzbar.
— Für den Fall, dass die Banken ausgeraubt werden, besitzen sie Versicherungen.

Die Nachteile

— Das Bankensystem hat eine einzige Fehlerquelle, es ist zentralisiert und kann leicht manipuliert werden.



— Regierungen können:

- die Geldmenge nach Belieben ausweiten und verringern.
- Bankkonten beschlagnahmen.
- Abhebungen ohne Vorankündigung blockieren.
- schwerwiegenden Problemen oder Hackerangriffen ausgesetzt sein.
- grundlegende Dienstleistungen abschaffen.
- Zinssätze und Steuern verwalten.

— Hohe Inflation und Negativzinsen lassen den Wert des Geldes sinken.

„Eine Bank ist ein Ort, an dem man dir bei schönem Wetter einen Regenschirm leiht und ihn wieder zurückverlangt, wenn es zu regnen beginnt."

- Robert Lee Frost

1.3 Definition von Geld

Wir bezahlen mit Bargeld, Schecks und/oder Kreditkarten im Austausch für Waren und/oder Dienstleistungen.

• Wir denken **nicht** darüber nach, dass all diese Zahlungsmittel nur Zahlungsversprechen sind.

Hast du dich jemals gefragt, was Geld ist? Das folgende Video beschäftigt sich genau damit.

— SATOSHI

https://youtube.com/watch?v=InwVM6s7WoY&feature=shareb

Funktionen des Geldes

Geld hat **drei Funktionen:**

1. Wertaufbewahrungsmittel, das investiert, gespart, geliehen oder verliehen werden kann.
2. Zahlungsmittel, um für Waren und Dienstleistungen zu bezahlen.
3. Maßeinheit, mit der wir die Preise von Produkten vergleichen können.

- **Wertaufbewahrungsmittel:** Es neigt dazu, seinen Wert im Laufe der Zeit zu erhalten.
- **Zahlungsmittel:** Beseitigt das komplexe Tauschsystem, indem es einen effizienteren Warentausch sowie eine effizientere Schuldbegleichung ermöglicht.
- **Maßeinheit:** Ermöglicht einen universellen Standard des Preissystems, ein einziges Preissignal, um den Wert von Waren und Dienstleistungen auszudrücken.

Praktische Übung: Schreibe die richtige Funktion des Geldes in die freien Felder!

_____. Das Geld erleichtert den Austausch, weil es von jedem für Zahlungen akzeptiert wird.

_____. Das Geld hilft uns, unseren Wohlstand zu erhalten, da wir es sparen und in der Zukunft ausgeben können.

_____. Mit Geld können wir den Wert von Waren und Dienstleistungen messen und Vergleiche zwischen verschiedenen Waren anstellen. Ein teures Preisschild sagt uns etwas über den Wert der Ware.

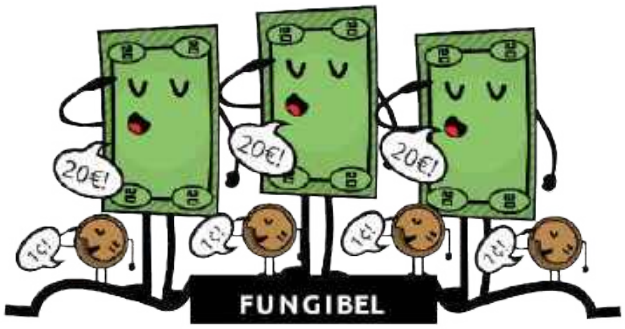
Einführung: Das Geldsystem

Eigenschaften des Geldes

Geld kann viele Formen annehmen. Je mehr eine Geldart von den folgenden Eigenschaften aufweist, desto besser ist sie.

- **Langlebigkeit**: Geld muss dem physischen Verfall widerstehen und über die Zeit hinweg haltbar sein. Es muss in der Lage sein, in einem akzeptablen und erkennbaren Zustand in der Wirtschaft zu zirkulieren.

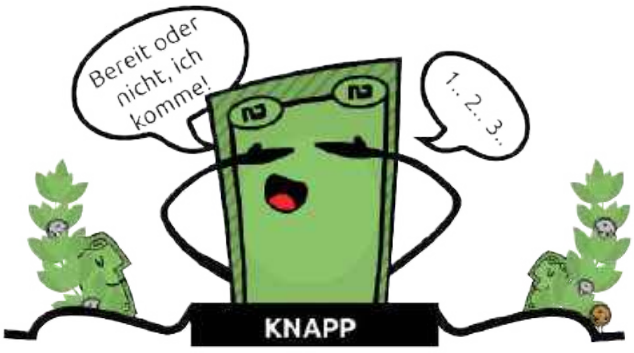
- **Einheitlichkeit oder Fungibilität:** Jede Geldeinheit muss wie jede andere, d. h. genau gleich sein.



- **Tragbarkeit:** Es muss sich leicht von einem Ort zum anderen bewegen lassen. Man muss in der Lage sein, großen Wert in einem kleinen Gewicht anzuhäufen.

- **Akzeptanz:** Der als Geld verwendete Gegenstand muss von allen als Geld anerkannt werden.

- **Knappheit:** Der Wert des Geldes hängt von Angebot und Nachfrage ab. Je mehr Geld geschaffen wird, desto mehr sinkt sein Wert.



- **Teilbarkeit:** Es muss sowohl gegen teure als auch gegen billige Waren gehandelt werden können und leicht teilbar sein, ohne seinen Wert zu verlieren.

TEILBAR

Konventionelles Geld und Geldvermögenswerte

- **Konventionelles Geld** ist das Geld, das in einem bestimmten Land allgemein verwendet wird.

  • Es umfasst den Bargeldumlauf, Bankeinlagen und Zentralbankreserven.
  • Das meiste Geld besteht aus Krediten oder elektronischen Buchungen.
  • Es behält **nicht unbedingt** seiner **Wert** über die **Zeit**.

- **Geldvermögenswerte** behalten im Allgemeinen ihren **Wert** über die **Zeit.**

Arten von Geld

- **Warengeld**

  • schwer abzubauen, knapp.
  • attraktives Wertaufbewahrungsmittel.
  • Gold und Silber haben sich über Jahrhunderte hinweg als gutes Geld bewährt.
  — [Geldvermögenswerte]

- **Stellvertretende (Teil-)Zertifikate**

  • durch Gold oder Silber gedeckte Banknoten.
  • Jeder Geldschein ist gegen seinen Gegenwert in Metall eintauschbar.
  • In der modernen Geschichte wurde der Goldstandard bis 1971 beibehalten.
  — [Zu Beginn Geldvermögenswert, wird aber mit der Zeit zu konventionellem Geld, wenn die Geldmenge erhöht wird].

- **Fiat-Geld**

  • wird von einer Regierung als Monopol eingeführt und nach Belieben herausgegeben.
  • ist nicht durch ein physisches Produkt gedeckt.
  • hat keinen intrinsischen Wert. Der Wert hängt ab von:

    - dem Verhältnis von Angebot und Nachfrage.
    - der Stabilität der Regierung, die die Emission steuert.

  — [Konventionelles Geld. Das Gegenparteirisiko von digitalem Fiat-Geld ist größer als das physische Risiko].

- **Bitcoin**

  • ist knappes digitales Geld.
  • funktioniert dezentralisiert.
  • Der Zahlungsverkehr basiert auf Software und „Peer-to-Peer“-Kryptographie.
  — Geldvermögenswert

Einleitung: Das Geldsystem

Praktische Übung: Mache ein Kreuz, wenn der Gegenstand die angegebene Eigenschaft hat! **Welchen Gegenstand würdest du als Geld wählen?** ** Fülle die letzte Spalte „Bitcoin" erst aus, wenn du die Lektion 4 abgeschlossen hast!*

Eigenschaft	 Äpfel	 Muscheln	 1 Unze Gold	 1 Euro	 Bitcoin
Einheitlichkeit/Fungabilität					
Teilbarkeit					
Tragbarkeit					
Seltenheit					
Beständigkeit					
Akzeptanz					

Welchen Gegenstand würdest du als Geld wählen und warum?

Übung: Sind Rosinen gutes Geld?

Gemeinschaftsübung: Warte auf die Anweisungen der Lehrkraft, um diese Übung durchzuführen!

Lektion 2

Geschichte, Entwicklung und Entwertung des Geldes

2.1 Geschichte des Geldes
2.2 Übung: Tauschhandelsspiel
2.3 Entwicklung des Geldes im Laufe der Zeit
- Der internationale Währungsstandard in der Geschichte

2.4 Plötzlicher Wechsel zu Fiat
2.5 Zentralbanken
2.6 Gemeinschaftsübung: Mindestreserve (fractional reserve)

Geschichte, Entwicklung und Entwertung des Geldes

2.1 Geschichte des Geldes

Geld ist etwas, das wir jeden Tag benutzen, aber wir halten selten inne, um darüber nachzudenken … Woher kommt es? Wie haben unsere Vorfahren Handel betrieben?

- Was Geld ausmacht, hat sich im Laufe der Zeit und von Ort zu Ort verändert.

- Geld ist so alt wie die Sprache selbst. Es ist ganz einfach eine Form der Kommunikation, eine Technologie.

- Es besteht kein allgemeiner Konsens darüber, was es wirklich ist.

- Im Prinzip bräuchte man kein besonderes Gut, wie zum Beispiel eine Banknote, um zu erkennen, wem man Waren und/oder Dienstleistungen schuldet.
  - Jeder kann sein eigenes Kassenbuch führen.
  - Unsere Vorfahren handelten auf diese Weise und/oder durch Tauschhandel, ohne dass sie Banken oder herkömmliches Geld benötigten.

2.2 Übung: Tauschhandelsspiel

Zurück in die Vergangenheit: Tauschhandel

Damit ein Tauschhandel stattfinden kann, müssen die Bedürfnisse in **zweifacher Hinsicht übereinstimmen**.

- Wer etwas tauschen will, muss einen Handelspartner finden, der das hat, was er will, und der das will, was er hat.

- Diese Form des Austauschs von Waren und Dienstleistungen ist zeitaufwendig, schränkt die Wirtschaftstätigkeit ein und begrenzt die Spezialisierung.

- Geld lindert diese Probleme.

Gemeinschaftsübung: Warte auf die Anweisungen der Lehrkraft, um diese Übung durchzuführen!

1. Was ist Tauschhandel?

2. Was sind die Hauptprobleme beim Tauschhandel?

3. Was ist Warengeld?

4. Welche Probleme treten bei der Verwendung von Warengeld auf?

5. Was ist Geld?

6. Warum sind die Menschen bereit, Geld anzunehmen?

Geschichte, Entwicklung und Entwertung des Geldes

2.3 Entwicklung des Geldes im Laufe der Zeit

Die Evolution des Geldes im Laufe der Zeit

- Der Tausch von materiellen Gütern oder Dienstleistungen gegen andere Güter oder Dienstleistungen — ist — **der Tauschhandel.**
  - wo Geld nicht im Spiel ist
- entsteht — als eine Notwendigkeit der Gemeinschaft und der gesellschaftspolitischen Strukturen.
  - Geld ≠ Währungseinheiten

WARENGELD

stellt einen Vermögenswert als Geld dar

welches einen
- **innerer Wert**
- **Nutzwert**

hat, und erfüllt die Merkmale, um als
- akzeptiertes Zahlungsmittel,
- Wertmaßstab,

verwendet zu werden.

- Salz
- Kakao
- Vieh

MÜNZGELD

Dieses wird ausgedrückt

in
- **Münzen**
- **Metallarten**

die dadurch gekennzeichnet sind, dass sie
- leicht zu transportieren,
- teilbar,
- speicherbar sind.

Die ersten Münzen wurden geprägt aus
- Gold
- Silber
- Kupfer

PAPIERGELD

Die Ausstellung von Zertifikaten, hinterlegt

mit **Edelmetallen** (die von allen akzeptiert werden),

zeichnete sich dadurch aus, dass sie
- leicht zu transportieren,
- teilbar,
- vollständig von der Regierung gedeckt sind.

FIAT-GELD

Es wird durch das ***Vertrauen*** einer Gesellschaft gestützt,

das nicht auf dem Wert,

sondern

auf der allgemeinen Überzeugung beruht, dass dieses Geld einen Wert hat,

was zur Gründung von Zentralbanken führte.

Das autoritäre Monopol

PLASTIKGELD

Schaffung des Kredit- und Debitkartensystems

sowie
- elektronischer Geldbörsen und
- Karten.

Es funktioniert wie

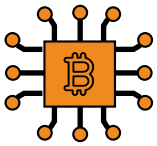
Banktransaktionen (bieten einen Ersatzwert für Bargeld).

KRYPTO-GELD

Ein digitales Tauschmittel, das starke Kryptographie verwendet,
- um Transaktionen zu sichern,
- Einheiten zu schaffen,
- die Übertragung von Vermögenswerten zu verifizieren.

Es ist unabhängig von Banken,

der Wert hängt ab von
- Nutzbarkeit,
- Angebot und
- Nachfrage.



Der internationale Währungsstandard in der Geschichte

Bimetall- Standard (17.-19. Jahrhundert)
Banknoten konnten in Gold und Silber umgetauscht werden.

Goldstandard (1870 - Erster Weltkrieg)
Jeder Bürger konnte sein Papiergeld in eine festgelegte Menge Gold umtauschen.

Zwischenkriegszeit
Die beiden Kriege und die Krise von 1929 setzten der Goldkonvertibilität für Privatpersonen ein Ende.

Bretton-Woods-Pakt
Am Ende des Zweiten Weltkriegs im Jahr 1945 legten die Alliierten fest, dass Währungen in US-Dollar konvertierbar sind.

Die Krise der 1970er Jahre
1971 veranlasste die wirtschaftliche Lage der USA in Verbindung mit dem Vietnamkrieg die Zentralbanken Europas dazu, zu versuchen, ihre Dollar in Gold zu konvertieren, was zu einer Krise in den USA führte und Nixon dazu veranlasste, die Konvertibilität des Dollars in Gold auszusetzen.

Gegenwärtige Phase
Ab 1973 bis heute ist Geld Fiat- und Digital-Geld.

https://m.youtube.com/watch?v=zcYw8a4RJC4

- Geld hat sich im Laufe der Zeit weiterentwickelt und war mit Herausforderungen und sich ändernden Bedürfnissen konfrontiert.
  - Normalerweise wurde die Geldform gewählt, die die besseren Eigenschaften aufwies.
  - Aber da der Wert der Währungen, die ursprünglich auf Geldwerten beruhten, durch den Übergang von Edelmetallen zu papiergebundenen Metallen verwässert wurde:
    - haben wir uns von der natürlichen Auswahl der leistungsfähigsten Form des Geldes hin zu einer einfachen Handhabung, besseren Tragbarkeit und Teilbarkeit entwickelt.
  - Es kam zu einer Verlagerung hin zur Zentralisierung.

2.4 Plötzlicher Wechsel zu Fiat

Das Industriezeitalter markiert den Beginn der Zentralisierung:

- Ziel war es, die produzierten Waren richtig zu verteilen.
  - Es wurden Zentralbanken geschaffen.
  - Das Kredit- und Debitkartensystem war geboren.
- Wenn Geld zentralisiert wird, können tiefgreifende Probleme entstehen.
  - Die Regierungen überwachen die Wirtschaftstätigkeit ihrer Bürger genau.
  - Machtmissbrauch kann führen zu:
    - wirtschaftlichen Anreizen und staatliche Interventionen.
    - Schuldenexplosion und verantwortungslosen Konsum.
    - zunehmender Vermögensungleichheit.

Bis 1971 wurde repräsentatives Geld verwendet als:
Zahlungsmittel und Wertaufbewahrungsmittel.

- Seit 1971 haben wir uns von gesundem Geld zu einer auf Schulden basierenden Welt entwickelt.
  - Richard Nixon hat die freie Konvertierbarkeit von Gold in Geld abgeschafft. Wir sind zum aktuellen Experiment übergegangen, dem ***Fiat-Geld***.
  - Modernes Geld ist eher per Dekret als durch Konsens gültig.
  - ***Fiat*** kommt aus dem Lateinischen und bedeutet „per Dekret“: Es wird per Gesetz bestimmt und festgelegt.

„Was gestern funktioniert hat, muss heute nicht mehr unbedingt funktionieren.“

- Jordan Peterson

2.5 Die Zentralbanken

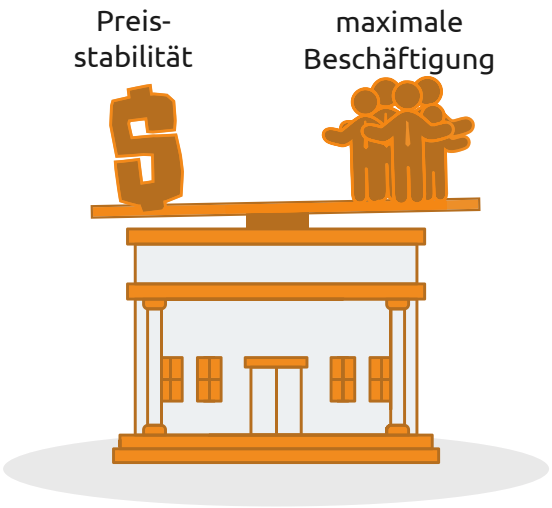
● Der Zweck und die Funktion einer ***Zentralbank***:

• Kontrolle der Geldpolitik des Landes, um die Stabilität zu gewährleisten.
• Ihre Aufgabe ist es, der Bankier der Banken zu sein.
• Ihre Hauptaufgabe: die Manipulation der umlaufenden Geldmenge.

- Steuerung der Inflation und Maximierung der Beschäftigung durch wirtschafts- und finanzpolitische Maßnahmen.

• Die US-Zentralbank wird ***Federal Reserve*** genannt.

Die Federal Reserve hat ein doppeltes Mandat:



● Wer definiert diese Ziele und wer profitiert davon?

• Große Banken – sie können die Politik auf staatlicher und sogar globaler Ebene beeinflussen.

● Wie verändert die Federal Reserve die Geldmenge?

• Durch das **Mindestreserve-Bankensystem**.
• Die Banken in den USA halten nur 10 % ihrer Einlagen als Reserve.
• Das Mindestreserve-Bankwesen führt zu einem **Geldschöpfungsmultiplikator**.

- In der Wirtschaft eines Landes verwenden mehr als zwei Personen das gleiche Geld zur gleichen Zeit.

Die Banken sind verpflichtet, einen bestimmten Prozentsatz aller Einlagen in der Bank zu halten. Eine Verringerung dieses Prozent-satzes bedeutet, dass mehr Geld zirkulieren kann, eine Erhöhung, dass weniger Geld zirkuliert.

● Welche Probleme kann das **Mindestreserve-Bankwesen** verursachen?

• Banken nehmen „langfristige Kredite auf und vergeben sie."

- Die Abhebungen von Einlagen übersteigen die Barreserven.
- Die Banken erleiden hohe Verluste.
- Im schlimmsten Fall kommt es zu einem Sturm auf die Banken.

• Änderungen der Zinssätze oder der Kapitalkosten wirken sich auf das Risiko aus.

- Mehr Geld im Umlauf bedeutet billigere und weniger anspruchsvolle Kredite.

● Offenmarktgeschäfte *(zur Erhöhung oder Verringerung des Bargeldumlaufs)*.

• Der Staat kauft oder verkauft monetäre Wertpapiere (hochliquide Schuldtitel).

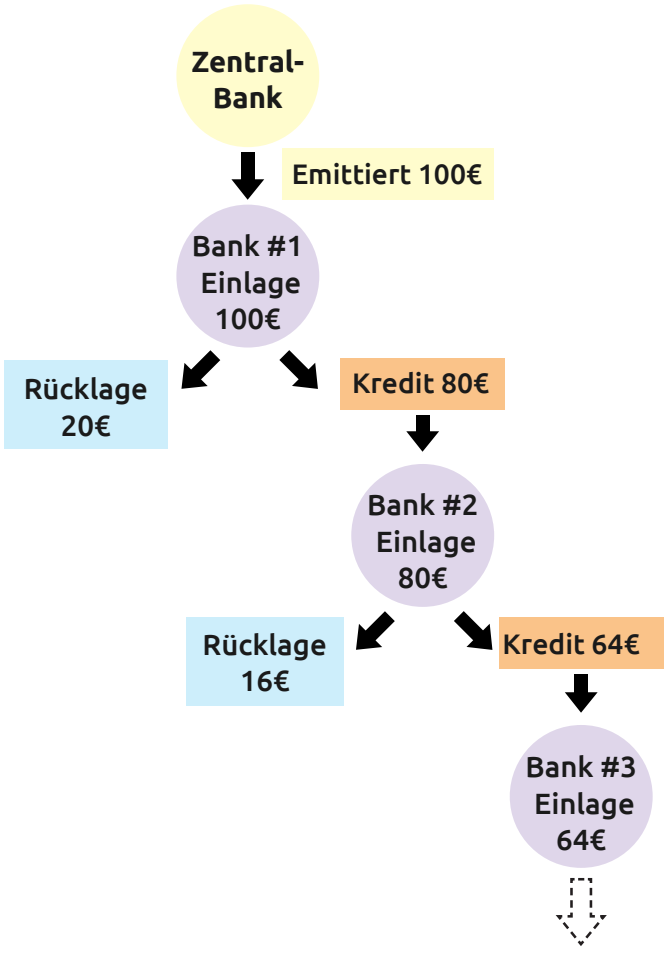
- Wenn er den Umlauf erhöhen will, *kauft* er Staatsanleihen.
- Wenn er den Umlauf verringern will, *verkauft* er Staatsanleihen.

2.6 Übung: Mindestreserve (fractional reserve)

Gemeinschaftsübung: Warte auf die Anweisungen der Lehrkraft, um diese Übung

BANKENREGISTER

	Euro-Darlehen	Euro-Einlage	10% Mindestreserve-pflicht
Einzahler A			
Darlehensnehmer A			
Einzahler B			
Summe in Euro			



Lektion 3

Die Auswirkungen von Fiat-Geld und Zentralisierung

3.1 Übung: Auktion!
3.2 Inflation
- Warum interessiert uns das?
- Was lehren uns die modernen Ökonomen?
- Ursachen für Inflation
- Inflation im Laufe der Zeit

3.3 Überwachung
3.4 Einschränkungen
3.5 Zentralisierung versus Dezentralisierung
3.6 Fazit

3.1 Übung: Auktion!

Gemeinschaftsübung: Warte auf die Anweisungen der Lehrkraft, um diese Übung durchzuführen!

3.2 Inflation

https://youtube.com/watch?v=sylf-1nkImg&feature=shareb

- Der Begriff **Inflation** wurde ursprünglich verwendet für die Erläuterung von:
  - dem Wertverlust einer Währung und
  - der Abwertung ihrer Kaufkraft, die durch die Erhöhung ihres Angebots verursacht wird.

- In der Regel kommt es zu diesem Wertverlust, was für die Währung bedeutet:
  - Die Preise für alle Waren und Dienstleistungen steigen allgemein und anhalt-end.

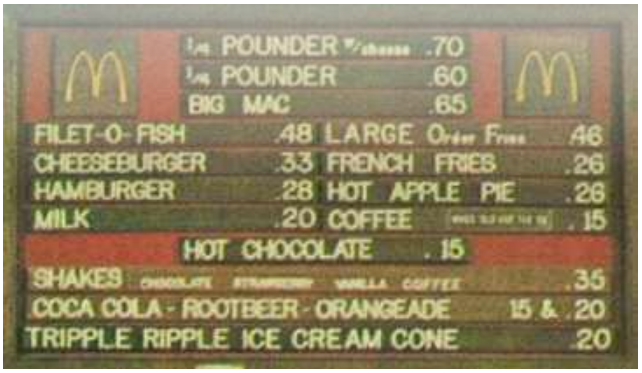
- Der Begriff „Inflation" wird inzwischen für Preissteigerungen verwendet,
  - ungeachtet der Ursache.

Warum interessiert uns das?

- Wenn mehr Geld für dieselbe Menge an Waren ausgegeben wird:
  - steigen die Preise.

- Wenn die Produktpreise schneller steigen als die Löhne und Gehälter:
  - werden die Menschen ärmer.

McDonalds im Jahr 1970



McDonalds im Jahr 2020

Was lehren uns moderne Ökonomen?

- Wir müssen die Inflation ankurbeln, um eine Nation effektiv zu führen.

- Wenn wir keine Anreize für Ausgaben und Investitionen schaffen (durch Währungsabwertung):
  - riskieren wir eine geringere Nachfrage.
  - Dies führt zu verminderter Produktion.
  - Schlimmstenfalls kann dies zu einer stagnierenden Wirtschaft führen.
  - All dies suggeriert, dass es schwierig, unmöglich oder sogar unklug ist, zu sparen.

Die Auswirkungen von Fiat-Geld und Zentralisierung

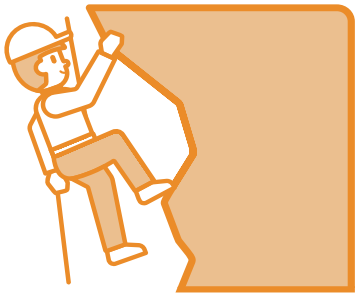
- Die derzeitige Situation ermutigt uns, Ausgaben zu tätigen. Diese Theorie ist kontraproduktiv.
  - Wir denken nicht an eine Zukunft, die über ein paar Tage, Wochen oder Monate hinausgeht.
  - Wir sollten in der Lage sein, uns auf die Zukunft unserer Enkelkinder vorzubereiten.
  - Inflation hindert uns an finanzieller Disziplin.
- Unsere Entscheidungen haben Konsequenzen.
  - Dies wird als „**Opportunitätskosten**" bezeichnet.

STUDIEREN

- **beste Karrieremöglichkeiten**
- **besser vorbereitet**
- **akademisches Ansehen**

ARBEITEN

- **Gehalt bekommen**
- **Arbeitserfahrung**
- **soziales Ansehen**



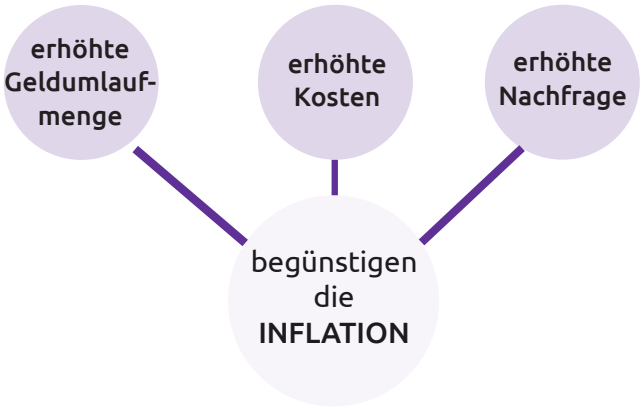
➡ Man hat eine **hohe Zeitpräferenz**, wenn man Dinge, die man jetzt bekommen kann, den Dingen vorzieht, die man vielleicht in der Zukunft bekommt.

➡ Man hat eine **geringe Zeitpräferenz**, wenn man es vorzieht, Dinge in der Gegenwart zu tun, um in der Zukunft bessere Dinge zu bekommen.

- Die Inflation fördert eine **hohe Zeitpräferenz**, was bedeutet, dass wir lieber heute 100 Dollar als in zwei Jahren 200 Dollar hätten.
- Unser Ziel sollte es sein, eine **niedrige Zeitpräferenz** zu schaffen.

Hohe Zeitpräferenz	Niedrige Zeitpräferenz
Geld ausgeben	Geld sparen
Fast Food	selbst kochen
Soziale Medien	ein Buch lesen
fernsehen	trainieren
Content konsumieren	Content erstellen

Ursachen für Inflation



Im folgenden Video erfahren wir die drei Gründe, warum Inflation auftritt.

https://m.youtube.com/watch?v=_DpyCXNiY7E

1. Kosten- oder Angebotsinflation

○ Erhöht den Preis von Rohstoffen und wird verursacht durch:

• Staatliche Vorschriften, Kriege, Dürreperioden, Lieferkettenprobleme und andere Situationen.

• Steigende Steuersätze erhöhen die Kosten für Rohstoffe.

• Fachkräfte werden teurer.

- Mangel an Fähigkeiten oder Ressourcen in der Gesellschaft.

• Neue Technologien sind in der Regel sehr teuer.

- Mit der Zeit senken sie die Kosten für die Produkte.

2. Nachfrageinflation

○ Das Angebot an Waren reicht nicht aus, um die Nachfrage zu decken.

○ Durch eine Steuersenkung (oder Senkung der Kreditzinsen) wird ein Anstieg des verfügbaren Einkommens erzielt:

• Überschüssiges Geld beginnt auf dem Markt zu zirkulieren.

• Es gibt einen Wettbewerb um die gleichen Waren mit mehr Geld.

- Das führt zu höheren Preisen.

○ Schließlich steigt das Angebot und die Preise sinken wieder.

3. Inflation durch Politik

○ Die Politik finanziert das Defizit, indem sie mehr Geld druckt.

• Sind die Arbeitsplätze/Projekte, die durch die Inflation geschaffen werden, real?

• Warum ist es für die Politik wichtig, dass die Menschen mit ihrem Geld etwas kaufen?

• Welche Arten von Gütern kaufen wir als Gesellschaft, wenn mehr Geld in der Wirtschaft vorhanden ist? Sind es lebensnotwendige Güter?

• Was passiert wenn in einer Volkswirtschaft die Steuersätze schneller steigen als die Löhne?

● Inflation bedeutet, dass die Arbeit, die man vor einiger Zeit geleistet hat, weniger wert ist als heute.

• Letztes Jahr wurden 10 Dollar verdient und 10 Mittagessen zu je 1 Dollar gekauft.

• Wenn man das Geld nun spart:

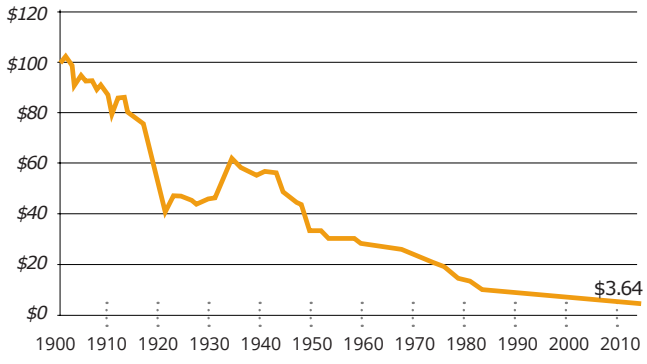
- zirkuliert dann mehr Geld in der Wirtschaft.
- gibt es mehr Menschen, die Mittagessen kaufen wollen.
- wird jedoch die gleiche Anzahl an Mittagessen zum Verkauf angeboten.
- Der Preis steigt auf 2€/Mittagessen.

• Mit den gesparten 10€ kann man nur 5 Mittagessen kaufen.

• Theoretisch ergibt es keinen Sinn. Wenn man 8 Stunden arbeitet, ändert sich diese Tatsache nicht, auch wenn 10 Jahre vergangen sind. Diese Energie sollte man behalten können.

• Man könnte sagen, dass die Inflation eine Art Diebstahl von Werten ist.

● Die folgende Grafik zeigt den Wertverlust des Dollars (USD).



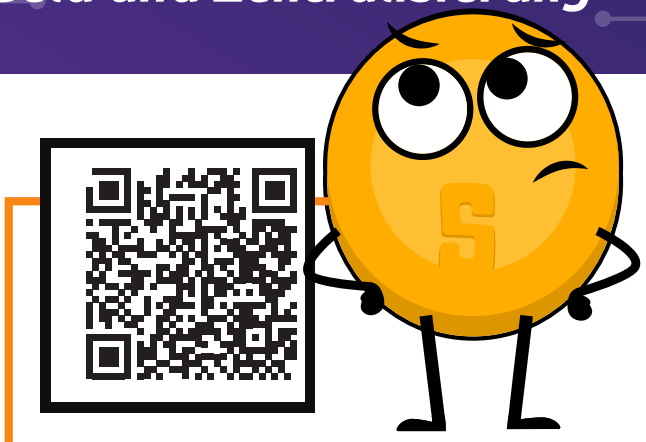
Die Auswirkungen von Fiat-Geld und Zentralisierung

Inflation im Laufe der Zeit

- Die Inflation zwischen 1970 und 2020 war viel höher als die des vorangegangenen 50-Jahre-Zeitraums (1920 bis 1970).

  • Was wird passieren, wenn wir so weitermachen wie bisher?

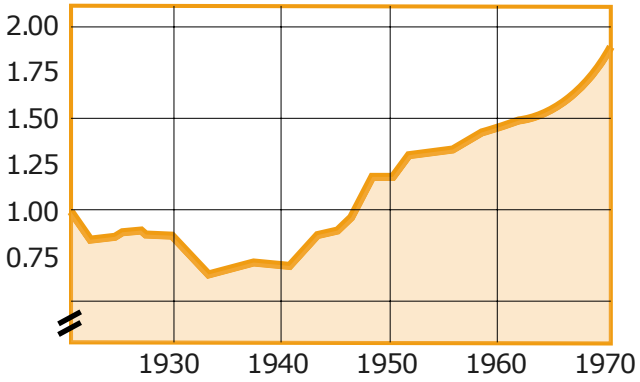
  • Wer wurde wirtschaftlich mehr bestraft, die Generation deiner Großeltern oder die Generation deiner Eltern?



Weitere Grafiken und Analysen zu anderen Zeiträumen findet man hier.

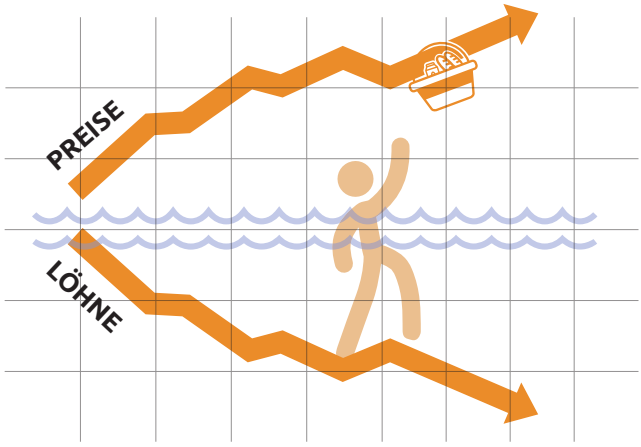
https://www.wolframalpha.com/input?i=1+1920+usd+in+2020

$1 von 1920 bis 1970

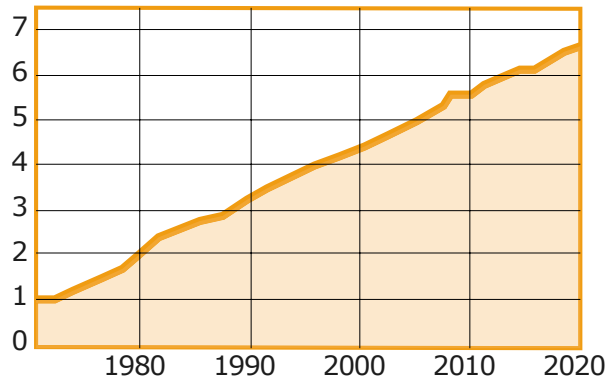


Ergebnis: **$1,94**
Durchschnittliche Inflationsrate: **1,33% pro Jahr**
Gesamtinflation: **93,72%**

- Glaubst du, dass die Löhne gleich gestiegen sind wie die Preise?



$1 von 1970 bis 2020



Ergebnis: **$6,67**
Durchschnittliche Inflationsrate: **3,87% pro Jahr**
Gesamtinflation: **566,60%**

- Anders ausgedrückt: Was wir heute (2022) mit 100 Dollar kaufen, hätte uns 1920 etwa 7 Dollar gekostet.
- Inflation führt zu **Kaufkraftverlust:**

  - Der Anstieg der Löhne ist geringer als der Anstieg der Lebensmittelpreise.
  - Der Einzelne ist gezwungen, seinen Konsum zu reduzieren.
  - Die Kaufkraft wird reduziert.

GEWINNER DER INFLATION	VERLIERER DER INFLATION
DER STAAT Weil höhere Preise und Löhne die Steuereinnahmen erhöhen, während die Ausgaben viel weniger steigen.	**SPARER** Sie sehen, wie ihre Ersparnisse immer weniger wert sind ...
DIEJENIGEN, DIE SICH ETWAS LEIHEN KÖNNEN Dank der Inflation wird es für sie leichter sein, Geld zurückzuzahlen, während die Schulden fest bleiben.	**KREDITGEBER** Denn wenn sie ihr Geld zurückbekommen, können sie damit weniger kaufen.
	RENTNER + ARBEITER Denn die Renten und Löhne steigen in der Regel weniger stark als die Preise.

3.3 Überwachung

- Regierungen erlassen Gesetze, um Personen ausfindig zu machen und zu fassen, welche Geld waschen oder andere illegale Geschäfte machen.

  • Überwachung ist ein zweischneidiges Schwert.
  • Je mehr Betrug geschieht, desto wachsamer werden der Staat und die privaten Unternehmen:

    - Dank des technischen Fortschritts dringen sie in unsere Privatsphäre ein.
    - Sie überwachen unsere Bewegungen in sozialen und wirtschaftlichen Netzwerken.
    - Austausch personenbezogener Daten als Gegenleistung für die Inanspruchnahme bestimmter Dienstleistungen.

- Einige der Konsequenzen sind:

  • digitaler Betrug, Online-Mobbing, Erpressung, Identitätsdiebstahl und andere Probleme, die die Privatsphäre und Sicherheit der Nutzer gefährden.
  • Unsere Kreditkartenkäufe werden erfaßt, analysiert und überwacht.

    - Es sei denn, wir bezahlen Waren und Dienstleistungen in bar.

  • Wenn jemand dein Internet-Banking-Passwort in Erfahrung bringt oder sich in die zentralen Server hackt, hat er Zugang zu all deinen Daten.

https://m.youtube.com/watch?v=-sWgOuFIaws

Wir brauchen Geld, das unsere Privatsphäre schützt und nicht alle unsere persönlichen Daten an Regierungen und private Unternehmen weitergibt.

3.4 Einschränkungen

- Es ist schwierig und kostspielig, Geld zwischen Staaten zu bewegen.

- Regierungen kontrollieren den Währungstausch, selbst wenn er zwischen zwei bekannten Personen stattfindet.

Hier findest du eine Liste von Maßnahmen und Möglichkeiten, wie dies geschehen kann:

Die Auswirkungen von Fiat-Geld und Zentralisierung

Politik der Regierung

- ***Kapitalverkehrskontrolle:*** Der Geldbetrag, den die Bürger ins Ausland überweisen, umtauschen oder mitnehmen können, ist beschränkt.
    - Beispiele:
        - *Argentinien, Russland, Indonesien, Kuba, China*
        - *Der durchschnittliche chinesische Einwohner kann nur bis zu 50.000 Renminbi (~8.000 USD) pro Jahr umtauschen.*

„Die einzige Lösung, die wir in Kuba gefunden haben, ist Bitcoin. Wir haben jetzt die gleichen Voraussetzungen, die gleichen Möglichkeiten, mit jedem anderen Land zu konkurrieren, denn wir haben vollen, freien, Zugang ohne Sanktionen oder Verbote zu jener Technologie, die es uns ermöglicht, etwas zu schaffen, zu wachsen und Verbindungen herzustellen."

- **Eric García Cruz**, kubanischer Unternehmer und Bitcoin-Enthusiast.

Bankenpolitik

- Die Banken haben Obergrenzen für den Bargeldbetrag, der von einem Konto abgehoben werden kann, oder einen Höchstbetrag, der überwiesen werden kann.

- Die meisten dieser Transaktionen sind mit Provisionen verbunden.
    - Beispiele:
        - *In Griechenland konnten die Bürger nach der Krise im Jahr 2015 nur 60 € pro Tag abheben.*
            - Dies ist eine deutliche Erinnerung daran, wer dein Geld wirklich kontrolliert.
        - *In El Salvador machen Provisionen für Geldsendungen 23 % des Bruttoinlandsprodukts (BIP) aus.*
            - Im Jahr 2020 waren es fast 6 Milliarden Dollar. Etwa 60 % kamen von Überweisungsdienstleistern und 38 % von Bankinstituten.
            - Unternehmen wie Western Union haben sehr hohe Gebühren.
            - Vor allem für Beträge unter 1.000 USD.

Provisionen oder Gebühren

- Diese Gebühren bereichern nur die Bankinstitute.
- Sie vergrößern auch die Kluft zwischen Arm und Reich.
    - Für kleine Beträge, z. B. 10 Dollar, kann die Provision mehr als drei Dollar, oder 33%, betragen.
    - Für 100 Dollar liegen die Sätze zwischen 12 und 15 %.

Zeitaufwand

- Beim Senden/Empfangen einer Überweisung:
    - müssen sowohl der Absender als auch der Empfänger sich zur nächstgelegenen Filiale begeben.
    - Natürlich muss dies während der Öffnungszeiten geschehen.

Sicherheit

- Das Aufsuchen von Western-Union-Büros birgt zusätzliche Risiken:
    - Die Menschen müssen ihr Bargeld persönlich vorbeibringen, was das Risiko eines Raubüberfalls erhöht.
    - Wenn die zentralen Server ausfallen (was häufig vorkommt), kann jedem Kunden der Zugang zu seinen Geldern verweigert werden.

3.5 Zentralisierung versus Dezentralisierung

- Die Zentralisierung der modernen Volkswirtschaften führt zu:
  - Zensur, Machtmissbrauch, Korruption, Chancenungleichheit, ungleiche Verteilung des Wohlstands und einzelne Ausfallquellen.
- Die Banken arbeiten mit zentralen Servern.
  - Sie haben Zugang zu allen finanziellen Aktivitäten ihrer Nutzer.

Was wissen Banken über ihre Kunden?

- Wieviel sie verdienen.
- Wofür sie ihr Geld ausgeben.
- An wen sie Geld senden.
- Alles, was mit ihrem Konto zu tun hat.

Eigenschaften eines zentralisierten Systems

- Die Kunden müssen darauf vertrauen, dass die zentralisierte Organisation ihre Daten sicher aufbewahrt.
- Es hat die vollständige Kontrolle über das System und die Kundendaten.
- Wenn die Hauptserver kompromittiert werden, sind ihre Daten in Gefahr.

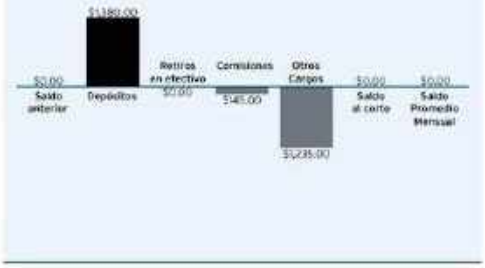
Die digitalen Währungen der Zentralbanken (CBDCs) sind eine Fortführung des derzeitigen Systems, allerdings in digitaler Form. Das heißt: veränderbar, zensierbar, geschlossen, zentralisiert, ausgrenzend und überwacht.

Carlos Pérez Pérez.
Av. Independencia # 543 interior 2.
Col central C.P 34004

BANK

Contrato:	25687451
Sucursal	1
Cuenta:	123321
Clave Interbancaria:	00000123321
Cliente:	963258
RFC:	PEPC920212R47

Comportamiento

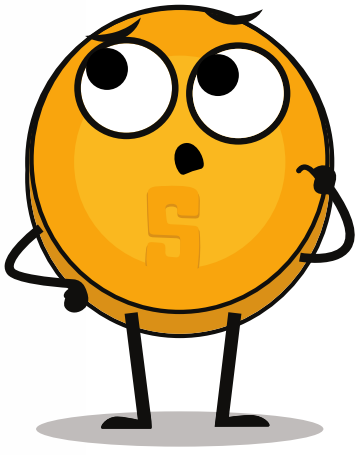


Resumen En Pesos Moneda Nacional

Saldo anterior	0.00
Depósitos	1,380.00
Retiros en efectivo	0.00
Otros cargos	1,235.00
Saldo al corte	0.00
Saldo promedio mensual	0.00

Detalle de Operaciones En pesos Moneda Nacional

FECHA	CONCEPTO	RETIROS	DEPÓSITOS	SALDO
25 DIC	SALDO ANTERIOR			0.00
11 ENE	PAGO RECIBIDO DE BBVA BANCOMER			
	POR ORDEN DE: MAURICIO DEL			
	MORAL DURAN REF.0000001			
	ARTICULOS RASTREO:			
	BNET01001601110002067854		1,380.00	1,380.00
11 ENE	IVA POR COMISION MANEJO DE			
	CUENTA	23.20		1,356.80
11 ENE	COMISION PENDIENTE MANEJO DE			
	CUENTA 8110401166	145.00		1,211.80
11 ENE	COBRO DE 600501077330			
	MAS9106148R6 Domi Asistencia			
	Familiar 10	89.00		1,122.80
11 ENE	RETIRO POR TRASPASO	1,122.80		0.00
22 ENE	COMISION MANEJO DE CUENTA			
	PENDIENTE POR: 145.00 MAS			
	I.V.A.			0.00



Die Auswirkungen von Fiat-Geld und Zentralisierung

Wie können wir diesen Phänomenen, die durch schlechte Politik verursacht werden, entgegenwirken?

Eigenschaften eines dezentralen Systems

Es wird als ***Peer-to-Peer-*** oder ***P2P-***System bezeichnet, da:

- die Menschen sich nicht ausweisen müssen, um über das Internet miteinander zu interagieren und in Verbindung zu treten.
- jeder für sein eigenes Gerät verantwort-lich ist, hat aber einen Anreiz seine Ressourcen zur Verfügung zu stellen und zu teilen.
- bei einem Angriff auf das Netz die Hacker die Kontrolle über die Mehrheit der Computer haben müssten, was nahezu unmöglich ist.
- im Falle eines Fehlers auf einem Server die anderen nicht betroffen wären.
- es zu einer gerechteren Gesellschaft führt, indem den mächtigen Konzernen die Kontrolle entzogen wird.

3.6 Fazit

Nochmals die Frage: Wird es eine Lösung für die heutigen Geldprobleme geben?

DAS **WAR GELD**

Gedeckt durch Gold und Silber.

DAS **IST PAPIER**

Gedeckt durch „den guten Glauben und Kredit der Regierung."

DAS IST DIE ZUKUNFT

Gedeckt durch die Bürger der Welt, durch den Einsatz von Technologie.

Lektion 4

Bitcoin

4.1 Warum wurde Bitcoin geschaffen?
- Welche Probleme müssen gelöst werden?
- Wie wurden diese Probleme gelöst?
- Wer hat diese Probleme gelöst?
- Welche Schwierigkeiten hatte Satoshi?
- Was ist das Problem der byzantinischen Generäle?
- Was hat das mit Bitcoin zu tun?

4.2 Einführung in Bitcoin

4.3 Unterschiede zwischen Bitcoin und Fiat

4.4 Die Teilnehmer von Bitcoin

4.1 Warum wurde Bitcoin geschaffen?

Der Anschlag auf die Twin Towers in New York im Jahr 2001 war ein schwerer Schlag für die Weltwirtschaft. Folglich begannen die USA mit der Unterstützung des Privatsektors und verfolgten das Ziel, die Hypothekenfinanzierung für Menschen mit geringem Einkommen zu erleichtern, indem sie die Zinssätze rasch auf ein noch nie dagewesenes Niveau senkten.

So wurden Darlehen und Kredite an Menschen ohne Einkommen, Vermögen oder Beschäftigung vergeben. Diese Art von Hypotheken wurden „Subprime-Hypotheken" genannt und hatten natürlich eine hohe Ausfallwahrscheinlichkeit. Die Auswirkungen der Krise sind heute noch spürbar. Der Höhepunkt wurde am 15. September 2008 erreicht, als die Investment-Bank Lehman Brothers Konkurs anmeldete. Von diesem Zeitpunkt an erlitten die Vereinigten Staaten einen wirtschaftlichen Zusammenbruch, gefolgt vom Rest der entwickelten Welt. Folglich wuchs Tag für Tag das Misstrauen gegenüber Banken aufgrund ihrer übermäßigen Risikobereitschaft und der nicht ausreichenden Regulierung der Branche.

Welche Probleme müssen gelöst werden?

- Mangel an individueller Souveränität
- Zentralisierung der Banken
- Inflation
- Überwachung
- Notwendigkeit von Zwischenhändlern
- schwacher Zugang zu Bankdienstleistungen
- hohe Kosten für internationale Überweisungen
- und mehr...

Wie wurden diese Probleme gelöst?

- Mit dem Einsatz der im Jahr 1991 entwickelten Technologie der ***Blockchain***.

Die ***Blockchain*** ist ein zentraler Bestandteil der Technologie hinter **Bitcoin**, der bekanntesten digitalen Währung. Die Blockchain ist eine dezentralisierte Online-Datenbank, die als Kassenbuch fungiert. Es handelt sich um ein dezentrales *Peer-to-Peer*-Zahlungsnetzwerk. Es nutzt kryptographische Schlüssel und wird über viele Computer verteilt und gemeinsam genutzt, wodurch das Risiko von Betrug und Fälschung verringert wird.

Wer hat diese Probleme gelöst?

- ***Satoshi Nakamoto*** tauchte im Oktober 2008 auf. Seine wahre Identität ist immer noch verborgen.

- Er stellte seine Idee eines neuen elektronischen Geldsystems vor. Dieses Geld sollte ***Bitcoin*** genannt werden.

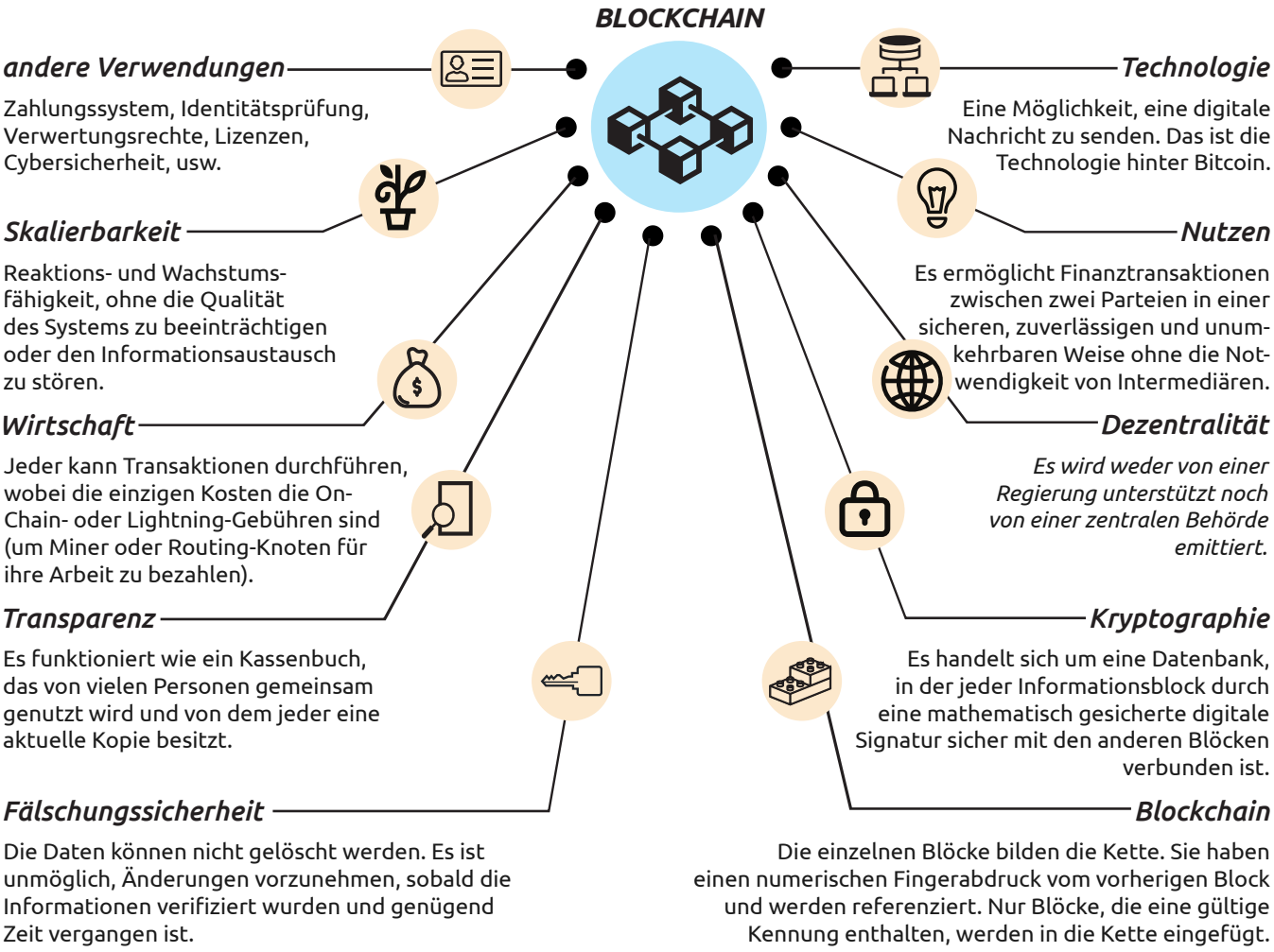
- Er widmete seine Zeit der Erstellung eines Leitfadens zur Erläuterung eines neuen Zahlungsmittels, das:

  • den schnellen und kostengünstigen Transfer von Werten ermöglicht.
  • nicht durch Regierungen oder Finanzinstitute kontrolliert oder manipuliert werden kann.

- Dank dieser Person oder Gruppe (das ist unklar) existiert eine Lösung für das Problem der ***„Doppelausgaben"***.

• Nun ist es nicht mehr möglich, dass jemand bereits ausgegebenes virtuelles Geld erneut ausgeben kann.

- Sein neunseitiges Dokument ist als ***Whitepaper*** bekannt.



• Satoshi teilte seine Idee in einer E-Mail-Liste der *Cypherpunks:*

- eine Gruppe, die sehr aktiv über Technik diskutierte.
- Die Diskussionen umfassen Mathematik, Kryptographie, Informatik, Politik und Philosophie und sogar persönliche Gründe.

● Satoshi war zynisch gegenüber dem traditionellen Geld- und Bankensystem.

• Dies ist im ***Genesis-Block*** zu sehen, in dem er folgende Nachricht hinterließ:

Hier kannst du das Whitepaper von Satoshi Nakamoto runterladen.

https://bitcoin.org/files/bitcoin-paper/bitcoin_de.pdf

Bitcoin

„The Times, 03.01.2009: Der britische Finanzminister steht kurz vor einem zweiten Rettungspaket für Banken."

- Satoshi Nakamoto, Genesis-Block.

- Er bezieht sich auf einen Artikel der Zeitung *The Times* mit dem Titel *„Chancellor on brink of second bank bailout"*.

  • Der britische Schatzkanzler stand vor der Entscheidung, ob er Milliarden britische Pfund in die Wirtschaft pumpen sollte, um die Banken zu retten.

- Hier sind einige weitere grundlegende Fakten, die wir über Satoshi, sein ***Whitepaper*** und die Entstehung von **Bitcoin** wissen:

1. Das Whitepaper umfasst nur 9 Seiten.

2. Es beschreibt ein „elektronisches Geldsystem" ohne Intermediäre.

3. Das Wort Blockchain wird dort nicht erwähnt, sondern „chain of timestamps".

4. Eine digitale Währung wird als eine Kette digitaler Signaturen definiert.

5. Der Begriff „Mining" wird als Analogie benutzt, um den „Arbeitsnachweis" oder Proof-of-Work zu verdeutlichen.

6. Die On-Chain-Transaktionen sind nicht auf Schnelligkeit, sondern auf Sicherheit angelegt.

7. Die Zunahme der Größe der Blockchain wurde auf 4,2 MB/Jahr geschätzt.

- Die erste *Bitcoin*-Transaktion wurde von Nakamoto an einen *Cypherpunk* namens Hal Finney gesendet.

- Bei seinem letzten bekannten „Lebenszeichen" hat Satoshi das Projekt an den Softwareentwickler Gavin Andersen weitergegeben:

  „ ... Ich habe mich anderen Dingen zugewandt, ... es ist bei Gavin und den anderen in guten Händen."

- In öffentlichen und sogar in privaten Nachrichten, die später veröffentlicht wurden, sprach Nakamoto nie über etwas Persönliches. Es ging nur um **Bitcoin** und den ***Code***.

- Viele Leute haben behauptet, Satoshi zu sein, aber wir wissen immer nocht nicht, wer er ist.

- Es wird geschätzt, dass Satoshi etwa 980.000 *Bitcoin* besitzt.

Welche Schwierigkeiten hatte Satoshi?

- Kann jemand dieselben Geldeinheiten an zwei Personen gleichzeitig schicken?

- Kann man im Internet jemand anderem vertrauen?

- Woher weiß man, ob jemand genug Geld auf seinem Konto (oder in seiner Wallet) hat, um ein Produkt von einem anderen zu kaufen?

- Wie wird sichergestellt, dass in einem dezentralisierten Netzwerk korrekte Entscheidungen getroffen werden, selbst wenn einige der Nodes (verbundene Netzwerkteilnehmer) unehrlich sind?

- Kann man ein verteiltes und zuverlässiges System schaffen, in dem man nicht automatisch davon ausgeht, dass die Teilnehmer ethisch handeln und im Interesse der Gruppe arbeiten?

- Woher weiß man, dass die Person, die über dieses System Geld erhalten möchte, auch die Person ist, die sie vorgibt, zu sein?

„Problem der Doppelausgabe = Problem der byzantinischen Generäle“

Was ist das Problem der byzantinischen Generäle?

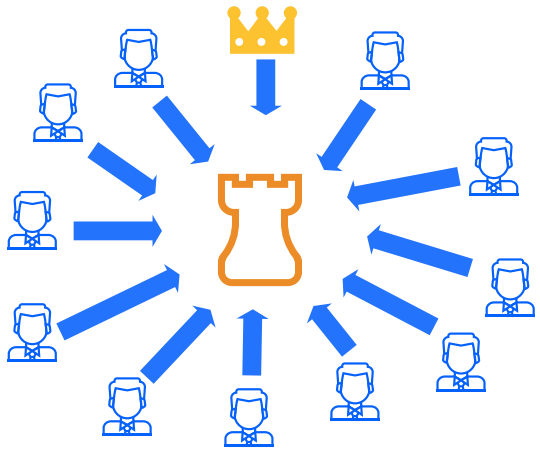
- Das Problem der byzantinischen Generäle ist eine Metapher für die Schwierigkeiten bei der Übermittlung zuverlässiger Informationen ohne das Eingreifen eines vertrauenswürdigen zentralen Koordinators.

Worin besteht die Allegorie?

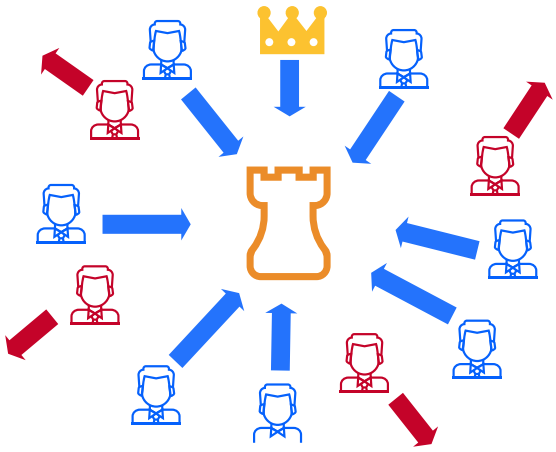
- Es gab eine Burg in Persien, die sehr gut versorgt und befestigt ist.
- Die byzantinischen Generäle haben die Burg umstellt und planen einen Angriff.
- Da die Streitkräfte so weit verstreut sind, gibt es keine zentrale Steuerung.
- Die Kommunikation zwischen den Generälen geschieht durch Boten.
- Die beiden möglichen Befehle sind „Angriff“ und „Rückzug“.
- Sie müssen sich alle darauf einigen, die persischen Streitkräfte gleichzeitig anzugreifen.
- Wenn einer von ihnen es separat versuchen sollte, würden sie die Schlacht verlieren.
- Wenn es einen Verräter gibt, könnte er die Einigung zwischen den Loyalisten verhindern.
    - Er könnte zum Beispiel einem General die Anweisung „Angriff“ und dem anderem die Anweisung „Rückzug“ geben.
- Eines Morgens erhält ein General folgende Nachricht: *„Der Angriff wird am Dienstag erfolgen.“* Sie wurde von keiner zentralen Instanz unterschrieben.

Wie kann sich der General sicher sein, dass es sich um einen echten Befehl handelt und nicht um eine Täuschung des Feindes, der Informationen übermittelt, die der Strategie der Streitkräfte widersprechen?

Was passiert, wenn der Absender der Nachricht ein Verräter ist und plant, die Streitkräfte zu hintergehen? Was passiert, wenn der General selbst korrupt ist und versucht, Zwietracht unter den anderen Generälen zu säen?



Ein koordinierter Angriff führt zum Sieg.



Ein unkoordinierter Angriff führt zur Niederlage.

Die Lösung für dieses Problem wurde ursprünglich als Methode zur Vermeidung von E-Mail-Spam eingesetzt.

Was hat das mit Bitcoin zu tun?

Das Problem der byzantinischen Generäle beschreibt folgendes:

- Die Schwierigkeit von dezentralen Systemen, sich auf eine einzige Wahrheit zu einigen.
- Es ist dasselbe wie die Überweisung von Geld ohne einen zuverlässigen Intermediär.
  - Dabei muss überprüft werden, dass die Nachricht nicht verändert wurde, was bis zum Aufkommen von Bitcoin mit seinem ***Konsensmechanismus*** nicht möglich war.
- Der Einsatz von Kryptographie ist in diesem Prozess unerlässlich, aber was ist ***Kryptographie***?
  - Es ist die Kunst, ***Nachrichten mit geheimen Schlüsseln*** so zu verschlüsseln, dass sie nur von der Person entschlüsselt werden können, an die sie gerichtet sind oder die den Schlüssel besitzt.
- *Bitcoin* verwendet auch einen Mechanismus des ***Arbeitsnachweises*** und eine ***Blockchain***, um das Problem der „Doppelausgabe" zu lösen.
- *Bitcoin* ermöglicht:
  - 1) die Übertragung eines digitalen Vermögenswerts (oder Geld) an einen anderen Nutzer über das Internet,
  - 2) in einer Weise, dass nur der Eigentümer den Vorgang auslösen,
  - 3) und nur der Empfänger den übertragenen Wert empfangen kann.
  - 4) Jeder kann die Überweisung validieren,
  - 5) und sie wird von allen Teilnehmern anerkannt.
  - 6) Außerdem ist sie unveränderlich, d. h. sie kann nicht rückgängig gemacht oder gelöscht werden.
  - 7) All dies geschieht auf vollständig ***verteilte*** und ***dezentralisierte*** Weise.
- Im Kontext der Blockchain ist jeder General ein ***Knotenpunkt (Full-Node) im Netzwerk.***
  - Die Full-Nodes müssen einen Konsens erreichen, um den aktuellen Status des gemeinsamen Buchführungsregisters zu bestimmen.
    - Wenn die Mehrheit des ***Netzwerks*** auf der ***Blockchain*** zustimmt, wird der Transaktionsverlauf der gesendeten und erhaltenen Zahlungen der Nutzer aktualisiert.
    - Ist der Großteil des Netzes böswillig, dann ist das System anfällig für Störungen.

4.2 Einführung in Bitcoin

https://www.youtube.com/watch?v=Oztd2Sja4k0

Was ist Bitcoin? Was ist Bitcoin?

- Es hat viele Anwendungen:

Geld: Es ist eine virtuelle und immaterielle Währung, die die drei Funktionen des traditionellen Geldes erfüllt: eine Recheneinheit, ein Wertaufbewahrungsmittel und ein Zahlungsmittel.

- **Software:** Es ist eine Software, die man auf jedem Computer runterladen und ausführen kann.

  - Ein ***Zahlungssystem*** ohne Zentralbank oder einer einzigen Behörde.

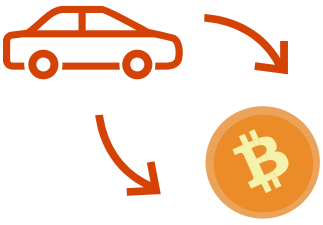
- **Netzwerk:** Es ist ein Konstrukt aus Menschen und Computern, die durch Konsens zusammenarbeiten, um nahtlos zu funktionieren.

Es ist eine Währung, wie andere auch.

Aber es ist digital.

Keine Kontrolle durch eine zentrale Behörde.

Es ist gegen Waren und Dienstleistungen eintauschbar.



Es ist transportabel und sicher.

Es kann in Tausenden von Geschäften verwendet werden und hat überall auf der Welt den gleichen Wert.

Was ist der Unterschied zwischen Bitcoin und Bitcoin in diesem Buch?

Bitcoin bezieht sich auf das Netzwerk von Computern, die mit dem selben Programm arbeiten, während ***Bitcoin*** für den digitalen Vermögenswert (€) steht, der innerhalb des Netzwerks verwaltet wird. Mit anderen Worten: ***Bitcoin*** ist eine kryptographisch verschlüsselte Einheit einer virtuellen Währung, die uns zum Austausch von Werten innerhalb des ***Bitcoin*** -Netzwerks dient.

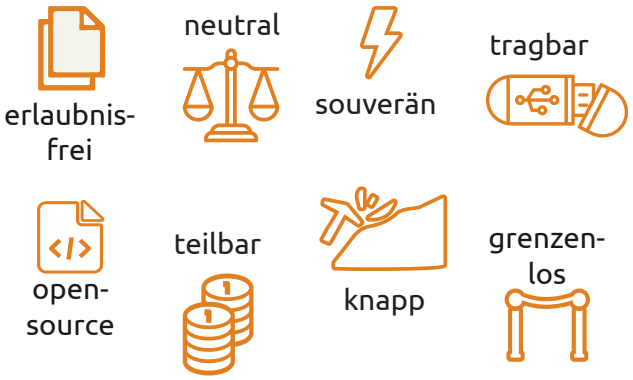
Was ist seine hauptsächliche Funktion?

- Es ermöglicht den direkten Zahlungsverkehr zwischen zwei Personen (P2P), ohne Intermediäre, kostengünstig und ohne internationale Schranken. Und es ist ein Wertspeicher.

Welchen technologischen Durchbruch hat es erzielt und warum wird es das Bankwesen revolutionieren?

- So wird verhindert, dass die Menschen das gleiche Geld zweimal ausgeben.
- Damit entfällt die Notwendigkeit einer zentralen Behörde zur Überwachung der Transaktionen.

Was macht es wertvoll?



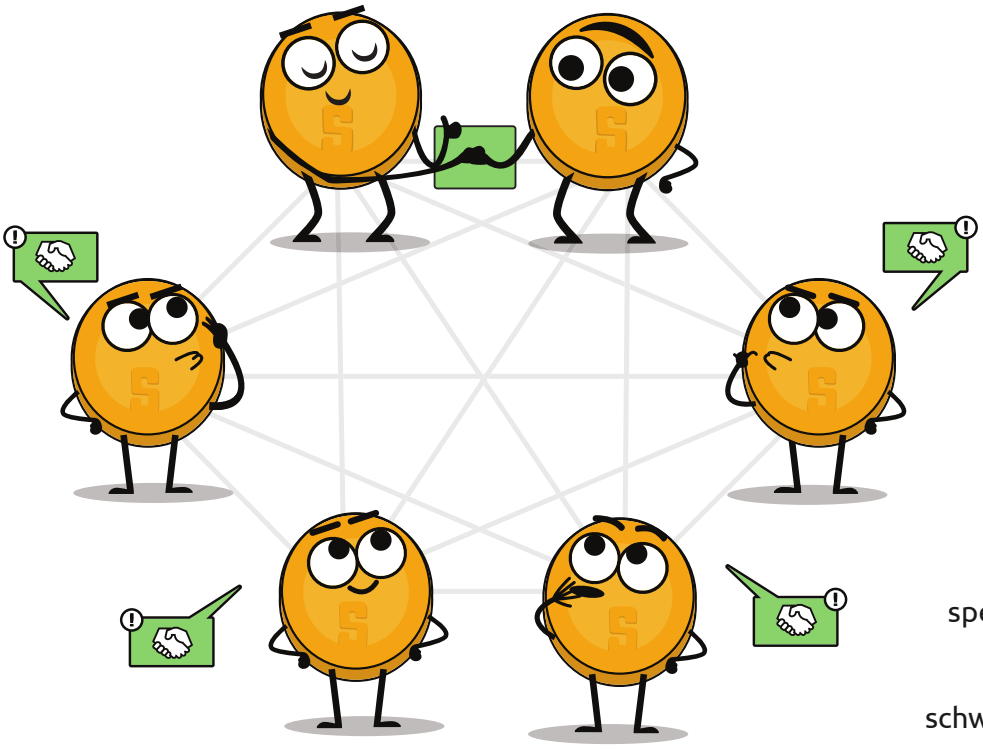
Bitcoin

Welche Beziehung besteht zwischen Blockchain und Bitcoin?

- Die Blockchain ist das öffentliche Kassenbuch, in dem alle On-Chain-Transaktionen des *Bitcoin*-Netzwerks dauerhaft aufgezeichnet werden.
- *Bitcoin* ist die einzige Blockchain, die mit der *Bitcoin* -Währung getätigte Transaktionen aufzeichnet.

Woraus bestehen die Bitcoin-Einheiten?

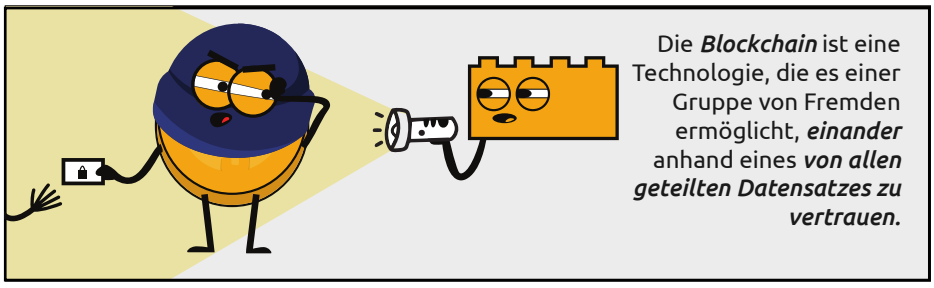
- Sie sind nicht so wie eine Banknote, die man physisch anfassen kann.
- Es handelt sich lediglich um eine Reihe von digitalen Zahlen und Buchstaben.
- Sie besitzen eine einzigartige Identität (so wie ein Fingerabdruck jemanden eine einzigartige Identität verleiht).



Die ***Blockchain*** ist ein sicherer Transaktionsdatensatz, da sie unter den Netzwerkteilnehmern verteilt ist.

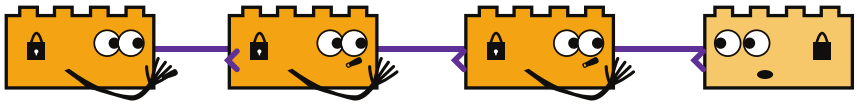
Jede Transaktion wird für alle dauerhaft aufgezeichnet, sodass keine Bewegungen verborgen werden können.

Die Daten werden in verschlüsselten Blöcken gespeichert, die sequenziell miteinander verbunden bzw. „verkettet“ sind, sodass es schwierig ist, die Informationen ohne den Konsens des gesamten Netzes zu ändern.



Die ***Blockchain*** ist eine Technologie, die es einer Gruppe von Fremden ermöglicht, ***einander*** anhand eines ***von allen geteilten Datensatzes zu vertrauen.***

Durch die Eigenschaften könnte diese Technologie die Transparenz von Prozessen wie öffentliche Staatsausgaben und sogar Wahlen erhöhen.



Ist Bitcoin anonym?

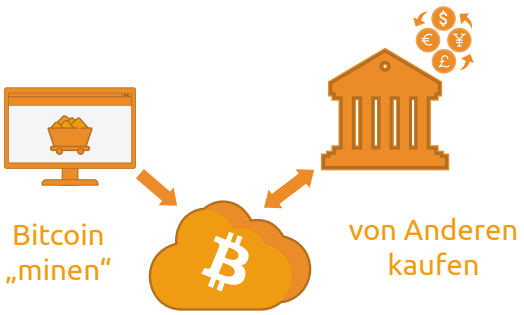
- Nein, es ist ***pseudonym***. Die Transaktionen sind für jeden sichtbar, zugänglich und transparent.
- Personen werden nicht durch Vor- und Nachnamen identifiziert, sondern durch eine Reihe von Buchstaben und Zahlen.

Wer kann Bitcoin nutzen?

- Im Gegensatz zum traditionellen Bankensystem kann jeder, der Zugang zum Internet hat, ***Bitcoin*** nutzen.

Wie kann man Bitcoin bekommen?

- Man kann sie online auf Tauschplattformen oder ***Börsen kaufen***.
- Durch einen Arbeitsprozess namens ***Mining werden neue Bitcoin emittiert.***



Was sind die Zugangsbarrieren zu Bitcoin?

- Für Bitcoin-Transaktionen braucht man einen Internetzugang.
- Einige Ländern verbieten den Zugang, aber es ist unmöglich, den Austausch zu verbieten.

Wo werden Bitcoin aufbewahrt?

- Sie verlassen nie die Blockchain. Das Zugangsrecht zu Bitcoin kann man auf einer Wallet, auf die man mit einem privaten Schlüssel zugreift, sichern oder erhält es über eine Börse.

Wie kann eine Währung, die in der physischen Welt nicht existiert und die durch nichts und niemanden gestützt wird, einen Wert haben?

- Der Wert wird durch *das Vertrauen der Nutzer*, *die Seltenheit*, *den Nutzen*, *die Nachfrage* und anderen Faktoren erzeugt.

Ist Bitcoin sicher?

- Ziel des Minings ist es, böswillige Akteure zu entmutigen und unerwünschte Verhaltensweisen wie Doppelausgaben und Spam zu verhindern.
- Kryptographie schützt Informationen auf sehr sichere Weise. Sie verwendet:

• **öffentliche Schlüssel** (ähnlich wie eine Bankkontonummer, aber für jede Transaktion einzigartig).

• **private Schlüssel** (ähnlich wie eine geheime PIN, die zu diesem Bankkonto gehört).

Von wem und wie wird gewährleistet, dass die Transaktionen fehlerfrei ausgeführt werden?

- Durch die Miner und das Mining.
- Das Ziel besteht darin, böswillige Akteure zu entmutigen und unerwünschtes Verhalten zu erschweren.

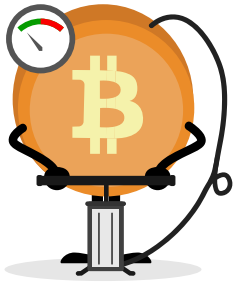
Was sind einige der Vorteile von Bitcoin gegenüber Fiat-Geld?

- Der Wert von Bitcoin ist in allen Ländern der Welt gleich.
- Es gibt keine Grenzen.
- Seine Inflation wird kontrolliert und seine Emission ist vordefiniert.
- Die Regierungen haben keine Entscheidungsbefugnis über die Verwaltung des Systems.

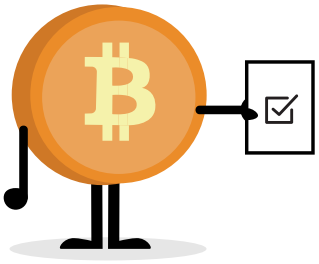
4.3 Unterschiede zwischen Bitcoin und Fiat

	Bitcoin	Fiat
Greifbarkeit	Es ist eine virtuelle Währung und kann nur in digitaler Form verwendet werden.	Es kann sowohl physisch (Münzen und Scheine) als auch digital (d. h. Überweisungen, Zahlungsdienstleister) verwendet werden.
Regulierung	Es wird durch Mining emittiert und von einem verteilten und dezentralen System von Computern kontrolliert.	Es wird von einer Zentralregierung und/oder einer Zentralbank geschaffen und kontrolliert. Es ist das gesetzliche Zahlungsmittel in dem Land, dessen Regierung seine Schaffung genehmigt hat.
Verwaltung	Ein freiwilliger Konsensmechanismus, der ein hohes Maß an Zustimmung erfordert.	Es wird von der Zentralregierung verwaltet.
Wert	Unterstützt durch das Vertrauen der Nutzer. Je mehr Nutzer, desto stabiler wird der Wert sein.	Bestimmt durch Angebot und Nachfrage und anfällig für Inflation.
Angebot	Begrenzt auf 21 Millionen.	Es gibt keine Obergrenze.
Validierung der Transaktionen	Durch Kryptographie und den Einsatz der Blockchain-Technologie.	Über eine Bank oder einen Intermediär.
Kosten der Transaktion	Minimal.	Signifikant, denn es gibt mehrere Intermediäre.
Zeit und Schnelligkeit der Transaktion	Im Durchschnitt 10 Minuten (bei Bitcoin On-Chain), und sofort (über das Lightning-Netzwerk).	Sofort (in bar), Tage oder sogar Monate (Banktransaktionen).
Sicherheit	Kryptographie (Zweig der Mathematik). Verhindert einen 51%-Angriff auf die Nodes.	Interne Sicherheit der Banken, die durch unterschiedliche Regierungspolitik negativ beeinflusst werden kann.
Änderungen	Bitcoin-Transaktionen können nicht rückgängig gemacht, geändert oder storniert werden.	Es ist üblich, dass es bei Transaktionen zu Streitigkeiten, Änderungen oder Rückbuchungen kommt.

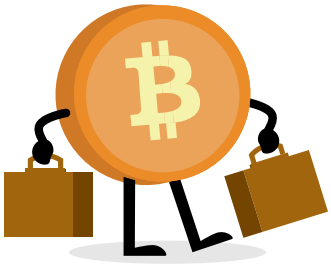
Bitcoin versus Fiat



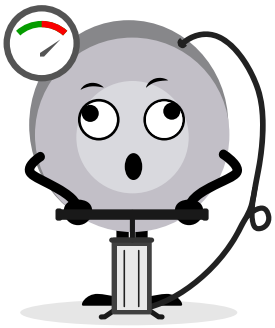
Kontrollierte, abnehmende Inflation, vorhersehbare und im Voraus festgelegte Umlaufmenge.



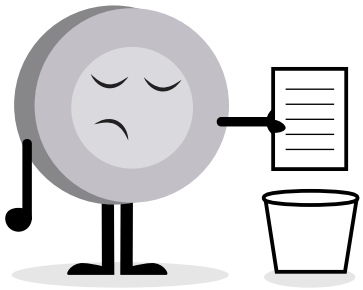
Änderungen können nur übernommen werden, wenn ein Quorum von Full-Nodes sie akzeptieren.



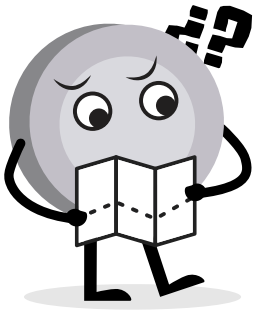
Es gibt keine Grenzen, es kann von jeder Person auf der Welt akzeptiert werden.



Die Inflation kann unbegrenzt steigen. Das Drucken beliebig vieler zusätzlicher Geldscheine führt zur Abwertung des Geldes.



Änderungen geschehen nach dem Belieben der Verantwortlichen und ohne die Bürger zu konsultieren.



Es wird nur innerhalb des Ausstellungslandes akzeptiert und kann meistens nicht außerhalb des Landes verwendet werden.

Praktische Übung: Beende die Übung von Lektion 1 auf Seite 16! Mache ein Kreuz in der Spalte „Bitcoin“, wenn das angegebene Merkmal erfüllt wird!
Welchen Gegenstand würdest du als Geld wählen?

4.4 Die Teilnehmer von Bitcoin

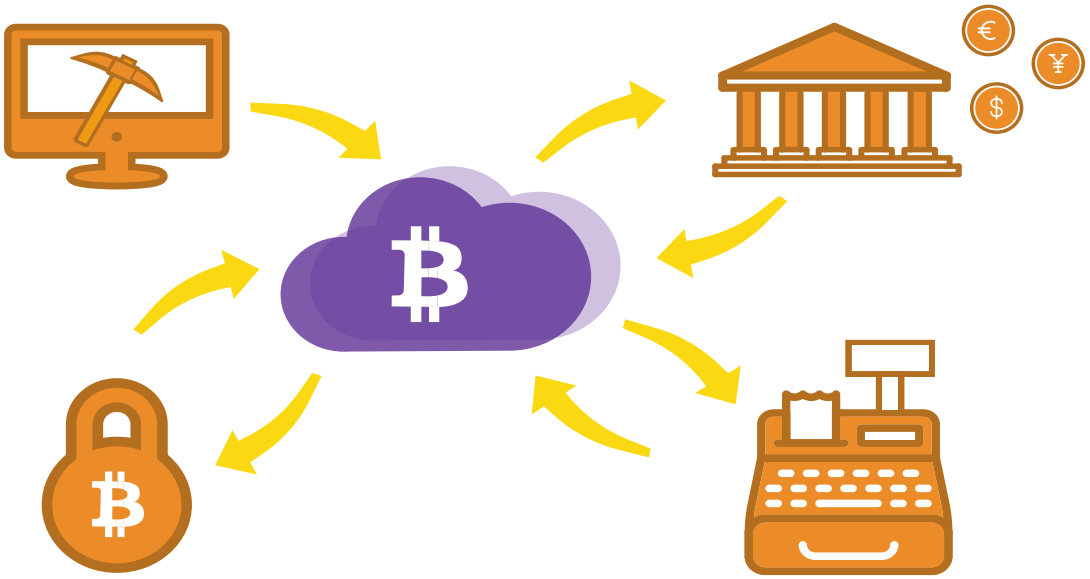
Um zu verstehen, wie jemand oder ein System am Bitcoin-Netzwerk teilnimmt, müssen wir uns die folgenden Fragen stellen:

- *Kann diese Person oder dieser Computer nur die Transaktionen sehen, an denen sie bzw. er beteiligt ist?*
- *Hat man Zugriff auf weitere Informationen?*
- *Welche Transaktionen kann man durchführen?*
- *Welche Berechtigungen hat man für das Netzwerk?*
- *Wie interagiert man mit dem Netzwerk?*
- *Hat man Zugriff auf eine Kopie der gesamten Blockchain?*

- **1. Miner:** Spezialisierte Computerausrüstung.
  - Sie konkurrieren beim Berechnen mathematischer Funktionen miteinander, um neue *Bitcoin* zu emittieren.
  - Sie bestätigen Transaktionen und gewährleisten die Sicherheit des Netzes.
    - Ähnlich wie Angestellte in einer Bank werden sie für ihre Arbeit bezahlt.
- **2. Börsen oder Tauschportale:** Sie tauschen Fiat-Währungen gegen *Bitcoin* und andere *Kryptowährungen*.
  - Sie bieten denjenigen, die keine Miner sind, eine Möglichkeit, in den Markt ein- und auszusteigen.
  - Ähnlich wie Banken bieten sie den Nutzern Dienstleistungen an.
- **3. Wallets:** Anwendungen, die zum Speichern, Senden und Empfangen von *Bitcoin* auf den On-Chain-Adressen verwendet werden.
  - Dies ist vergleichbar mit Bankkonten oder Apps, die für Online-Überweisungen verwendet werden.
- **4. Nodes:** An ein digitales Netzwerk angeschlossene Geräte, die BTC-Transaktionen validieren, übertragen, verarbeiten und speichern (ne-ben der Funktion als Wallets haben sie noch viele weitere Funktionen).
  - Sie bestehen aus zwei Komponenten: Hardware und Software.
    - So ähnlich wie bei einem Mobiltelefon und einer App.
    - Die Hardware ist das physische Material, das zur Ausführung der Software erforderlich ist.
- **5. Entwickler:** Sie pflegen den Code und schlagen Verbesserungen vor.

Die **Miner** erhalten neu emittierte *Bitcoin* mit Hilfe von Computern, die mathematische Funktionen lösen, und überprüfen in diesem Prozess auch frühere Transaktionen.

Die **Börsen** tauschen die konventionellen Währungen gegen *Bitcoin* um und bieten den Nicht-Minern eine Möglichkeit, in den Markt einzusteigen und Geld auszuzahlen.



Die Nutzer laden eine **Wallet** herunter, die wie eine E-Mail-Adresse funktioniert und eine Möglichkeit bietet, Verwaltungsrechte über Währungen zu speichern und zu empfangen. Rechte über *Bitcoin* können über einen Web-Browser oder eine Smartphone-App von einer Wallet zur anderen übertragen werden.

Die Unternehmen erstellen eine **Wallet** auf die gleiche Weise wie Privatpersonen, in der Regel über eine Schaltfläche auf der Website, um *Bitcoin*-Zahlungen zu ermöglichen. Für Unternehmen mit einem physischen Ladengeschäft können QR-Codes verwendet werden, damit Kunden schnell und einfach bezahlen können.

Lektion 5

Kauf, Verwahrung und Übertragung von Bitcoin

5.1 Ein- und Ausstiegsrampen
- Habe ich genug Geld, um Bitcoin zu kaufen?

5.2 Verwahrung von Bitcoin
- Arten von Wallets und das Lightning-Netzwerk
- Wie sende und empfange ich Satoshis?

5.3 Der Ablauf einer Transaktion (on-chain)
- Was ist eine Bitcoin-Transaktion?
- Schnittstellen und Hindernisse für Transaktionen
- Wie funktioniert eine Transaktion, Schritt für Schritt?
- UTXO – „Nichtausgegebene Geldeinheiten“
- Die Bestätigung einer Transaktion

Kauf, Verwahrung und Übertragung von Bitcoin

5.1 Ein- und Ausstiegsrampen

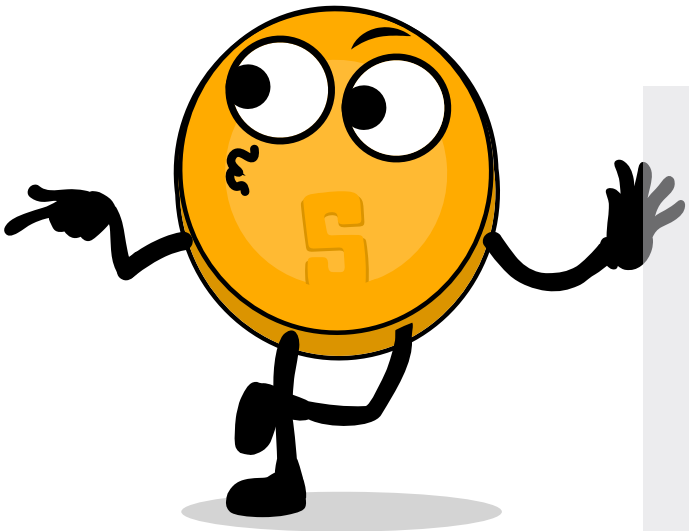
- Der erste Schritt, um *Bitcoin* zu erhalten, ist der Kauf. Es gibt mehrere Möglichkeiten:
  - *Wechselstuben, Makler, Bitcoin-Geldautomaten, Fintech-Unternehmen, Geschenkkarten usw.*
- Klassisches Geld (Euro, Dollar usw.) wird in seinen Gegenwert in *Bitcoin* umgetauscht.
- Die Dienste, die diese Funktionen bereitstellen, werden ***„Einstiegsrampen"*** genannt.
- Die Regierungen können die Ein- und Ausstiegsmöglichkeiten regeln.
  - Banken könnte es verboten werden, Geld an oder von *Bitcoin*-Börsen zu senden.
    - Dies könnte unsere Möglichkeit beeinträchtigen, *Bitcoin* zu kaufen oder zu verkaufen, aber es wäre unmöglich, *das Senden und Empfangen von Bitcoin zu verhindern.*

Habe ich genug Geld, um Bitcoin zu kaufen?

- **BTC** ist die übliche Einheit der *Bitcoin*-Währung.
- Das Symbol ₿ kann für *Bitcoin* verwendet werden, so wie **USD** oder **$** für den US-Dollar.
- *Bitcoin* hat zu jedem Zeitpunkt einen entsprechenden Wert gegenüber allen anderen Währungen der Welt.
  - Zum Beispiel: 1 ₿ = 21.464 US-Dollar oder 1 ₿= 95.288.229 COP (Kolumbianischer Peso)
- *Bitcoin* ist viel besser teilbar als der US-Dollar, 1 US-Dollar = 100 Cent. Es gibt keine 1/2-Cent oder 1/10-Cent eines US-Dollars.
- Ein *Satoshi* (oder kurz ***Sat***) ist die kleinste Einheit der *Bitcoin*-Währung.
  - 1 BTC = 100.000.000 sats
  - 1 sat ≈ 0,0003 US-Dollar
  - Das bedeutet, dass ein *Bitcoin* in hundert Millionen Einheiten unterteilt werden kann.
- ***Voreingenommenheit bzgl. der Einheit:***
  - Man muss nicht einen ganzen *Bitcoin* kaufen, sondern kann so viele ***Sats*** kaufen, wie man will.

„Wenn man ein wenig zu etwas Wenigem hinzufügt und es wiederholt, wird das Wenige bald viel sein."

- Hesíodo



Satoshi	Bitcoin
1	0,00000001
10	0,0000010
100	0,000100
1.000	0,00001000
10.000	0,0010000
100.000	0,010000
1.000.000	0,10000000
10.000.000	1,00000000
100.000.000	

5.2 Verwahrung von Bitcoin

Wie verwahrt man Bitcoin?

- **Wenn Sats** auf einer Website gekauft werden, werden sie höchstwahrscheinlich einer „Geld-börse“ (Wallet) gutgeschrieben.
    - Ähnlich wie eine Gutschrift auf einem Bankkonto, wenn Geld darauf überwiesen wird.
- Es mag den Anschein haben, dass die Person die *Bitcoin* besitzt, aber in Wirklichkeit ist das Geld im Besitz einer dritten Partei.
- Daher ist es wichtig, die Risiken einer Investition in *Bitcoin* zu verstehen und zu beginnen:
    - Kenntnisse über die besten Möglichkeiten zum Halten von *Bitcoin* auf dem Markt zu sammeln.
    - eine ***Wallet*** zu benutzen.
        - *Welche bietet die beste Sicherheit?*
        - *Wie findet man die für die eigenen Bedürfnisse am besten geeignete Lösung?*
    - die Vor- und Nachteile der ausgewählten Wallets zu analysieren.
        - *Man muss sich klarmachen, dass es keine ideale Wallet gibt, die alle Bedürfnisse erfüllt.*

Arten von Wallets und das Lightning-Netzwerk

Wer kontrolliert meine Bitcoin?

- **Selbstverwahrte Wallets**
    - *Vorteile:*
        - Dies ist die einzige Möglichkeit, um der absolute Eigentümer der gekauften *Bitcoin* zu werden.
        - Es ist nicht notwendig, um Erlaubnis zu fragen, um den Dienst zu nutzen.
        - Es braucht keine Genehmigung für ein Konto.
        - Jeder kann eine Wallet downloaden und sofort verwenden.
        - Das ist so, als würde man sein Geld zu Hause aufbewahren, anstatt es der Bank anzuvertrauen.
        - Die Selbstverwahrung von *Bitcoin* wird ausdrücklich empfohlen, um Diebstahl zu vermeiden.
        - Kein Unternehmen/keine Regierung hat die Kontrolle/Befugnis über Transaktionen.
        - Keine Drittpartei kann willkürlich *Bitcoin* beschlagnahmen, die sich in Selbstverwahrung befinden.
        - In Zeiten von Krisen können wir uns darauf verlassen, dass unsere *Bitcoin* sicher sind.
    - *Risiken:*
        - Es gibt keine Möglichkeit, Gelder wiederzuerlangen, wenn **private Schlüssel** verloren gehen.
        - Es gibt selten oder keinen Kundendienst.
        - Die Verantwortung wird nicht verteilt.
- **Fremdverwahrte Wallets**
    - Eine Drittpartei verwahrt die *Bitcoin*.
    - Die Gelder (die **privaten Schlüssel**) stehen unter der Kontrolle des Wallet-Anbieters.
    - *Vorteile:*
        - Wenn man den Zugang zum Konto verliert oder vergessen hat, kann man das Geld einfach zurückbekommen.
    - *Risiken:*
        - Sie sind ständig mit dem Internet verbunden, was sie angreifbarer macht.

Selbstverwahrung | **Fremdverwahrung**

Software | Hardware | (Drittpartei)

Kauf, Verwahrung und Übertragung von Bitcoin

Welche ist die bequemste Wallet?

- **Hardware-Wallet [Cold]**

  • *„Nicht angeschlossene"* Wallets benötigen, wie der Name schon sagt, kein Internet, um zu funktionieren.
  • Sie sind die sichersten Wallets.
  • Sie sind ideal für die Aufbewahrung großer Mengen an *Bitcoin*.
  • Die Schlüssel sind auf einem Speichermedium gesichert (z. B.: Coldcard MK3).
  • Der Verlust der Wallet ohne Backup führt zu Verlust des Geldes.

- **Papier-Wallets [Cold]**

  • **Private Schlüssel** werden zur Sicherung auf Papier notiert.
  • Eine der sichersten, aber extrem ineffizienten Möglichkeiten, *Bitcoin* zu speichern.
  • Bei jeder Transaktion muss ein neuer **privater Schlüssel** kopiert werden.

- **Software-Wallets [Hot]**

  • Sie sind mit dem Internet verbunden.
  • Sie können über eine mobile Anwendung oder über das Internet installiert und/oder abgerufen werden.

  - **Handy-Wallets**

  • Sie sind tragbar und bequem; ideal für Peer-to-Peer-Transaktionen.
  • App-Stores könnten sie ohne Vorankündigung entfernen.
  • Wenn das Gerät beschädigt wird oder verloren geht, kann es schwierig sein, das Geld wiederzuerlangen.

    - Ideal für die Verwendung mit QR-Codes.

  - **Desktop-Wallets**

  • Die Nutzer können die vollständige Kontrolle über die Geldmittel haben.
  • Einige bieten Unterstützung für Cold-Wallets.
  • Die Verwendung von QR-Codes bei Transaktionen ist schwierig.
  • Anfällig für Viren, mit denen *Bitcoin* gestohlen werden.

Bitcoin-Wallet-Architektur

Sicherheit	Benutzerfreundlichkeit: EINFACH	Benutzerfreundlichkeit: SCHWIERIG
HOCH	Cold-Wallets selbstverwahrt	Cold-Wallets fremdverwahrt
NIEDRIG	Hot-Wallets selbstverwahrt	Hot-Wallets fremdverwahrt

Wie sende und empfange ich Satoshis?

- **Auf der Blockchain (on-chain):**

  • Durch Wallets, die mit dem „Hauptnetzwerk" verbunden sind.
  • Dies ist ein sehr sicherer, aber zeitaufwändiger Weg – bis zu 10 Minuten, um die Transaktion zu bestätigen.
  • Die Gebühren für jede Transaktion sind proportional zu ihrer digitalen Größe, nicht zu ihrem Betrag.

    - Wenn man einen Wert von 1 US-Dollar on-chain versendet und 1 US-Dollar an Gebühren gezahlt wird, entspricht dies 100 %.
    - Wenn man 10.000 US-Dollar on-chain versendet und 1 US-Dollar an Gebühren zahlt, entspricht das 0,01 %.

- **Lightning-Netzwerk (off-chain):**

  • Es ist eine „Layer-2-Lösung“, die das Senden und Empfangen von *Bitcoin* ermöglicht.

  - Es ermöglicht nahezu Echtzeitüberweisungen mit äußerst geringen Gebühren.

  • Es wird in Ländern verwendet, in denen:

  - lokale Richtlinien und Bestimmungen die Masseneinführung von Bitcoin fördern.
  - eine schnelle, private, kostengünstige und effiziente Transaktionslösung benötigt wird.

5.3 Der Ablauf einer Transaktion (on-chain)

Was ist eine Bitcoin-Transaktion?

Das, was über das *Bitcoin*-Protokoll verschickt und gespeichert wird, sind *Bitcoin*, nicht Pesos oder Dollar.

- Dieser Geldtransfer wird als **Transaktion** bezeichnet.

- Ein Werttransfer zwischen zwei Wallets, der in der Blockchain (*Bitcoin*) aufgezeichnet wird.

Wenn eine neue Transaktion das Netzwerk erreicht:

- muss diese einen Verifizierungsprozess durchlaufen, um von den Nodes akzeptiert zu werden.

  • ***Gültige*** Transaktionen:

  - werden von einem Computer zum anderen übertragen, bis sie von allen kopiert wurden.
  - Ungefähr alle zehn Minuten werden Tausende von Transaktionen gebündelt.
  - Ein neuer Block wird durch einen Prozess namens ***Mining*** erstellt.
  - Neue Transaktionen werden für immer in dem Block gespeichert.
  - Es ist nicht möglich, sie zu ändern, zu löschen oder ihnen Informationen hinzuzufügen.

  • ***Ungültige*** Transaktionen:

  - Sie werden einfach zurückgewiesen und verbreiten sich nicht über das Netzwerk.

Schnittstellen und Hindernisse für Transaktionen und BTC-Speicher

Eine Transaktion über eine Wallet ähnelt dem folgenden Prozess:

- Stellen wir uns vor, dass alle existierenden *Bitcoin* in Bankschließfächern aufbewahrt werden.

  • Alle mit unterschiedlichen Mengen an BTC, aber völlig transparent.
  • Jeder kann sehen, wie viel Bitcoin sich in jedem Fach befindet und wie sie dorthin gekommen ist.

- Jedes Fach hat eine ***Adresse***, die nur einem Eigentümer gehört.

- Diese Adresse ist mit einem Sicherheitsschloss geschützt, für das zwei verschiedene Schlüssel erforderlich sind:

  • Einer der Schlüssel, der *private Schlüssel*, ***öffnet*** das Schloss und ***ermöglicht den Zugriff auf die darin befindlichen BTC.***
  • Der andere Schlüssel, der *öffentliche Schlüssel*, ***schließt*** das Schloss und ***schützt die BTC.***

- Jeder Teilnehmer des Netzes ***bewahrt*** seine *privaten Schlüssel* an sehr sicheren Orten auf.

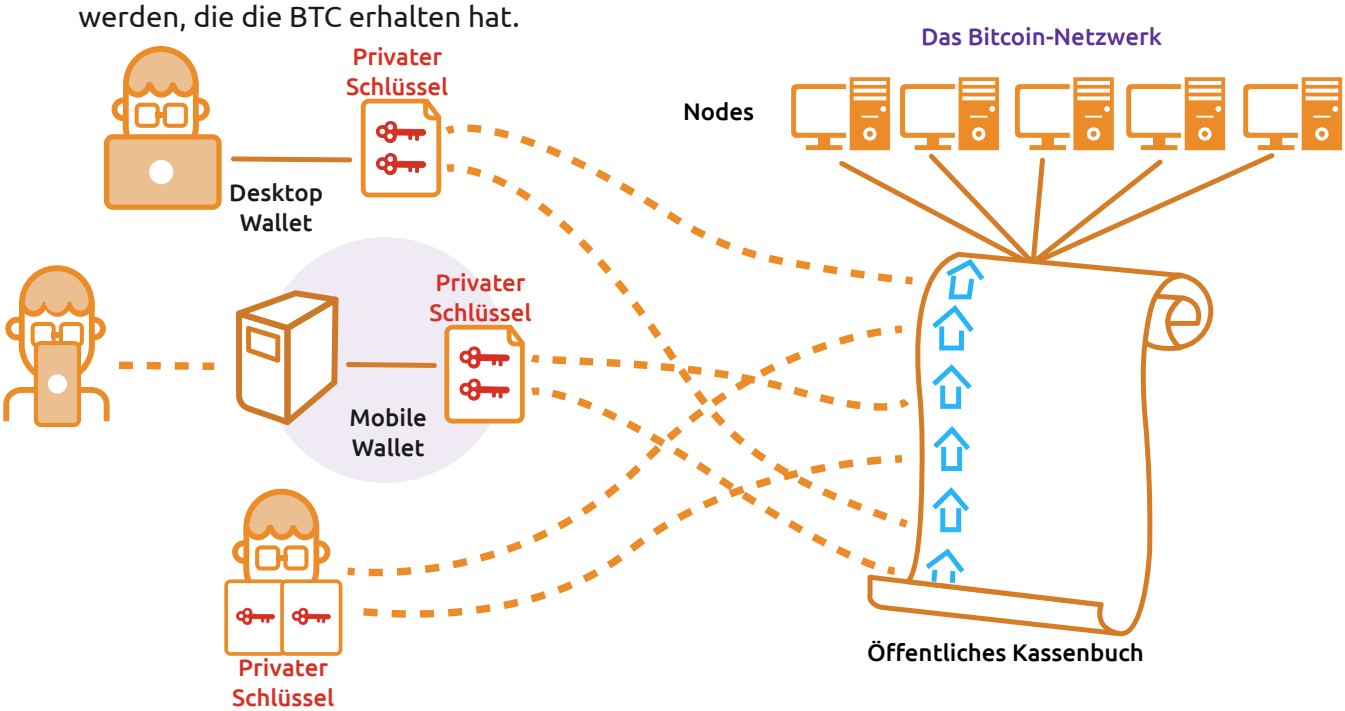
Kauf, Verwahrung und Übertragung von Bitcoin

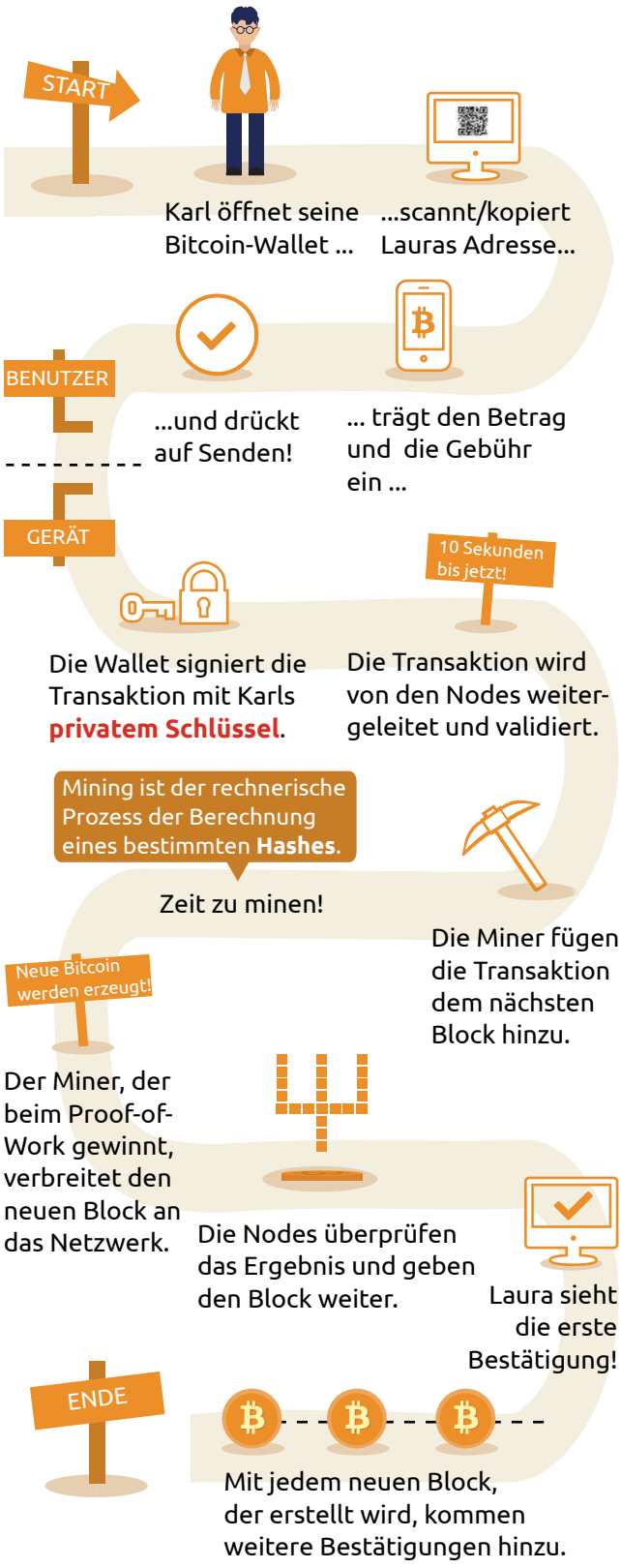
● Wenn ein Fach *Bitcoin* enthält, kann der Besitzer jederzeit sein Fach öffnen:

- und einen beliebigen Betrag in ein anderes Fach überweisen.
- Doch zunächst muss man berücksichtigen, dass es Tausende und Abertausende von Fächern gibt:
  - Man benötigt eine genaue Adresse, um sicherzustellen, dass die BTC in das richtige Fach eingezahlt werden.
- Zum Schluss muss das Schließfach mit dem **öffentlichen Schlüssel** des Fachs geschlossen werden.
  - Somit hat niemand außer der Empfänger Zugriff auf die *Bitcoin*.
- In Zukunft kann das Fach nur mit dem **privaten Schlüssel** der Person geöffnet werden, die die BTC erhalten hat.

Wie funktioniert eine Transaktion, Schritt für Schritt?

Ein erfolgreicher Geldtransfers in einem dezentralisierten Netzwerk wurde nur unter der Bedingung erreicht, dass jede Transaktion einzigartig und wiedererkennbar ist.





● Angenommen, Karl will 0,5 *Bitcoin* an seine Schwester Laura schicken. Beide haben Wallets.

• Es ist notwendig, eine Transaktion zu erstellen, die eine ***eindeutige und nicht wiederholbare Kennung*** trägt.

- Die Kennung ist der ***Fingerabdruck*** von jeder Transaktion.
- Damit soll verhindert werden, dass zwei Transaktionen als identisch erscheinen.
- Dies macht auch den Überprüfungsprozess einfach.

- Damit dies sicher, aber effizient geschehen kann, muss jede Transaktion verschlüsselt, entschlüsselt, signiert und verifiziert werden.

▫ **Verschlüsselung:** Karl muss die *Bitcoin* über einen sicheren Kanal senden, ohne dass sie von jemandem abgefangen werden können.

▫ **Entschlüsselung:** Laura muss das Geld empfangen und sicherstellen, dass niemand sonst darauf zugreifen und es verwenden kann.

▫ **Signieren:** Karl muss Laura beweisen, dass das Geld, das er geschickt hat, ursprünglich ihm gehörte und dass er den richtigen Betrag schickt.

▫ **Verifizierung:** Die Netzwerkbenutzer müssen verifizieren, ob Karl das Geld tatsächlich auf seinem Konto hatte, um es auszugeben, sie müssen es von seinem Gesamtkonto abziehen und es Lauras Konto hinzufügen.

Schauen wir mal, wie das geschieht:

● **1.** Karl öffnet seine Handy-Wallet und fragt Laura nach ihrer Adresse (dem **öffentlichen Schlüssel**).

● **2.** Laura teilt diesen (*als QR-Code, E-Mail, oder anderweitig*).

● **3.** Bei dieser Transaktion scannt Karl den QR-Code und verknüpft ihn mit dem Betrag, den er senden will.

• Er fügt eine kleine Gebühr als Anreiz für die ***Miner*** hinzu, seine Transaktion für den nächsten Block zu wählen.

● **4.** Mit einem Klick wird verifiziert ob Karl genügend Sats in der Wallet hat.

● **5.** Karls Wallet ***signiert*** die Transaktion mit seinem **privaten Schlüssel**.

• Seine *Bitcoin* werden für Laura verfügbar.

● ***6.*** Die Transaktion wird über das Netz an die ***Nodes*** weitergeleitet, die sie überprüfen und genehmigen.

• Nach der Verifizierung verbleibt sie in einem Wartebereich.

● **7.** Die ***Mining-Nodes*** wählen Tausende von Transaktionen aus und lehnen ungültige Transaktionen ab.

• Sie fügen sie zu neuen „potenziellen Blöcken" hinzu, die noch nicht akzeptiert wurden.
• Sie komprimieren alle Informationen und erstellen jeweils eine Block-Kennung.

● **8.** Beginn eines Wettbewerbs zwischen **Nodes** (ähnlich einer Tombola zwischen den Block-Kennungen),

• um zu sehen, wer als nächstes einen Block zur Blockchain hinzufügen darf.

● **9.** Der Gewinner-Block enthält die Karl-Laura-Transaktion und verteilt sie an die anderen Nodes.

● **10.** Die Nodes überprüfen die Kennung des erfolgreichen Blocks und fügen ihn der Blockchain hinzu.

• Alle Transaktionen des Blocks werden in der Blockchain ***bestätigt***.
• Sie können weder geändert noch gelöscht werden und sind für immer an dieser Stelle registriert.

● **11.** Laura wird die rechtmäßige Besitzerin dieser *Bitcoin*.

• Sie wird ihre 0,5 BTC in ca. 10 Minuten erhalten haben.
• Karl wird der Betrag von seiner ***Wallet*** abgezogen.

● ***12.*** Die Transaktion ist dann erfolgreich abgeschlossen.

UTXO – „Nichtausgegebene Geldeinheit"

Transaktionen sind ganz einfach **In- und Outputs** (Ein- und Ausgänge) von *Bitcoin* von einer Wallet zur anderen.

● Alle Bitcoin, die noch nicht ausgegeben wurden, werden als ***UTXO*** – *Unspent Transaction Output* – bezeichnet.

● Der ***aktuelle Stand*** der Blockchain ist die ***UTXO***-Datenbank.

● ***Inputs*** beziehen sich auf das Geld, das für das ***Erstellen einer Transaktion*** verwendet wird.

● Die ***Outputs*** zeigen im Allgemeinen zwei Punkte an, an die die ***Transaktion gerichtet*** ist:

• Ein Output geht an die Person, an die die Zahlung geleistet wird.

● Wenn ein Nutzer seine UTXO mit seinem **privaten Schlüssel** entsperrt, um ihn an einen anderen Nutzer zu senden,

• kann das Guthaben in Gefahr sein, weil das Schließfach geöffnet ist.
• Aus diesem Grund ist es immer ratsam, das Guthaben auf eine neue Wallet zu übertragen.

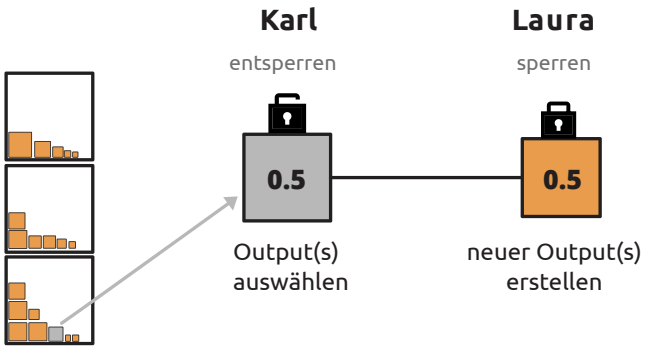
- Wenn die ursprüngliche *Wallet* ein Guthaben aufweist:
    - geht der andere Output an eine neue Adresse, die für den Empfang der Überweisungen eingerichtet wurde.
        - Dieser Betrages wird in einen neuen ***UTXO*** umgewandelt.
- Für die Nodes im Netzwerk ist es einfach, einen Konsens zu erreichen, da:
    - alle eine Kopie derselben Datenbank besitzen.
    - Sie können die Salden der einzelnen Adressen überprüfen.

Die Bestätigung einer Transaktion

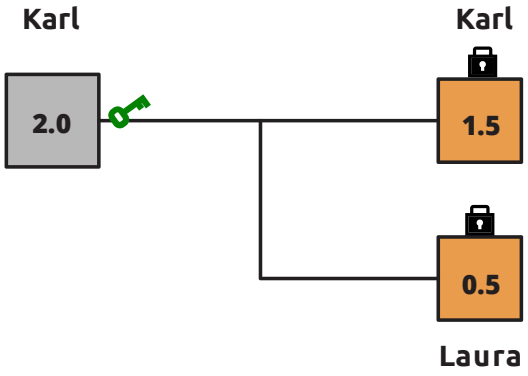
- Um einen beliebigen *Bitcoin*-***Output*** aus einer Wallet zu autorisieren und zu **versenden**:
    - muss die Transaktion mit dem **privaten Schlüssel** *signiert* werden.
    - Dieser Schritt ist notwendig, um nachzuweisen, dass man der Eigentümer des Geldes ist.
- Um einen **Betrag** in einer Wallet zu empfangen:
    - muss ein Benutzer seine ***Adresse*** dem Sender mitgeteilt haben.
- Die Transaktion ist ***BESTÄTIGT***, wenn:
    - **Bitcoin** die Menge an *Bitcoin* ***erfasst*** hat, die auf ***die neue Adresse*** eingezahlt wurde,
    - und den Betrag von der Wallet ***des Senders abgezogen*** hat.

Sehen wir uns an, wie eine Transaktion bestätigt wird:

- Die orangen Kästchen stehen für den UTXO.
- Die grauen Kästchen stellen Wallets dar, in denen sich keine *Bitcoin* mehr befinden (komplett leer).



- Der Node bestätigt, dass genügend *Bitcoin* auf der ursprünglichen Adresse sind (0,5 BTC in Karls Wallet), um die Transaktion durchzuführen.
- Wenn die Transaktion bestätigt wird, wurde ein bestimmter Betrag an *Bitcoin* an zwei verschiedene Adressen verteilt.
- In einigen Wallets befinden sich jetzt mehr *Bitcoin* (Lauras), in der ursprünglichen Wallet (Karls) dagegen weniger.



- Nachdem die Transaktion bestätig wurde, überwacht die Blockchain nur noch die Wallets, die das Geld erhalten haben: die 1,5-BTC-Wallet und die 0,5-BTC-Wallet.

- Dies ist nun der nicht ausgegebene *Bitcoin* oder ***UTXO***.

Lektion 6

Bitcoin als Wertspeicher und Zahlungsnetzwerk

6.1 Das Problem der Doppelausgaben
6.2 Der Wartebereich oder „Mempool“
6.3 Übung: Verifizierte, aber nicht bestätigte Transaktionen
6.4 Das Bitcoin-Netzwerk (On-Chain)
- Full-Nodes
- Übung: Status der Transaktionen

6.5 Das „Lightning-Netzwerk“ (Off-Chain)
- Was ist der Unterschied zwischen Layer 1 und Layer 2?
- Übung: Die Funktionsweise von Lightning

Bitcoin als Wertspeicher und Zahlungsnetzwerk

6.1 Das Problem der Doppelausgaben

Bevor wir ins Detail gehen, sollten wir Folgendes bedenken:

- **Bitcoin ist digitales Geld.** Das bedeutet, dass es anders ist als konventionelles Geld:
  - Es kann nicht wie anderen Arten von digitalen Dateien (Fotos, Videos, etc.) vervielfältigt werden.
  - Es kann nicht *kopiert, gefälscht* und/oder *an mehrere Personen gleichzeitig gesendet* werden.
  - Es kann nicht wie bei der Zahlung mit Kreditkarte doppelt abgebucht werden.

Was sind die Vorteile dieser Eigenschaften von Bitcoin? *Lasst uns das anhand eines Beispiels erläutern:*

- Es ist üblich, dass die Menschen ihre Quittungen aufbewahren und/oder über ihre Ausgaben Buch führen.
  - Sie vergleichen regelmäßig ihre Rechnungen mit den Bankguthaben und überprüfen, ob es keine Unstimmigkeiten bei den Ausgaben gibt.
- Beispielsweise wird von jemanden festgestellt, dass ein Restaurant seine Kreditkarte zweimal belastet hat:
  - Am Mittwoch, den 26. Januar 2022, gibt es zwei Abbuchungen von jeweils 5,08 €.
  - Ihm wurde dasselbe Mittagessen doppelt in Rechnung gestellt.
  - Wahrscheinlich geht er zur Bank oder ruft dort an und versucht, eine der Zahlungen rückgängig zu machen.
  - Im besten Fall bekommt er sein Geld in ein paar Monaten zurück, wenn die Bank seinen Widerspruch akzeptiert.
  - Im schlimmsten Fall behauptet das Restaurant, dass es sich um zwei Einkäufe handelt, und verweigert die Rückerstattung des Geldes.

- Um die Idee der „Doppelausgaben" zu veranschaulichen, untersuchen wir nun weitere alltägliche Beispiele:

- **Tag 1**: Angenommen, Katja bestellt für 10 € ein Mittagessen an einem Imbiss.
  - *Sie bezahlt in bar mit zwei 5-Euro-Scheinen.*
  - *Die Zahlung wird sofort bestätigt.*
  - *Beide Parteien waren dabei physisch anwesend.*
  - *Es war ein direkter Austausch von Essen gegen Geld.*

- **Tag 2**: Katja bestellt das gleiche Essen und hat wieder zwei 5-Euro-Scheine.
  - *Aber einer ist ein Original und der andere eine Fälschung (eine exakte Kopie). Sie bezahlt mit diesen Scheinen.*
  - *Der Kassierer könnte leicht erkennen, dass es sich um eine Fälschung handelt, da die Seriennummern identisch sind,*
  - *oder er akzeptiert einfach die Zahlung wie am Vortag.*
  - *Der an diesem Tag viel beschäftigte Kassierer nimmt die Zahlung an, ohne die Geldscheine zu begutachten.*

- **Tag 3**: Katja ist gut gelaunt, hat aber Angst, erneut zu dem Imbiss zu gehen.
  - *Jetzt probiert sie, ihre Bitcoin so zu kopieren wie ihren Schein beim Imbiss.*
  - *Sie schuldet sowohl Elisa als auch Peter 0,2 BTC, hat aber nur 0,2 BTC auf ihrer Wallet.*
  - *Katja öffnet ihre Wallet sowohl auf ihrem Telefon als auch auf dem Telefon ihrer Mutter mit der Seed-Phrase.*
  - *Sie schickt von ihrem persönlichen Telefon 0,2 BTC an Elisa*
  - *und von dem Telefon ihrer Mutter 0,2 BTC an Peter.*
  - *Sie stellt sicher, dass beide Transaktionen genau zur gleichen Zeit gesendet werden.*

○ *Zwei verschiedene Nodes empfangen die beiden Transaktionen.*
○ *Wir erinnern uns daran, dass Katja nur 0,2 BTC in ihrer Wallet hatte, die sie ausgeben konnte.*

● Die Nodes bemerken das und eine der beiden Transaktionen wird abgelehnt.

● Aber wie funktioniert das? Wenn wir ein System haben, für das kein Computer zuständig ist, wie wird dann entschieden, welche Transaktion abgelehnt und welche unveränderbar in die Blockchain geschrieben wird?

● Satoshi Nakamoto ist es gelungen, einen Mechanismus zu finden, der genau das ermöglicht:

• Bevor eine Transaktion der Blockchain hinzugefügt wird, wird überprüft, ob sie gültig ist oder nicht, und zwar durch Konsens zwischen allen Netzwerkteilnehmern.
• Es ist eine geniale Lösung für Probleme wie die oben genannten.

Wie funktioniert das?

6.2 Der Wartebereich oder „Mempool“

● Bevor die Transaktion ausgeführt und in einen Block gesetzt werden kann,

• gelangt sie in einen Wartebereich, der Memorypool oder **„Mempool“** oder Speicherpool genannt wird.

Worum handelt es sich dabei und was passiert mit den Transaktionen, die hier eingehen?

● Es handelt sich um eine Website, auf der es Tausende von verifizierten, jedoch unbestätigten Transaktionen gibt.

● Da es keinen *globalen Mempool* gibt, muss jeder Node:

• die Gültigkeit jeder Transaktion verifizieren, bevor sie in seinen ***Mempool*** aufgenommen wird.
• verifizierte Transaktionen an benachbarte Nodes weiterleiten.
• ungültige Transaktionen ablehnen.

Hier kann man sehen, wie schnell gültige Transaktionen von Node zu Node weitergeleitet werden.

https://dailyblockchain.github.io

● Die Nodes müssen entscheiden, ob die Transaktionen gültig sind oder nicht.

• Wenn sie angenommen werden:
- wird darauf gewartet, dass ein Miner sie auswählt und zum nächsten Block hinzufügt.
- Schließlich werden sie *dauerhaft* in der gemeinsamen Datenbank gespeichert.

• Im Gegensatz dazu können sie abgelehnt werden, wenn:
- ein Konflikt mit anderen Transaktionen besteht.
- nicht genug Mittel für eine Überweisung vorhanden sind.
- die Signatur ungültig ist und man nicht überprüfen kann, ob der BTC-Betrag ausgegeben werden kann.

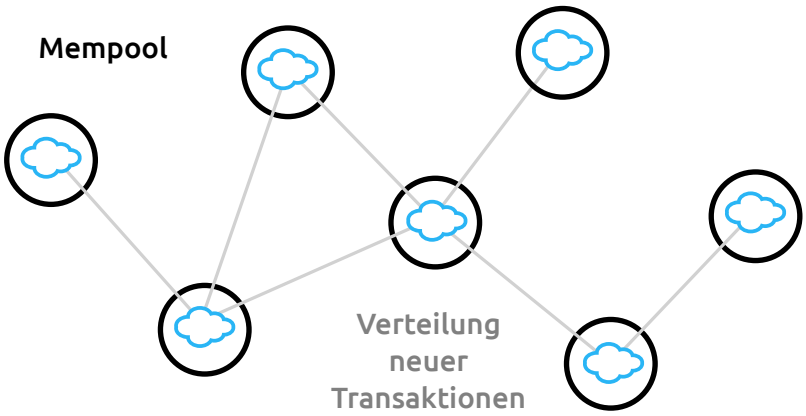
• Manche Transaktionen verbleiben im Wartebereich, wenn sie keinen ausreichend attraktiven finanziellen Anreiz für die Miner bieten.

- Wenn eine Transaktion länger als eine bestimmte Dauer unbestätigt bleibt, wird sie abgelehnt.

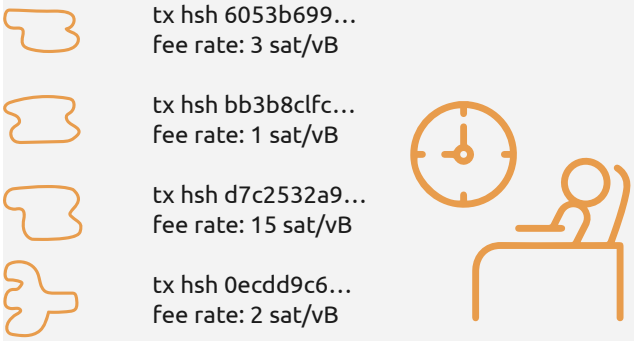
● Der Mempool bietet eine zusätzliche Sicherheitsebene und Resistenz gegen ***DDoS-Angriffe***.

• Bei einem DDoS-Angriff wird ein Netzwerk mit kleinen Transaktionen überflutet.

- Dadurch werden unüberschaubare Staus verursacht.



Ein ***Mempool*** ist der Ort, an dem die Transaktionen darauf warten, in einem Block bestätigt zu werden.

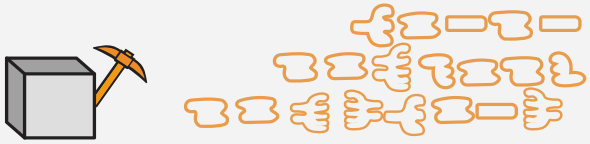


Wenn ein Node eine Transaktion zum ersten Mal von einem Peer empfängt, muss er ***überprüfen***, ob die Transaktion legitim ist. Niemand will fehlerhafte oder irreführende Transaktionen.

Hauptzweck des *Mempools:*

1 Übermittlung unbestätigter Transaktionen.

2 Versorgung der Miner mit Transaktionen, damit sie Mining betreiben können.



6.3 Übung: Verifizierte, aber nicht bestätigte Transaktionen

https://bits.monospace.live

Gemeinschaftsübung: Befolge die Anweisungen der Lehrkraft, um diese Übung durchzuführen! Um zu beginnen, folge dem Link des QR-Codes!

- Unten sieht man eine echte, unbestätigte Transaktion:
  - mit eindeutiger Kennung *(dem Fingerabdruck der Transaktion)* = Transaktions-ID/TxID.
  - mit dem Speicherplatz, den sie belegt.
  - mit den gezahlten Gebühren.
  - mit dem Betrag der Überweisung.

TxID: **a434948b2de9de18398294f84e42436ec59fb86faf34a21052bd640a97cd94b7d**

_____ input ➡ _____ outputs

Size: _____ vbytes	*(Größe; belegter Speicherplatz)*
Fee Rate: 27.01 sats/vbyte	*(aktueller Gebührensatz pro vbyte)*
Fee: _____ sats	*(Transaktionsgebühr)*
Total Value: ₿ _____ BTC ≈ $ _____ USD	*(Gesamtwert der Transaktion)*

- ***Lasst uns eine andere Transaktion bzw. weitere Transaktionen damit vergleichen!***

  - Ist der Betrag höher oder niedriger?
  - Haben die Nutzer eine höhere oder niedrigere Gebühr gezahlt?
  - Welche Transaktion wird man im nächsten Block am ehesten finden? Warum?
  - Was bedeutet es, wenn ein Block in den Abgrund fällt?
  - Was bedeutet es, wenn eine Transaktion bestätigt wird?

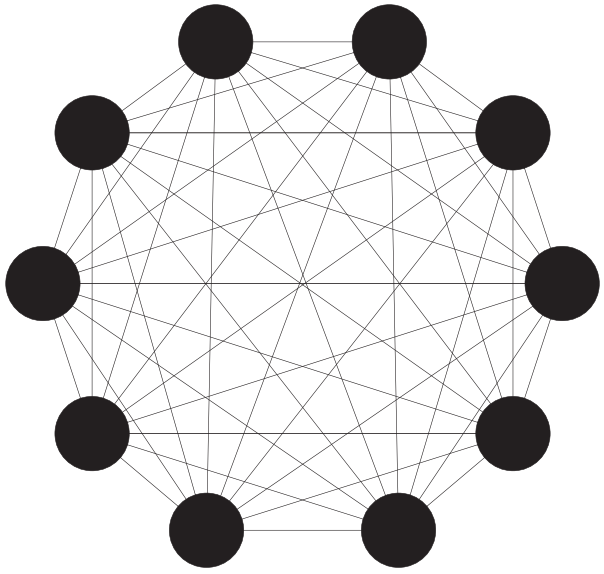
6.4 Das Bitcoin-Netzwerk (On-Chain)

● Es besteht aus *Bitcoin*-Knotenpunkten (Nodes).

• Das sind kleine Computer, die sich an ein bestimmtes Regelwerk halten (die Software Bitcoin Core).

- Sie kommunizieren über den Cyberspace miteinander und bilden so ein Netzwerk.
- Jeder von ihnen führt seine eigene Version der *Bitcoin*-Software aus.

Das Bitcoin-Netzwerk
Die verbundenen Nodes folgen einem gemeinsamen Regelwerk.



● Von diesen Verbindungspunkten aus kann man Informationen (d. h. Transaktionen) erstellen, senden und empfangen.

• Es gibt verschiedene Arten von Nodes; jede hat eine andere Aufgabe im Netzwerk.

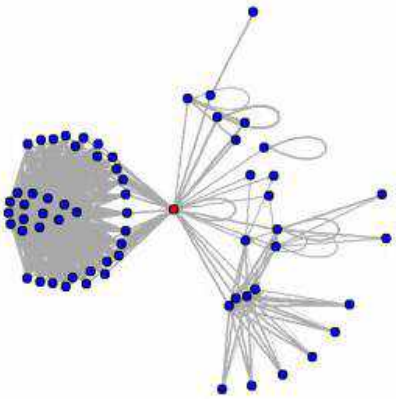
Full-Nodes

● Sie führen die *Bitcoin*-Software aus.

• Sie können ihre eigenen Entscheidungen treffen, allerdings durch Konsensbildung:

- Sie treffen dieselben Entscheidungen, was sie zu einem zuverlässigen und sicheren dezentralen Netzwerk macht.
- Full-Nodes haben drei verschiedene Funktionen:

▫ **1. Weitergabe von Informationen** *(an benachbarte Nodes).*



Diese Grafik stellt die Weiterleitung einer Transaktion dar.

• Es gibt zwei Arten von Transaktionen, die von den Nodes geteilt werden:

— **A: neue Transaktionen**

- Diese gehen direkt in den ***Mempool***.
- Die Nodes sind für die Verifizierung oder Ablehnung dieser Transaktionen zuständig.

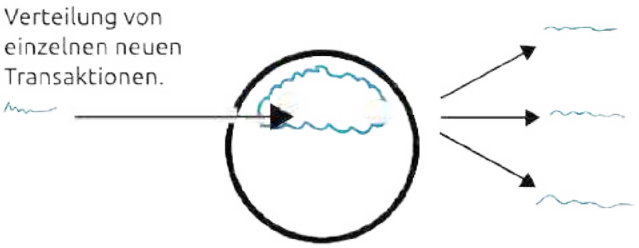
- Sie stützen sich auf die Geschichte der *Blockchain* und dem Regelwerk der Software.

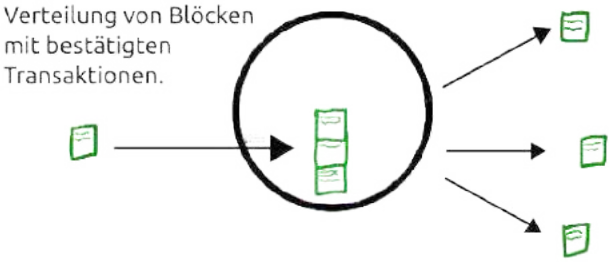
- Sie leiten gültige Transaktionen an ihre benachbarten Nodes weiter.

- Niemand möchte fehlerhafte oder böswillige Transaktionen erhalten.

— B: bestätigte Transaktionen

- Transaktionen, die *„bestätigt"* und in einen Block geschrieben wurden.
- Diese werden gruppiert und bilden die Blöcke; sie werden nicht einzeln geteilt.





▫ 2. Speichern einer Kopie der bestätigten Transaktionen

- Sie pflegen eine vollständige Kopie aller Blöcke in der Blockchain.
- Mit jeder ***Bestätigung*** wird das Risiko, dass eine Transaktion rückgängig gemacht wird, um ein Vielfaches verringert.

https://mempool.space/

▫ 3. Validieren der Blöcke und Konsensbildung mit anderen Nodes

- Bevor die in einem ganzen Block enthaltenden Informationen in die Blockchain aufgenommen werden, müssen sie von allen teilnehmenden Nodes einstimmig akzeptiert werden.
- Eine Kopie der Blockchain wird sicher verwahrt und mit anderen Nodes geteilt.

● Der Status der neuen und bestätigten Transaktionen kann online abgerufen werden.

Wie funktioniert das?

- Die Block-Explorer sind ein Fenster zu allen Blockchain-Transaktionen.
- Dadurch kann man den Kontostand jeder Adresse überprüfen, die Details jeder Transaktion einsehen und vieles mehr.

Übung: Status der Transaktionen

Gemeinschaftsübung: Geht auf den folgenden Link, wo man verschiedene Eigenschaften der Transaktionen betrachten kann!

https://www.blockchain.com/explorer?view=btc

Beantworte die Fragen auf der nächsten Seite!

Über den Link ***blockchain.com*** können wir alle folgenden Informationen erhalten:

- der Gesamtbetrag, der übertragen wird.
- die Anzahl der In- und Outputs.
- die Größe *(oder den Speicherplatz, der im Block eingenommen wird)*.
- die ID einer beliebigen Transaktion.
- den Status der Transaktion.
- ob die Transaktion bereits bestätigt wurde sowie die Gesamtzahl der bisherigen Bestätigungen.

Welche Informationen erkennst du wieder? Was überrascht dich? Was ist der Wert der letzten Transaktion? Wurde sie bereits bestätigt?

● Nicht alle Benutzer haben genügend Festplattenspeicher, um einen Knotenpunkt (Node) zu betreiben.

• In diesem Fall kann man eine Wallet herunterladen und Überweisungen tätigen oder BTC langfristig sparen.

6.5 Das „Lightning-Netzwerk" (Off-Chain)

Was ist der Unterschied zwischen Layer 1 (oder Basis-Layer) und Layer 2?

Was macht man mit einer sicheren, aber überlasteten Straße? Ganz einfach, man verbindet eine zusätzliche Straße, um den Verkehr zu entlasten. Das genau ist der Unterschied zwischen Layer-1- und Layer-2-*Blockchain*-Netzwerken.

● Viele wichtige Aspekte der ***Bitcoin***-Technologie und sogar viele Transaktionen finden nicht auf der „Blockchain" statt.

● ***Bitcoin*** ist revolutionär, denn es ist der *Basis-Layer des dezentralen Internets.*

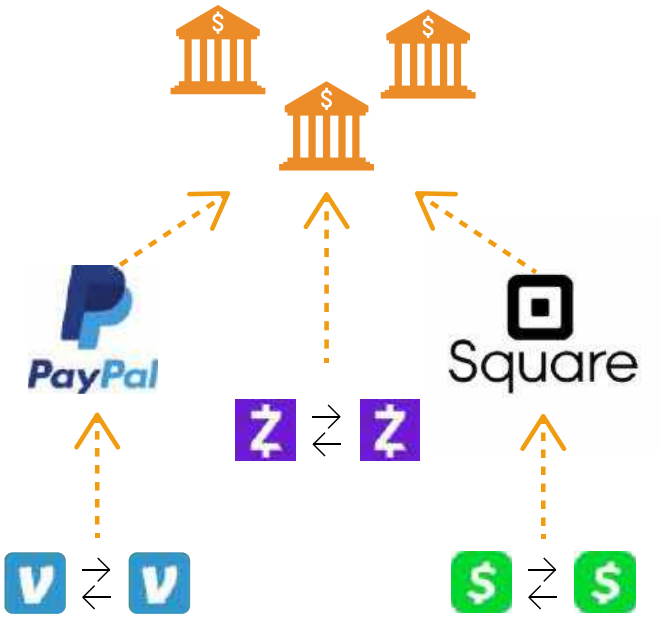
- Aber es gibt ein grundsätzliches Problem mit der Skalierbarkeit.
- ***Bitcoin***-Transaktionen können langsam und kostspielig sein.
- Es wird argumentiert, dass ***Bitcoin*** nicht als Zahlungsmittel verwendet werden kann, weil es für Kleinstzahlungen zu langsam und teuer ist.
- Es gibt Transaktionen im Wert von 1 bis 2 Euro, die bei der Nutzung des Hauptnetzwerks mehr als 5 Euro kosten.
- Visa verarbeitet bis zu 65.000 Transaktionen pro Sekunde (tps), während ***Bitcoin*** nur 7 tps bewältigen kann.

● Hier hilft die Magie von ***Layer-2-Lösungen*** wie ***Lightning***.

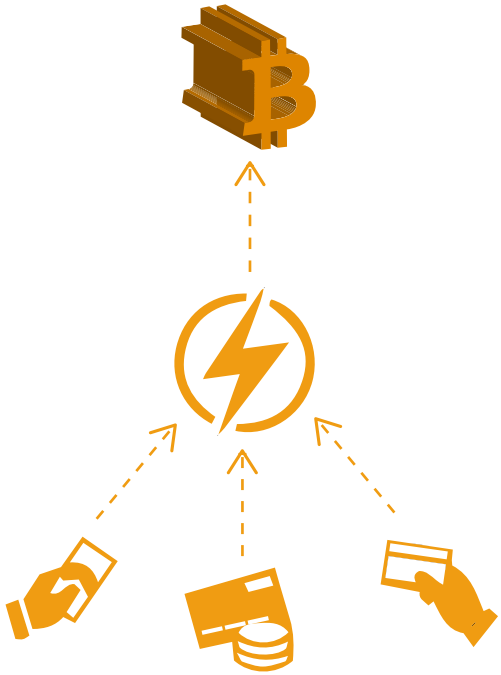
- Mit dem ***Lightning-Netzwerk*** hat ***Bitcoin*** das Potenzial, das Geld des digitalen Zeitalters zu werden.

- schnell
- unveränderlich
- dezentralisiert

moderne Währungssysteme = geschlossene Netzwerke
Die Banken bewahren die Endgültigkeit.



Bitcoin-Geldsystem = offenes Netzwerk
Bitcoin bewahrt die Endgültigkeit.



Alle Anwendungen, die auf dem **Lightning-Netzwerk** aufbauen, sind interoperabel.

- ***Lightning*** ist ein Regelwerk (Smart Contracts), das auf ***Bitcoin*** aufbaut.
  - Es ermöglicht sofortige Transaktionen,
  - bewältigt großes Transaktionsvolumen,
  - ist vom Hauptnetzwerk getrennt,
  - wobei es nicht notwendig ist, alle Transaktionen im Netzwerk aufzuzeichnen,
    - sondern in einem effizienteren Alternativnetz,
    - das die Sicherheit von ***Bitcoin*** bietet, ohne einige der Nachteile,
      - aber mit verschiedenen Arten von Vergütungen.
  - Es bietet mehr Privatssphäre als Layer 1.
  - ***Lightning*** nimmt die Skalierungsprobleme von ***Bitcoin*** in Angriff.
- Betrachten wir dazu folgende Analogie:
  - Ein Gast checkt in einem Hotel ein und wird im Voraus nach seiner Kreditkarte gefragt,
    - zur Deckung der Zimmer- und Nebenkosten für den Aufenthalt.
  - Das ist *effizienter* und *kostengünstiger*, als die Karte jedes Mal zu belasten, wenn eine Ausgabe getätigt wird.
  - Das Hotel führt Buch über alle Ausgaben des Gastes.
  - Im Hotel gibt es eine eigenständige Apotheke und einen Friseursalon.
    - Der Gast kauft Produkte, nimmt Dienstleistungen in Anspruch und lässt dabei die Rechnung auf sein Zimmer schreiben.
    - Das Hotel erhebt dabei eine Provision für die Vermittlung der Zahlungen zwischen dem Gast und dem Unternehmen.
  - Wenn der Gast ein Problem oder eine Reklamation hat, wird der erforderliche Betrag von der Rechnung des Gastes abgezogen.
  - Die Karte wird erst nach dem Aufenthalt belastet, wenn der Gast überprüft hat, dass die Kosten und der Saldo korrekt sind.

Bitcoin als Wertspeicher und Zahlungsnetzwerk

Hier erfährt man mehr über das Lightning-Netzwerk und seine Vorteile.

https://youtube.com/watch?v=YWuYEF-qmLA&feature=shareb

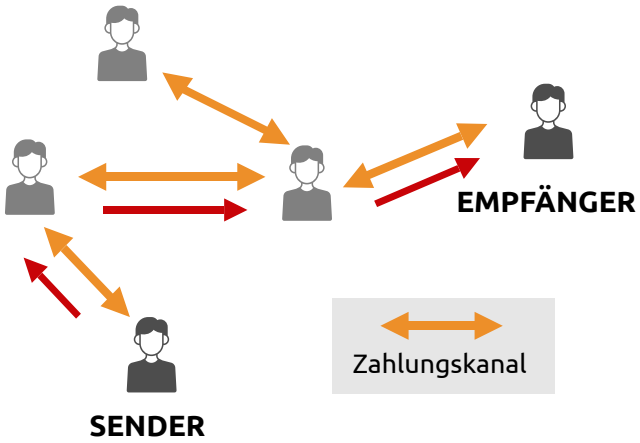
Das ***Lightning-Netzwerk*** funktioniert auf ähnliche Weise wie die Analogie, aber anders. ***Inwiefern?***

- Die Analogie ist gleich, wobei die Notwendigkeit des Vertrauens ausgeschlossen ist.
  - Dies ist ein häufiges Missverständnis von ***Lightning:*** Es ist kein *Kreditsystem*.
  - Die ***Lightning***-Transaktionen sind keine Schuldscheine:
    - Es sind gültige ***Bitcoin***-Transaktionen, die *echte UTXOs* bewegen.
- Anstatt jemanden eine Kreditkarte zu geben und ein offenes Konto zu gestatten,
  - können zwei Nodes einen ***Zahlungskanal*** oder eine Transferroute eröffnen.
  - Die Parteien können so viele Transaktionen durchführen, wie sie möchten,
    - wobei das Saldo immer auf den neuesten Stand gebracht wird.
  - Je größer der Kanal,
    - desto größer ist die Menge an ***Bitcoin***, die in beide Richtungen übertragen werden kann.
  - Mit allen Personen, mit denen Transaktionen getätigt werden, können Routen erstellt werden.
  - Je mehr Kanäle man eröffnet,
    - desto mehr Verbindungen und kürzere Verknüpfungen zu bestimmten Zielen hat man.
  - Wenn eine direkte Route existiert,
    - ist alles ganz einfach und eine Transaktion wird entsprechend der Größe des Kanals durchgeführt.
  - Wenn die Verbindung über eine dritte Partei (Routing-Node) erfolgt bzw. überbrückt wird,
    - zahlt man für die Route eine Gebühr.
  - Um einen neuen Kanal zu eröffnen, zahlen beide Nodes eine kleine Gebühr an die Miner.
  - Es besteht keine Notwendigkeit, jede Transaktion im Netzwerk zu aktualisieren und zu verifizieren.
    - Dies wäre zu kostspielig und zeitaufwendig.
    - Stattdessen wird jede Bewegung mit beiden digitalen Signaturen genehmigt.
  - Wenn eine der beiden Parteien beschließt, den Kanal zu schließen,
    - kann sie die letzte Transaktion einseitig an das ***Bitcoin***-Netzwerk übermitteln.

Unter folgendem Link findet man eine Visualisierung:

https://lnrouter.app/graph/zero-base-fee

- Wenn **A** einen Kanal zu **B** und **B** einen Kanal zu **C** geöffnet hat, kann **A** über **B** BTC an **C** senden, ohne **B** vertrauen oder kennen zu müssen.



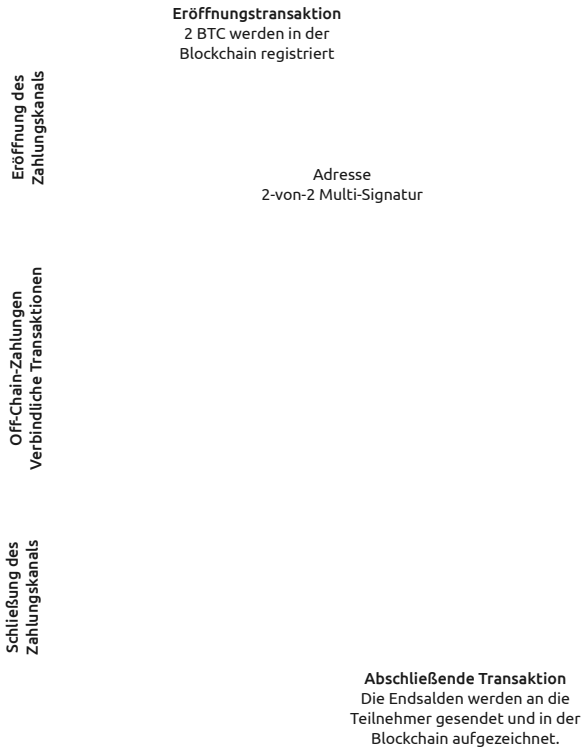
Übung: Die Funktionsweise von Lightning

Gemeinschaftsübung: Wir werden uns einen Simulator ansehen. Wartet auf die Anweisungen der Lehrkraft, um diese Übung durchzuführen!

https://www.robtex.com/lnemulator.html?conf=A5-5B,B5-5C&send=A2C

- Die Nutzung von ***Lightning*** ist so günstig und schnell wie das Versenden einer E-Mail,

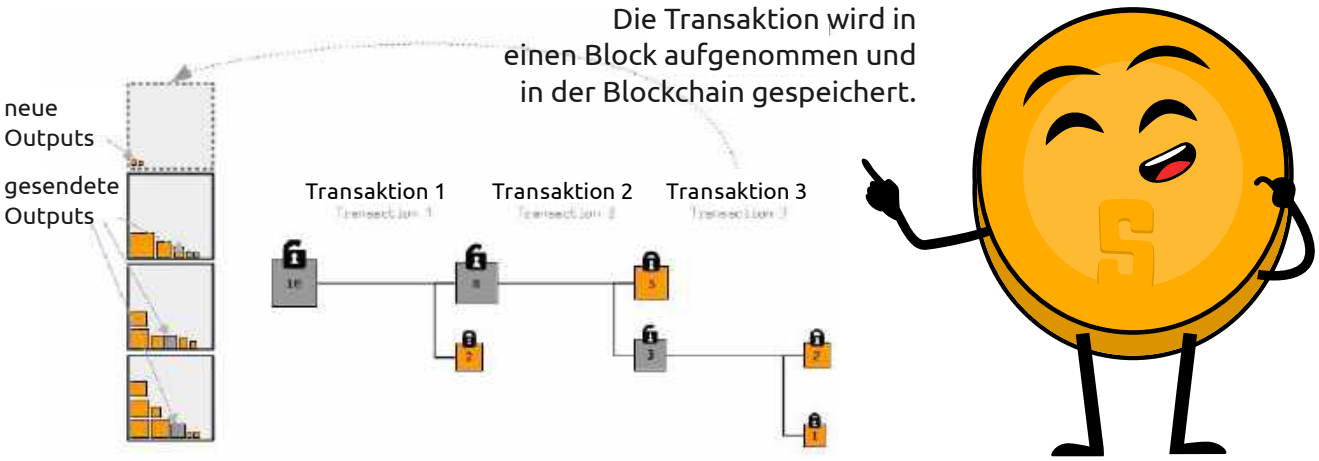
  - bloß mit dem zusätzlichen Vorteil, dass *Bitcoin* sicher ist und ohne Vertrauen funktioniert.
  - Nur die beiden Personen, die Geld in einem offenen Kanal aufbewahren, wissen, *wie viel, wie oft und wann dieses Geld bewegt wird.*



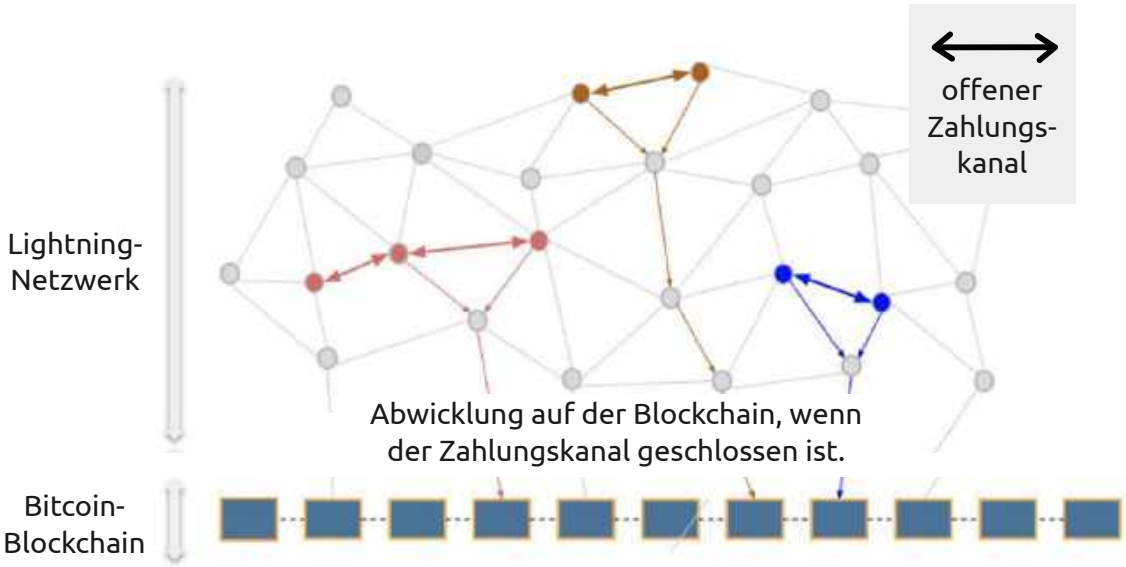
- Im Vergleich dazu würden hingegen drei „On-Chain"-Transaktionen durchgeführt werden, d. h. *sie würden im **Basis-Layer** verbleiben:*

  • Die Transaktionen wären viel langsamer und teurer gewesen.

• An jeder dieser Transaktionen müssten alle Netzwerkteilnehmer beteiligt sein.
• Man könnte sich das folgendermaßen vorstellen:



So funktioniert das Lightning-Netzwerk:



Lektion 7

Die Miner und das Bitcoin-Mining

7.1 Mining-Nodes
- Wie funktioniert der Wettbewerb zwischen den Minern?

7.2 Ein kleiner Exkurs zum Verständnis von Hashes
- Was ist eine Funktion?
- Was ist ein Hash?
- Was ist SHA256?
  - Übung: Hashes erstellen
- Was ist eine „Nonce“?
- Was ist ein Merkle-Baum?

7.3 Das Mining
- Vertrauen ist gut, Kontrolle ist besser
- Der Hash des Blocks
- Die Nonce des Blocks
- Übung: Echtzeit-Analyse von Blöcken

Die Miner und das Bitcoin-Mining

7.1 Mining-Nodes

● Sie sind darauf ausgelegt, als erstes die mathematischen Aufgaben zu lösen und neue Blöcke zu erzeugen.

• Ziel ist es, monetäre Prämien zu verdienen.
• Sie müssen nachweisen, dass sie dafür Arbeit aufgewendet haben.
• Dadurch tragen sie dazu bei, das Netzwerk zu sichern.

● Die Miner betreiben nicht nur einen *Full-Node*, sondern sie:

• fassen auch gültige Transaktionen zusammen, erstellen Blöcke und schlagen sie dem Netzwerk vor.

- Dies geschieht durch einen Mechanismus, der dem Netzwerk Sicherheit verleiht, genannt ***PoW*** (***Proof-of-Work***, z. Dt. ***„Arbeitsnachweis“***).
- Er ist notwendig für die Sicherheit, wodurch Betrug verhindert und abgeschreckt sowie Vertrauen innerhalb des Netzwerks ermöglicht wird.

● Die Prämie für das Mining jedes Blocks besteht aus:

• neuen *Bitcoin*, die von der *Bitcoin*-Software emittiert werden,
• sowie den Transaktionsgebühren für alle im Block enthaltenen Transaktionen.

● Ein wesentlicher Unterschied zwischen ***Full-Nodes*** und ***Mining-Nodes:***

• ***Mining-Nodes*** können dem *Bitcoin*-Netzwerk neue Blöcke vorschlagen.
- Sie versuchen, kryptografische Puzzle in einem Prozess zu lösen, der „Mining“ genannt wird.
- Sie müssen nachweisen, dass sie die für das Mining des Blocks erforderliche Arbeit geleistet haben.
- Deshalb können sie ***Prämien*** für die Blöcke erhalten.
• ***Full-Nodes*** können keine neuen Blöcke vorschlagen
- und daher auch ***keine*** Prämien erhalten.

Wie funktioniert der Wettbewerb zwischen den Minern?

● Lasst uns nochmal auf eine Analogie zurückkommen:
○ Jeder Miner hat einen speziellen Würfel mit den Zahlen 1 bis 1000, d. h. er hat 1000 Seiten.
○ Die Miner machen sich bereit, an einem Wettbewerb teilzunehmen, bei dem es darum geht, in den nächsten 10 Minuten etwas mehr als 6,25 *Bitcoin* zu gewinnen.
○ *Bitcoin* wählt eine Zielzahl zwischen 1-1000 aus und veröffentlicht sie für alle sichtbar im Netzwerk. Nehmen wir an, es trifft die Zahl 8.
○ Nun ist das Ziel, eine kleinere Zahl als 8 zu würfeln.

- Einige Miner sind im Vorteil und haben eine höhere Gewinnchance. Warum?
- Sie haben mehr Kaufkraft und mehr als einen Würfel gekauft.
- Manche würfeln mit einer höheren Geschwindigkeit als andere.

○ Der Wettbewerb beginnt:

• Die Miner beginnen, ihre Würfel Hunderte von Malen zu werfen, aber das erfordert viel Arbeit. Ihre Hände ermüden.
• Ein glücklicher Miner hebt die Hand und sagt: „Ich habe gewonnen!“
• Alle anderen Miner hören auf zu würfeln und schauen auf den Tisch, auf dem gespielt wird.
• Auf diese Weise können alle überprüfen, ob der Miner die Wahrheit sagt.

• Wenn die Mehrheit im Konsens beschließt, dass der Miner der Gewinner ist, erhält er seine Prämie.
• Und das Spiel beginnt von vorn.

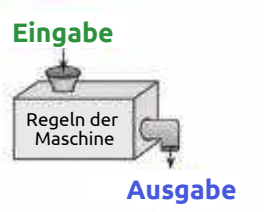
○ Wenn mehr Miner am nächsten Wettbewerb teilnehmen, senkt ***Bitcoin*** die Zielzahl, sodass es immer etwa zehn Minuten dauert, bis jemand gewinnt.

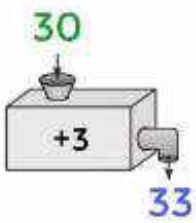
7.2 Ein kleiner Exkurs zum Verständnis der Bedeutung von Hashes

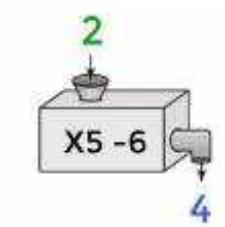
Was ist eine Funktion?

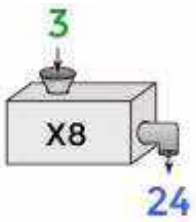
● Wie bei einer Verarbeitungsmaschine

• gibt man etwas hinein, verändert es nach strengen Regeln und es entsteht etwas völlig anderes.
• Das heißt, die Eingabedaten, x, oder die Daten, die man eingibt, werden vorgegeben.
• Auf sie werden vordefinierte mathematische Operationen (*Addition, Subtraktion, Mulitplikation, usw.*) angewendet.
- Das Ergebnis ist eine Ausgabe, **f(x), y**.









Eingabe	Ausgabe
5	8
17	20
30	33

● Beispiel: f(x)=3x+4, sagt mir:

• Multipliziere die Eingabedaten (x) mit 3, addiere 4 dazu und erhalte die *Ausgabe* von f(x), oder y.
• Was wäre die Antwort von f(2)? Das heißt was ist das Ergebnis von y, wenn x=2?
• Wie lautet hier nun die Frage? **f(x)=15**. Suchen wir die Eingabe oder die Ausgabe? Ist es möglich, den Wert zu finden? Schauen wir mal ...

f(x)=3x+4=15 ***3x+4=15*** ***x=?***

● Einige Funktionen sind *unidirektional*.

• Sie haben die Eigenschaft, dass sie leicht zu berechnen, aber schwer umzukehren sind.
• Selbst wenn wir das *Ergebnis* kennen, sind wir nicht in der Lage, die *Eingabedaten* zu entschlüsseln.

● Wenn man Mathe hasst, kann man eine Analogie benutzen, die beim Verständnis dieses Konzepts hilft.

Wir wollen einen roten Fruchtsaft produzieren.

• Das sind die *Eingabedaten*: *(t=Tasse)*
• 1 t Wasser, 3 Eiswürfel, 18 Himbeeren, 8 Erdbeeren, 15 Brombeeren und 1/5 t Zucker.
• Die *Durchführung der Funktion*:
- Mixe alles im Mixer zusammen.
• Ergebnis der *Ausgabedaten*:
- Es entsteht ein leckerer Saft.
• Es ist für eine andere Person nahezu unmöglich, die genauen Zutaten und Portionen herauszufinden.
• Das ist mit einer unidirektionalen Funktion gemeint.
• Der Saft kann nicht in seine Eingabedaten zurückverwandelt werden.

Die Miner und das Bitcoin-Mining

Was ist ein Hash?

● ***Bitcoin*** nutzt Kryptographie – einen Zweig der Mathematik.

• Sein Eingabe- und Ausgabeprozess ist sehr ähnlich.
• Eine kryptografische ***Hash***-Funktion:

- ist eine kryptografische Operation, die eine beliebige Menge von Daten nimmt,
- und einen Hash-Wert mit ***einzigartigen und einmaligen*** Merkmalen ausgibt, der ***deterministisch und chaotisch*** ist.

Mein erster Bitcoin → **Hash-Funktion** → eb03bc4a5308-598665b441a0-1dabc9d0b6b5-c43267f27612-d422e3ab8ded-fb02

● Es gibt keine Einschränkungen für die Eingabedaten:

• Der ***Hash*** ergibt immer die gleiche Länge an Zeichen.
• Der ***Hash*** wird auch als ein *Fingerabdruck* der Eingabedaten betrachtet.

GLOSSAR

Deterministisch: *Die gleichen Eingaben oder Buchstaben führen immer zu den gleichen Ausgaben oder Ergebnissen.*

Chaotisch: *Eine geringfügig abweichende Eingabe führt zu einer völlig anderen und bezugslosen Ausgabe.*

Was ist SHA256?

● Die spezielle Hash-Funktion, die ***Bitcoin*** nutzt, heißt ***SHA256*** (Secure Hash Algorithm 256).

• Ihr *Ergebnis* oder ***Hash*** ist immer hexadezimal (mit Zahlen zwischen 0 und 9 sowie Buchstaben von A bis F).

- SHA256(Eingabe)=Hash

● Lasst uns ***Hashes*** erstellen. Schauen wir uns die folgenden Beispiele an:

SHA256(Dalia) =
bbadb37bc80b041a1cafdfadf1efd93d6386117b33046d650e75ec2cb101758c

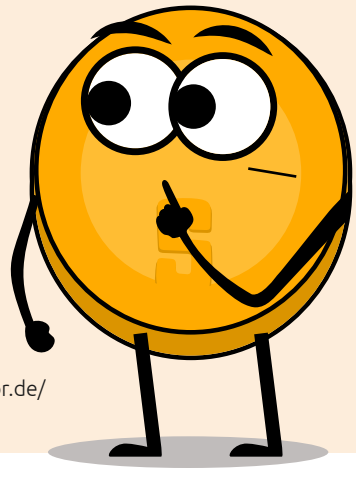
SHA256(DaliaP) =
25cad1f3deb7bc5ba54ccf1f0fe8e8f4a17f58826847b8cae2ddbd6cd6ab77

SHA256(Hallo, ich heiße Dalia. Ich komme aus Medellin in Kolumbien.) =
dc6cf56b55951f58074b489ae3ede688-ab949a62cfa121fae019e2aa69714785

Übung: Hashes erstellen

Gemeinschaftsübung: Wie erstellt man einen Hash? Auf der folgenden Website können wir dies üben:

https://hashgenerator.de/



Zunächst einmal, was passiert, wenn du bei dem 256er-Hash *Dalia* oder *Mein erster Bitcoin* eingibst?
Vergleiche ihn mit den hier aufgelisteten Hashes!

Ist dir bewusst, dass obwohl das Ergebnis zufällig ist,

- das Ergebnis einer bestimmten Eingabe immer das gleiche sein wird.

- es nicht das Problem gäbe, dass es zwei „Marias“ oder zwei „Josefs“ in der Klasse gibt, wenn wir uns anstelle von Vorname, Nachname und Geburtsdatum mit einer Zahl wie dieser identifizieren würden.

Wie lautet der Hash deines Namens? Dein vollständiger Name?

Was passiert, wenn du einen Buchstaben in deinem Namen änderst? Hättest du diesen Hash vorhersagen können?

Was ist eine „Nonce“?

- Der Begriff **„Nonce“** kommt von „number used once“.

  • Es handelt sich einfach um eine einmalig verwendete Zahl.
  • **„Nonce“**-Zahlen sind für das Mining sehr nützlich, da eines der Hauptziele darin besteht, SHA256(Eingabe)-Ergebnisse zu finden, die bestimmte vorgegebene Bedingungen erfüllen.

- Angenommen, das **Ziel** ist es, einen Hash zu finden, der **mit der Zahl „Null“ beginnt**.

  • Nur die letzte Ziffer in SHA(Dalia**P**) wird geändert. Die Nonce würde das „P“ ändern.

SHA(Dalia**1**) = c2cb88c9aec429a7fe9194351e-748247f668241f75c708b43ea83ecd730268f

SHA(Dalia**2**) = 17df2ae3b1dec56c7bde0cf8b-161f24329d351e08cb797adbd76af46401dadf3

... Wir hatten Glück und mussten es nur acht Mal versuchen, um unser Ziel zu erreichen:

SHA(Dalia**8**) = **0**93d4ddb855114f49f3b775803-529ed1cbd5598b5995c327091552bab5672658

Was ist ein Merkle-Baum?

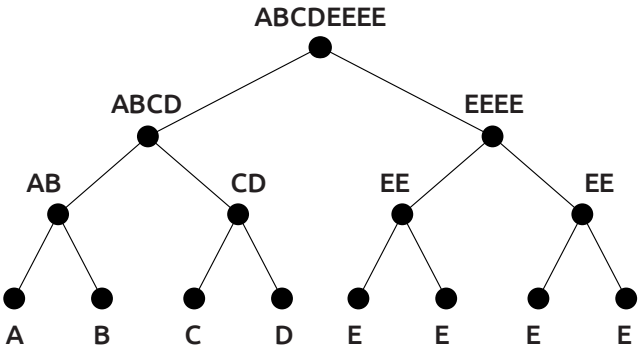
- Eine Datenstruktur, die in mehrere Schichten von Hashes unterteilt ist, mit denen die *Informationen aller Transaktionen* schnell und effizient überprüft werden können.

- Er ist wie ein umgedrehter Baum, bei dem man von den Blättern ausgehend über die Äste bis zum *Wurzelknoten* aufsteigt.

- Der Wurzelknoten ist der Hauptidentifikator, der die Überprüfung des gesamten Datensatzes ermöglicht.

- Die endgültige, eindeutige Wurzel, die alle Informationen über alle Transaktionen enthält,

  • wird als ***Merkle Root*** oder ***Merkle-Wurzel*** bezeichnet.



7.3 Das Mining

Nun zurück zum Mining-Prozess von ***Bitcoin***.

- Die Miner können frei wählen, welche Transaktionen sie in ihren nächsten Block aufnehmen wollen.

  • Sie wählen neue verifizierte Transaktionen aus und gruppieren sie zu einem neuen „potenziellen Block".

Welche Transaktionen sollten sie für ihren „potenziellen Block" auswählen?

- Sie wählen die Transaktionen aus, die den *größten finanziellen Anreiz* bieten und am *wenigsten Speicherplatz* beanspruchen.

  • Die Einzahler fügen Provisionen (oder Gebühren) hinzu, um Anreize für die Miner zu schaffen.
  • Zusätzlich werden die Miner zu ehrlicher Arbeit motiviert.

- Umso mehr Transaktionen sich im Mempool befinden, desto stärker ist das Netzwerk ausgelastet.

  • Die monetären Anreize (Gebühren) sind im Allgemeinen größer, wenn es viele Zahlungen gibt.
  • Bei hohem Zahlungsverkehr wählen die Miner Transaktionen mit höheren Gebühren.
  • Sobald der Verkehr abgenommen hat, werden die Transaktionen mit niedrigeren Gebühren hinzugefügt.

Woraus besteht jeder potenzielle Block?

- Die Größe eines Blocks beträgt bis zu 4 MB.

- Jeder Block enthält höchstens ein paar Tausend Transaktionen, daher ist es wichtig, effizient auszuwählen.

  • Er enthält einen Block-Header.

    - Dieser Header des Blocks wird gehasht.

  SHA256(**Header**) = ERGEBNIS

Wofür wird dieses ERGEBNIS verwendet?

- Das Ziel ist es, einen gültigen Bezeichner für einen neuen Block zu erzeugen, der perfekt hinter den letzten Block in der bestehenden Kette passt.

  • Dazu muss ein Miner den passenden Hash erzeugen.

- Dieser Hash muss unter einem bestimmten „Zielwert“ liegen.

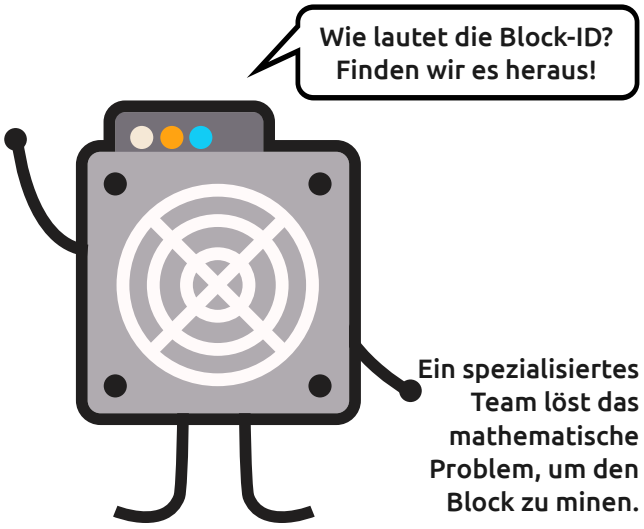
• Solange das ERGEBNIS größer ist als der gewünschte Hash,

- fügt der Miner eine ***„Nonce“*** hinzu und versucht es erneut.
- Die Miner wiederholen dies mehrere Tausend Mal pro Sekunde,
- um schließlich die Block-Prämie zu gewinnen,
- und erzeugen einen „Fingerabdruck“ oder einen einzigartigen Hash von diesem Block.

• Für diesen Prozess muss die Nonce zig Tausend Male geändert werden, wodurch viele mögliche ERGEBNISSE erzeugt werden, bis der passende Hash vor allen anderen Minern erreicht wird.
• So ähnlich wie bei unserem anfänglichen Beispiel, bei dem viele Male gewürfelt wird, bis ein Miner mit einem ERGEBNIS gewinnt, das unter dem Zielwert liegt.

● Das bedeutet, dass jeder Mining-Node einen neuen Block minen kann.

• Allerdings muss man dafür Energie aufwenden.



Ein spezialisiertes Team löst das mathematische Problem, um den Block zu minen.

Was passiert, wenn der passende Hash gefunden wurde?

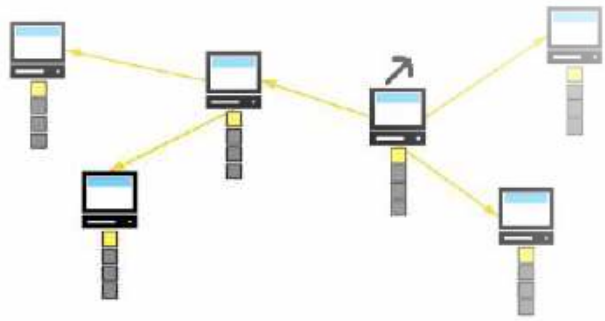
● Ein vom Glück begünstigter Miner produziert schließlich den passenden Hash

• und sendet ihn an das gesamte Netzwerk.

- Dieser Hash wird zum **„Hash des Blocks“** bzw. zur **eindeutigen Kennung des Blocks**.

● Für die übrigen Miner ist die Bestätigung der Gültigkeit des Blocks ein einfacher Prozess.

• Sie müssen nur sicherstellen, dass alle Transaktionen gültig bleiben
• und dass der Hash des Blocks kleiner als der „Zielwert“ ist.



● Wenn der Block verifiziert ist, fügen die anderen Nodes ihn der bestehenden Kette hinzu.

• Alle Transaktionen, die in diesem Block enthalten sind, werden dauerhaft auf der Blockchain gespeichert.

● Dieser Vorgang wiederholt sich etwa alle zehn Minuten.

• Die Miner versuchen, einen neuen, darauf folgenden Block zu minen.

Die Miner und das Bitcoin-Mining

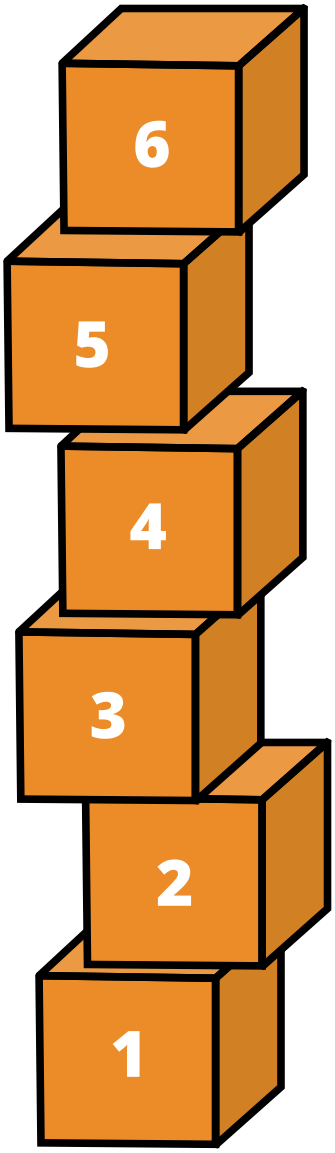
Wie erhält nun der Miner, der den Zielwert gefunden hat, die Belohnung?

- Alle gefundenen Blöcke erzeugen eine erste Transaktion, die eine Prämie enthält:
  - Sie enthält einen Betrag an neuen *Bitcoin*, der bei der Erstellung des Blocks freigegeben wird,
    - sowie alle Gebühren, die durch die ausgewählten Transaktionen generiert werden.
- Nur der erfolgreiche Miner kann diese Prämie erhalten,
  - für seine große Rechenleistung: ***PoW*** oder ***Proof of Work***.
    - ***PoW*** hat sich als erfolgreiche Methode erwiesen,
    - weil es extrem schwierig ist, den ***Hash*** zu finden, aber sehr einfach, ihn zu verifizieren.
- Diese Transaktion wird ***Coinbase*** genannt, wörtlich: Münzbasis.
  - Es ist die erste Transaktion in jedem Block der Blockchain.

Vertrauen ist gut, Kontrolle ist besser!

Was bedeutet das?

- Die Transaktionen erhalten eine Bestätigung, wenn sie in einen Block aufgenommen werden, und dann nach der Bestätigung jedes folgenden Blocks.
- Damit ein solcher Block in die Blockchain aufgenommen werden kann, muss er ordnungsgemäß mit dem zuletzt im Netzwerk erstellten Block verknüpft sein.
- Eine Bestätigung in der Blockchain bedeutet, dass „die Transaktion vom Netzwerk verarbeitet und validiert wurde und es sehr unwahrscheinlich ist, dass sie rückgängig gemacht wird".
- Es wird empfohlen, mindestens sechs Bestätigungen abzuwarten, um sicherzustellen, dass das Geld überwiesen wurde.
- Bitcoin ist bekannt als die sicherste und wahrheitsgetreuste Blockchain, die es gibt.



Block #6:
6 Bestätigungen
Deine Transaktion ist sicher.
60 Minuten

Block #5:
5 Bestätigungen
50 Minuten

Block #4:
4 Bestätigungen
40 Minuten

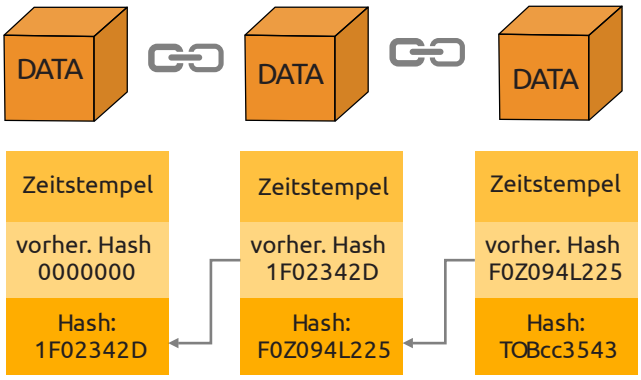
Block #3:
3 Bestätigungen
30 Minuten

Block #2:
2 Bestätigungen
20 Minuten

Deine Transaktion wurde bestätigt.
10 Minuten

Der Hash des Blocks

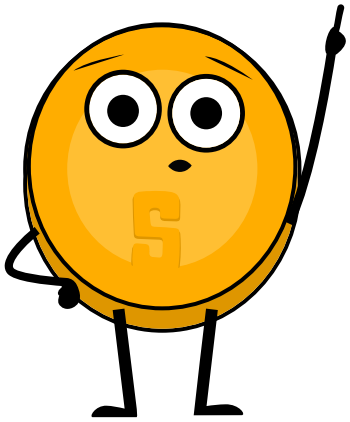
- Jeder Block verweist auf den vorherigen Block,
  - und zwar durch das Feld ***„vorheriger Block" (vorheriger Hash) im Block-Header.***
- Die Abfolge der Hashes, die jeden Block mit dem vorherigen verknüpft, bildet eine Kette, die bis zum ersten jemals erstellten Block zurückreicht.
  - Der erste Block wird als Genesis-Block bezeichnet.
- Jede geringfügige Änderung an einer Transaktion ändert den Hash des Blocks und löst den Bezug zum vorherigen Block auf.
- Wenn ein Hacker versucht, auch nur ein Komma einer Transaktion zu manipulieren, führt dies zu einer Kaskade an Fehlschlägen bei der Verifizierung der nachfolgenden Blöcke.
- Das liegt daran, dass jeder Block Informationen über den vorherigen Block enthält.
- Blöcke bestehen aus einem Block-Header und seinen Transaktionen.
- Der ***Header*** enthält:
  - **1.** die Zusammenfassung der Daten innerhalb des Blocks, d. h. alle Transaktionen komprimiert in einer ***Merkle-Wurzel***.
  - **2.** den ***Hash*** des vorherigen Blocks in der Blockchain.
  - **3.** eine ***Nonce***, die auf der Suche nach einem „Zielwert" so oft wie nötig geändert werden kann.
- Mit Hilfe der SHA256-Funktion werden alle im Block enthaltenen Informationen komprimiert.
  - Dieses Ergebnis ist der ***„Hash des Blocks"*** bzw. repräsentativ für seinen **„Fingerabdruck"**.



version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Hash des Blocks

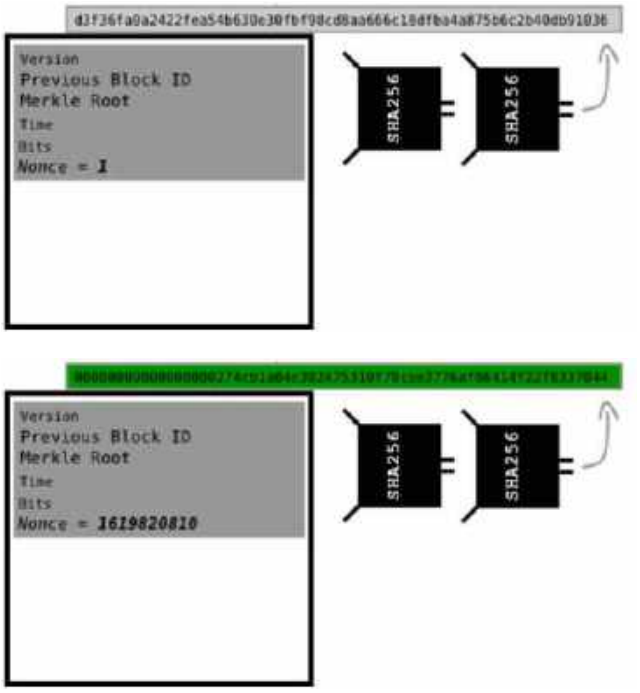
```
0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50
```



Die Miner und das Bitcoin-Mining

Die Nonce des Blocks

- Das ***Nonce***-Feld ist eine Zahl in dem Header eines Blocks.
  - Die Miner *ändern sie*, bis der ***Hash des Headers*** die ***Zielschwierigkeit*** oder den ***Zielwert*** ergibt.
- Die ***Zielschwierigkeit*** beginnt immer mit einer Anzahl von Nullen.
  - Die Anzahl der Nullen ist variabel.
  - Sie hängt davon ab, wie viele Miner versuchen, den Block zu minen.
- Wenn ein Miner eine ***Nonce*** findet, die, zum Header-Hash hinzugefügt, das Schwierigkeitsziel erfüllt, fügt er sie dem Header des neuen Blocks hinzu und sendet sie an das Netzwerk, damit die übrigen Miner die Gültigkeit der Lösung überprüfen können.



https://bits.monospace.live

Übung: Echtzeit-Analyse von Blöcken

Gemeinschaftsübung: Unter dem folgenden Link kannst du die Blockchain in Echtzeit analysieren. Beantworte die Fragen auf der Grundlage der Informationen auf der Website.

1. Welcher Block wurde zuletzt gemined?

2. Wie viele Transaktionen waren in diesem Block enthalten?

3. Wie hoch ist der Gesamtwert, der in Bitcoin gehandelt wurde?

4. Welche Größe hat der Block in MB?

5. Mit wie vielen Nullen beginnt die Nonce des Blocks?

6. Wie viel hat der Miner insgesamt verdient?

7. Wie hoch war der Gesamtwert der Gebühren, die der Miner für das Hinzufügen der Transaktionen zum Netzwerk erhielt?

8. Suche die Transaktion mit dem höchsten Wert in diesem Block! Auf wie viele Wallets wurde der BTC-Betrag verteilt?

Lektion 8

Knappheit, Kosten, Preis und Volatilität

8.1 Die Bedeutung der Blockprämie
8.2 Halving
- Halving-Ereignisse

8.3 Der Wert von Bitcoin im Laufe der Zeit
- Mittel- und langfristige Faktoren
- Der Lindy-Effekt

8.4 Die Belohnungen für die Miner
- Die Difficulty

8.5 Auf wen oder was muss man achten?
- Angriffe auf Bitcoin
- Was ist eine 51%-Attacke?

Knappheit, Kosten, Preis und Volatilität

8.1 Die Bedeutung der Blockprämie

Schaffung eines erfolgreichen dezentralen Wirtschaftssystems:

- Die Miner investieren Geld und Rechenarbeit, um *Bitcoin* zu schürfen.
- Sie sichern das Netzwerk ab, um Angriffe zu verhindern, und gleichzeitig:
  - erzeugen sie neue Münzen, die frei im Netzwerk zirkulieren können.
- Die Blockprämie dient als Subvention und Anreiz für die Miner.
  - Transaktionsgebühren oder Provisionen sorgen dafür, dass es keine Netzwerkausfälle gibt.

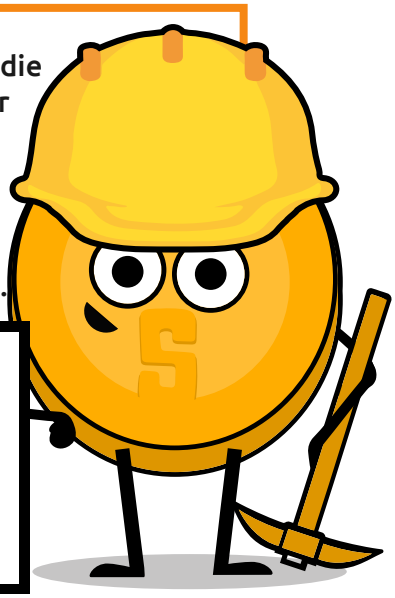
8.2 Halving

- Satoshi Nakamoto entwickelte einen sehr strategischen Weg, neue Bitcoin zu verteilen, ohne dass eine Person oder eine Gruppe die Verantwortung für die Verteilung hat.
- Um ein deflationäres Modell zu entwickeln, wurde folgendes festgehalten:
  - Alle 210.000 Blöcke halbiert sich die Anzahl der neu ausgegebenen *Bitcoin*.
    - Das passiert ungefähr alle vier Jahre.
  - Im Gegensatz zu den Problemen, die wir mit Fiat-Währungen haben, bei denen niemand wirklich weiß, wieviel Kredit oder Dollar im System sind,
    - hat *Bitcoin* eine fixe Menge von circa 21.000.000.
    - Die fixe Menge ist automatisch geregelt.
    - Es wird durch Konsens durchgesetzt.
  - Zu Beginn wurde die Belohnung mit 50 *Bitcoin* pro Block festgelegt.
  - Ungefähr alle vier Jahre wird die Prämie halbiert, daher spricht man von einem *Halving*.

Halving-Ereignisse

- Das erste *Halving* erfolgte Ende 2012.
  - Ab Block 210.001 wurden nur 25 BTC ausgegeben.
- Das zweite *Halving* erfolgte 2016.
  - Die Belohnung reduzierte sich auf 12,5 BTC.
- Und so wird es bis zum Jahr 2140 weitergehen.
  - Dann werden alle 21 Millionen *Bitcoin* gemined sein.
- Diese Halbierung der Belohnung wurde mit folgender Absicht hinzugefügt:
  - um Inflation zu verhindern.
  - um natürliche Knappheit hinzuzufügen.

Hier kann man die Gesamtzahl der verfügbaren Bitcoin sehen, die aktuell im Netzwerk im Umlauf sind.



https://www.blockchain.com/explorer/charts/

Warum also die Änderung? Warum nicht die gleiche Prämie? Ist das nicht unfair gegenüber den Minern?

Die Antwort auf diese Frage ergibt sich aus dem Gesetz von Angebot und Nachfrage.

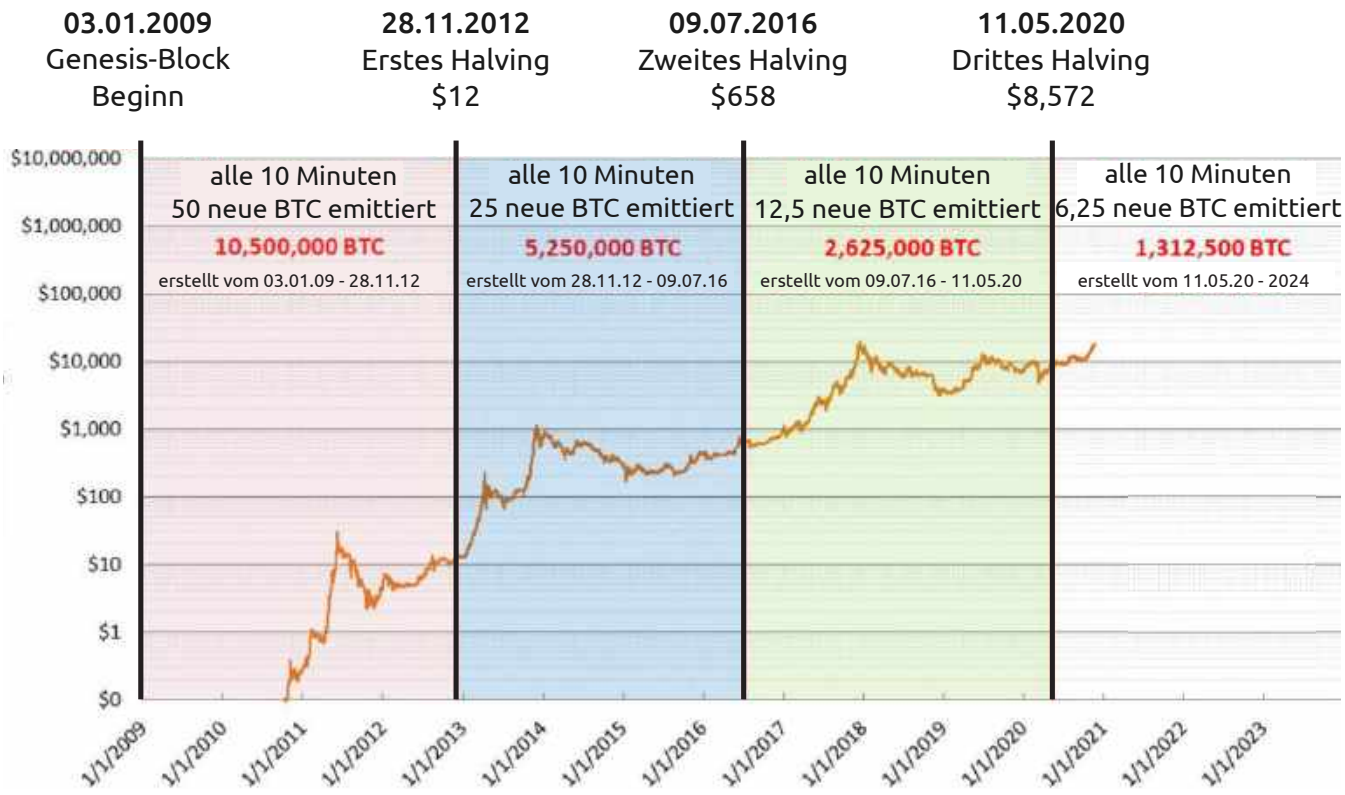
- Wenn *Bitcoin* zu schnell erzeugt werden und die Anzahl der *Bitcoin*, die erzeugt werden, nicht begrenzt ist:
  - werden schnell zu viele *Bitcoin* im Umlauf sein und ihr Wert wird sinken.
- Wenn alle 21 Millionen gleichzeitig herausgegeben worden wären:
  - hätten ein paar Leute es möglicherweise gehortet.
  - hätte niemand sonst die Möglichkeit gehabt, es zu erwerben.
- Die Folgende Grafik zeigt, wie sich das Halving im Laufe der Zeit auf den Preis auswirkt:

8.3 Der Wert von Bitcoin im Laufe der Zeit

Der Wert von *Bitcoin* ist gestiegen:

- von weniger als $ 0,01 im Jahr 2009 (bei der ersten Transaktion)
- bis zu einem Höchstbetrag von rund 67.000 US-Dollar im November 2021.
- Auch wenn es in den letzten zehn Jahren bis zu 80 % Kursverlust gab, hat es sich nicht nur erholt, sondern weist langfristig einen Aufwärtstrend auf.
- Die Faktoren, die Angebot und Nachfrage beeinflussen, sind vielfältiger geworden

— **Warum hat Bitcoin einen Wert?**
— **Warum ist der Preis so gestiegen?**
— **Warum ist es so volatil?**



Knappheit, Kosten, Preis und Volatilität

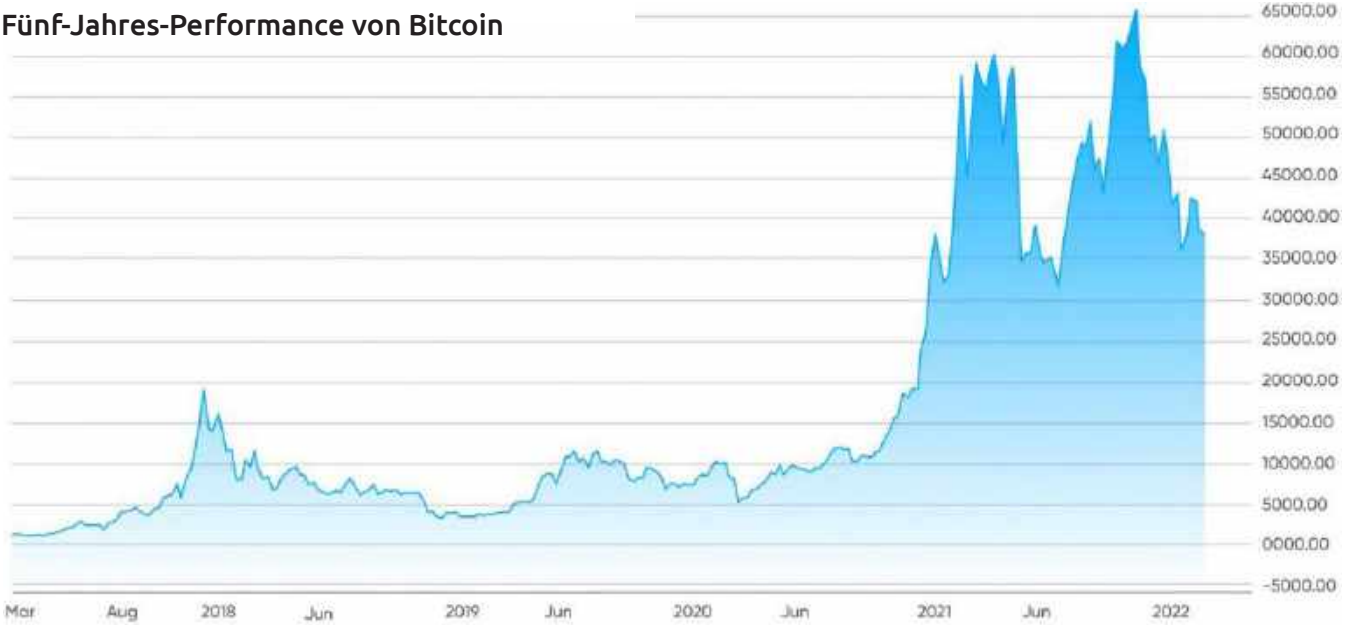
Um dies besser zu verstehen, müssen einige wichtige Begriffe definiert werden:

- **1. Umlaufmenge:**
  - Die bisher erzeugte Menge an *Bitcoin*.
  - Im Juli 2022 waren etwa 19.101.000 *Bitcoin* ***erzeugt worden.***
- **2. Gesamtangebot:**
  - Anzahl der Münzen im Umlauf, zuzüglich der noch nicht emittierten Münzen.
  - Insgesamt wird das Gesamtangebot von *Bitcoin* circa 21 Millionen betragen.
    - Es wird geschätzt, dass rund vier Millionen *Bitcoin* verschwunden sind oder als „verloren" gelten.
    - Vermutlich nicht auszahlbar aufgrund von verlorengegangener Passwörter, falscher Ausgabeadressen oder Programmfehler.
- **3. Marktkapitalisierung:**
  - Der gesamte Marktwert der Umlaufmenge von *Bitcoin* ausgedrückt in *Fiat-Währungen*.
  - Man muss den aktuellen *Bitcoin*-Preis (in USD) mit dem aktuellen Angebot multiplizieren.

Marktkapitalisierung = aktueller Preis x Umlaufmenge

https://coinmarketcap.com/currencies/bitcoin/

Fünf-Jahres-Performance von Bitcoin



- In der vorherigen Grafik sehen wir den *Bitcoin*-Preis der letzten 5 Jahre.
    - Es ist leicht erkennbar, wie empfindlich oder volatil der Preis ist.
        - Die **X**-Achse steht für die Zeit und die **Y**-Achse für den Preis in USD.

Welche globalen Ereignisse könnten mit den Preisveränderungen zusammenhängen?

Welche Faktoren bestimmen also den Preis?

Welche Rolle spielt das Mining?

Wann wirkt sich das Halving auf den Preis aus?

- Die Nachfrage nimmt weiterhin stetig zu.
- Das Emissionssystem ist unveränderlich.
- Es handelt sich um einen aufstrebenden Vermögenswert, der gerade erst reguliert wird.
    - Natürlich ist mit Preisschwankungen zu rechnen.
    - Sein Preis ist jedoch seit seiner Entstehung gestiegen

Analysiere den historischen Preis-Chart von Bitcoin.

ColinTalksCrypto.com

Mittel- und langfristige Faktoren

- Faktoren, die den Preis von *Bitcoin* bestimmen, können mittel- und langfristig analysiert werden. Als nächstes werden wir jeden von ihnen genauer betrachten.

Mittelfristige Faktoren:

- ***Täglicher Handel***
    - Ungleich zu anderen Finanzmärkten, wird es 24 Stunden 7 Tage die Woche gehandelt.
    - Transaktionen können über mobile Geräte getätigt werden.
        - Erlaubt den einfachen Umtausch von *Bitcoin* in beliebiger Höhe.
    - Für *HODLer* ist dies ein Albtraum, da sich der Preis an einem einzigen Tag
    - Für *Trader* ist dies eine Gelegenheit, diese Preisänderungen auszunutzen und Gewinne zu machen.
- ***Weltweite Nachrichten und Ereignisse***
    - Sensibel für internationale Ereignisse, Nachrichten und Spekulationen.
- ***Mining-Kosten***
    - Die Miner sind dafür verantwortlich, dass immer mehr *Bitcoin* zum Gesamtangebot hinzugefügt werden.
    - Wenn die Stromkosten steigen, sind Miner gezwungen 40-60 % ihrer *Bitcoin* zu verkaufen, um Rechnungen und Hardware-Kosten begleichen zu können.
- ***Marktblasen***
    - In den letzten Jahren sind die *Bitcoin*-Käufer vielfältiger geworden und ihre Kauf- und Spargewohnheiten haben sich verändert.
    - Der Umfang ihrer Beteiligung und ihr Verhalten im *Bitcoin*-Netzwerk können den allgemeinen Preis von *Bitcoin* verändern.
- ***Staatliche Regulierungen***
    - Die Regulierung von Kryptowährungen

nimmt täglich zu, was den Wert von *Bitcoin* beeinflussen kann.

- Joe Biden hat ein Gesetz erlassen, wonach Transaktionen mit digitalen Vermögenswerten im Wert von mehr als 10.000 US-Dollar von nun an an die *Steuerbehörde* gemeldet werden müssen.

Langzeitfaktoren:

• ***Halving***

- Die Blocksubvention wird ungefähr alle vier Jahre halbiert.

- Die Belohnungen für die Miner sinken zu diesen Zeiten drastisch.

• ***Massenadaption***

- Wenn jeder anfängt *Bitcoin* zu benutzen, ein Prozess, der ***Hyperbitcoinisierung*** genannt wird, und dadurch mehr Geld in *Bitcoin* investiert wird, wird der Preis exponentiell steigen.

1998 2005 2014 2021

2012 2013 2014 2021

• ***Der Lindy-Effekt***

- ist eine Theorie über die Alterung von unverderblichen Dingen.

- Je älter eine Idee oder Technologie ist, desto höher ist die Lebenserwartung.

- Unverderbliche Dinge, wie z. B. Technologie, altern linear in umgekehrter Richtung.

• ***Begrenztes Angebot***

- Die Tatsache, dass es nur eine endliche Menge an *Bitcoin* gibt, bedeutet, dass es nicht möglich ist, das System nach 2140 zu verwässern.

- Der **„Regenbogen-Chart“** verwendet eine logarithmische Skala, um den *Bitcoin*-Preis zu visualisieren.

○ Die Farbeinteilung:

- zeigt an, wann die Währung unterbewertet ist (blaue und grüne Zone).

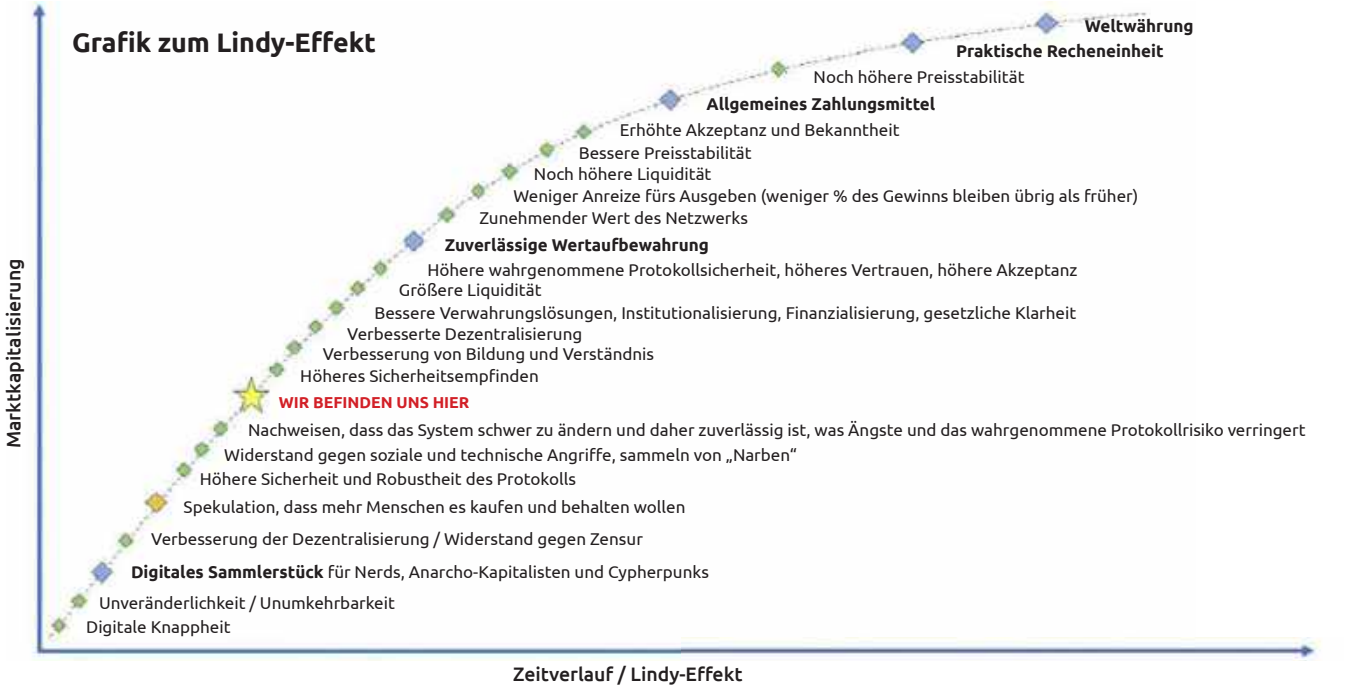
- oder wenn sie überbewertet ist (orange, rote und violette Zonen).

○ ***Dieses Diagramm liefert*** uns wertvolle Informationen, um Strategien für den Kauf und Verkauf von *Bitcoin* festzulegen.

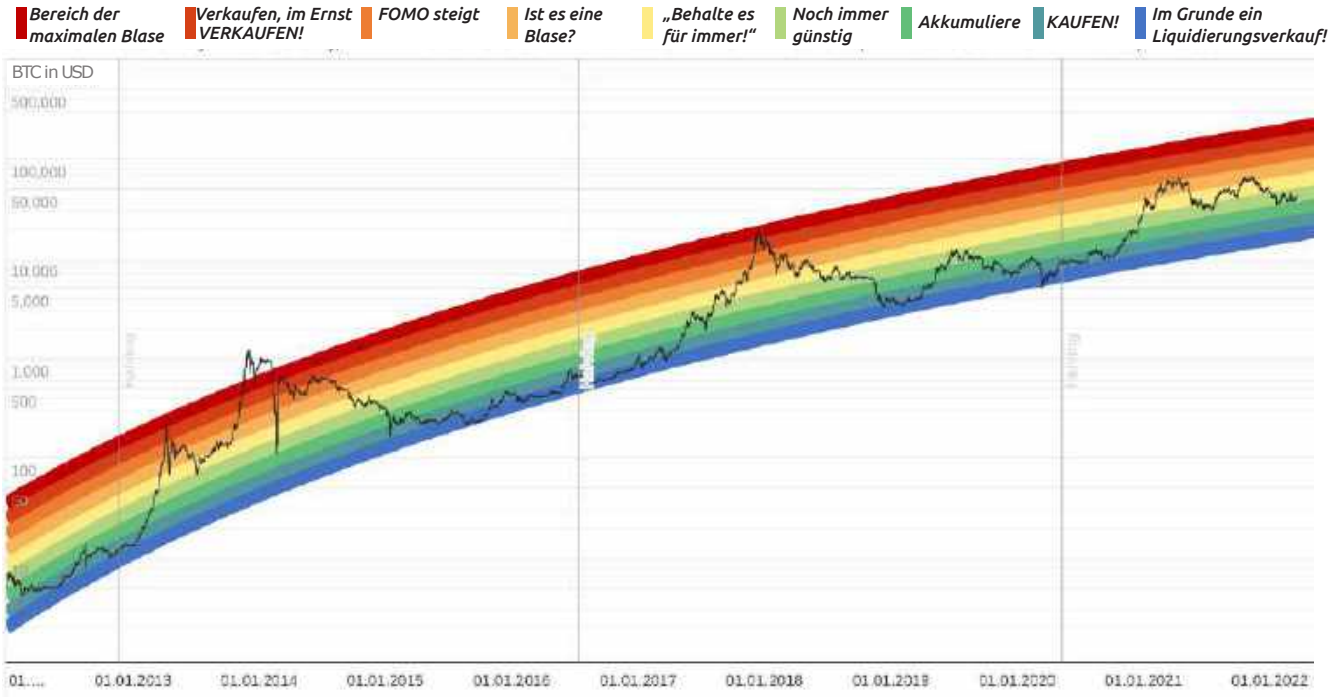
○ Einige sehr erfolgreiche Investoren warten geduldig:

- Sie kaufen wenn der Preis die blaue/grüne Zone erreicht.

- Sie verkaufen nach und nach, während der Preis den roten Bereich erreicht.



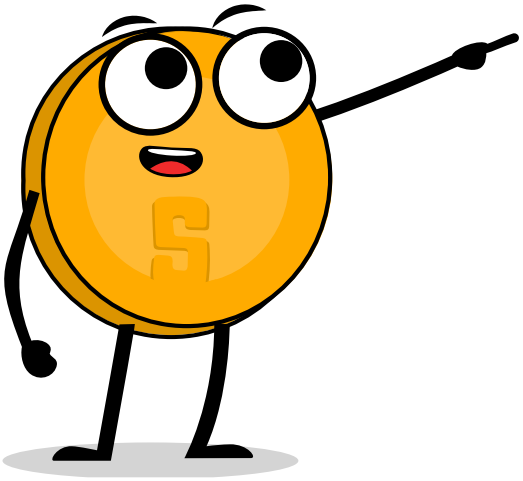
Regenbogen-Chart



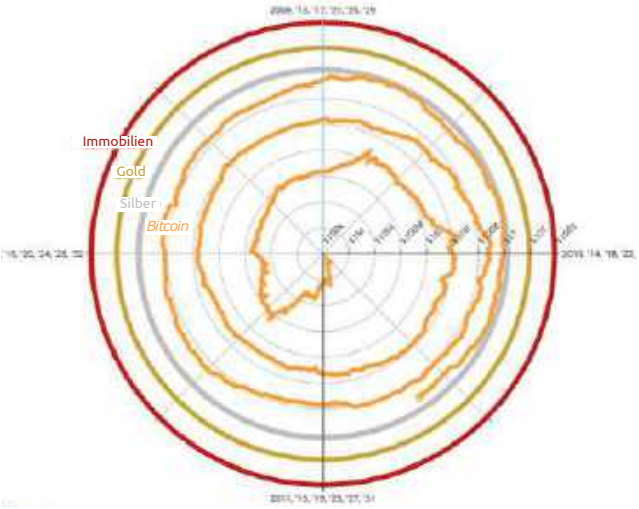
Knappheit, Kosten, Preis und Volatilität

- Betrachten wir die *Bitcoin*-Kapitalisierung im Vergleich zu anderen globalen Vermögenswerten und hinsichtlich der Vier-Jahres-Zyklen.

  - In der Grafik rechts sehen wir die *Bitcoin*-Marktkapitalisierung im Vergleich mit Gold, Silber und Immobilien.



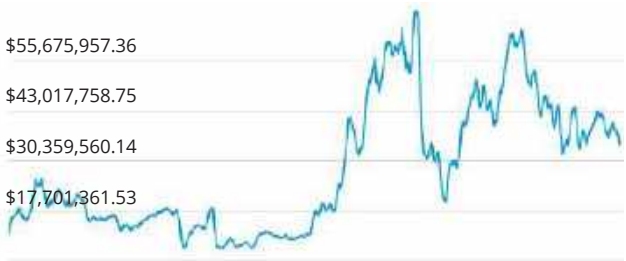
Cross-Asset-Spirale



8.4 Die Belohnung für die Miner

- Schauen wir uns an, wie sich die Belohnungen und monetären Anreize für Miner im Laufe der Zeit verändert haben, und halten wir fest, dass es Zeiten gibt, die profitabler sind als andere.

  • Der Anreiz für die Miner bleibt trotz der geringeren Belohnungen bestehen, da der Wert von *Bitcoin* langfristig steigt.



Gesamteinkommen der Miner
$34,688,409.61

Die Difficulty (Schwierigkeitsanpassung)

- Die Difficulty ist ein Maß dafür, wie schwierig es ist, einen *Bitcoin*-Block zu minen,

  • oder um einen Hash zu finden, der unter dem vorgegebenen „Zielwert" liegt.

- Die Difficulty wird alle 2016 Blöcke angepasst (ca. alle 2 Wochen),

  • sodass die durchschnittliche Blockzeit zehn Minuten beträgt.

- Die Difficulty-Einstellung hängt direkt mit der *gesamten Mining-Leistung* zusammen.

  • Sie wird in Terahash/Sekunde angegeben (TH/s). (Tera = Billion)

    - Das heutige Netzwerk hat die Kapazität, Billionen von Hashes pro Sekunde zu berechnen.

- Je höher die Difficulty, desto mehr Rechenleistung wird benötigt, um die gleiche Anzahl von Blöcken zu finden, was das Netzwerk sicherer gegen Angriffe macht.

8.5 Auf wen oder was muss man achten?

Obwohl ***Bitcoin*** einen weitaus größeren Schutz bietet als das traditionelle Finanzsystem, werden die Betrügereien mit ahnungslosen Opfern immer raffinierter. Zum Beispiel:

- Identitätsdiebstahl

• Die Angreifer können den Empfänger dazu zwingen, sensible Informationen preiszugeben.

- Sie stehlen seine Anmeldedaten, nachdem sie ihn dazu aufgefordert haben, sein Passwort zu ändern.
- Sie stehlen seine **privaten Schlüssel** und folglich seine ***Bitcoin***.
- Sie locken ihn auf eine Malware-Website und übernehmen die Kontrolle über seinen Computer.

- DNS- oder Browser-Erweiterungs-Hijacking:

• Die Angreifer kapern legitime Websites.

- Sie ersetzen sie durch betrügerische Schnittstellen.
- Sie bringen Benutzer dazu, ihre **privaten Schlüssel** auf diesen falschen Seiten einzugeben.

- Ein Hacker kann die SIM-Karten von zwei Handys austauschen und alle Daten stehlen.

• Cyber-Kriminelle versuchen, jede Situation auszunutzen. Unternehmen und Sicherheitsteams haben Mühe, damit Schritt zu halten.

Angriffe auf Bitcoin

https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md

- Keiner dieser Angriffe hat es geschafft, das ***Bitcoin***-Netzwerk zu schädigen.
- Wenn die **privaten Schlüssel** an einem sicheren Ort aufbewahrt werden:

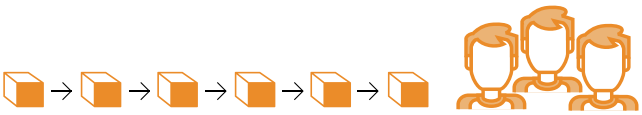
• werden Angriffe praktisch unmöglich.

- Trotzdem besteht eine geringe Chance für eine 51%-Attacke.

Knappheit, Kosten, Preis und Volatilität

Was ist eine 51%-Attacke?

- Um dies zu erreichen, bedarf es Arbeit, Energie und zentraler Datenverarbeitung.



Die meisten Miner aggregieren und übermitteln Blöcke an die öffentlichen Blockchain.

Ein Angreifer fügt Blöcke einer privaten Blockchain hinzu und übermittelt sie nicht der öffentlichen Blockchain.

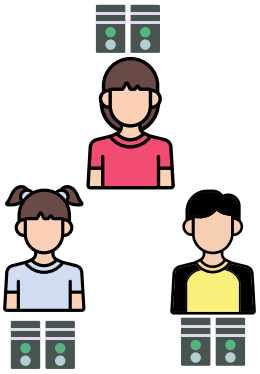
- Ein böswilliger Miner müsste mehr als 50 % der Rechenleistung des Netzwerkes besitzen.

  • Das Netzwerk *wäre nicht mehr dezentral*, jedoch kontrolliert und manipuliert durch besagtem Miner.

  • Eine neue Kette wird erstellt, die an die ursprüngliche Kette angehängt wird.

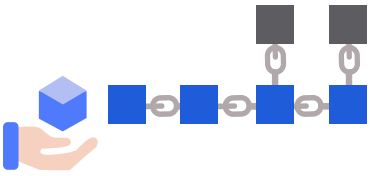
    - Dies würde einige Teilnehmer dazu verleiten, ihre Blöcke an die neue Kette hinzuzufügen.
    - Man könnte die Kette leicht zum eigenen Vorteil *manipulieren, verändern oder beeinflussen.*
    - Man kann Geld durch Doppelausgaben stehlen und/oder Transaktionen zensieren.

- Diese Art von Angriff hat es bei ***Bitcoin*** noch nie gegeben.



In PoW-basierten Netzwerken gibt es mehrere Teilnehmer (Mining-Nodes), die neue Blöcke hinzufügen und die Informationen in der Blockchain bestätigen.

Die Miner konkurrieren miteinander, um das Recht zu gewinnen, dass ihre Version eines neuen Blocks von der Mehrheit der Teilnehmer bestätigt wird.



Lektion 9

Bitcoin – heute und in der Zukunft

9.1 Energienutzung
9.2 Innovation
- Software – Bitcoin Core
- SegWit, Taproot und Schnorr-Signaturen
- Taro

9.3 Bitcoin und die Zukunft von El Salvador
9.4 Übung: Bitcoin-Simulator

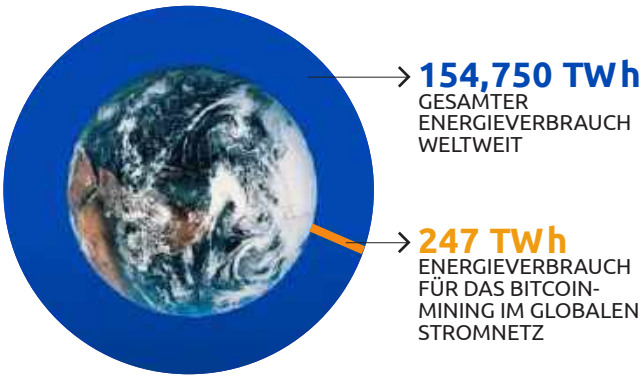
Bitcoin – heute und in der Zukunft

9.1 Energienutzung

Nutzt Bitcoin wirklich so viel Energie wie angenommen?

Steigerung der Einnahmen:

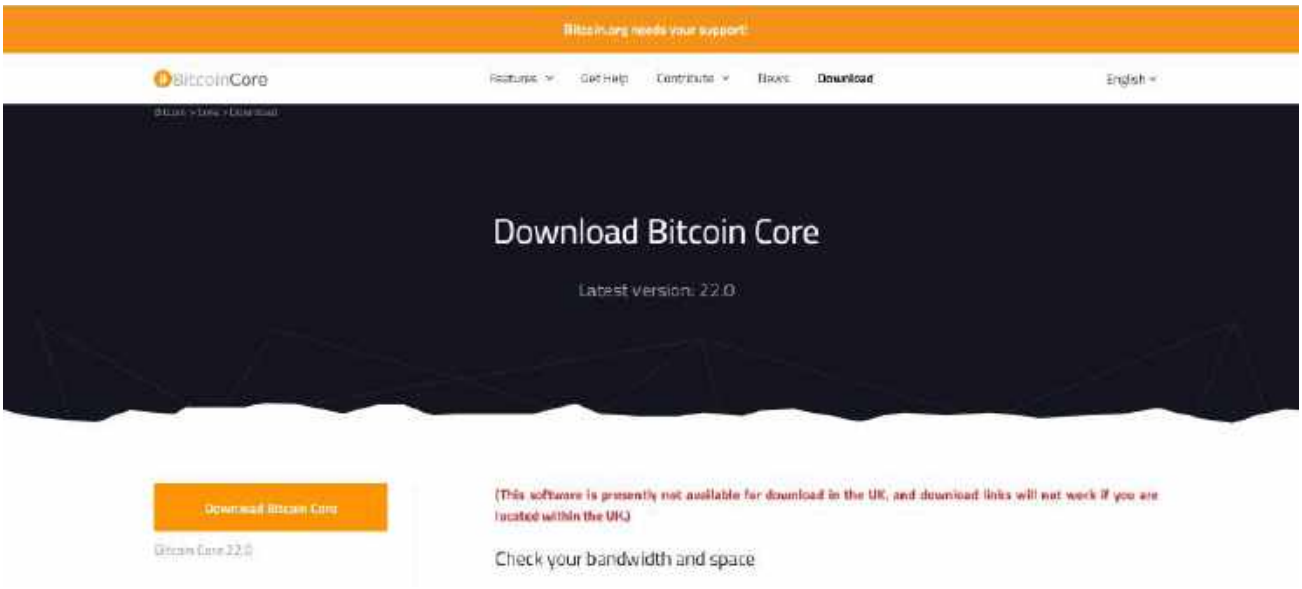
- Die Miner verbinden eine große Anzahl von Computern,
  - um ihre Chancen zu erhöhen, mehr *Bitcoin* zu erhalten.
- Die Computer laufen nahezu rund um die Uhr, Tag und Nacht, um die „Lotterien" zu gewinnen.
  - Aus diesem Grund ist der Stromnutzung sehr hoch.
- Die für das *Bitcoin*-Mining verwendete Technologie wird jeden Tag sauberer,
  - sodass dabei der Anteil der nachhaltigen Energie im April 2022 auf 59,5 % angestiegen ist.
- Obwohl die *Bitcoin*-Hashrate seit 2021 innerhalb eines Jahres um 23 % angestiegen ist,
  - ist der Stromverbrauch für das BTC-Mining 25 % niedriger als Anfang 2021.
- Die ASICs aus dem Jahr 2022 sind 100 Milliarden Mal schneller als die CPUs von 2009.
- Im Jahr 2022 entsprach die von *Bitcoin* genutzte Energie 0,16 % der weltweiten Energienutzung.



9.2 Innovation

Software – Bitcoin Core

- Bitcoin Core ist die ursprüngliche, von Satoshi Nakamoto entwickelte Software,
  - die so gestaltet ist, dass man sich mit Personen verbinden kann, die dasselbe Programm ausführen.
    - Dadurch wird ein Netzwerk von Computern geschaffen, die miteinander kommunizieren.
  - Somit arbeiten alle mit den gleichen Regeln, sobald man die Software runtergeladen hat,
    - um Transaktionen zu validieren
    - und zur Sicherheit und Dezentralität des Systems beizutragen.
  - Wer es ausführt, kann es wie jedes andere Programm installieren,
    - wobei eine zusätzliche Kopie der gesamten Blockchain runtergeladen und erstellt wird.
    - Dies ermöglicht auch die Übertragung der Transaktionen an andere Computer.
  - Solange man Internetzugang hat, kann man ohne Genehmigung:
    - die Software kostenfrei runterladen und/oder verwenden.
    - *Bitcoin* an andere Wallets senden oder von anderen erhalten.
    - das Angebot der Emission nachweislich verifizieren.
    - Erkenntnis über die Transaktionsgeschichte sowie die Eigentümer aller *Bitcoin* erlangen.
- Dutzende Software- und Kryptographie-Experten arbeiten an der Erhaltung und Verbesserung des Systems.
  - Wenn jemand eine Aktualisierung der Software vorschlägt, braucht er die mehrheitliche Zustimmung derjenigen, die sie implementieren sollen.



Offener Quellcode

Jeder kann ihn einsehen, Änderungen vorschlagen, modifizieren und nach Belieben weitergeben. Es ist vergleichbar mit einem Restaurantbesuch, bei dem man Zugang zu den Rezepten (dem Code) seiner Lieblingsspeisen hat ... aber dann kann man sie zubereiten und alle Zutaten, die man möchte, hinzufügen oder weglassen und die Speisen verfeinern.

SegWit, Taproot und Schnorr-Signaturen

Bitcoin wurde durch Konsens verbessert, durch Bitcoin Improvement Proposals, BIPs. Dadurch wurde es im Laufe der Jahre sicherer und effizienter gemacht.

- Erstens, ***SegWit*** – eine Soft-Fork, die im Jahr 2017 implementiert wurde.

  • Durch das Entfernen von Teilen der Transaktionen wurde die Begrenzung der Blockgröße erhöht.

  • Dadurch wurde die Verarbeitungsgeschwindigkeit von Bitcoin-Transaktionen verbessert.

  • Eine Schwachstelle im Protokoll wurde behoben, die es den Nodes ermöglichte:

    - Transaktionen (TxID) im Netzwerk zu manipulieren.
    - Die ***Manipulation*** einer Transaktion bedeutet, dass ein Angreifer den Hash einer Transaktion in der Blockchain modifizieren oder abändern kann.

- Zweitens, ***Taproot*** – wurde geschaffen, um die Privatsphäre zu verbessern und die Anonymität im Netzwerk zu erhöhen.

  • Taproot kann Transaktionen „tarnen".
  • Die Validierungszeiten der Transaktionen wurden verkürzt.

    - Dies könnte zur Förderung von *Bitcoin* als Zahlungsmittel beitragen.

  • Die Transaktionsgebühren könnten erheblich reduziert werden.

- Die Ersetzung des ***Elliptic Curve Digital Signature Algorithm (ECDSA)*** durch ***Schnorr***-Signaturen.

  • Dabei werden mehrere Schlüssel in eine komplexe Transaktion integriert und eine einzige Signatur erstellt.
  • Es vereinfacht Smart Contracts auf der Blockchain.
  • Es hilft bei der Skalierung von Zahlungskanälen auf dem Second-Layer, wie z. B. dem ***Lightning-Netzwerk***.

Taro

- Mit dem neuen Protokoll ***Taro*** soll die ***Bitcoin***-Technologie auf die nächste Stufe erhoben werden.
- Es wird die Emission von Stablecoins und anderen Vermögenswerten im Lightning-Netzwerk ermöglichen.
- Man kann jede Währung sofort und praktisch kostenlos in eine andere umtauschen.

9.3 Bitcoin und die Zukunft von El Salvador

- Die Originalität und die Möglichkeiten von ***Bitcoin*** haben Aufmerksamkeit auf sich gezogen:

  • von der Investmentwelt.
  • von der Unternehmenswelt.

    - Sowohl öffentliche als auch private Unternehmen sind den gleichen Auswirkungen der Inflation und der Zinsunterdrückung auf die Ersparnisse ausgesetzt.
    - Sie versuchen ihre Bilanzen zu stärken.
    - Sie verfügen über große Bargeldreserven.
    - Sie nehmen ***Bitcoin*** als langfristigen Wertspeicher an.

- El Salvador wird in Zukunft wahrscheinlich einen riesigen Vorteil gegenüber der Welt haben.

  • Es hat als erstes Land ***Bitcoin*** als gesetzliches Zahlungsmittel zugelassen, zusammen mit dem US-Dollar.

    - Bitcoin Beach ist bereits ein robustes und solides Projekt. Dabei wurde in einer Küstengemeinde erfolgreich eine Kreislaufwirtschaft geschaffen.

  • Der IWF und die Weltbank haben sich gegen diese Entscheidung ausgesprochen.

    - In der Zwischenzeit akkumuliert El Salvador weiter Satoshis.

- Welches Land wird das nächste sein, das ***Bitcoin*** zum gesetzlichen Zahlungsmittel machen wird?

  • Die Länder, die die Adaption früher durchführen, werden wahrscheinlich am meisten profitieren.

- Der US-Dollar scheint kurz vor dem Zusammenbruch zu stehen, während der Rubel (Russland)

und der Yuan (China) in der Geopolitik immer wichtiger werden.

- Beide sind Fiat-Währungen, die mit ***Bitcoin*** konkurrieren.

- Verschiedene Länder versuchen, ***digitale Zentralbankwährungen*** (CBDCs) einzuführen:
  - Das sind Versuche, Fiat-Geld mit digitalen Vorteilen zu schaffen.
  - Das bedeutet aber auch, dass die Regierung jede Transaktion überwachen kann.

Wer kauft Bitcoin?

- Russland will ***Bitcoin***-Zahlungen für Öl und Gas akzeptieren.
- Rio De Janiero will die Bezahlung der Grundsteuer mit ***Bitcoin*** akzeptieren.
- Einige Städte in den USA sind bereit, Steuerzahlungen in ***Bitcoin*** zu akzeptieren.
- Einige US-Regierungsbeamte nehmen bei ihren Gehaltszahlungen ***Bitcoin*** an.

- Bitcoin in der Zukunft:
  - Es wird massive Innovationen bei Second-Layer-Lösungen ermöglichen.
  - Es wird Verträge, Vermögenswerte und Nutzerdaten im privaten und öffentlichen Bereich modernisieren.
  - Es wird die Länder ermutigen, zu kooperieren, anstatt zu konkurrieren.
  - Es wird das Bestreben, die Volkswirtschaften durch das Drucken von Geld zu manipulieren, beenden.
  - Es könnte sogar sein, dass Länder und Nationalstaaten aufhören zu existieren und etwas Neues an ihre Stelle tritt, mit Hilfe von ***Bitcoin*** ... Wer weiß?

„Ob du glaubst, dass du es kannst oder nicht kannst –in beiden Fällen hast du recht.“

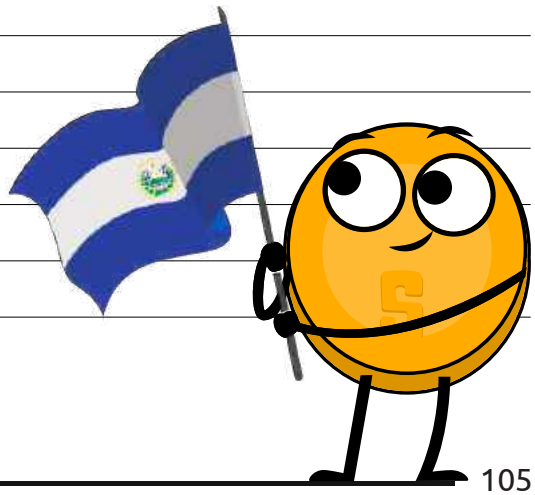
- Henry Ford

Gemeinschaftsübung: Beantworte die folgenden Fragen auf der Grundlage deiner Erkenntnisse aus den letzten Lektionen!

Was sind deiner Meinung nach die wichtigsten Vorteile von ***Bitcoin***?

Was könnte deiner Meinung nach in den nächsten zehn Jahren in El Salvador passieren?

Glaubst du, dass die Salvadorianer sich mit ***Bitcoin*** vertrauter machen und es als eine wichtige Technologie betrachten werden?



9.4 Übung: Bitcoin-Simulator

https://www.bitcoinsimulator.tk/blockchain?

Gemeinschaftsübung: Befolge folgende Anweisungen:

Erstelle eine neue Wallet!

Wir haben bereits eine Wallet erstellt – ***MiPrimerBitcoin.***

Der **private Schlüssel** lautet:
e17a9fe1f9cade3f1f8b6426f9fdabe27d0378d931fc8bb5bbb1d25d7c33e6e5

Es wurden zwei Blöcke gemined (2830, 2831) und eine Transaktion durchgeführt.

Du kannst nun also folgendes tun:

1. Mine einen Block, um deine ersten ***Bitcoin*** als Prämie zu erhalten!
2. Signiere Transaktionen und sende ***Bitcoin*** an andere Wallets!
3. Erstelle deine eigene private Blockchain und nutze den Simulator mit nicht-öffentlichen Gruppen oder Schulklassen!
4. Erstelle gefälschte Transaktionen unter falschem Namen und versuche, ***Bitcoin*** durch Betrug zu erhalten!
5. Führe einen 51%-Angriff durch, um später die Blockchain zu manipulieren!
6. Sprich mit anderen Menschen darüber!

Je mehr du verstehst, wie Bitcoin funktioniert, desto besser!

Lektion 10

Abschlussarbeit

- Warum Bitcoin?

Abschlussarbeit

Warum Bitcoin?

Praktische Übung: Schreibe einen ein- bis zweiseitigen argumentativen Aufsatz und achte darauf, alle folgenden Punkte zu berücksichtigen:

- Erkläre, was ***Bitcoin*** ist!
- Erkläre, wie ***Bitcoin*** funktioniert!
- Nenne mindestens zwei Aspekte, wie ***Bitcoin*** deiner Meinung nach die Funktionsweise der heutigen Welt verändert! Begründe deine Antwort!

Zusatzlektion

Die Magie der digitalen Signaturen

- Öffentliche und private Schlüssel
- Die digitale Signatur
- Gültige Transaktion

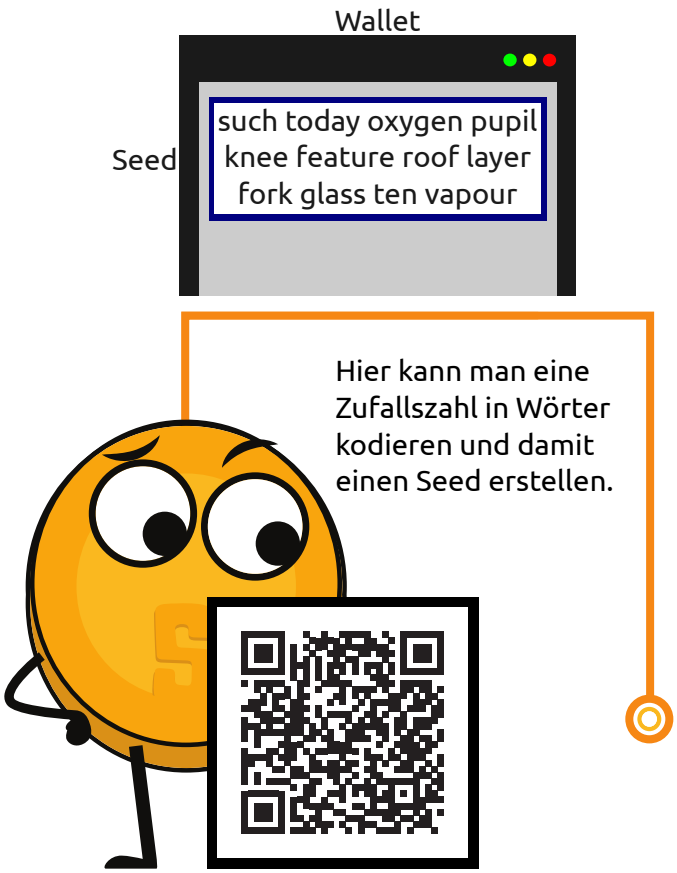
Die Magie der digitalen Signaturen

Öffentliche und private Schlüssel

Nachdem wir nun die Sicherheitsanforderungen verstanden haben, wollen wir zu den Wallets und Transaktionen zurückkehren.
Die meisten der sichersten Wallets bieten:

- einen „**privater Haupt-Schlüssel**“ oder ein „***Seed***“.
  - Es handelt sich um eine für die Wallet zufällig generierte Liste von 12 bis 24 Wörtern.

    - Niemanden sonst auf der Welt, außer dem Wallet-Nutzer, werden diese Wörter angezeigt.
    - Er ist der einzigartige Schlüssel, der den Zugriff auf die ***Bitcoin*** des Benutzers auf jedem Gerät ermöglicht.
    - Er wird als Ausgangspunkt für die Erstellung der einzelnen **privaten Schlüssel** verwendet.



https://learnmeabitcoin.com/technical/mnemonic

- Jeder **private Schlüssel** erzeugt einen **öffentlichen Schlüssel**.

- Jeder **öffentliche Schlüssel** ermöglicht es uns, eine ***Transaktion*** digital zu ***signieren***.

- Jede ***Transaktion*** ist mit einer eindeutigen **digitalen Signatur** versehen.

- Jede **Signatur** ermöglicht den Transfer von ***Bitcoin*** an eine bestimmte ***Adresse***.

Lass uns ins Detail gehen:
- private Key = privater Schlüssel
- public Key = öffentlicher Schlüssel
- address = Adresse
- generate = generieren

- **Privater Schlüssel**:
  - Er ist vergleichbar mit einem Passwort und muss vor Dritten sicher aufbewahrt werden.
  - Im Falle eines Verlustes der Wallet bietet er eine Möglichkeit, den Zugang zu den ***Bitcoin*** wiederzuerlangen.
  - Es sei denn, man hat einen ***„Seed“***.
    - Private Schlüssel sind völlig zufällige und sehr große Zahlen zwischen 1 und 1.157.920.892.373.161.954.235.709.850.086.879.078.528.375.646.427.907.490.438.605.163.141.518.161.494.336.
  - Jeder private Schlüssel wird in eine hexadezimale Struktur umgewandelt:
    - eine Zahl von 0-9, A-F, wobei A=10, B=11 und so weiter.
  - Es ist praktisch unmöglich, denselben privaten Schlüssel zweimal zu erzeugen.

Mit folgendem Link kannst du die Erstellung eines privaten Schlüssels üben.

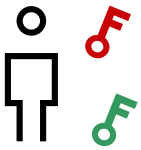
Learn Me a Bitcoin

https://learnmeabitcoin.com/technical/private-key

- **Öffentlicher Schlüssel**:
  - Es wird der **private Schlüssel** als Eingabedaten,
    - sowie eine sehr fortschrittliche mathematische Multiplikation verwendet, um den **öffentlichen Schlüssel** zu erzeugen.
  - Der Vorgang ist unidirektional – er kann nicht rückgängig gemacht werden.

https://learnmeabitcoin.com/technical/public-key

Beispiel für einen privaten Schlüssel



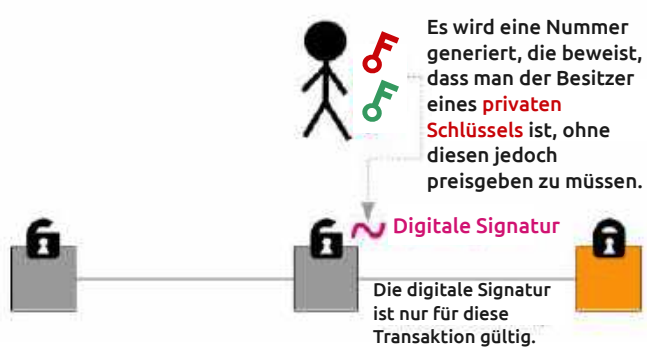
45871748790247694263681256141218050962540558073528157656117113257366684871118

28165556693891620773477477574559423752792107203189219630880988688806282470022 5

Der öffentliche Schlüssel wird aus dem privaten Schlüssel berechnet.

Die digitale Signatur

- Sie dient dazu, zu beweisen, dass wir den privaten Schlüssel kennen, ohne ihn öffentlich preiszugeben.
- Sie wird anhand des privaten Schlüssels und der in der Transaktion enthaltenen Informationen berechnet.
- Sie ist einzigartig, unwiederholbar und unmöglich zu fälschen.
- Sie ist obligatorisch, um die *Bitcoin* zu entsperren, die der Emittent übertragen will.



Lasst uns kurz darüber nachdenken …

Wenn ein Hacker deine Transaktion abfängt, glaubst du, dass er in der Lage sein wird, deinen privaten Schlüssel zu knacken und dein Geld zu stehlen? Das heißt, angenommen, eine böswillige Person hat Zugang zu der Adresse, an die du Bitcoin schickst, denkst du, er könnte sie in seine eigene Wallet umleiten?

Gültige Transaktionen

Der Zweck einer **digitalen Signatur** ist es, zu zeigen, dass man der Besitzer eines **öffentlichen Schlüssels** ist.

- Die Miner überprüfen die Signatur mit dem **öffentlichen Schlüssel** des Ausstellers.

- Die kryptografische Überprüfung ist ähnlich wie:
  - der Nachweis, dass das letzte Teil eines Puzzles richtig passt.
  - Wenn die Transaktion auch nur im Geringsten verändert wird:
    - ändert sich der Signatur-Hash automatisch, wodurch die Signatur falsch und veraltet ist.
    - Es ist extrem einfach, Transaktionen zu erkennen, die abgelehnt werden sollten.

Quellen

1. The Free Silver Movement, Scott Wolla, Federal Reserve Bank of St. Louis https://www.stlouisfed.org/-/media/project/frbstl/stlouisfed/education/lessons/pdf/the-free-silver-movement-and-inflation.pdf.

2. Video – ¿Qué es el Dinero? MagicMarkers. TV, Colombia. https://youtu.be/2yCIKkq8gKA.

3. Functions and Characteristics of Money, Chapter 3, Segment 301, Federal Reserve Bank of Philadelphia, https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/functions-and-characteristics-of-money-lesson.pdf.

4. „Why Money", Bonnie T. Meszaros, Federal Reserve Bank of Philadelphia, https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/money-grades-6-8.pdf.

5. „Focus on the Fed - Grade 9 –12", Federal Reserve Bank of Kansas, https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf.

6. Geschichte von 1870 bis 1971 in 10 Minuten, Robert Breedlove, Für den Abschnitt 1870-1914, https://www.forbes.com/sites/nathanlewis/2013/01/03/the-1870-1914-gold-standard-the-most-perfect-one-ever-created/?sh=70c6dc4a4a6a.

7. Video – Economia Desde Cero: Dinero, Canal Encuentro, Argentina, https://youtu.be/zcYw8a4RJC4.

8. „Focus on the Fed - Grade 9 –12", Activity 5, Auction, Federal Reserve Bank of Kansas, https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf.

9. Video – Qué es la Inflación, Banco de la República de Colombia, Colombia, https://youtu.be/gkDQGribCfc.

10. Video – ¿Cómo Nos Vigilan en Internet?, Magic Markers, https://youtu.be/-sWgOuFIaws.

11. McDonalds Menü,1973, https://muddyrivernews.com/opinion/daily-dirt-where-were-you-in-72-or-once-upon-a-time-when-a-big-mac-was-65-cents/20220323091958/.

12. McDonalds Menü, 2022, McDonalds, El Salvador, Twitter.

13. Video – Causas de la Infación, Banco de la República, Colombia.

14. Declining purchasing power of the US dollar strengthens Bitcoin, Toju Ometoruwa, https://cryptopotato.com/is-there-a-pattern-between-usd-dow-jones-and-bitcoin/.

15. Ejemplo de Estado de Cuentas, https://www.ejemplode.com/59-finanzas/4274-ejemplo_de_estado_de_cuenta.html.

16. Video – ¿Qué es Bitcoin y Cómo Funciona?, MagicMarkers.TV, Colombia, https://youtu.be/S2HxMK7iO4c.

17. Querying the Bitcoin blockchain with R, http://beautifuldata.net/2015/01/querying-the-bitcoin-blockchain-with-r.

18. Video – Que es La Red Relámpago, Whiteboard Crypto en Español, https://youtu.be/lD8WQbS8-T8.

19. Bitcoin in numbers, Nick Carter, Bitcoin Demystified.

20. Bitcoin, Will the Price of Bitcoin Rise or Fall?, Capital.com Research Team, 08:00 (UTC), 31 March 2022, https://capital.com/de/bitcoin-prognose.

21. U.S. dollar inflation visualized at the top versus bitcoin's deflation at the bottom, Lark Davis, @TheCryptoLark.

22. https://www.bitcoincharts.com

23. https://www.blockchaincenter.net/en/bitcoin-rainbow-chart/

24. https://www.blockchain.com/charts/miners-revenue


Mi
Primer
Bitcoin
EL SALVADOR