BITCOINEXPLAINED

HANDOUT

Teil 1

Basiswissen für alle Einsteiger

INHALT

Handout zum Basiswissen-Kurs von BITCOINEXPLAINED.DE

Geldsystem und Grundkenntnisse Bitcoins

GESCHICHTE DES GELDES

Geld dient als Tauschmittel, welches nicht direkt konsumiert oder zur Produktion von Waren eingesetzt wird. Stattdessen ist es durch seine Akzeptanz in der Gesellschaft **zu einem späteren Zeitpunkt einsetzbar**, um Güter zu akquirieren, welche für die Produktion von Waren oder für den eigenen Konsum benötigt werden.

- Ohne einheitliche Währungen bleibt nur der **direkte Tausch** von Waren
- Je größer die Volkswirtschaft, desto schwieriger der direkte Handel, da mehr angebotene Waren auch zu einer größeren Menge Umrechnungskurse führen
- Bei 1.000 unterschiedlichen Waren sind es fast eine halbe Million Umrechnungskurse
  Formel: $\frac{n(n-1)}{2}$, n ist die Anzahl der angebotenen Güter

Weitere Voraussetzungen zum direkten Tausch:

- Übereinstimmung der Bedürfnisse - wird mit wachsendem Angebot unwahrscheinlicher
- Übereinstimmung der **Maßstäbe** - was man erwerben möchte, ist möglicherweise nicht gleichwertig mit dem, was man selbst anbieten kann
- Übereinstimmung des **Zeitrahmens** - ein Geschäft mit verderblichen Gütern ist problematisch, da deren Lagerung für einen Tausch über längere Zeiträume nicht möglich ist
- Übereinstimmung des **Ortes** - Handel mit ortsgebundenen Gütern ist kompliziert, da sich das begehrte Gut möglicherweise an einem anderem Ort befindet

Diese Voraussetzungen machen den direkten Tausch von Gütern sehr unpraktisch. Damit Menschen ihre Bedürfnisse effizienter befriedigen können, findet noch eine andere Form des Handels statt: der **indirekte Tausch**. Der indirekte Tausch ist mit Gütern sinnvoll, welche **liquider** sind, d. h. sich einfacher und schneller verkaufen lassen als die, die man selbst anbietet. Für eine Wirtschaft mit vielen Teilnehmern ist die beste Lösung, ein einzelnes oder wenige Ersatzgüter als zwischengelagertes Tauschmittel zu benutzen.

Geld ist nicht dafür gedacht direkt konsumiert zu werden, somit ist eine Wertstabilität vorausgesetzt.

Geld kann **physisch** getauscht werden oder als **Forderung** abgetreten werden, wobei die Zahlung der Geldsumme zu einem späteren Zeitpunkt erfolgt.
Folgende Gegenstände wurden in der Geschichte als Geld benutzt:

- Physische Tauschmittel: Perlen, Muscheln, Glas, besondere Steine, Salz, Vieh, verzierte Tierzähne, Felle, Kupfer, Silber, Gold oder auch Alkohol und Zigaretten
- Forderungen: Inschriften auf Stein- und Tontafeln, Markierung in Rai-Steinen (ab dem 14. Jh. entstand die doppelte Buchführung und somit ebenfalls eine Zentralisierung durch den Buchhalter)

Je nach Situation und Stand der Technik haben oder hatten alle dieser Zahlungsmittel eine wichtige Gemeinsamkeit: Die Schwierigkeit, die Versorgung drastisch zu erhöhen und dabei dasselbe zu entwerten.

FUNKTION DES GELDES

Geld muss die Funktion als **Tauschmittel** erfüllen, damit der indirekte Handel ermöglicht wird. Geld muss als **Recheneinheit** geeignet sein, damit der Marktpreis verschiedener Waren in festen Einheiten angegeben werden kann.
Geld muss als **Wertspeicher** dienen. Die Wertaufbewahrungsfunktion ist besonders wichtig, da Geld auch zu einem späteren Zeitpunkt einsetzbar bleiben muss.

EIGENSCHAFTEN DES GELDES

Was macht Geld nun aber zu Geld?
Verschiedene Ökonomen haben dem Geld im Laufe der Geschichte unterschiedliche Eigenschaften für Geld definiert. Einige dieser Eigenschaften finden sich häufig wieder:

- **Transportabel** - Kleine als auch große Summen müssen leicht transportiert werden können
- **Haltbar** - Geld befindet sich ständig im Umlauf und sollte sich somit nicht abnutzen
- **Teilbar** - Nach einer Teilung muss der Wert in Summe gleich bleiben
- **Fungibel** - Für einen problemlosen Tausch müssen alle Einheiten dieselben Eigenschaften besitzen
- **Verifizierbar** - Jeder Marktteilnehmer muss das Geld prüfen und die Echtheit erkennen können
- **Wertstabil** - Geld muss seine Kaufkraft über lange Zeiträume erhalten

SOLIDES GELD

Damit Geld wertstabil bleibt muss es **schwer reproduzierbar** sein. Die Menge des sich im Umlauf befindenden Geldes darf nicht einfach erhöht werden können und muss durch Arbeits- bzw. Energieaufwand limitiert sein.

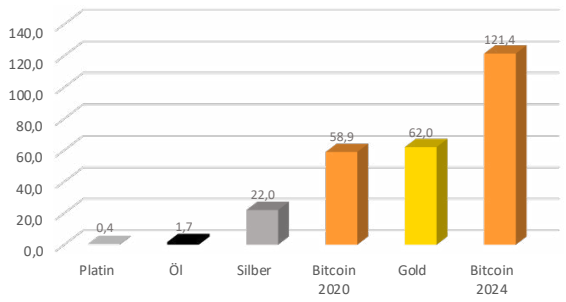
- Begrenzung der Produktion des Gutes, welches als Geld gewählt wird bestimmt die Härte
- Ein limitierter Nachschub des Gutes schafft Sicherheit und stabilisiert seinen Wert
- Gold ist solides Geld, da es enormen Aufwand zur Förderung braucht und von Natur aus limitiert ist

STOCK-TO-FLOW

Das Stock-To-Flow-Verhältnis macht die **Härte des Geldes messbar**. Es beschreibt das Verhältnis zwischen dem gesamten Bestand eines Gutes und seiner Produktionsmenge. Je größer das Stock-To-Flow-Verhältnis, desto geringer ist die Inflation des Gutes. So braucht es bspw. 62 Jahre bei der momentanen Fördermenge, um den bereits vorhandenen Goldbestand zu verdoppeln (stand 2020), da Gold nicht zerstörbar ist und alles jemals geförderte Gold noch immer vorhanden ist. Warum das Stock-To-Flow-Verhältnis für die meisten Güter eine Rolle spielt, soll folgendes Beispiel verdeutlichen:
Wir gehen von einem starken Anstieg der Nachfrage nach Gold aus. Der Goldpreis steigt dadurch rasant und durch den hohen Preis wird die **jährliche Produktion verdoppelt** (Minen produzieren mehr).

Für alle anderen Güter würde die Verdopplung der Produktion die vorhandenen Lagerbestände winzig erscheinen lassen, wodurch der Preis sofort fallen würde. Nicht so bei Gold, da die Bestände des vorhandenen Goldes stetig mitwachsen und es **praktisch unmöglich ist, Mengen zu fördern, die dem Goldpreis schaden**.
Seit 1942 hat das jährliche Wachstum der Goldbestände die 2%-Marke allerdings auch nie überschritten.

$$\frac{\text{Stock}}{\text{Flow}} = \frac{\text{Gesamtbestand}}{\text{Jährlich produzierte Menge}}$$



FIATGELD

Der Begriff „fiat" hat seinen Ursprung im Lateinischen (Fiat-lux = es werde Licht). Fiatgeld ist Geld, das per Dekret, also auf Befehl erschaffen wird und weder über einen Fundamentalwert verfügt, noch ein Zahlungsversprechen beinhaltet und somit gewissermaßen **aus dem Nichts** entsteht (Fiatgeld = es werde Geld).
Dieses **per Erlass** auferlegte Geld soll keine Wahl bieten, andere Zahlungsmittel zu verwenden. Es ist keine Währung oder kein Geld, welches am freien Markt auf Grund seiner Eigenschaften gewählt wurde.
Der Begriff wurde ursprünglich für Bargeld benutzt. Bargeld kann einzig und allein von der entsprechenden Zentralbank ausgegeben werden. Die Menge des sich im Umlauf befindlichen Bargelds kann auf unterschiedliche Weise erhöht werden:

- Geschäftsbanken fragen von sich aus mehr Bargeld nach
- Durch sog. Offenmarktgeschäfte kauft die Zentralbank Forderungen von den Geschäftsbanken ab
- Die Regierung erhöht das Zentralbankguthaben durch Ausgaben

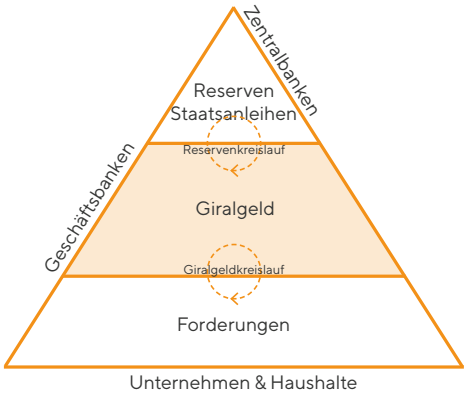
Neben dem Zentralbankgeld existiert auch das sogenannte **Giralgeld**, welches von Geschäftsbanken beispielweise bei der Kreditvergabe an Privatpersonen oder Unternehmen erzeugt wird.

KREDITGELDSYSTEM

In den Bilanzen der Banken erscheint das gedruckte bzw. virtuell erstellte Geld entweder als Forderung oder als Verbindlichkeit. Guthaben auf dem Kundenkonto ist für die Bank eine **Verbindlichkeit**, da dieses theoretisch jederzeit von den Kunden abgehoben werden kann. Giralgeld wird deswegen auch Kreditgeld genannt, da es nichts anderes ist als ein **Versprechen** der Banken das Geld in das gesetzliche Zahlungsmittel zu tauschen. Kredite, die von den Banken vergeben werden, erscheinen auf der bilanziellen Aktivseite als **Forderung** für die Banken. Durch eine Kreditvergabe kommt es zu einer Bilanzverlängerung des Kreditgebers. Wenn ein Kredit zurückgezahlt wird, kommt es zu einer Bilanzverkürzung. Die Menge des Geldes, die durch dieses Verfahren geschaffen werden kann, **ist unbegrenzt**.

Geld ist immer ein Schuldverhältnis. Zahlungsmittel der oberen Stufen stellen immer Verbindlichkeiten gegenüber den unteren Stufen dar.
Privatpersonen oder Unternehmen haben Forderungen gegenüber den Geschäftsbanken. Die Geschäftsbanken haben alle Konten bei der Zentralbank und können die darauf vorhandenen Reserven gegen Bargeld eintauschen und umgekehrt. Die Einlagen der Geschäftsbanken auf den Konten der Zentralbank sind also eine Verbindlichkeit aus Sicht der Zentralbank.

Staatsanleihen sind Zahlungsversprechen der zentralen Regierung des Staates. Diese können unbegrenzt emittiert werden und werden in Europa von der EZB über den Sekundärmarkt von den Geschäftsbanken aufgekauft, da die EZB diese nicht direkt kaufen darf, um direkte Staatsfinanzierung zu vermeiden. Eine der Aufgaben der EZB ist es, die **Bank des Staates** zu sein.



DEFICIT SPENDING

Die Defizitfinanzierung der Staaten wurde durch die Aufhebung des Goldstandards und vor allem auf Grund der Finanzierung von Kriegen ermöglicht.
Mittlerweile wird das gleiche Prinzip aber auch von Sozial- und Wohlfahrtsstaatlern benutzt. Hohe Staatsausgaben können normalerweise nur mit einer hohen Steuerlast finanziert werden. Um es in den Worten von Alan Greenspan (ehemaliger Vorsitzender der Federal Reserve Bank in den Vereinigten Staaten) zu sagen, „ist der Wohlfahrtsstaat ein Mechanismus der Regierung, welcher das Vermögen der produktiven Mitglieder einer Gesellschaft konfisziert, um damit Sozialhilfeprogramme zu finanzieren". Ob nun ein Krieg oder Sozialprogramme des Staates mit Defiziten finanziert werden - eine Sache ist für die Regierung wichtig, um die Macht zu erhalten: die Steuerlast muss möglichst niedrig bleiben.
Um ein solches Programm mit einer niedrigen Steuerlast zu vereinbaren, muss sich der Staat daher Geld borgen, indem Staatsanleihen ausgegeben werden. Bei einem gedeckten Geld (Goldstandard) ist die Summe des Kredites, den eine Volkswirtschaft tragen kann, von den vorhandenen greifbaren Werten abhängig, wie Goldreserven. Eine Defizitfinanzierung ist also bei einem Goldstandard limitiert. Ohne diese Limitierung können Kredite in unlimitierter Höhe geschaffen werden, da die Banken und Zentralbanken die Staatsanleihen wie greifbare, gedeckte Güter oder tatsächliche Einlagen ähnlich Gold behandeln. Der Staat verspricht also das geliehene Kapital durch spätere Steuereinnahmen wieder zurückzuzahlen. Es werden also **zukünftige Generationen in die Schuld genommen, um den heutigen Wohlstand zu finanzieren**.

Eine weitere Folge ist, dass durch die ständige Ausweitung dieser Praxis mehr Forderungen ausstehend sind als Vermögenswerte vorhanden. Unweigerlich erhöht sich daher die Menge der Forderungen im System relativ zu den materiellen Gütern der Wirtschaft und führt zu steigenden Preisen. Im Umkehrschluss verlieren die Ersparnisse der produktiven Mitglieder der Gesellschaft an Wert.

Wenn die Schöpfung von Währungen also einer zentralen Instanz obliegt dann ist die Versuchung immer groß diese Macht auszunutzen. Das Szenario der Geldmengenausweitung wiederholt sich im Laufe der Geschichte immer wieder. **Zentralisierung von Macht und Zentralisierung von Geldschöpfung führen unausweichlich zur Entwertung des Geldes**, dem Zerfall von Währungen und letztendlich zum Zerfall von eben jenen staatlichen Strukturen.

Die Geldentwertung wird mittlerweile sogar als Mandat gesehen. 2% Inflation sollen die Wirtschaft stimulieren oder helfen mit der Produktivität mitzuhalten.

Der Grund ist allerdings eigentlich unser Schuldgeldsystem. Würde eine Deflation stattfinden oder eine Währung benutzt werden, die nicht ständig an Kaufkraft verliert, würde es zu fallenden Steuereinnahmen, fallenden Asset-Preisen und einer nominalen Aufwertung von Schulden kommen. Durch die Überschuldung des Systems haben Schuldenabbau und Preisdeflation allerdings weitreichende Folgen für Banken, Staaten und Unternehmen. Durch das Kreditgeldsystem **sind niedrige Zinsen notwendig**, da die Schuldner (Privatpersonen, Unternehmen und Staaten) sonst nicht mehr zahlen könnten. Auf Unternehmensebene sorgt dieser Zustand für sogenannte „Zombiefirmen", für die das Erfolgskriterium nicht mehr darin liegt einen Mehrwert für die Gesellschaft zu schaffen, sondern darin, sichere Finanzierungen zu niedrigen Zinsen zu erhalten.

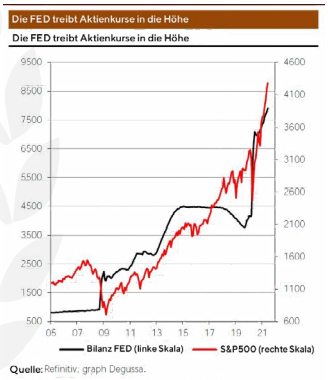
Niedrige Zinsen und Kontrolle durch den Staat sind also ein Muss um das System weiterhin zu erhalten.

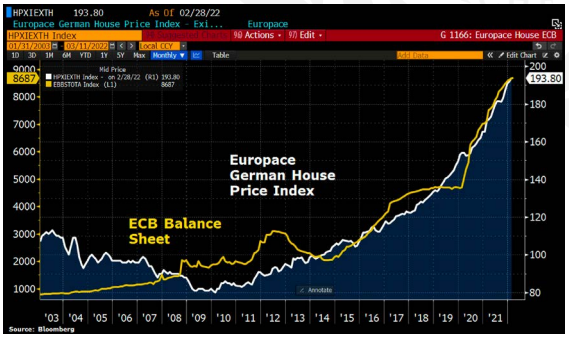
CANTILLON-EFFEKT

Der Cantillon-Effekt beschreibt die Auswirkung einer **Veränderung der Geldmenge** auf die verschiedenen Marktteilnehmer.
Die konstante Erhöhung der Geldmenge und die damit einhergehende Entwertung des Geldes führt dazu, dass das Einkommen und Vermögen der Besitzer schwinden, während das Vermögen derjenigen steigt, **die das neu geschaffene Geld zuerst erhalten**. Benannt ist diese Umverteilung nach dem gleichnamigen Ökonomen: Richard Cantillon. Er veröffentlichte eine Schrift, in der er zeigte, in welcher Weise die Veränderung der Geldmenge das Wirtschaftsgeschehen berührt. Cantillon argumentiert, dass ein Ausweiten der Geldmenge **zunächst** zu einem Aufschwung führt. Doch ein solcher Aufschwung erweist sich als nicht nachhaltig. Es muss früher oder später in einer Finanz- und Wirtschaftskrise enden. Er stellte außerdem fest, dass das Ausweiten einer Geldmenge niemals neutral verläuft.

Das bedeutet, dass in einem inflationären Szenario eine **Umverteilung des Vermögens von Gläubigern zu Schuldnern** stattfindet, da die Schuldner das Geld zuerst erhalten und es somit noch zu vorinflationären Preisen ausgeben können. Die Tilgung der Schulden erfolgt auf die ursprüngliche Geldmenge. Ein Verkauf der vorher erworbenen Güter, Leistungen, Immobilien oder Ähnlichem erfolgt jedoch zu einem späteren Zeitpunkt für mehr Geld. Für die Gläubiger bedeutet dies, dass sich die Kaufpreise zu ihren Ungunsten ändern.

Neugeschaffenes Geld landet meistens zuerst bei den Banken, die es weiterverleihen können oder nutzen können, um zu einem frühen Zeitpunkt Vermögenswerte, wie bspw. Aktien, zu erwerben. Für alle späteren Käufer, die das Geld erst erhalten, nachdem es weiter durch den Wirtschaftskreislauf geschleust wurde, sind die Preise der Vermögenswerte schon gestiegen. Somit kann auch erklärt werden, warum viel billiges Geld zuerst zu einem Aufschwung führt, **letztendlich aber nicht substanziell ist**, da die Unternehmen bspw. unter schlechten Absatzperspektiven leiden. Die Erhöhung der Geldmenge und somit Ausweitung der Zentralbankbilanz führt ebenso zu steigenden Assetpreisen.
Die sogenannte **Asset Price Inflation** oder das Ansteigen der Aktien- und Immobilienmärkte lässt sich nicht mehr ausschließlich durch die Produktivität der Wirtschaft erklären, sondern vor allem durch das Ansteigen der Geldmenge und der Ausdehnung der Zentralbankbilanzen. Hier kann man die vorher beschriebene Umverteilung erkennen (siehe Charts).





FOLGEN DES FIATGELD-SYSTEMS

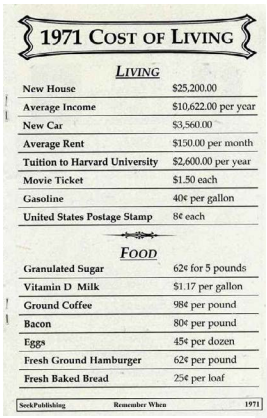
Das Fiatgeld-System bringt einige Nachteile mit sich:

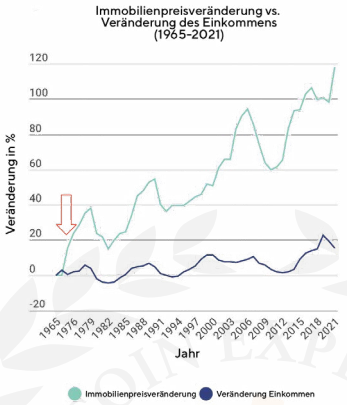
- Die gesamte Geldmenge ist außer für die Zentralbank nicht validierbar
- Es besteht immer die Abhängigkeit von einer Zentralbank im Hinblick auf Geldmenge und Zinsen
- Zahlungsströme sind immer unter zentraler Kontrolle und Teilnehmer des Systems können somit jederzeit ausgeschlossen werden (Einfrieren von Konten etc.)

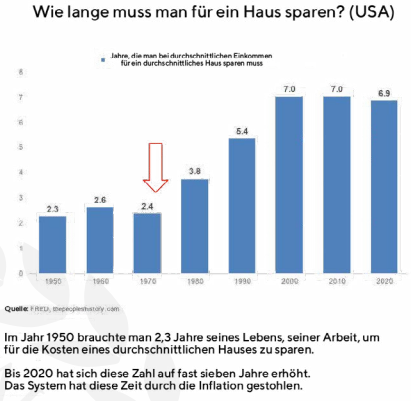
FOLGEN DES FIATGELD-SYSTEMS

Von 775 Fiatwährungen, die bisher existierten befinden sich bereits 599 nicht mehr in Zirkulation oder wurden ersetzt. 156 dieser Währungen wurden durch eine Hyperinflation zerstört.

Im Gegensatz zu rohstoffbasiertem Geld, wie Goldmünzen, ist Fiatgeld nur durch das Vertrauen in die Regierung oder dem ihr zur systemischen Sicherung unterstellten Militärapparat gedeckt.
Folgen dieses Systems sind allumfassend und beeinflussen nahezu alle Lebensbereiche, da Geld als Informations- und Tauschmittel in der Gesellschaft ebenso nahezu alle Lebensbereiche berührt.

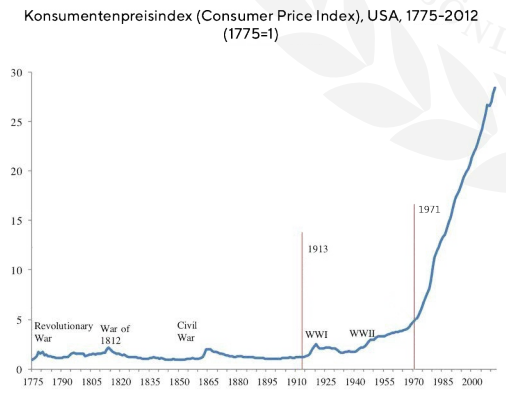


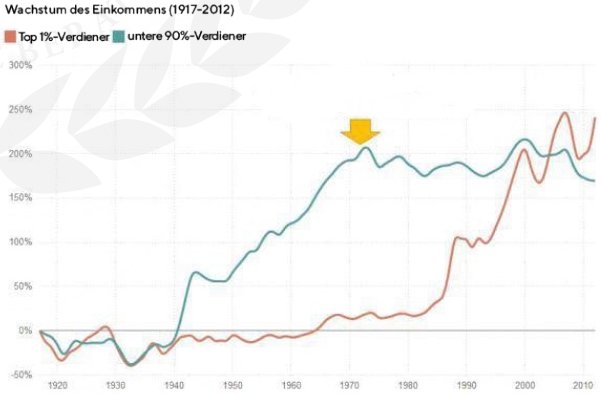




Seit 1971 (Aufhebung des Goldstandards) kann man beobachten, dass die Lebenshaltungskosten und Assetpreise stark steigen, während sich das Einkommen nicht proportional dazu verändert. Dies führt zu Ungerechtigkeiten, sozialen Problemen (wie z. B. Altersarmut, Wohlstandseinbußen und Vermögensumverteilung) und letztendlich sozialen Verwerfungen.

Fehlanreize in der Wirtschaft durch zu viel billiges Geld sind der Grund für Fehlinvestitionen und somit die Ursache für Blasenbildung an den Märkten (bspw. Dotcom-Blase 2000, Immobilienblase 2008, Everything-Bubble 2021).





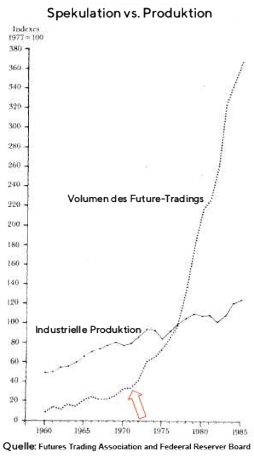
Quelle: Bureau of Labor Statistics, Historical Statistics of the United States, and Reinhart and Rogoff (2009).

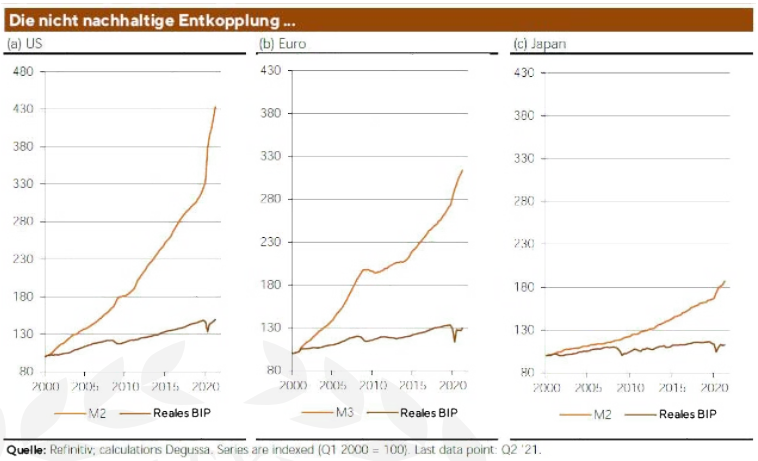
Die Konsumentenpreise steigen stetig, was **nicht** auf Gier von Unternehmen, sondern auf Kaufkraftverlust des Geldes zurückzuführen ist. Nichtsdestotrotz steigen die Einkommen der Top 1% begünstigt durch bspw. den Cantillon-Effekt immer weiter.

Der Verlust der Kaufkraft hat weitere Effekte, wie eine **hohe Zeitpräferenz**. Dies bedeutet, dass weniger gespart wird und Geld direkt verkonsumiert wird. Schneller Konsum führt zu Überproduktion, sinkender Qualität der Produkte und bspw. auch zu Umweltverschmutzung und Ressourcenverschwendung.

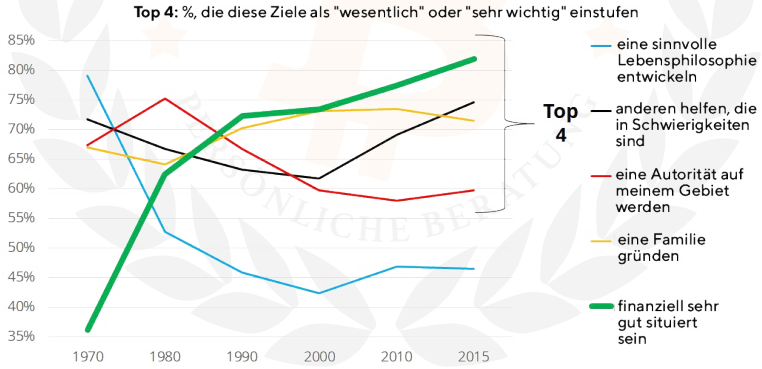
FOLGEN DES FIATGELD-SYSTEMS

Ohne die Möglichkeit zu sparen ist man gezwungen zu investieren oder zu spekulieren, um so die Kaufkraft seines Geldes zu erhalten. An den Finanzmärkten führt dies, wie weiter oben beschrieben zu Fehlanreizen und Spekulationsblasen. Es entsteht ein Delta zwischen der realen Produktion und den Finanzmärkten.





Weiterhin steht die Geldmengenausweitung schon lange nicht mehr im Verhältnis zum realen Wirtschaftswachstum.
Doch auch **soziale Effekte** sind erkennbar, wie die nächste Statistik zeigt. Für einen Großteil der Menschen hat der Wunsch finanziell in einer guten Position zu sein, den Wunsch ein bedeutungsvolles Leben zu führen ersetzt. Existenzielle Sorgen sind somit vorherrschend für die meisten Menschen.



Defizitfinanzierung und das Fiatgeld-System ermöglichen die Finanzierung von immer fortwährenden Kriegen, welche nur schwer möglich wären wenn diese durch Steuereinnahmen finanziert werden müssten.

INFLATION

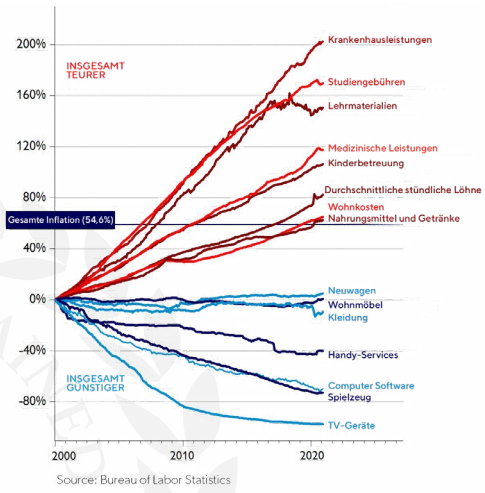
Inflation ist ein oft missverstandener und für die meisten Menschen schwer greifbarer Begriff.
Im Sinne der österreichischen Denkschule, welche sich vor allem der Markt- und Geldtheorie widmet, **ist Inflation die Ausweitung der Geldmenge**. Aus dieser Ausweitung der Geldmenge geht die Teuerung von Produkten als Folge hervor. Diese klassische Definition wurde später im Zuge der keynesianischen Theorien, wie der „Modern Monetary Theory" geändert.
Mittlerweile wird die Inflation anhand eines Warenkorbes definiert. Dieser Warenkorb soll sich aus Gütern zusammensetzen, die ein normaler Haushalt alltäglich benötigt und verbraucht. Darunter fallen Güter wie Benzin, Lebensmittel, Hygieneprodukte und Ähnliches.

INFLATION

Aus diesem Warenkorb wird der Konsumentenpreisindex (Consumer Price Index - CPI) abgeleitet. Der Warenkorb **kann sich ständig ändern und neu definiert werden**.

Zentralbanken erschaffen Geld vor allem dann, wenn bspw. eine wirtschaftliche Krise droht. Neues Geld soll den Konsum und Investitionen stimulieren, um zu verhindern, dass eine Rezession eintritt. Wenn die Geldmenge allerdings schneller steigt als die Wirtschaftsleistung der Volkswirtschaft (Bruttoinlandsprodukt oder Gross Domestic Product - GDP), dann führt das zur Teuerung der Güter, da diesen plötzlich mehr Geldeinheiten gegenüberstehen.

Über die letzten 20 Jahre kann man beobachten, dass vor allem Güter, bei denen staatliche Intervention stattfinden, im Preis gestiegen sind. Dies betrifft bspw. Medizin, Bildung und Wohnungen.Technologie hingegen ist nicht so stark reguliert, unterliegt damit größeren Innovationen und ist deshalb sehr deflationär, was zu fallenden Preisen führt. Die roten Linien unterliegen den Eingriffen von staatlicher Regulierung, während die blauen Linien eher den Kräften des freien Marktes unterliegen.



Die zentrale Intervention im Markt durch bspw. Subventionen oder steuerliche Anreize führt ebenso wie viel billiges Geld zu falschen Signalen und **verhindert, dass der freie Markt wirken kann**.

Wenn die Geldmengenausweitung zu schnell vonstatten geht, kann es vor allem in wirtschaftlich schwierigen Zeiten zu **Hyperinflationen** kommen.

Die Folgen davon sind fatal:

- Die Währung wertet im Gegensatz zu anderen Währungen stark ab und verliert schnell an Kaufkraft
- Konsumenten bevorraten sich in Erwartung höherer Preise mit Verbrauchsgütern, was zu Lieferengpässen führen kann
- Konsumenten heben ihr Geld von den Banken ab und vermeiden es, neue Einzahlungen zu tätigen und verhindern somit die Möglichkeit der Banken, Geld weiter zu verleihen
- Weniger Produktion und Konsum bedeutet weniger Steuereinnahmen und zwingt Staaten ein Budgetdefizit in Kauf zu nehmen und bspw. Sozialleistungen zu streichen

In Ungarn 1946 fand die schlimmste Hyperinflation nach dem zweiten Weltkrieg statt, in der die tägliche Inflationsrate bei über 200% lag. Das bedeutet, **dass sich die Preise für alle Güter und Dienstleistungen alle 14,8 Stunden verdoppelten**. Dies ist nur eines von vielen Beispielen, wie Inflation und zentrale Planung Menschen in die Armut zwingt.

Im Jahr 2008 erreichte der Zimbabwe-Dollar pro Banknote einen „Wert" von 100 Billionen Dollar. Die Geschichte der Geldentwertung durch zentrale Kontrolle und Intervention reicht bis in das römische Reich zurück.

Es ist an der Zeit das Geldsystem zu revolutionieren.

BITCOIN

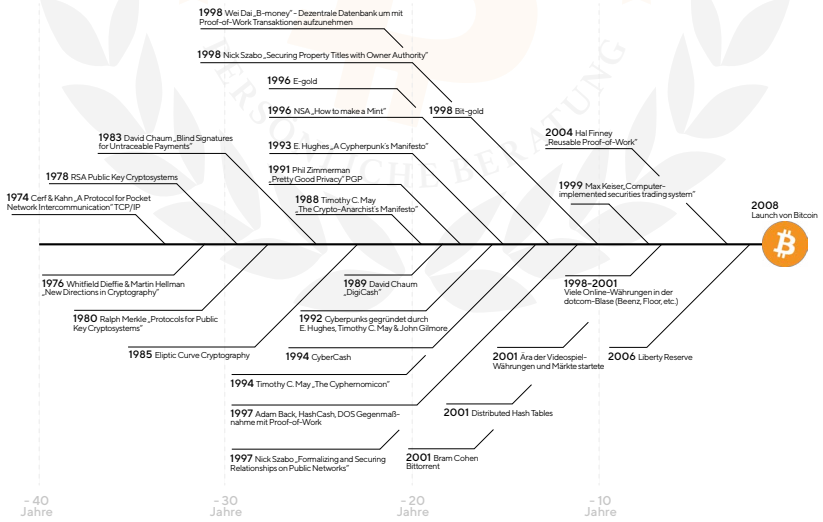
Was macht Bitcoin nun aber anders oder besser?
Bitcoin ist ein **offenes, dezentrales Netzwerk**. Es ist ein Open-Source-Internetprotokoll, welches von jedem eingesehen und validiert werden kann. Keine Institution, Stiftung, Unternehmen oder Team kontrolliert es oder kann Einfluss darauf nehmen. Es gibt keine zentrale Stelle und somit auch keinen einzelnen Angriffspunkt für das Netzwerk.

Man unterscheidet zwischen:
Bitcoin - das Netzwerk
Bitcoin - das Protokoll
Bitcoin - die Einheit

Bitcoin ist dadurch **zensurresistent, neutral, apolitisch und operiert weltweit** ohne Ländergrenzen. Ein Kommunikationskanal wie das Internet, Telefon, Radio oder Satellit reicht, um Teilnehmer des Netzwerks sein zu können. Jeder Netzwerkteilnehmer hat die Möglichkeit, Kontrolle über sein Geld (seine Bitcoin-Einheiten) auszuüben. Komplette Eigentumsrechte ohne staatliche oder institutionelle Kontrolle sind somit möglich.

Bitcoin hat einen im Protokoll fest vorgeschriebenen, unveränderbaren Schöpfungszeitplan und eine begrenzte Menge. Es wird niemals mehr als 21.000.000 Bitcoin geben. Jeder Bitcoin ist in 100.000.000 sogenannte Satoshis teilbar (ähnlich wie 1€ in 100 Cent teilbar ist). 1 Satoshi ist die kleinste Einheit im Netzwerk.

Die Entstehungsgeschichte von Bitcoin und den Vorgängern reicht bis in das Jahr 1974 zurück und ist aus einer Bewegung heraus entstanden, welche heute als „Cypherpunk-Movement" bekannt ist. Die Cypherpunks haben erkannt, dass eine zunehmende Digitalisierung des Geldes gewisse Gefahren birgt, da bei jeder elektronischen Zahlung immense Mengen an Daten über den Käufer preisgegeben werden. Es können Rückschlüsse auf den Lebensstil, die politische oder religiöse Gesinnung und die Vorlieben gezogen werden, wenn diese Daten vorhanden und gespeichert sind.



Es ist wichtig zu wissen, dass Bitcoin nicht, wie oft dargestellt, 2008 plötzlich entstanden ist, sondern auf vielen anderen technologischen Errungenschaften basiert und aufbaut. Dies macht Bitcoin, neben vielen anderen Eigenschaften, gegenüber anderen Coins und Tokens („Altcoins") überlegen.

„As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: boring grey in colour, not a good conductor of electricity, not particularly strong [..], not useful for any practical or ornamental purpose [..] and one special, magical property: can be transported over a communications channel."
- Satoshi Nakamoto (27.08.2010) -

BLOCKCHAIN

Bevor die weiteren Besonderheiten und Eigenschaften beschrieben werden, muss zunächst ein wichtiger Baustein erklärt werden, der das Fundament für die Funktionsweise bildet: die Blockchain (auch: **Timechain**).

Die Blockchain kann man sich als **öffentliches Register** vorstellen, welches alle jemals getätigten Bitcoin-Transaktionen in pseudonymer Form gespeichert hat. Dieses Register ist als Kopie auf alle Netzwerkknotenpunkte (sogenannte Nodes) verteilt und somit **nicht veränderbar und von jedem einsehbar**. Rückwirkend ist es nicht möglich etwas zu ändern und es gibt keine zentrale Stelle, welche bspw. einen Fehler bei der Eingabe einer Empfangsadresse korrigieren kann.
Im Bitcoin-Netzwerk ist jeder für sich selbst verantwortlich und muss für die eigene Sicherheit sorgen.

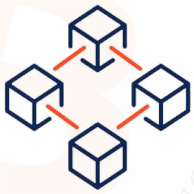
Bitcoin ermöglicht somit erstmalig echtes digitales Eigentum und weiterhin die Möglichkeit, seine eigene Bank zu sein.

Die Blockchain dient somit dazu, festzustellen, welche Werte zu welchen Adressen gehören. Es wird eine zeitliche Chronologie über die Transaktionen und somit über die Verteilung der Eigentumsrechte geschaffen.

1. Eine Transaktion wird im Netzwerk gestartet. Dies geschieht von einem kommunikationsfähigem Endgerät aus.

2. Die Transaktion wird innerhalb des gesamten Netzwerkes bekannt gegeben und im sog. Mempool gespeichert.

3. Die Transaktion wird durch Verwendung von asymmetrischer Kryptographie validiert. Dies ist eine digitale Signatur.



4. Aus der Sammlung aller unbestätigten Transaktionen (Mempool) werden zuerst die mit der höchsten angefügten Gebühr in den nächsten Datenblock aufgenommen.

5. Der neue Datenblock wird der Blockchain hinzugefügt. Der Konsens des Netzwerkes entscheidet über die gültige Kette.

6. Die Transaktion ist bestätigt und kann durch den Konsens im Netzwerk durch niemanden revidiert oder aufgehalten werden.

Technologisch gesehen basiert die Blockchain auf der sogenannten **SHA256-Verschlüsselung**, eine Form der Kryptographie. Dieser Verschlüsselung liegt eine nicht-umkehrbare mathematische Formel zu Grunde, welche die eingegebenen Daten in **eine immer gleich lange** (64 Zeichen) Zahlen- und Buchstabenkombination umwandelt. Wird die Formel mehrmals auf dieselbe Datenreihe angewendet, kommt immer dasselbe Ergebnis, der sogenannte „Hash" dabei heraus. Wird die eingegebene Datenreihe nur minimal verändert, dann ändert sich auch der Hash. **Man kann einen Hash also mit einem digitalen Fingerabdruck vergleichen.**

Das Wort „bitcoin" übersetzt sich bspw. in den Hash:
6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b
Wenn das Wort „Bitcoin" eingegeben wird dann erhält man den Hash:
b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

Ein Hash kann durch die nicht-umkehrbare Formel in einem öffentlichen Netzwerk identifiziert werden, ohne etwas über die enthaltenen Daten preiszugeben.

BLOCKCHAIN

Da in der Blockchain jeder neu erstellte Block im Prinzip ein Datenpaket ist, welches die getätigten Transaktionen enthält, kann auch hier ein Hash für jeden Block generiert werden. Dieser Hash verweist dann einzig und alleine auf den spezifischen Block. Zusätzlich enthält jeder Block den Hash vom vorherigen Block, wodurch die Reihenfolge klar nachvollziehbar wird. Denn wenn die Daten innerhalb eines Blocks geändert werden, ändert sich auch der Hash. Wenn der Block innerhalb der Blockchain schon weiter zurück liegt, dann müssten entsprechend alle nachfolgenden Blöcke ebenfalls wieder geändert werden, um die Änderung zu validieren.

Im Bitcoin-Netzwerk arbeiten die Miner immer an der längsten Kette (die Kette, in die am meisten Energie geflossen ist), da diese immer als Wahrheit angesehen wird. Wenn man nun eine in der Vergangenheit getätigte Transaktion ändern möchte, müsste man alle sich an den geänderten Block anschließenden Blöcke neu berechnen, neu „hashen", und zusätzlich noch schneller neue Blöcke generieren als der gesamte Rest des Netzwerkes. Dazu bräuchte man mindesten 51% der gesamten Rechenleistung im Netzwerk. Durch die dezentrale Struktur und der Verteilung der Bitcoin-Miner über verschiedene Kontinente, Firmen, Individuen und Interessengruppen ist dies allerdings nahezu unmöglich. Je länger die Blockchain wird, desto schwieriger wird es daher eine Änderung vorzunehmen. **Dies trägt zur Sicherheit von Bitcoin bei.**

Jeder Block hat weiterhin einen sogenannten „Nonce-Eintrag". Die Nonce ist die primäre Quelle für die Variation der Blockerstellung und sorgt dafür, dass Blöcke mit ansonsten äquivalenten Inhalten dennoch unterschiedliche Hashwerte aufweisen können.
Der Hash eines Blocks muss immer unter einem gewissen Schwellenwert liegen, damit er vom Netzwerk als valide angesehen wird. Dafür sorgt die Nonce. So definiert das Netzwerk die Anzahl der Nullen, die am Anfang eines jeden Block-Hashes stehen müssen. Dies erhöht weiterhin auch die Schwierigkeit für die Miner einen validen Block zu finden. Im Kapitel „Difficulty Adjustment" wird darauf später näher eingegangen.
Das Bitcoin-Netzwerk ist ein sogenanntes **Peer-to-Peer Netzwerk**, in dem alle Benutzer die gleichen Rechte haben und direkt miteinander verbunden sind. Das Netzwerk besteht aus den Nutzern, Nodes und Minern. Die Blockchain stellt das Register oder auch Kassenbuch dar, in dem alle Transaktionen festgehalten sind.

Für eine anschauliche Erklärung der Blockchain **empfehlen wir dieses Video** (EN).

Im Schnitt wird alle 10 Minuten ein neuer Block an die Blockchain angefügt. Die Miner bestätigen die Transaktionen und füllen dadurch die Blöcke mit Daten. Alle unbestätigten Transaktionen werden im Memory Pool oder auch kurz Mempool gesammelt und warten dort auf die Bestätigung. In der Regel kann man durch die Zahlung einer höheren Transaktionsgebühr als der Durchschnitt somit auch sicher sein, dass die eigene Transaktion im nächsten Block mit aufgenommen wird. Wenn ein neuer Block durch die Miner erstellt wurde, wird dieser im gesamten Netzwerk bekannt gegeben. Da jeder Teilnehmer die Möglichkeit besitzt, eine eigene Node, einen Knotenpunkt, zur Validierung der Blöcke zu betreiben, ist die Blockchain entsprechend als Kopie auf jeder dieser Knotenpunkte verteilt. Würde ein einzelner Teilnehmer etwas ändern, so würden die Nodes in der Kommunikation bemerken, dass bspw. der Hash des letzten Blocks bei der manipulierten Kopie ungültig ist und somit nicht anerkennen.

Eine Bitcoin-Node kann mit jedem beliebigen Computer betrieben werden, was zur weiteren Dezentralisierung beiträgt.

So reicht bspw. auch ein sogenannter
Raspberry Pi mit einer Festplatte, wie im Bild zu sehen.

Diese Netzwerk-Knotenpunkte garantieren, dass die im Bitcoin-Protokoll festgeschriebenen Regeln auch umgesetzt werden, da jeder Nutzer selbst entscheidet welche Version er benutzt, um die Node zu betreiben.

BLOCKCHAIN

Die Blockchain lässt sich, wie beschrieben, mit einem Kassenbuch vergleichen. Sie speichert also, mit welcher Adresse die Bitcoin verknüpft sind. Die Adressen sind vergleichbar mit herkömmlichen Bankkontonummern, nur dass sie im Bitcoin-Netzwerk statt Euro, Dollar etc. Bitcoin „enthalten".
Die Blockchain speichert jeden Kontostand und jede Bewegung in Form von Transaktionen seit Entstehung des Netzwerkes. Jede Transaktion jedes einzelnen „Kontos" ist aufgezeichnet und für jeden einsehbar. Dadurch entsteht **ein komplett transparentes Geldsystem**, jedoch kein transparentes Bankkonto.

Adressen sind mit keiner persönlichen Identifikation in dem Kassenbuch Blockchain verknüpft. Aber der Besitz von Bitcoin kann aus Beobachtung der Transaktionsverläufe abgeleitet werden. Jede kleinste Einheit Bitcoin (1 Satoshi = 1 Sat) kann mittels jeder Transaktion, in der sie involviert war, bis zu der ursprünglichen Erstellung zurückverfolgt werden. **Jede Transaktion ist innerhalb der Blockchain berücksichtigt**, alles summiert sich und passt perfekt zusammen - der Traum eines jeden Buchhalters. Wäre Bitcoin komplett anonym, wäre die Verifizierung der Integrität des Geldsystems als Ganzes nicht möglich.

Die Blockchain ist das Kassenbuch des gesamten Geldsystems, zu dem durchschnittlich alle 10 Minuten eine neue Seite mit Transaktionen hinzugefügt wird.
Würde man das Prinzip auf ein physisches Kassenbuch übertragen, so wäre eine Seite auf die Transaktionen der vergangenen 10 Minuten begrenzt. Die Häufigkeit, mit der die Seiten im Buch umgeblättert werden, um neue Transaktionen hinzuzufügen, ist daher begrenzt. Das Buch wächst stetig weiter, da die Seiten im Buch (analog zu den Blöcken der Blockchain) immer mit der vorherigen Seite verknüpft sind.
Der Zweck besteht nicht nur darin, neue Daten in die richtige chronologische Reihenfolge zu bringen, sondern auch darin die Blöcke digital zu verbinden, sodass jede Änderung an den vorherigen Blöcken zukünftige Blöcke ungültig macht. Das macht die Historie dieses Geldsystems **manipulationssicher**. Das Mining macht das System letztendlich **fälschungssicher** (siehe Abschnitt Mining).

KRYPTOGRAPHIE

Die asymmetrische Kryptographie, die im Bitcoin-Netzwerk verwendet wird, dient der Beweiserbringung und Kontrolle. Alle Nutzer können dadurch Transaktionen überprüfen und legitimieren. Durch diese Art der Kryptographie wird geprüft, ob die Transaktion durch den tatsächlichen Eigentümer des Guthabens initiiert wurde. Diese Überprüfung erfolgt durch zusammenhängende Schlüsselpaare und wird auch als **„Public-Key-Kryptographie"** bezeichnet.

Jeder Netzwerk-Nutzer hat ein digitales Schlüsselpaar, welches aus einem Public Key und einem Private Key besteht. Hierüber werden Adressen zum Versenden und Empfangen von Bitcoin erzeugt. Wenn man Bitcoin besitzt, so besitzt man eigentlich einen exklusiven, einzigartigen Private Key. **Der Private Key muss unter allen Umständen geheim bleiben**, da der Zugriff auf diesen Schlüssel mit dem Zugriff auf das Guthaben gleichgesetzt werden kann. Der Private Key verschlüsselt ausgehende Transaktionen, indem eine Signatur (Hash) erstellt wird, welche beweist, dass man im Besitz der Bitcoin ist, die man versenden möchte.
Nur der zugehörige Public Key kann die Nachricht/Transaktion wieder entschlüsseln.

KRYPTOGRAPHIE

Der Public Key dient dazu, die Signatur zu überprüfen und zu bestätigen. Der eigene Public Key, die Empfangsadresse, kann weitergegeben werden.
Die digitale Signatur ist also dazu da, um zu zeigen, dass man den Private Key kennt, welcher zu einem bestimmten Public Key gehört, ohne den tatsächlichen Private Key der Öffentlichkeit preizugeben. Durch den Hash wird ebenfalls wieder sichergestellt, dass für jede Transaktion eine eigene Signatur erstellt wird.

Bei der Erstellung der Adressen wird eine sogenannte „Trapdoor-Function" benutzt, welche es sehr einfach macht, die Public Keys aus den Private Keys zu generieren. Durch diese spezielle Programmierung ist es aber ebenso nahezu unmöglich die Kryptographie umzukehren und die Private Keys zu einem bekannten Public Key zu finden. Dies ist auf die Verwendung von den folgenden Techniken zurückzuführen: modulare Arithmetik, Exponentialfunktionen und sehr große Primzahlen. Der gesamten Kryptographie-Funktion von Bitcoin liegt daher die Mathematik zu Grunde (beruht auf der SHA-256-Verschlüsselung).
Kann nun jemand meinen Private Key erraten?
Rein theoretisch ist dies möglich. Allerdings würde es Unmengen an Rechenleistung kosten, um eine sogenannte „Brute-Force-Attack" durchzuführen, da der oder die Computer alle Zahlen durchgehen müssten, um schließlich einen Private Key zu finden. Die nachstehende Grafik verdeutlicht, wie unwahrscheinlich es ist, dies zu schaffen.

Stärke der Verschlüsselung in 2^n	Chance = 1 zu ...	
1	2	
10	1.024	
20	1.048.576	
27,06	139.838.160	6 Richtige + Superzahl bei Lotto 6 aus 49
30	1.073.741.824	
40	1.099.511.627.776	
50	1.125.899.906.842.620	
60	1.152.921.504.606.850.000	
70	1.180.591.620.717.410.000.000	
80	1.208.925.819.614.630.000.000.000	
90	1.237.940.039.285.380.000.000.000.000	
100	1.267.650.600.228.230.000.000.000.000.000	
110	1.289.074.214.633.710.000.000.000.000.000.000	
120	1.329.227.995.784.920.000.000.000.000.000.000.000	
130	1.361.129.467.682.750.000.000.000.000.000.000.000.000	
140	1.393.796.574.908.160.000.000.000.000.000.000.000.000.000	
150	1.427.247.692.705.960.000.000.000.000.000.000.000.000.000.000	
160	1.461.501.637.330.900.000.000.000.000.000.000.000.000.000.000.000	
170	1.496.577.676.626.840.000.000.000.000.000.000.000.000.000.000.000.000.	
180	1.532.495.540.865.890.000.000.000.000.000.000.000.000.000.000.000.000.000	
190	1.569.275.433.846.670.000.000.000.000.000.000.000.000.000.000.000.000.000.000	
200	1.606.938.044.258.990.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	
210	1.645.504.557.321.210.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	
220	1.684.996.666.696.920.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	
230	1.725.436.586.697.640.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	
230,186	1.962.577.783.683.320.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	Den privaten Schlüssel irgendeiner Wallet erraten
240	1.766.847.064.778.380.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	
256	115.792.089.237.316.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000	Den privaten Schlüssel einer bestimmten Wallet erraten

Der Private Key zu dem eigenen Wallet besteht aus einem randomisierten Binärcode, welcher aber durch ein Umrechnungs- bzw. Übersetzungsverfahren in Wörter übersetzt werden kann. So bestehen die Private Keys heutzutage aus 12-24 einzelnen Wörtern, damit man sich nicht die binäre Zahlenfolge merken muss, welche der Übersetzung in die Computersprache dient.

Für mehr Informationen, wie dieser Umrechnungsvorgang funktioniert,
sowie um mehr zu der Erstellung, Verwaltung und Sicherung der Private Keys zu erfahren,
verweisen wir an dieser Stelle auf unseren Kurs „Bitcoin kaufen und verwalten".

Hier klicken, um Teil 2 zu buchen

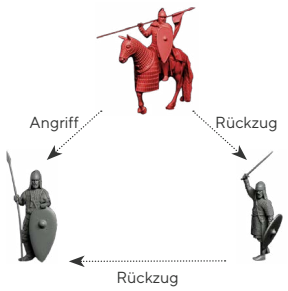
MINING

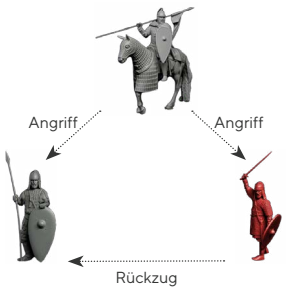
Das Mining ist ein weiterer essentieller Bestandteil des Netzwerkes.

Miner stellen ihre Rechenleistung zur Verfügung, um im Trial-and-Error-Verfahren Identifikationsnummern (ID-Nummern) zu erraten und somit einzelne unbestätigte Transaktionen als (Daten-)Block zusammenzufassen. Für jeden neu an die Blockchain angeknüpften Block **gibt es eine Belohnung in Form von Bitcoin** (Block Subsidy und die Transaktionsgebühren), wodurch ein Anreizsystem zur Stabilisierung des Netzwerkes geschaffen wird. Zur Wiederholung: Nodes bestätigen die von den Minern aufgenommenen Transaktionen alleine durch den Abgleich der Transaktionshistorie und machen diese so manipulationssicher (Konsensus über **eine** gültige Version der Blockchain).

Die gesamte Transaktionshistorie wird allerdings erst durch die Miner auch wirklich fälschungssicher, da Arbeit geleistet werden muss, um Blöcke zu finden. Der **Nachweis der Arbeit** dient dazu, eine unwiderlegbare Transaktionshistorie zu schaffen. Bekannt ist dieses Prinzip unter „Proof of Work".
Das Problem, welches hierbei gelöst wird, ist schon lange unter dem Namen **„Problem der byzantinischen Generäle"** bekannt: **in einem dezentralen System gibt es keine einzelne Quelle der Wahrheit**. Satoshi Nakamoto hat zu diesem Problem erstmalig eine Lösung in einem dezentralen Netzwerk gefunden. Genannt wird die Lösung: Nakamoto-Consensus.
Das Problem der byzantinischen Generäle ist ein Gedankenspiel, bei dem mehrere Generäle gemeinsam eine Entscheidung treffen müssen. Die Generäle sind hier als Bildnis für Teilnehmer in einem dezentralen Netzwerk zu verstehen.
Wir stellen uns eine Stadt vor, welche von der byzantinischen Armee belagert wird. Die Armee wird von mehreren Generälen befehligt und greift entsprechend von allen Seiten aus an. **Nur ein koordinierter Angriff führt zum Sieg**. Ein unkoordinierter Angriff führt dazu, dass jeder Teil der Armee einzelnd eine Niederlage erleidet. Es muss daher ein gemeinsamer Befehl vereinbart werden, was allerdings ohne Mittel der zeitgleichen Kommunikation schwierig ist. Rauchzeichen, Fackeln oder Tonsignale können nicht verwendet werden, da der Feind diese sehen/hören und deuten könnte. Die Nachrichten müssen daher zwischen den Generälen mit einem Kurier übermittelt werden. Das Problem hierbei ist, dass die Nachricht vom Feind abgefangen und verfälscht werden kann oder ebenso die Möglichkeit besteht, dass einer der Generäle ein Verräter ist. Die Nachrichten können also auf verschiedene Art und Weise abgefangen, verfälscht oder aufgehalten werden.

Weiterhin muss es eine Bestätigung geben, dass die Nachricht angekommen ist und der Angriff oder Rückzug stattfinden soll. Hierbei besteht das gleiche Problem. Und bei dieser Nachricht können die Generäle, die sie verschicken, ebenfalls nicht sicher sein, ob sie angekommen ist oder manipuliert wurde. Das Problem besteht also bei der Originalnachricht, aber auch bei den Bestätigungen. **Somit kann sich keiner der Generäle je sicher sein, was zu tun ist**.





In beiden obigen Beispielen übernimmt der General zu Pferd die Initiative und kommuniziert eine Strategie. Der linke General erhält widersprüchliche Informationen und muss versuchen den Verräter (jeweils in rot eingefärbt) zu identifizieren. Das Problem hierbei ist, dass aus Sicht des linken Generals beide Situationen exakt gleich aussehen, obwohl beim linken Szenario der Verrat vom berittenen General ausgeht und im rechten Beispiel der General auf der rechten Seite der Verräter ist. Für den General auf der linken Seite **ist es unmöglich, Wahrheit und Lüge zu unterscheiden** und sich mit dem jeweiligen loyalen General abzustimmen.

MINING

Durch die Unklarheit über die Ehrlichkeit kann es dazu kommen, dass einige Generäle nicht angreifen und dies zur Niederlage führt. Durch die Unstimmigkeit mit nicht vertrauenswürdigen Akteuren kommt es zu diesem Fehler. In der Informatik spricht man vom „Byzantine Fault", wenn unklar ist, ob ein Akteur in einem Computersystem richtig funktioniert (oder sich an die Regeln hält) oder nicht.
Auf Bitcoin übertragen ist jeder Knotenpunkt ein General und daher muss davon ausgegangen werden, **dass theoretisch alle anderen Netzwerkteilnehmer böswillig sind** und das System stören oder ausnutzen wollen. Dies könnte bspw. durch das sogenannte „Double-Spending", das doppelte Ausgeben von Bitcoin-Einheiten, passieren. Satoshi Nakamoto hat aus diesem Grund ein **Sicherheitsfeature** eingebaut, welches dies verhindern soll: Proof-of-Work. PoW ist ein Mechanismus, welcher dazu dient, dass alle Teilnehmer im Netzwerk wahrheitsgetreu agieren und Konsens über eine einzige Wahrheit herrscht. Miner erstellen die Blöcke, indem sie Rechenleistung verwenden und beliebige Transaktionen aus dem Memory Pool aufnehmen. Die Transaktionen müssen allerdings legitim sein und dürfen nicht mit einer anderen Transaktion in dem Block in Konkurrenz stehen, was bei dem Versuch eines Double Spends der Fall wäre. Ein Block, der diese Bedingungen nicht erfüllt, **wird vom Rest des Netzwerkes abgelehnt**. Durch die Identifikationsnummern und der somit entstehenden Reihung der Blöcke betrachten die Netzwerkteilnehmer immer jene Version der Kette als den aktuellen Zustand des Registers/Hauptbuches, welche ausschließlich legitime Transaktionen beinhaltet und die längste Kette des Systems darstellt. Eine Veränderung der dominanten Kette wird folglich nur dann möglich, wenn ein Netzwerkteilnehmer in der Lage ist, alle ungültig gewordenen Blöcke neu zu erstellen und die alternative Kette zur längsten Kette heranwachsen zu lassen. Durch dieses Feature ist ein Angriff auf das Netzwerk nur möglich, wenn eine Entität über 51% der gesamten Rechenleistung des Netzwerkes kontrolliert, was wie bereits beschrieben, durch die Verteilung der Rechenleistung auf verschiedene Interessengruppen und Kontinente nahezu unmöglich ist.
Die Miner einigen sich somit stets auf eine einzige Wahrheit im Netzwerk. Durch die Rechenleistung wird von den Minern versucht, eine passende Zahl zu finden, welche gewisse Parameter erfüllt. Wenn ein Miner die korrekte Lösung gefunden hat, verbreitet er diese im Netzwerk, womit jeder Netzwerkteilnehmer die Lösung zu den vorherigen, bereits gefundenen Lösungen hinzufügen muss (siehe Abschnitt Blockchain).

Die Suche nach einem gültigen Block kann man sich wie ein Puzzle vorstellen, bei dem nur noch ein letztes Teil zur Fertigstellung fehlt. Es gibt allerdings eine sehr große Anzahl von Teilen zur Auswahl, welche alle durcheinander auf einem Berg von potenziell passenden und sich ähnelnden Teilen liegen. Somit bleibt nur übrig, ein Teil nach dem anderen auszuprobieren, um irgendwann das passende Teil zu finden.

Innerhalb des Bitcoin-Netzwerkes suchen zeitgleich viele dieser Miner mit Hilfe ihrer Computerleistung nach dem passenden Teil. Einige spezielle Computer (sogenannte ASICs) sind darauf spezialisiert, einen bestimmten Vorgang auszuführen und sind daher besonders für das Mining geeignet. Sie können mehrere Billionen potenzielle Lösungen in der Sekunde überprüfen. Der Berg an Puzzlestücken **reguliert sich allerdings durch das Protokoll selbst** und wird dadurch immer so groß gehalten, dass das gesamte Netzwerk durchschnittlich **immer** 10 Minuten benötigt, um das passende Teil zu finden.
Je mehr Teilnehmer partizipieren, desto größer wird auch die Anzahl potenzieller Lösungen. Das sogenannte „Difficulty Adjustment" ist eine weitere geniale Implementierung von Satoshi Nakamoto. Es sorgt dafür, dass **alle 2016 Blöcke** (ca. alle 14 Tage) die Schwierigkeit, die Lösung zu finden, erhöht oder verringert wird - je nachdem wie viel Rechenleistung (Hashpower) im Netzwerk vorhanden ist.
Das Ausprobieren der Lösungen kostet sehr viel Energie, was dem Miner, der die Lösung findet, letztendlich eine Belohnung in Bitcoin bietet.

MINING

Der Anreiz neue Bitcoin zu finden, ist es, was das Netzwerk ständig sicherer und resistenter gegen potenzielle Angriffe macht. Im Jahre 2017 war die gesamte Rechenleistung, die das Netzwerk stützt, bereits äquivalent zu **2 Billionen** herkömmlichen Laptops und somit 200.000-mal größer als die 500 leistungsstärksten Supercomputer zusammen. Seitdem ist die Hashrate stetig weiter angestiegen.

31.12.2017 ~ 15 Ehash/s
01.01.2022 ~ 201 Ehash/s } +1.340%

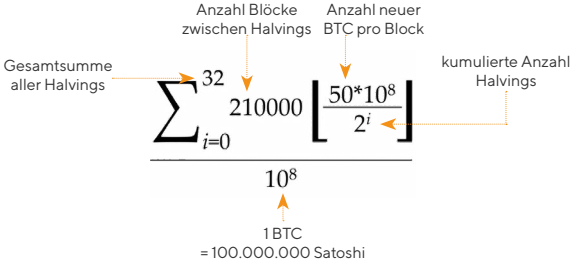
Je höher dieser Wert ist, desto sicherer ist das Netzwerk, denn die Hashrate gibt an, wie oft die Miningrechner innerhalb einer Sekunde einen Versuch unternehmen, einen gültigen Block zu finden. Bei 200 Exahashes bedeutet dies, dass in der Sekunde 200.000.000.000.000.000.000 Versuche im gesamten Netzwerk unternommen werden.
Bitcoin ist somit das weltweit größte Computernetzwerk, welches einen einzelnen Zweck verfolgt: **die Sicherung von monetären Wert und somit indirekt von geleisteter Arbeit**. Hinter dem Mining steckt also weitaus mehr als nur die Jagd nach neuen Bitcoin, wie es gerne dargestellt wird. Das Anreizsystem funktioniert, indem die Miner für die Sicherung des Netzwerkes belohnt werden, aber somit auch keinen Vorteil haben, das Netzwerk zu attackieren, da sonst ihr eigenes Geschäftsmodell obsolet ist. Bei steigender Kaufkraft von Bitcoin steigt durch höheren Anreiz ebenso die Teilnehmerzahl im Netzwerk. Es wird für Betrüger immer schwieriger, einen Double Spend durchzuführen oder das Register auf andere Art und Weise zu manipulieren bzw. zu attackieren.

Aus welchem Grund Bitcoin-Mining keine Energieverschwendung ist und sich sogar positiv auf den weltweiten Energieverbrauch auswirken kann, haben wir in einem Artikel zusammengefasst.

Hier klicken, um den Artikel zu lesen

HALVING

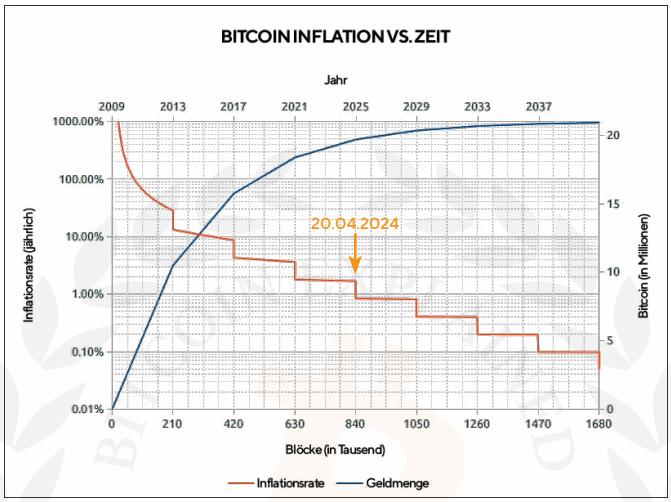
Die sogenannten Halvings sind die nächste wichtige technologische Besonderheit. Wie bereits beschrieben, erhalten die Miner zur Belohnung Bitcoin ausbezahlt. Mit jedem gültigen Block wird der sogenannte „**Block Reward**“ ausbezahlt, welcher sich aus der „**Block Subsidy**“ und allen **Transaktionsgebühren** des entsprechenden Blocks zusammensetzt. Die Block Subsidy ist eine festgeschriebene Summe neuer Bitcoin. Die Transaktionskosten können schwanken, je nach Auslastung des Netzwerkes und Bereitschaft der Nutzer zur Zahlung höherer Gebühren, um Transaktionen schneller vollziehen zu können.
Die Block Subsidy wird als sogenannte „**Coinbase-Transaktion**“ an die Miner ausgeschüttet. Die Coinbase-Transaktion ist immer die erste Transaktion in jedem neuen Block. Durch diese kommen **neue Bitcoin planbar in den Umlauf**. Der Schöpfungszeitplan von Bitcoin ist planbar, da dieser im Protokoll festgeschrieben ist und nicht verändert werden kann. Die Summe von neu ausgegebenen Bitcoin wird ca. alle 4 Jahre oder präzise **alle 210.000 Blöcke halbiert**. Um dies zu gewährleisten wird nachstehende Summenformel verwendet:



HALVING

Anhand der Formel kann man ableiten, wie viele Halvings es insgesamt geben wird und somit auch ungefähr prognostizieren, wann diese auftreten werden. Durch das Difficulty Adjustment bleibt die durchschnittliche Blockzeit bei 10 Minuten und somit wird alle vier Jahre ein Halving durchgeführt werden, bis in das Jahr 2140, in dem dann das letzte Halving stattfinden wird und somit auch die letzten Satoshis an die Miner ausgeschüttet werden. Danach werden sich die Miner nur noch durch die Gebühren finanzieren müssen.

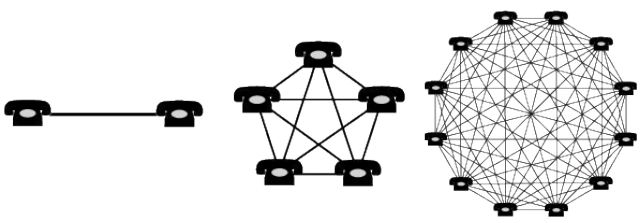
Zur Geburtsstunde des Netzwerkes wurden 50 Bitcoin pro Block erzeugt. Am 28. November 2012 wurde die Anzahl auf 25 reduziert. Am 9. Juli 2016 und am 11. Mai 2020 fanden die nächsten beiden Halvings statt, womit die Menge der Block Subsidy im Jahr 2022 nun nur noch bei 6,25 Bitcoin liegt.



Durch diesen festgelegten Plan kann auch die Inflationsrate von Bitcoin vorhergesagt werden. Durch die sinkende Inflationsrate und die restlichen beschriebenen Eigenschaften, wird **erstmalig echte digitale Knappheit** erreicht. Jedes digitale Objekt, welches versendet werden kann, wird eigentlich kopiert. Egal ob E-Mails, Textdokumente oder andere Dateien, sie alle bleiben für den Absender reproduzierbar und dieser hat nach wie vor Zugriff. Bitcoin-Einheiten erlauben dem Absender als erstes digitales Gut nach einem Transfer an eine andere Person keinen Zugriff mehr, womit es nicht unendlich reproduziert, verändert oder verfälscht werden kann. Herkömmliche digitale Güter können im Gegensatz dazu auch als multiple Kopien und ohne Probleme von mehreren Nutzern gleichzeitig benutzt werden.

NETZWERKEFFEKTE

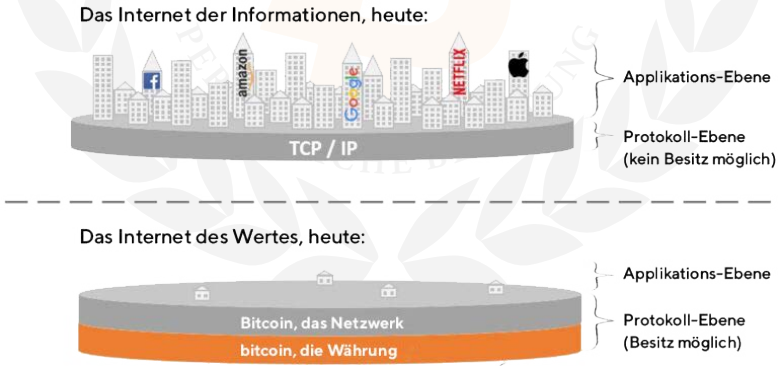
Der Netzwerkeffekt beschreibt die positive Veränderung des Nutzens für ein Produkt oder eine Dienstleistung für den individuellen Verbraucher, wenn sich die Anzahl der gesamten Mitgliederzahl erhöht. **Der Produktnutzen für den einzelnen Verbraucher ist also von der gesamten Benutzeranzahl abhängig**.
Eines der frühen Beispiele für diesen Effekt ist das Telefonnetz. Der Nutzen des Telefonnetzes ist recht gering, wenn es nur zwei Telefone gibt. Der Nutzen steigt aber, sobald mehr und mehr Menschen sich ein Telefon anschaffen, da nun mehr Verbindungen möglich sind. Die nachstehende Grafik verdeutlicht dies.



NETZWERKEFFEKTE

In der Netzwerkökonomie greift man auf das Metcalfesches Gesetz (Metcalfes Law) zurück, um dies zu erklären. Diese Effekte treten vor allem bei Technologie- und Kommunikationsnetzwerken auf. Prinzipiell unterscheidet man zwischen direkten und indirekten Netzwerkeffekten. Der direkte Effekt besteht aus der steigenden Nutzeranzahl (Beispiele: Telefon, Whatsapp etc.). Der indirekte Netzwerkeffekt besteht aus komplementären Produkten. Beispiele für den indirekten Effekt sind unter anderem Betriebssysteme. Denn je mehr Nutzer es gibt, desto mehr Apps oder Programme werden dafür bereitgestellt und je mehr Programme verfügbar sind, desto mehr Nutzer gibt es wiederum. Es entsteht ein positiver Kreislauf.

Auch auf Bitcoin treffen die Effekte bzw. Gesetze von sozialen und technologischen Netzwerken zu. Sowohl der Wert des Netzwerkes, als auch der Wert der Einheiten steigt bei zunehmender Nutzeranzahl, da mehr Kapital (geleistete Arbeit) gebunden wird, es mehr Transaktionsmöglichkeiten gibt und mehr Dienstleistungen und Waren für Bitcoin angeboten werden. Welchen Nutzen der indirekte Handel für eine Volkswirtschaft bringt, wurde eingangs schon beschrieben. Wie das Internet hat Bitcoin eine Protokoll- und eine Applikations-Ebene. Ein Unterschied zum Internetprotokoll TCP/IP besteht darin, dass **durch Bitcoin der Besitz der Protokoll-Ebene möglich gemacht wird**, denn ohne die Währung wäre auch das Netzwerk als solches nutzlos. Die Applikations-Ebene kann stetig weiter ausgebaut werden. So brachte das Internet Firmen wie Amazon, Google etc. hervor. Die Applikations-Ebene von Bitcoin ist hingegen noch immer in der Entwicklung, was bedeutet, dass der Nutzen und somit auch der Wert weiter zunehmen wird, sobald weitere Möglichkeiten zur Nutzung und Verbesserung erschlossen werden. So ist das sogenannte Lightning-Netzwerk, welches als zweite Ebene auf Bitcoin aufsetzt, bspw. eine solche Entwicklung. Nehmen die Nutzer von Bitcoin zu, steigt somit der Nutzen, mehr Menschen werden ebenfalls das Lightning-Netzwerk nutzen und somit werden mehr Anreize für neue Entwicklungen geschaffen. Lightning ist bspw. sehr viel schneller als Transaktionen auf der untersten Bitcoin-Protokoll-Ebene durchzuführen und ermöglicht ebenfalls einen höheren Durchsatz mit sehr geringen bis gar nicht vorhandenen Gebühren. Somit sind Mikrotransaktionen möglich, welche bspw. für das „Value for Value-Modell" im Podcasting genutzt werden können. Ebenso sind auch viele andere Applikationen und Einsatzmöglichkeiten denkbar, welche die positiven Kreisläufe und Effekte weiterhin verstärken.



Die Grafik verdeutlicht nochmals, welches unglaubliche Potenzial besteht und dass sich Bitcoin **noch am Anfang der Entwicklung befindet**. Jedoch gibt es schon viele vielversprechende Firmen, die sich auf die Entwicklung von Projekten und Dienstleistungen, vor allem basierend auf dem Lightning-Netzwerk, spezialisiert haben.

Für mehr Informationen zum Thema Lightning, der Funktionsweise und Nutzung verweisen wir an dieser Stelle auf unseren Kurs „Für fortgeschrittene Nutzer".

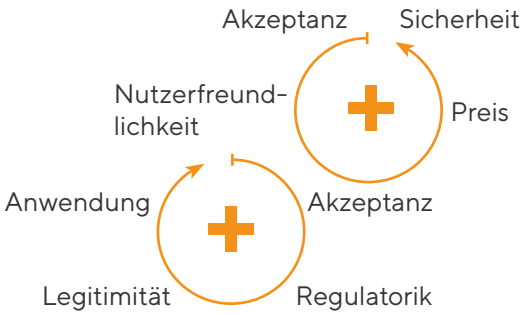
Hier klicken, um Teil 3 zu buchen

NETZWERKEFFEKTE

Welche Netzwerkeffekte kann man beobachten und zu welchen positiven Kreisläufen führen diese?
Bei Bitcoin wirken durch das Anreizsystem, welches Leute dazu bringt am Netzwerk zu partizipieren, viele verschiedene positive Kreisläufe, die sich gegenseitig ebenfalls wieder begünstigen.
Anreize können durch äußere Einflüsse geschaffen werden. Beispielsweise wenn autoritäre Regierungen ihren Bürgern den Zugang zu Bankkonten verwehren. Es können aber auch ökonomische Anreize sein, wie das Steigen des Preises und der Wunsch davon zu profitieren. Anreize können aber auch im sozialen Sinne bestehen, in der Hoffnung ein faireres, offeneres und freiheitlicheres Geldsystem für die Welt zu schaffen oder möglichst viele Menschen über dieses System aufzuklären.

In der westlichen Welt wird für die meisten Leute der Profit der größte Anreiz sein, am Netzwerk teilnehmen zu wollen, **obwohl der Preis nach dem Studium von Bitcoin, die am wenigsten interessante Eigenschaft sein wird**. Anders schaut es aus, wenn man sich die Akzeptanz in Argentinien, El Salvador oder Afrika anschaut. Hier sind die Menschen durch Repressionen der Regierung oder durch Hyperinflationen dazu gezwungen aus dem herkömmlichen System auszusteigen, um die eigene Kaufkraft oder das eigene Überleben zu schützen.

Folgenden Kreislauf kann man feststellen: je höher die Hashrate ist, desto mehr Nodes gibt es insgesamt und desto sicherer und resilienter ist das Netzwerk. Dies fördert die Akzeptanz (ob von Unternehmen oder Privatpersonen). Die Akzeptanz nimmt wiederum Einfluss auf den Preis. Wenn der Preis steigt, steigt ebenfalls die Hashrate, da ein höherer Anreiz besteht, Bitcoin-Mining zu betreiben. Die Akzeptanz kann ebenfalls durch Anwendungsbeispiele vorangetrieben werden. So kann man verschiedene Anwendungsfälle für Bitcoin feststellen, welche sich in Zukunft vermutlich vermehren werden, da mehr und mehr Applikationen entstehen. Die Anwendungsfälle können durch politische Entscheidungen begünstigt und legitimiert werden, wie bspw. die Entscheidung, Geld zu drucken oder Gold zu verbieten etc. Ebenso kann die Regulatorik in der Politik auch zur Legitimierung und somit zur weiteren Akzeptanz führen (Beispiel: offizielles Zahlungsmittel in El Salvador). Der umgekehrte Fall kann aber genauso eintreten: durch eine hohe Akzeptanz in der Bevölkerung ist die Politik gezwungen Bitcoin zu legitimieren.
Wichtig hierbei ist, dass Bitcoin keinerlei Legitimierung benötigt und auch keinerlei Regulatorik unterliegt. Die Nutzung ist frei und kann durch kein Gesetz oder Maßnahme verhindert werden.



Nun kann die höhere Akzeptanz aber auch zu einer verbesserten Nutzerfreundlichkeit durch einfachere Applikationen, mehr Möglichkeiten zum Kauf oder bessere Aufbewahrung der Private Keys führen, die wiederum ihrerseits für mehr Akzeptanz sorgt.

NETZWERKEFFEKTE

Durch Unternehmen, die aufmerksam werden, steigt der Druck auf die Politik und die Regulatorik. Durch positive Gesetze, Vergünstigungen, Steuersenkungen oder andere Subventionen wird wiederum Legitimität geschaffen und die Anwendungsfälle erweitern oder festigen sich. Somit steigt die Akzeptanz weiter. Ebenso zu berücksichtigen sind selbstverständlich Produkte und Dienstleistungen, die über und auf Bitcoin angeboten werden, die Integration in bereits existierende Produkte und der Anreiz für Entwickler für das Netzwerk tätig zu werden. All diese Effekte wirken sich positiv auf das Netzwerk aus, schaffen weitere Anreize für neue Nutzer und können sich gegenseitig oder selbst begünstigen.
Bitcoin ist durch die bestehenden Netzwerkeffekte, die nicht mehr einfach aufgeholt werden können, prädestiniert dafür der Standard für eine Art „Internet des Geldes" oder „Internet für Werte" zu werden.

WARUM BITCOIN?

Nachstehend finden sich einige Thesen, die für den Kauf von Bitcoin sprechen können. Wichtig ist, dass dies nicht als Finanzberatung zu verstehen ist.

Bitcoin als Chance

Bitcoin's Erfolg ist nicht garantiert. Dennoch gibt es nichts, was so sicher erscheint, wenn man die Funktionsweise erstmal besser versteht. Deshalb kann man Bitcoin quasi als asymmetrische Wette betrachten. Wie viele andere Dinge, könnte Bitcoin scheitern. Aber kaum etwas hat so viel Potential nach oben. Bitcoin ist eine Bereicherung für jedes Portfolio. Selbst wenn man den Fiatwährungen weiterhin Vertrauen schenkt, bietet Bitcoin als eine Technologie, welche noch in den Kinderschuhen steckt, eine riesige Chance auf Kursgewinne. Diese sind alleine schon in den Netzwerkeffekten begründet und darin, dass es kaum Gegenparteirisiko (auch Kontrahentenrisiko genannt) gibt. Bitcoin ist kein Unternehmen, bei dem es durch vertragliche Verpflichtungen mit Drittparteien zu Ausfällen oder Zahlungsunfähigkeit kommen kann. Für Bitcoin gibt es keinen zentralen Entscheider, der Einfluss nehmen kann und es gibt auch keine sonstigen Verpflichtungen, die eingehalten werden müssen. Für Bitcoin ist nur wichtig, dass durchschnittlich alle 10 Minuten ein neuer Block im Netzwerk bekannt gegeben wird.

Bitcoin als Vorsorge oder Sparen

Wie erläutert wurde, eignen sich Fiatwährungen nicht als Wertspeicher. Ein Wertspeicher ist aber wichtig, um seine Kaufkraft zu erhalten und somit indirekt die eigene geleistete Arbeitszeit zu konservieren und über längere Zeit hinweg zu erhalten. Durch die vorherbestimmte Knappheit und Unveränderbarkeit ist Bitcoin die beste Spar-Technologie, welche die Menschheit bisher hervorgebracht hat. Der eigene Anteil kann nicht verwässert werden und niemand kann auf das Ersparte zugreifen.

Bitcoin als Eigentum

Dieses einmalig dezentrale Netzwerk wird von niemandem kontrolliert und schafft somit die Möglichkeit von echtem Eigentum, da es keine Instanz gibt, welche Einheiten konfiszieren, Transaktionen umleiten oder einfrieren kann. Bitcoin bietet finanzielle Freiheit und Unabhängigkeit. Es ist ein faires und inklusives System, an dem jeder teilnehmen kann. Es ist grenzenlos, leicht zu transportieren und bietet Zugang zum Finanzsystem für alle bankenlosen Menschen.

Bitcoin als Sicherheit

Das dezentrale Design macht ein Versagen oder ein Verbot sehr unwahrscheinlich. Durch die Spieltheorie, welche auf Bitcoin wirkt, ist es weiterhin sehr unwahrscheinlich, dass Bitcoin überall gleichzeitig verboten wird. Durch das Anreizsystem besteht immer die Motivation für einzelne Länder, Staaten, Regierungen oder Privatpersonen, Bitcoin zu nutzen und Profit daraus zu erwirtschaften. Bitcoin ist seit Einführung und Erstellung des ersten Blocks sicher und beständig und ohne Unterbrechung verfügbar. Das Abschalten des gesamten Netzwerkes ist selbst mit Abschalten des weltweiten Internets nicht möglich. Weiterhin bietet Bitcoin einen Interventionsschutz, der vor übergriffigen Parteien (einzelnen Akteuren oder auch Staaten) schützt.

WARUM BITCOIN?

Sollte bspw. das Mining in einem Land verboten werden, so kann durch die Mobilität der Miner schnell der Standort gewechselt werden. Dies wurde im Mai 2021 bewiesen, als China ein Mining-Verbot aussprach und sich ein großer Teil der Hashrate innerhalb kürzester Zeit über die gesamte Welt in andere Länder verteilt hat. Das Netzwerk operierte problemlos weiter und die Hashrate ist seitdem weiter angestiegen. Darüber hinaus ist Bitcoin ein System mit klaren Regeln, bei denen man sich sicher sein kann, dass diese nicht mehr geändert werden: die Menge von insgesamt 21 Millionen Stück, das Difficulty Adjustment, was verhindert, dass bei mehr Rechenleistung auch mehr Bitcoin generiert werden oder auch der Halving-Mechanismus.
Bitcoin is a system with rules but no rulers - Bitcoin ist ein System mit Regeln aber ohne Herrscher.

„It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy. Once it gets bootstrapped, there are so many applications [...]."
- Satoshi Nakamoto (17.01.2009) -

FAZIT

Durch die im Protokoll hinterlegten Mechanismen und die Begrenzung auf maximal 21.000.000 Bitcoin ist das Netzwerk bereits heute disinflationär und ab einem bestimmten Punkt deflationär. Das bedeutet, dass Bitcoin gegenüber anderen Gütern stets im Wert steigt. Das Stock-To-Flow-Verhältnis von Bitcoin wird mit dem nächsten Halving im Jahre 2024 einen Wert erreichen, welches Bitcoin zum seltensten Gut und somit gleichzeitig zum härtesten Geld auf der Erde werden lässt.
Das ewige Dilemma, dem die Menschen gegenüberstehen, ist die Frage, wie der durch den Einsatz der eigenen Zeit erarbeitete Gegenwert für die Zukunft gespeichert werden kann. Für den Menschen war bisher die einzig endliche Ressource, seine eigene Zeit. Alle anderen Rohmaterialien oder Produkte können unendlich gefördert oder hergestellt werden. Zumindest ist nicht bekannt, wie viel von dem Rohstoff vorhanden ist und ob in der Zukunft eventuell mehr gefunden wird. So wurden bspw. Asteroiden entdeckt, welche die Menge an Gold enthalten, die bisher in der gesamten Menschheitsgeschichte gefördert wurde.
Wird der erarbeitete Wert in Form von Fiatwährungen auf einem Bankkonto „gespart", unterliegt das eigene Vermögen ständig einer Finanzrepression in Form von Entwertung durch Inflation oder niedrigen Zinsen. Die Zinsen müssen künstlich niedrig gehalten werden und liegen unter der Inflationsrate. Sparer erhalten also de facto negative Realzinsen. Der Staat kann somit seine Schulden nach und nach durch eine Umverteilung von Vermögen auf Kosten der Sparer und Anleger abbauen. Deutsche Sparer verlieren dadurch pro Jahr rund 14 Milliarden Euro bei Tagesgeld, Giro- und Sparkonten.
Der Kaufkraftverlust des Euros ist also durchaus real und ernst zu nehmen. Ebenfalls davon betroffen, sind die anderen Fiatwährungen, die alle nach demselben Geldschöpfungsprinzip funktionieren. Bitcoin ist daher eine wunderbare Alternative seine Kaufkraft für die Zukunft zu garantieren, da es nicht inflationiert und somit entwertet werden kann.

1 BTC = 1 BTC

1 Bitcoin wird immer 1 Bitcoin wert sein. Es gibt nichts, was dieses Verhältnis verwässern, verfälschen oder manipulieren kann. Alle anderen Güter oder Dinge können theoretisch unendlich vermehrt werden, wenn der Mensch unbegrenzt Zeit zur Verfügung hätte. Bitcoin ist neben menschlicher Zeit das einzig knappe Gut. Der Wert von Bitcoin schwankt nur, wenn dieser in anderen Gütern oder Währungen, wie Fiat, gemessen wird. Bitcoin ist wie ein Rohstoff zu betrachten, eine Maßeinheit für Wert.
Momentan kann man Bitcoin noch gegen Fiat eintauschen oder mit Fiat kaufen. In einer Welt, in der Bitcoin überall als Zahlungsmittel benutzt wird, ist dies nicht mehr möglich. Dann muss Bitcoin durch geleistete Arbeit verdient werden.

FAZIT

Nichtsdestotrotz wird man bei Bitcoin immer einen festen Anteil von der gesamten Menge besitzen können. In der Welt der Fiatwährungen wird dieser Anteil ständig verwässert. Folgende Visualisierung ist hierfür sehr hilfreich:

$$\text{Bitcoin: } \frac{\text{dein Geld}}{21.000.000} \qquad \text{Fiat: } \frac{\text{dein Geld}}{\infty}$$

Weiterhin lässt sich das Vertrauen in Bitcoin rechtfertigen, da Bitcoin durch die Anonymität des Entwicklers oder der Entwickler komplett unpolitisch und durch die Dezentralität global und von der gesamten Bevölkerung ungehindert über Grenzen hinweg verwendbar ist. Die Transaktionskosten sind im Vergleich zu anderen Zahlungsweisen oder dem Bewegen von Gold marginal, gerade auch durch Lightning nahezu nicht vorhanden. Bitcoin nutzt sich mit der Zeit auch nicht ab und der Zugang zu den eigenen Private Keys kann besonders leicht und sicher gestaltet werden, indem man sich einfach 12-24 Wörter merkt. Der Wert ist nicht direkt an physische Objekte gebunden und die Einheiten können somit weder gefälscht, noch verwässert oder multipliziert werden.
Und trotzdem ist Bitcoin durch das Mining und Proof-of-Work mit der realen Welt verankert und benötigt einen messbaren Arbeitsaufwand, um in den Umlauf gebracht zu werden.

Bitcoin bringt alle Eigenschaften mit, die ein gutes Geld haben muss und trennt die Verbindung zwischen Geld und Staat. Somit ist die Möglichkeit gegeben, ein Geld zu benutzen, welches nicht korrumpierbar, unkaputtbar, unveränderbar, erlaubnislos und zensurresistent ist.

Bitcoin kann auch in den ärmsten Ländern dieser Welt Bankzugang („be your own bank"), beziehungsweise Zugang zum Finanzsystem bedeuten, da internetfähige Mobiltelefone sehr viel weiter verbreitet sind als Bankkonten.
Bitcoin löst erstmals das Double-Spending-Problem auf eine dezentrale Art und Weise, schafft wirtschaftliche Anreize für jeden Teilnehmer und löst ebenfalls das Orakel-Problem, welches immer zutrifft, wenn einer zentralen Partei vertraut werden muss. Dies war das größte Problem bei Gold. Außerdem verhindert Bitcoin Inflation und könnte viele positive Auswirkungen auf die Gesellschaft im Allgemeinen haben, da eine niedrige Zeitpräferenz propagiert wird.

Bitcoin zeigt uns deutlich die Probleme auf, die im bisherigen System bestehen und präsentiert gleichzeitig eine Lösung. Da Geld reine Information ist und die menschliche Zivilisation zu großen Teilen auf dieser Information aufbaut, wird durch Intervention eine Anreizstruktur geschaffen, welche zu Korruption, Fehlinvestitionen, Subventionen und anderen staatlichen Eingriffen in den freien Markt führt. Bitcoin ist der Gegenpol und bietet ein ehrliches und gutes Geldsystem, welches langfristiges Handeln wieder attraktiv werden lässt und somit eine prosperierende Zukunft einläutet.

„Fix the money - Fix the world"

BILDQUELLEN

Seite 2

Stock-To-Flow
eigene Darstellung nach dem Vorbild Saifedean Ammous (The Bitcoin Standard (2018), S. 24)

Seite 3

Geldsystem
eigene Darstellung nach dem Vorbild Dirk Ehnts (Geld und Kredit: eine €-päische Perspektive (2014), S. 69)

Seite 5

Charts Bloomberg-Terminal übernommen von Holger Zschäpitz
https://tinyurl.com/3tc7muv9
https://tinyurl.com/3299h2sb

Seite 6, Seite 7, Seite 8

Folgen des Fiatsystems
https://wtfhappenedin1971.com/

Seite 9

Bitcoins Historie
eigene Darstellung nach dem Vorbild @dergigi
https://dergigi.com/2021/06/13/bitcoin-is-an-idea/

Seite 13

Bitcoins Verschlüsselung
eigene Darstellung nach dem Vorbild bisonapp.com
https://bisonapp.com/wp-content/uploads/2020/07/infografik-verschluesselung-bitcoin.png

Seite 17

Bitcoins Inflation über die Zeit
https://bitcoinblockhalf.com/

Seite 18

Darstellung übersetzt nach dem Original von @Croesus_BTC
https://twitter.com/croesus_btc/status/1367165017280237569

ABSCHLIESSENDE BEMERKUNGEN

Bitcoin ist generell ein komplexes Thema und der Umgang mit eigenen Werten sollte immer mit Bedacht durchgeführt werden. Gerade die technische Seite von Bitcoin auch nur im Ansatz zu verstehen, erfordert viel Recherche und natürlich Interesse.

Es ist möglich, dass sich gewisse Funktionen im Laufe der Zeit verändern und einige der hier festgehaltenen Informationen damit ungültig werden. Wir versuchen unsere Materialien ständig auf dem aktuellsten Stand zu halten. Bevor mögliche finanzielle Entscheidungen getroffen werden oder größere Werte gesichert bzw. transferiert werden, sollte immer nochmal geprüft werden, ob sich bspw. die Funktionsweise geändert hat oder technische Neuerungen entstanden sind.

Wir empfehlen weiterhin sich immer erst mit einer Wallet oder einer Handelsplattform vertraut zu machen, bevor tatsächlich Transaktionen durchgeführt werden und eigene Werte (Bitcoin) gesichert werden. Weiterhin empfehlen wir selbst dann, bei den ersten Versuchen **immer erst mit einem kleinen Anteil zu starten** und sowohl das Versenden, Empfangen und Wiederherstellen im Falle einer Wallet oder das Kaufen und Verkaufen im Falle einer Handelsplattform auszuprobieren.
Generell ist es sinnvoll, mit Summen zu starten, die man bereit ist zu verlieren, um sich mit der gesamten Funktionsweise der Technologie vertraut zu machen.

Unsere Materialien werden nach dem besten Wissen und Gewissen erstellt. Wir übernehmen allerdings keinerlei Haftung für verlorene Schlüssel, Codes oder Passwörter. Weiterhin übernehmen wir keinerlei Haftung für sich ändernde Funktionen in der beschriebenen Software, Webseiten oder Bitcoin-Applikationen.

Jeder Nutzer ist verantwortlich, die hier beschriebenen Informationen selbst zu prüfen.

Dieses Handout dient daher nicht als finanzielle Beratung oder Handlungsempfehlung. Wir haben hier unsere eigenen Erfahrungen, Meinungen und Praktiken dargelegt.