Bitcoin - Deutsch
Deutsch - Bitcoin

Wie sage ich es meinen Eltern

Torsten Kreuziger-Leonhardt

Bitcoin - Deutsch

Deutsch - Bitcoin

Wie sage ich es meinen Eltern

Ein Buch von Torsten Kreuziger-Leonhardt
Vertrieb über Leon-Verde | Bitcoin verstehen, https://leon-verde.com
Covergestaltung: Torsten Kreuziger-Leonhardt

Inhaltsverzeichnis

Über dieses Buch.

Der Autor versucht in diesem Buch die Welt des Bitcoin, nicht der Kryptowährungen, zu erklären und diese Erfindung aus dem Zwielicht in die Mitte der Gesellschaft zu holen, wo sie nach eigener Überzeugung zurecht angesiedelt werden soll. Es wird erklärt, warum Bitcoin anders ist als die restlichen zig tausende Kryptowährungsprojekte und was dieses neue, wilde Ding uns als Individuen und als Menschheit im Ganzen für Möglichkeiten und Chancen ermöglicht, die es so noch nie gab.

Dazu gehört neben dem technischen Aspekt, der Bitcoin ganz extrem kennzeichnet, auch der gesellschaftliche Ansatz, der aus einer einzigartigen Erfindung eine noch nie dagewesene Chance macht unsere Zukunft in Frieden und Kooperation zu gestalten. Aber keine Angst. Ich werde den technischen Teil so erklären, dass dies von Otto Normal auch verstanden werden kann und nicht erst ein Informatikstudium abverlangt wird.

Außerdem soll mit diesen ganzen Mythen, Vorurteilen und Desinformationen aufgeräumt werden. Nach der Lektüre dieses Buches ist Jeder, und ich betone Jeder, in der Lage, von seinem individuellen Standpunkt aus weiter zu gehen und die Vorteile, als auch Gefahren und Risiken von Bitcoin zu erkennen, für sich anzunehmen und in das eigene Leben zu integrieren. Wer nur schlicht seinen Besitz sichern will, der sichert eben nur seinen Besitz, wer Bitcoin als Spekulationsobjekt nutzen will, der macht das und ich wünsche viel Glück dabei, aber wer den Weg der Freiheit einschlagen will, dem werden Flügel wachsen. Das ist die Reise, die es wirklich zu erleben gilt.

In der Gemeinschaft der Bitcoiner wird immer vom Kaninchenbau, angelehnt an die Geschichte von Alice im Wunderland, gesprochen, den es zu ergründen gilt. Mit jedem Aspekt, den man durch das vertiefte Studium der Welt und ihrer Zustände versteht, ergeben sich viele neue Standpunkte und Sichtweisen, die sehr viele von uns so noch nie gesehen oder zugelassen haben. Bitcoin ist eine sehr spannende Reise und ich lade Sie herzlich ein die ersten Schritte mit mir gemeinsam zu gehen. Wichtig bei der Betrachtung von Bitcoin und unserer Welt ist, dass wir versuchen dies so nüchtern wie möglich zu tun. Ich persönlich bin von Bitcoin vollkommen überzeugt und argumentiere dadurch bisweilen etwas enthusiastisch. Sobald Ihnen das auffällt, bitte ich Sie unbedingt wachsam zu sein und das Geschriebene sorgfältig mit den eigenen Erfahrungen abzugleichen und kritisch zu hinterfragen. Nur wer seine eigenen Gedanken und Erfahrungen mit einbringt, wird Bitcoin für sich auch zur Gänze verstehen und muss nicht der Meinung eines anderen hinterherlaufen. Ein Kredo in der Bitcoingemeinde ist „Don't trust, verify!“, was so viel heißt wie traue keinem, prüfe selbst.

Das Buch ist grob in zwei Teile aufgeteilt. Der erste Teil beschreibt Bitcoin in seinen verschiedenen Aspekten und der zweite Teil ist eine Art Glossar oder Wörterbuch, in dem die ganzen Fachbegriffe und Redewendungen, die immer wieder mit Bitcoin aufkommen ausführlich erklärt werden.

<u>Achtung:</u> Dieses Buch bietet keine Finanzberatung und möchte niemanden dazu überreden in jedwede Finanzprodukte zu investieren. Auch ist es nicht geeignet steuerliche Ratschläge zu geben. Bei Fragen zu Steueranliegen wenden Sie sich bitte an Ihren Steuerberater.

An wen richtet sich dieses Buch? Ein Verleger möchte an dieser Stelle immer nur ein Wort sehen – ALLE. Ich habe beim Schreiben zwei Menschen vor Augen. Einerseits meinen achtzigjährigen Schwiegervater Fritz, der immer selbstständig im Handwerk gearbeitet, immer Geld verdient und dann investiert hat, aber nie wirklich verstanden, was der Banker, Broker, Finanzberater mit seinem Geld in Wahrheit gemacht hat. Und auf der anderen Seite meinen Freund aus Kindertagen Andreas.

Wohlhabend, Bildungsbürger, Kosmopolit und doch immer am Limit, wenn es um das eigene Tun und Sein geht. Andreas ist ein klassischer Fall vom Hamsterrad. Alles läuft super, alle Zeichen stehen auf grün, nur mit dem einen, kleinen Nachteil, dass wenn man nicht mehr kann oder möchte dieses gigantische Kartenhaus aus Luxus, Anspruch und Verpflichtung zusammenbricht und ihn sehr wahrscheinlich unter sich begräbt.

Das sind die beiden, mit denen ich im Kopf immer im Zwiegespräch bin und denen ich versuche klarzumachen, warum die Dinge sind wie sie sind und warum Bitcoin für fast alle Probleme die wir haben eine Lösung sein kann. Aber wenn man es genereller sagen möchte, dann versuche ich hier allen, die keine Finanzexperten und Elektrotechniker oder Programmierer sind, das Prinzip und die grobe Technik von Bitcoin näher zu bringen.

Warum glaube ich, dass ich in der Lage bin jemanden etwas über eine recht junge Technologie beibringen zu können?

Zum einen wuchs ich noch in einer Zeit auf, als Denglisch nicht Weltsprache war und man beim Fernmeldeamt noch einen Antrag stellen musst, wenn man anstatt der 4 Meter Standardlänge ein 10 Meter langes Kabel an seinem Haustelefon haben wollte. Also ich komme aus einer Zeit, die heutigen 20 bis 30 jährigen Menschen so fremd ist wie das Mittelalter.

Zum anderen habe ich in all meinen Jahren in der Gastronomie und später als Energieberater viel mit Menschen gesprochen, bin ihnen auf einem ganz einfachen Level begegnet und wir konnten uns fast immer so verständigen, dass beide das Gefühl haben zu verstehen was das Gegenüber sagt. Kompetenz, Wissen und Können, verpackt in eine Sprache, die nicht einen Duden neben sich voraussetzt. Das klingt dann nicht mehr so akademisch, und auch nicht neudeutsch fancy, aber dafür kann man einen Satz nach dem ersten mal lesen auch verstehen und muss ein Kapitel nicht zwei- und dreimal durchlesen, nur weil man nebenher noch eine neue Sprache lernen soll.

Ich habe meinen ersten Computer zur Konfirmation von meinem Onkel geschenkt bekommen. Einen Sincair ZX-81. Der hatte sage und schreibe ein Kilobyte (1024 Byte) RAM und keine Möglichkeit der Speicherung. Also immer wenn ich etwas mit diesem Gerät tun wollte, musste ich erst mal Code eintippen, auf das dann etwas geschah. Das ist heute unvorstellbar, aber ich als kleiner Junge habe das so angenommen, wie man heute ganz selbstverständlich auf seinem Smartphone herum tippt. Ich fand das damals sehr faszinierend und habe mit Hilfe von Zeitschriften und Büchern mir selbst das Programmieren beigebracht und das tue ich heute noch, zwar in vollkommen anderen Konzepten, aber alles was ich kann, habe ich selbst zusammengetragen und autodidaktisch gelernt. Über die Jahre habe ich ein sehr tiefes Verständnis für die Funktionsweise von Computern und ihrer Software bekommen.

Wie bin ich zu Bitcoin gekommen?

Für mich fing die Reise mit Bitcoin 2020 an, als meine Ehefrau die Thematik mehrfach ansprach und ich, geprägt von der – Achtung jetzt kommt das böse Wort – Propaganda der Notenbanken und Banken, der Staatsorgane und Journalisten, brav wiederkäute, was ich in den Magazinen und Zeitungen gelernt hatte. „Bitcoin ist irreal“, „Das kann man nicht anfassen. Da sind Bits und Bytes und sonst nix“. Diese ganzen Sprüche, die wahrscheinlich heute jeder kennt. Das schlimme bei mir war nur, dass ich ja schon mindestens 15 Jahre zuvor begriffen hatte, dass das herrschende Geldsystem der größte Betrug aller Zeiten ist. Doch damals konnte ich eins und eins noch nicht richtig zusammenzählen.

Auf jeden Fall hat sie dann so ein wenig herum experimentiert und erreichte beachtliche monetäre Erfolge, was man natürlich als Mann dann nur schlecht rechtfertigen kann. Oder anders gesagt, ich wurde neidisch. Aber jetzt war noch immer die Indoktrination in mir und alle für mich Hörbaren haben gesagt, dass Kryptowährungen des Teufels sind. Ja genau alles Kriminelle! Also habe ich mir die Thematik angeschaut und je mehr ich las und sah, desto faszinierender wurde die Sache.

Und dann begann meine Reise in den Kaninchenbau...

Bitcoin ist die Antwort, aber wie lautet die Frage?

Bevor wir anfangen uns über eine geniale Lösung wie Bitcoin zu freuen, müssen wir erst einmal eine Bestandsaufnahme machen, welche Probleme eigentlich existieren und wo deren Ursachen zu verorten sind. Wir müssen uns vor Augen halten, was alles in unseren modernen Gesellschaften dysfunktional ist und da sind wir schon beim ersten der vielen Dilemma, denen wir tagtäglich begegnen. Unsere Gesellschaft ist so facettenreich, dass niemand wirklich mehr den Durchblick hat. Alle Teilbereiche sind so spezialisiert, dass wir nach dem ersten Draufschauen uns oft abwenden, denn uns beschleicht die Befürchtung, dass wir sowieso nicht genau wissen, wie die Dinge zusammenhängen und für die Einarbeitung haben wir keine Zeit und auch keine Lust. Wir sind also in den allermeisten Bereichen der Gesellschaft auf Glauben angewiesen. Wir müssen den Experten glauben und vertrauen, denn wir selbst wissen es nicht besser. Das ist ein, auf jeden Fall für mich, maximal unbefriedigender Zustand - der moderne Mensch sagt „No go“.

An den Anfang möchte ich noch so etwas wie eine Warnung stellen, denn die nächsten Seiten werden, eingedenk der Thematik, einfach nicht schön, obwohl Bitcoin ein so grandios positives Thema selbst ist. Es macht keinen Spaß dies zu schreiben und sich darüber Gedanken zu machen, aber leider ist es unausweichlich sich der Problematik unserer Welt zu widmen, bevor wir eine Lösung erarbeiten können. Wer nicht weiß was er kurieren soll, der wird keine Heilung herbeiführen können. Also gehen wir das mal an.

Wir leben unsere Leben so vor uns hin und bis auf ganz wenige Ausnahmen sind wir damit unzufrieden, denken, hoffen, es würde irgendwann mal besser werden und normalerweise gehen wir dann wieder frustriert ins Bett. Schauen wir uns die häufigsten Menschengruppen einmal an.

Haben wir kein Geld ist das mies. Die ganze Zeit ist man mental damit beschäftigt was alles nicht geht, wie man mit Behörden umzugehen hat, was man alles nicht essen kann, und so weiter, und so fort. Für viele ist dieser Zustand so schlimm, dass sie einen geistigen Ausweg suchen und diesen dann in Computerspielen, Alkohol und anderen Drogen vermeintlich finden. Das Problem dabei ist nur, dass all diese Lösungen zur Vereinsamung und weiteren Verelendung führen. Die Gegenbewegung des Party-Machens führt weiter in die Besitzlosigkeit und nach dem kurzen guten Gefühl stellt sich der selbe Zustand wie vorher ein. In Deutschland besteht nach der Einführung des Bürgergeldes sicher keine direkte, lebensbedrohliche Armut, auf jeden Fall verglichen mit Staaten in Afrika, Asien oder Lateinamerika, aber in einem Land wie Deutschland, in dem jeder Schritt draußen irgendwie Geld kostet, ist man, auch wenn der Staat vieles bezahlt, immer noch ständig pleite. Sehr schlimm ist auch die Situation der einfachen Rentner, die, meist aus Scham, mit ihren Renten, die weit unter dem Lebensminimum liegen, versuchen auszukommen, anstatt sich Hilfe von Behörden zu holen. Die erschütternden Bilder von alten Menschen, die in den Mülleimern nach Pfandflasche suchen ist einem Industrieland mehr als unwürdig, gehört aber leider heute zum normalen Straßenbild.

Haben wir normal viel Geld, reicht es nicht für die ganzen Dinge, die man doch auch gern haben möchte, für den Urlaub, den man sich verdient hat, kann man sich doch nie ein eigenes Haus leisten und das Auto wird ewig der Bank gehören. Es ist ein ewiges Leben von der Hand in den Mund. Und

dafür gehen wir Tag für Tag zur Arbeit? Wir laufen den ganzen Tag der Karotte am Stock hinterher, die irgendwer uns vor die Nase hält. Dieser Zustand macht uns unzufrieden und fördert Neid und Abgunst. Wir kommen uns ständig irgendwie betrogen vor, obwohl wir uns anstrengen und Leistung bringen. Doch all unser Tun verpufft ständig und alles was wir erwirtschaften zerrinnt wie Sand durch die Hande.

Aber wenn wir mehr Geld haben, als wir benötigen, dann stellt sich ganz aktiv die Frage, was man mit dem Geld noch machen kann. Sparen geht heute nicht mehr. Man bekommt mittlerweile zwar wieder minimale Zinsen, aber die werden von der Inflation sofort aufgefressen, heißt das klassische Sparbuch kann man sich gar nicht mehr leisten. Es gibt Aktien und Fonds und jede Menge andere Möglichkeiten Geld anzulegen, doch wenn man in diesem Spiel nicht versiert ist, bezahlt man nur die Party der Anderen. Und versiert zu sein ist nicht gerade leicht. Um zum Beispiel den Aktienmarkt im Auge zu behalten, braucht man sehr viel Zeit. Man sollte die ganzen drögen Artikel lesen, die über die Unternehmen geschrieben werden, die man schon im Portfolio hat und dann ist man ja natürlich ständig auf der Suche nach den neuen Zugpferden, die einen noch weiter nach vorne bringen. Überlässt man dies lästige Informationsflut dem Fondmanager, dann verdient der wenigstens Geld und man selbst ist so weit wie mit dem Sparbuch – vielleicht ein bisschen besser.

Man kann also sagen, dass viele Bereiche unseres Lebens mit dem Haben oder nicht Haben von Geld zu tun haben. Irgendwie hängt also etwas mehr am Geldbeutel, als man auf den ersten Blick vermutet. Was die vorangegangene Aufzählung zeigt ist, dass Geld uns ständig Stress macht, egal ob wir zu wenig oder zu viel haben.

Menschen die richtig reicht sind gibt es, aber die werden dieses Buch nie lesen, denn deren Welt ist vollkommen in Ordnung und die Probleme des Normalbürgers werden sie nicht verstehen. Wer reich im aktuellen System ist, sieht in Bitcoin eher eine Gefahr, als eine Lösung. Und mit diesem Gedanken im Hinterkopf leuchten wir auch schon mit unserer Taschenlampe in den dunklen Kaninchenbau.

Bitcoin ist Interdisziplinär

Bitcoin macht es den Menschen teilweise sehr schwer ihn zu verstehen, da der Ansatz so radikal[1] ist, weil er wirklich an die Wurzel (fast) allen Übels geht. Dazu müssen wir jetzt gemeinsam einen recht weiten Bogen spannen. Um das Konzept von Bitcoin zu verstehen brauchen wir die Fachgebiete Finanzwissenschaft, Geldpolitik, Volkswirtschaft, Sozialwissenschaft, Geopolitik, Energiewirtschaft, Softwareentwicklung und Computertechnik.

Diese Auflistung zeigt, wie ich finde, eindrucksvoll welche mentale Leistung Satoshi Nakamoto[2] erbracht hat, da alle diese Gebiete in der ursprünglichen Konzeption[3] von Bitcoin in einer ungeahnten Tiefe enthalten sind. Das Konzept endet nicht wie sonst üblich in der Forschung an den Grenzen des eigenen Fachbereichs, nein. Es wurden die Übel, oder besser gesagt die Fehler des aktuellen Systems analysiert, wirklich gesehen und eine Lösung aus der Sicht des Einzelnen und der Menschheit als Ganzes gefunden und nicht so wie bis dato üblich, rein aus der Sicht der Machthaber. Was wir als aller erstes und, wie ich finde, wichtigstes Merkmal von Bitcoin festhalten müssen ist, dass Bitcoin eine echte Graswurzelbewegung war und heute teilweise noch ist und nicht eines dieser vielen staatlich initiierten oder geförderten Trojanischen Pferde, die dem weiteren Machterhalt dienen sollen. Bitcoin gehört niemanden und kann von keiner zentralen Instanz kontrolliert oder verändert werden. Diesen Fakt darf man niemals aus den Augen verlieren. Er ist es, der Bitcoin wirklich einzigartig macht.

1 Radix, lat. Die Wurzel
2 Erfinder von Bitcoin. Es ist nicht klar wer dies ist, ob Einzelperson oder Gruppe
3 Das Konzept von Satosh Nakamoto - https://bitcoin.org/files/bitcoin-paper/bitcoin_de.pdf

Ich will hier einen kurzen Abriss aufzeigen, wie Bitcoin in den einzelnen Fachbereichen wirkt.

Als erstes nehmen wir uns der Softwareentwicklung und Computertechnik an, die ganz offensichtlich den Kern der ganzen Geschichte ausmacht. Bitcoin basiert auf den Erkenntnissen von fast 40 Jahren Kryptographie, sprich mathematischer Verschlüsselungstechnik. Der eigentliche Code der so genannten Blockchain ist recht trivial; ist eine Blockchain doch nichts anderes als eine ineffiziente Art einer Datenbank. In dem Konzeptpapier, dass Satoshi Nakamoto am 31. Oktober 2008 veröffentlicht hat, wurde festgelegt, dass die Menge aller jemals existierender Bitcoin auf knapp 21.000.000 Stück begrenzt ist und nach welchen Kriterien diese in 32 Zyklen geschöpft und verteilt werden. Das ursprüngliche Konzept wurde auf lediglich neun Seiten verfasst und zeigt eindrucksvoll, wie stringent und tief die Gedanken schon zu dieser Zeit waren. Das Protokoll ist selbstverständlich Open Source, heißt für alle zugänglich, und widerspricht der gängigen Industriepraxis der Geheimhaltung und Patentierung. Satoshi Nakamoto hat ganz bewusst, der Tradition der Cipherpunks[4] folgend, das große Ganze in den Vordergrund gestellt. Fast alle später erschienen Kryptowährungen basieren auf den damals veröffentlichten Grundannahmen, doch muss hier auch schon eingestreut werden, dass keine, in Worten, keine andere Kryptowährung die Qualitäten und die Sicherheit aufweist wie Bitcoin es tut.

Das Herz von Bitcoin ist die zugrundeliegende Datenbank, die man Blockchain nennt. Doch was ist eine Blockchain? Eigentlich ist es ganz einfach. Wir stellen uns eine Adressensammlung vor. Während klassische Datenbanken ähnlich wie eine Tabelle aufgebaut sind, ist die Blockchain wie eine Kette. Wenn wir uns einen Karteikasten vorstellen, so haben wir bei der klassischen Datenbank Reiter mit den Anfangsbuchstaben und dahinter finden wir dann alle Adresskarten zu diesem Buchstaben weiterhin alphabetisch geordnet. Der Zugriff auf die Information ist extrem schnell und effizient.

Bei der Blockchain müssten wir im gleichen Beispiel immer von der ersten Karte ausgehend schauen, mit welcher nächsten Karte diese verbunden ist, denn jede Karte bekommt einen Zeiger auf seinen Vorgänger und Nachfolger. Und so hangeln wir uns von Karte zu Karte, bis wir die richtige gefunden haben. Das klingt nicht besonders effizient, hat aber den bestechenden Vorteil, dass jede Adresskarte für sich beweist, dass die vorherige Karte wirklich in unsere Adresssammlung gehört und nicht rein geschmuggelt wurde. Und dann macht die Kette noch etwas revolutionäres, denn alle Informationen der Adresskarte, des Blockes, werden mathematisch zu einer Zahl transformiert, dem sogenannten Hash[5], sowas wie ein digitaler Fingerabdruck des vorherigen Blocks, die wiederum Teil des Zeigers auf den vorherigen Block ist. Das bedeutet, dass nicht nur immer und zu jeder Zeit bewiesen wurde, dass die Adresskarte zur Sammlung gehört, sondern auch dass alle Daten, die die Karte beinhaltet unverändert sind. Auf diese Weise wurde zum ersten mal ein Mechanismus geschaffen, der ein digitales Gut, ein Datenfeld, eindeutig verifizierbar macht. Das ist die eigentliche technische Revolution. Aber zugegeben, effizient ist das nicht und muss es auch gar nicht sein.

Aber es geht noch weiter. Das Verfahren des Minings[6], das heiß nichts anderes als einen neuen Block an die Kette anhängen, funktioniert nach einem bis dorthin unbekannten Verfahren. Der Miner, das sind Computer, die die ganze Zeit nichts anderes machen als eine Art Puzzle zu lösen, verbrauchen bei diesem Vorgang Strom und wandeln diesen in Wärme um. Zu der viel diskutierten

4 Cypherpunk ist eine politische und technologische Bewegung, die sich für Verschlüsselung, digitale Privatsphäre und Anonymität im Internet einsetzt. Ihre Ziele sind der Schutz der individuellen Freiheiten und die Dezentralisierung von Macht gegenüber staatlicher und korporativer Kontrolle.

5 Hash, engl. Streuwert kann als digitaler Fingerabduck verstanden werden.

6 Mining, engl. schürfen

Energieverschwendung muss auch noch einiges gesagt werden, aber wichtig für uns ist im Moment nur, dass der Miner Strom braucht.

Es ist absolut unabdingbar, dass die Miningcomputer Strom verbrauchen müssen um dieses ominöse Puzzle zu knacken. Wer das als erster schafft, darf den Block an die Kette anhängen und bekommt dafür eine Anzahl Bitcoins ausbezahlt. Bis dato waren dies 6,25 Stück und seit dem 20. April 2024 sind es nur noch 3,125 Stück. Das hängt mit dem sogenannten Halving[7], der Halbierung der Auszahlung, zusammen, aber auch dazu später mehr.

Wir müssen uns klar machen, warum dieser Strom verbraucht werden muss, um eine der ganz fundamentalen Säulen von Bitcoin zu verstehen. Nur wer Strom und Zeit für den Betrieb von Computern aufwendet kann überhaupt dieses ominöse Puzzle lösen und beweist dadurch, gebunden an die fundamentalsten Gesetze der Physik, dass dies ehrlich vollbracht wurde und je mehr Computer sich an diesem Prozess beteiligen, desto schwieriger wird das Rätsel. Das bedeute aber auch und jetzt ist wirklich ein Trommelwirbel von Nöten – tataaaa – man kann Bitcoins nicht einfach so erzeugen. Man kann nicht wie eine Notenbank einfach mal 10 Milliarden Dollar/Euro/Yen/Rubel/Renminbi erzeugen, auf Knopfdruck, mit einem Kreditvertrag oder Staatsanleihen, nein geht nicht. Und der Takt, in dem diese neuen Blöcke gefunden werden können ist auf zirka 10 Minuten festgelegt, das ist quasi der Herzschlag von Bitcoin. Daraus folgt ganz konsequent, egal was passiert, man kann nicht auf die Schnelle mal 1000 Bitcoin produzieren. Das kann niemand und wird niemals jemand können. Wir werden noch erfahren warum. Aktuell werden etwa 450 Bitcoin (3,125 Stück x 6 Stück pro Stunde x 24 Stunden) am Tag geschürft und alle 4 Jahre halbiert sich diese Menge. Dieser Vorgang geht noch so weiter bis ins Jahr 2140 da endet das Schürfen aber auch dazu werden wir später mehr erfahren und warum dann nicht alles zusammenbricht.

Aber wir müssen noch kurz klären, was den jetzt so toll an so einem Block ist, außer das derjenige, der ihn findet sich bereichern darf. Ganz einfach. Dies ist die einzige Möglichkeit neue Daten, neue Adresskarten wenn man so will, in die Datenbank einzupflegen. Man kann sich das in etwas so vorstellen wie ein riesiges T-Konto und in jedem Block stehen neue Transaktionen, die das Konto immer weiter verlängern. Es wird dokumentiert, wer besitzt was zu welcher Zeit und übergibt an wen. Mehr ist es im Grunde nicht – ein Kassenbuch. Ein weitere Clou ist, dass die maximale Größe der Blocks begrenz ist auf im Original 1 Mega Byte (1 Million Byte), was 2017 durch eine Regeländerung auf 4 Mega Byte vergrößert wurde. Warum ist das wichtig? Ganz einfach. Das gewährleistet, dass die gesamte Datenbank nicht so groß werden kann, als dass nur noch institutionelle Parteien mit Großrechenzentren die Datenbank verwalten können, sonder jeder von uns. Jeder kann die gesamte Blockchain zuhause haben.

Um den kleinen Exkurs in den technischen Teil abzuschließen müssen wir uns noch damit befassen, wie dieses komische Bitcoin – Blockchain – Halbierungsding eigentlich funktioniert. Alles voran geschriebene ist eine tolle Sache, hat aber nur den klitzekleinen Nachteil, dass es nur funktioniert, wenn wir sicherstellen können, dass alle Menschen auf der Welt mit den selben Daten arbeiten, oder in dem Beispiel der Adresssammlung, dass alle nur auf die im Karteikasten hinterlegten Adresskarten zugreifen können. Und hier kommt das Internet ins Spiel und die tausenden Knotenpunkte aus denen Bitcoin besteht, auch Nodes[8] genannt. Hier sehen wir auch den bestechenden Vorteil, wenn die Datenmenge klein ist und von sehr vielen Benutzern verwaltet werden kann.

7 Das Halving beschreibt die Halbierung Ausschüttung für neu gefundenen Blocks. Diesen Vorgang wird es insgesamt 32 mal geben.

8 Node – engl. für Knoten, oder Knotenpunkt

Der Mechanismus, den die normale Bankenwelt benutzt um sicher zu stellen, dass ein bewegter Dollar/Euro/Yen auch wirklich nur einmal bewegt wird, nennt sich Clearing. Das sind Dienstleister, die den ganzen Tag nichts anderes machen als, einem Notar gleich, zu bestätigen, dass Geld von A nach B ging, wann das war und wie viel. Und das schöne daran ist, dass diese Menschen das alles nicht umsonst machen. Wir produzieren jede Menge Gebühren. Mit jeder Kartenzahlung im Supermarkt, oder mit der Kreditkarte im Internet, beim Zahlen mit dem Telefon und auch wenn wir Bargeld zur Bank schleppen, denn das geht ja irgendwann auch wieder zur Zentralbank und muss streng bewacht werden. Ständig verdient jemand mit und diese Dienstleister wissen sehr genau, was wir den lieben langen Tag so machen. Wer den Geldstrom kontrollieren kann, kann den Menschen kontrollieren. Und auch in diesem Punkt ist Bitcoin sensationell, denn jeder kann die gesamte Blockchain, also die gesamte Datenbank, bei sich zu Hause haben und nimmt damit den Clearingdienstleistern ihr Geschäftsmodel weg. Das bedeutet nichts weniger, als dass Bitcoin es geschafft hat ein vertrauensloses Netzwerk zu erschaffen, denn mit zirka 250 € kann man sich einen Knotnpunkt, neudeutsch Node, holen und selbst im Keller nachverfolgen, was alles in der Blockchain passiert. Und wenn die Daten nicht mit denen im Keller übereinstimmen dann gibt es keinen neuen Block, dann gibt es keine neue Transaktion, dann werden keine neuen Bitcoin ausgeschüttet. Nur wenn alle einverstanden sind, und ich meine alle, geht die Ampel auf grün. Bitcoin ruiniert also das klassische Bankengeschäft und diese müssen in einer Bitcoin-Welt sich bessere und nachhaltigere Geschäftsmodelle ausdenken, wenn sie nicht dem Vergessen anheim fallen wollen. Man muss das nochmals ganz explizit sagen. Dadurch, dass viele tausend verteilte Knotenpunkte weltweit ständig kontrollieren, dass die vereinbarten Regeln befolgt werden, hat Bitcoin es geschafft, ganz ohne Vertrauen ein weltweit funktionierendes Netzwerk zu sein. Weil Jeder zu jeder Zeit alles kontrollieren kann, muss niemand niemandem vertrauen.

Jetzt haben wir also ein nicht manipulierbares, nicht unbegrenzt ausweitbares, knappes und noch dazu vertrauenloses Gut, voll digitalisiert und mit ständigem Zugriff. So etwas gab es noch nie und ich prophezeie, dass es das auch nie wieder geben wird, denn damit hat sich Bitcoin bei den Mächtigen dieser Welt maximal unbeliebt gemacht.

Eine Kleinigkeit müssen wir noch anfügen. Ein Grund, warum Bitcoin einen so schlechten Ruf bei der traditionellen Autoritäten hat ist, dass es fast anonym ist. Mittlerweile ist dies nicht mehr wirklich so, aber in der Blockchain steht nicht drin, wer welche Transaktion ausgeführt hat, sondern welche Adresse, welche Transaktion ausgeführt hat. Eine Adresse ist dabei eine alphanumerische Zeichenfolge, die einem bestimmten Muster folgen muss. Klarnamen erscheinen nicht. Und dies ist einer der Hauptgründe, warum Bitcoin verschrien ist bei den Mächtigen und ihren Helfern der Polizei. Heute ist es ein Sekundenaktion die Bankkonten eines normalen IBAN-Bankkunden zu analysieren. Und die Staaten machen regen Gebrauch davon. Bitcoin ist da sehr viel schwieriger, aber in letzter Konsequenz ist man nicht vollständig anonym.

Geld regiert die Welt

Als nächstes wollen wir uns anschauen, in wie weit Bitcoin in die Finanzwissenschaften, die Geldpolitik und in die Betriebs- und Volkswirtschaft eingreift. Ein Wort vorweg – das tut Bitcoin nicht zu knapp. Ich verwende den Begriff Geld hier für alle verschiedenen Formen von Zahlungsmittel, auch wenn diese im strengeren Sinne kein Geld sind, denn allen ist eines gemeinsam. Es ist immer Betrug.

Zuerst haben wir eine Bestandsaufnahme zu erledigen. Wir müssen uns die Fragen beantworten. Was ist Geld? Woher kommt Geld? Wer kontrolliert das Geld? Diese drei sehr kurzen Fragen gehören zu den großen Mysterien unserer modernen Welt. Bis vor zirka 10 Jahren wurden noch

selbst von Professoren und Bankvorständen die wildesten Theorien verbreitet, dass unser Geld bei Banken im Keller liegt und bei Bedarf an Häuslebauer als Kredit ausgegeben wird. Mittlerweile ist der Druck auf diese Personen so groß geworden, dass niemand mehr ernsthaft bestreitet, dass wir in einem Fiatgeldsystem[9] leben. Doch beginnen wir ganz vorne.

In den letzten 5.000 Jahren gab es verschiedene Geldformen, die im Regelfall auf Rohstoffen aufgebaut haben. Sei es nun Gold oder Silber, aber auch Muscheln wurden als Geld verwendet. Davor wurde direkt getauscht, also keinerlei Transmitter verwendet. Eines der frühesten Zahlungsmittel war das so genannte Elektron, ein Gemisch aus Gold und Silber welches in Kleinasien, der heutigen Türkei und dem südlichen Griechenland, verwendet wurde. Dabei wurde das Metallgemisch auf Tontafeln gewogen um seinen Wert zu bestimmen und es im Tausch einzusetzen. Rohstoff basiertes Geld bezieht seine Werthaltigkeit aus verschiedenen Attributen des Rohstoffes. Bei Gold und Silber ist es die Knappheit und vor allem die Unverwüstlichkeit. Beide Metalle hatten in der Antike keinerlei technologischen Wert, im Gegensatz zu heute, wo sehr viel Silber in der Industrie eingesetzt wird und auch Gold in produktiven Prozessen Verwendung findet. Es war sehr schwer an die Edelmetalle zu gelangen. Stollen mussten tief in die Erde getrieben werden und die Logistik für den Unterhalt von Minen war beträchtlich. Das Produkt waren Metalle, die nicht verwitterten. Sie hatten die chemische Beständigkeit wie Stein, waren aber in jeder Weise formbar. Man konnte Schmuck herstellen oder eben Münzen prägen. Der wichtigste Aspekt bei der Verwendung von Gold und Silber als Tausch und Zahlungsmittel war aber mit Sicherheit, dass diese Abbaustätten durch wie auch immer geartete Machthaber kontrolliert werden konnten. Damit wurde zum einen das Monopol auf den Rohstoff als auch die eigene Verfügbarkeit sicher gestellt.

Aber es gab in der frühen Geschichte auch schon abstraktere Formen von Geld. Die Sumerer aus Mesoputamien, deren Keilschrift als die älteste bislang bekannte Schriftform gilt, verewigten auf Tontafeln Verträge, Transaktionen und eben auch Schuldverschreibungen. Es wurde zum Beispiel festgehalten, dass ein Schafhirte mit einer Herde von 100 Schafen auszog und bei seiner Ankunft wurde nachgezählt und der Überschuss, sprich der Naturalzins, wurde festgestellt. Diese Tontafeln galten als rechtliche Titel und wurden, laut den Archäologen, gehandelt, wie wir heute auch mit Wertpapieren handeln. Damit ist dies im Grunde die älteste Form von abstraktem Geld. Wichtig ist zu erkennen, dass Geld heute im Gegensatz zur Frühzeit nur mit einer „rechtlichen“ Grundlage funktionieren kann. Im Normalfall ist dies das Gewaltmonopol des Staates, oder des Regenten, der seine Bürger dazu zwingt sein Geld zu verwenden. Bei den Sumerern beruhte dies noch auf Freiwilligkeit und dem Konsens des Nutzens. Spätestens im antiken Griechenland und Rom war es mit der Freiwilligkeit allerdings vorbei.

Geld ist also das was wir als Geld ansehen, uns als Geld angeboten wird. Es wird sehr oft von intrinsischen[10] Werten von Geld gesprochen. Nach meiner festen Überzeugung ist dies vollkommener Nonsens. Geld war zu keiner Zeit mit einem intrinsischen Wert ausgestattet, ganz im Gegenteil; was könnte auch ein intrinsischer Wert von Geld sein? Ein intrinsischer Wert wäre zum Beispiel der Nährwert, sprich, ob das Geld jemanden satt macht, oder der Heizwert, oder jede andere Form von direkten Bedürfnisbefriedigungen der ersten beiden Stufen der Maslowschen Bedürfnispyramide. Jeder kennt den Ausdruck, dass man Geld nicht essen kann, was veranschaulicht, dass es den Menschen schon seit Jahrtausenden vermutlich klar ist, dass Geld nur in der Interaktion in der Gruppe Wert erhalten kann und logischerweise die Gruppe, die, wenn man so will, Intrinsizität beziehungsweise den inneren Wert erzeugt. Die Mär vom inneren Wert des Geldes ist, man kann es nicht anders sagen, eine der ältesten Lügen, oder netter formuliert, Unwahrheiten, die keinen anderen Zweck verfolgt, als das Herrschaftsmittel Geld, und es ist nichts

9 Fiat, lat – es werde

10 Intrinsisch, lat – aus sich stammend, aus sich selbst hervorbringend

anderes, in einem Licht darzustellen, dass es für jeden begehrlich macht. Nur wenn die Menschen sich durch welche Mittel auch immer auf einen Standard einigen, zum Beispiel den Golddinar, dann erhält der Golddinar Bedeutung und Wert. Es sind die Attribute Knappheit, Authentizität (Reinheit), Verfügbarkeit, Akzeptanz, Freiheit und Zwang, die egal welches Gut dieser Welt, zu Geld machen, aber niemals die spezifische Dichte oder das schöne Äußere. Gold wird, lässt man es einfach liegen, niemals irgend etwas bewirken. Sein Wert in der Umwelt, getrieben durch Angebot und Nachfrage mag sich stark verändern, aber von sich aus macht Gold einfach nichts. Gar nichts. Das heißt nicht, dass Edelmetalle nicht als Geld taugen. Die Bindung von Metallen an das herrschende Geld ist ein recht mächtiger Mechanismus um einem Auswuchs des Geldes, der Inflation[11], Herr zu werden, doch zeigt die Geschichte auch hier, dass dies sehr viel öfter nicht gelungen ist als das Erfolge zu verzeichnen waren.

Der Ethnologe David Graeber hat in seinem Buch, Schulden, die ersten 5.000 Jahre[12], wie ich finde, eindrucksvoll aufgezeigt wie die madagassische Urgesellschaft durch die französischen Kolonialherren von einer Tauschgesellschaft in eine zutiefst abhängige Geldherrschaft gestoßen wurden, mit allen möglichen und unmöglichen Unappetitlichkeiten, die das Besatzertum zu bieten hat. Und dabei war die Ausbeutung des Landes, vor allem die Produktion von Vanille und Gewürznelken, nicht an vorderster Stelle zu sehen, sondern die Ausweitung des französischen Währungsraumes.

Damit sind wir beim nächsten dunklen Kapitel von Geld, dem Wachstumszwang. Damit ein vereinbartes Geld stabil bleibt, ist es nahezu unausweichlich, dass sich der Währungsraum vergrößert und damit mehr Wertschöpfung an den Herausgeber fließt. Am Beispiel der Kolonialisten war dies so, dass beispielsweise das englische Imperium in der viktorianischen Epoche[13] Region für Region unterjocht hat und die produktiven Gewinne ins englische Mutterland geflossen sind. Auf diese Weise sind Teile der englischen Gesellschaft extrem reich geworden. Jetzt kann man glauben, dass dies nur durch die Zwangsarbeit der versklavten Menschen möglich war, aber der eigentliche Mechanismus, war der, dass die englischen Aristokratie diejenigen zur Kasse gebeten haben, die vor Ort in Indien, Amerika, Afrika, der Karibik und sonst wo auf der Welt, die eigentliche „Drecksarbeit“ gemacht haben, in dem Land und Menschen erbarmungslos ausgebeutet wurden. Der Hochadel hat die Landbesitzer und Plantagenbetreiber vor Ort ausgenommen wie Weihnachtsgänse, die, um selbst dennoch reich zu werden, noch extremer nach unten getreten haben. Kein König oder Kaiser hat sich selbst die Hände schmutzig gemacht, sondern durch das Erheben von Steuern und Abgaben, sowie durch die Vergabe von Schuldverschreibungen und ganz besonders durch das aufblähen und schrumpfen der Geldmenge wurden die Reichtümer transferiert. Und jeder Kolonialherr hat selbstverständlich nur seine eigene Währung als Zahlungsmittel akzeptiert. Diesen Umstand sollte sich wirklich jeder vor Augen halten, wenn man in London, Paris, Amsterdam, Madrid und so weiter auf der Sightseeingtour die Prachtbauten bestaunt. Erschaffen aus dem größtmöglichen Elend, aus Blut und Tod anderer Zivilisationen. Abgesaugt und angehäuft von ein paar Wenigen. Natürlich sind die Bauwerke architektonisch toll und die Juwelen imposant, aber die heutigen Nutznießer sind sehr bemüht, die menschenfeindliche Grundeinstellung, die heute noch genauso ist wie damals, zu verschleiern oder zu relativieren. Wir haben vor nicht all zu langer Zeit eine Bewegung in der westlichen Welt erlebt, die sich kritisch mit dem Kolonialismus auseinandergesetzt hat. Diese Bewegung wurde gezielt so radikalisiert bis hin zum Bildersturm, als Denkmäler abgerissen wurden, so dass sie in der Gesellschaft keine Akzeptanz mehr gefunden hat und sehr schnell wieder eingeschlafen ist. Schauen wir uns die Finanziers dabei an kommen die üblichen Stiftungen wie die Ford Foundation, die Bill & Melinda Gates Foundation, aber auch die

11 Inflare, lat – Aufblähen, anschwellen
12 David Graeber – Schulden die ersten 5.000 Jahre, ISBN 9783608947670
13 Viktorianische Epoche – von 1837 bis 1901 ist die Zeit der Königin Victoria, sehr starker Imperialismus

Open Society Foundations zum Vorschein. Alles sogenannte Nichtregierungsorganisationen, die immer dabei sind, wenn es etwas zu holen gibt, oder systemkritische Tendenzen eingefangen werden sollen. Ein anderes Beispiel für diese Art der Lahmlegung und Unterwanderung von Protest war Occupy Wallstreet.

Im September 2011 begann eine Protestbewegung gegen die wirtschaftliche Ungleichheit und den Einfluss der Finanzindustrie auf die Politik in den USA. Alles startete mit einer Demonstration im Zuccotti Park in New York City, die von der Zeitschrift "Adbusters" initiiert wurde. Die Demonstranten nannten sich selbst "die 99 Prozent" und richteten sich gegen die "1 Prozent" der Bevölkerung, die den größten Teil des Vermögens und der Macht innehaben. Sie kritisierten den Einfluss von Großkonzernen und Finanzinstituten auf das politische System sowie wachsende soziale Ungleichheit. Die Bewegung verbreitete sich schnell in viele andere Städte der USA und auch international. Besetzte Plätze und Straßenlager wurden zu Zentren des Protests. Die Polizei ging teilweise mit Gewalt gegen die friedlichen Demonstranten vor. Vor allem aber wurden in allen großen Zeitungen „Berichte“ und „Artikel“ veröffentlicht, die sehr kritisch mit den Demonstranten umgingen. Diese sogenannte Berichterstattung wurde wieder durch die üblichen Geldgebern gekauft und der Protest so abgewiegelt. Auch hier verlor die Bewegung durch gezielte Manipulation an Akzeptanz und damit schlief sie ein.

In der Währungstheorie wird behauptet, dass eine Währung wachsen muss, damit wirtschaftliche Stabilität erhalten werden kann. Dies folgt der selben Logik, wie die Geschichte von ewigen Wirtschaftswachstum, ohne dem die sich immer höher auftürmenden Schulden nicht mehr finanziert werden können. Der Wachstumswahn wird auf alle Teile der Wirtschaft und eben auch auf das Geld selbst ausgeweitet. In Wahrheit ist es aber so, je stärker eine Währung missbraucht wird, desto größer muss ihr Verbreitungsrahmen sein um zu verhindern, dass die Währung abgelehnt werden kann. Wir sehen es heute am US-Dollar, der aktuellen Weltleitwährung. Durch die extreme Ausdehnung und den de facto Zwang zur Verwendung des sogenannten Petro Dollars haben die Vereinigten Staaten die Möglichkeit riesige Summen an Geld in Umlauf zu bringen, wofür sie in absehbarer Zeit niemals eine Gegenleistung erbringen müssen. Einfach, weil man die meisten internationalen Geschäfte in US-Dollar abwickelt, müssen Käufer den US-Dollar vorhalten (Für den Euro gilt es äquivalent in abgeschwächter Form.) Dieser Mechanismus wurde begründet, nach dem der US-Präsident Richard Nixon 1971 den so genannten Goldstandard „temporär“ ausgesetzt hatte, da die amerikanische Wirtschaftsleistung nicht ausreichte um den damals tobenden Vietnamkrieg zu bezahlen. Zuvor war 1944 im Abkommen von Bretton Woods festgelegt worden, dass für eine Unze Gold, das sind 28,34 Gramm, fix 35 Dollar bezahlt werden musste. Nachdem der Goldstandard offiziell aufgekündigt wurde, konnten die USA Staatsanleihen in nahezu unbegrenzter Menge ausgeben und ihre desaströse Militärpolitik finanzieren. In den folgenden Jahren hat sich dieses System immer weiter verselbstständigt, und damit der Dollar nicht total inflationiert, kam die Administration von Richard Nixon auf die geniale Idee, mit dem arabischen Königshaus Saud auf der arabischen Halbinsel, die unverhofft auf riesigen Ölmengen saßen, zu vereinbaren, dass nur noch saudisches Öl gegen US-Dollar verkauft werden darf. Dafür sicherten die USA dem Königshaus bedingungslose Waffenbruderschaft zu. Man kann auch sagen, egal was die Saudis machen, die USA wird jeden Gegner weg bomben, damit die eigene Währung nicht zusammen bricht. Dieses Abkommen war deshalb so unglaublich erfolgreich, weil Rohöl das meist gehandelte Gut dieser Erde ist und so wurden alle Staaten dazu verdammt, US-Dollar vorzuhalten. Anzumerken ist, das der saudische Ölkonzern Saudi Aramco der größte Ölkonzern der Welt ist und im Vergleich aller Konzerne auf Platz vier rangiert. Wenn wir uns die Unternehmen auf den Plätzen 1 bis 3 anschauen, dann sehen wir sofort wie das neue Öl unserer Zeit heißt und auch diese Firmen sind unter amerikanischer Kontrolle. Heute sind Daten und EDV Dienstleistungen so wertvoll, oder vielleicht noch wertvoller als die klassischen Rohstoffe.

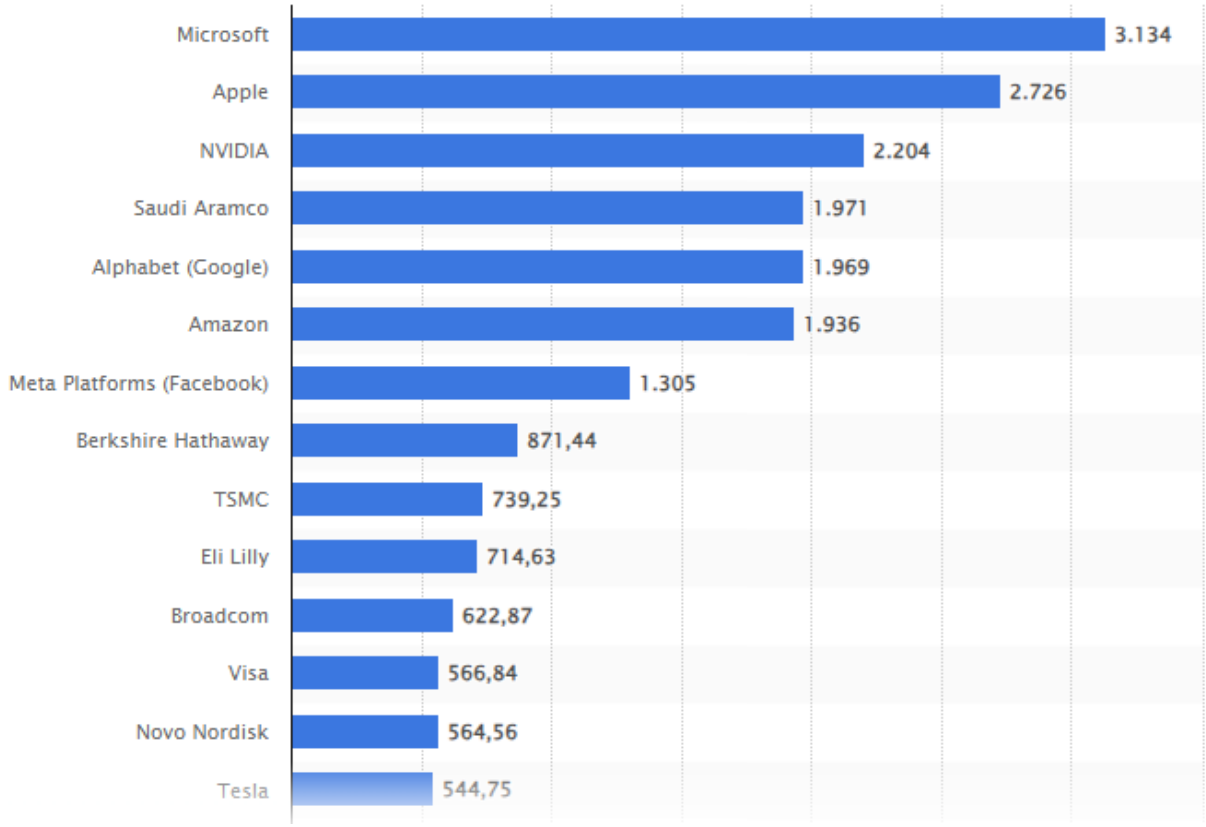


Abbildung 1: Liste der wertvollsten Unternehmen der Welt nach Markkapitalisierung – Quelle Statista

Was geschah 1971?

Wir müssen mal kurz innehalten und diesen Punkt der Aufhebung des Goldstandards noch näher ausführen, denn mit dieser Entscheidung der US-Administration wurde unsere moderne Welt von den Füßen auf den Kopf gestellt. Auf der Seite des Blocktrainers[14] gibt es einen sehr guten Artikel dazu. Es ist vollkommen klar, dass zuvor mit der Goldbindung nicht alles sprichwörtlich Gold war, was glänzte, aber die Menschen hatten in einem modernen Umfeld eine relative Sicherheit und konnten im Rahmen einer normalen Familienstruktur zu angemessenem Wohlstand gelangen. Mit der Aufhebung des Goldstandards und der so genannten Liberalisierung Anfang der 1980er Jahre brachen alle Dämme und die Menschen wurden in ihre Hamsterräder gesperrt, in denen sie bis heute noch rennen und zappeln. Es ist bisweilen putzig wie vor allem linke Politiker immer beschwören, dass wenn man sie nur an die Macht ließe, wieder Zustände wie in den 80er und 90er Jahren herrschen würden und das mit ein paar Reformen alles wieder gut würde. Nichts kann weiter von der Wahrheit weg sein als diese Theorien. Auf der Basis der heutigen Geldschöpfung ist Wohlstand für alle unmöglich.

14 Quelle – Blocktrainer | https://www.blocktrainer.de/wtf-happened-in-1971-deutsch/

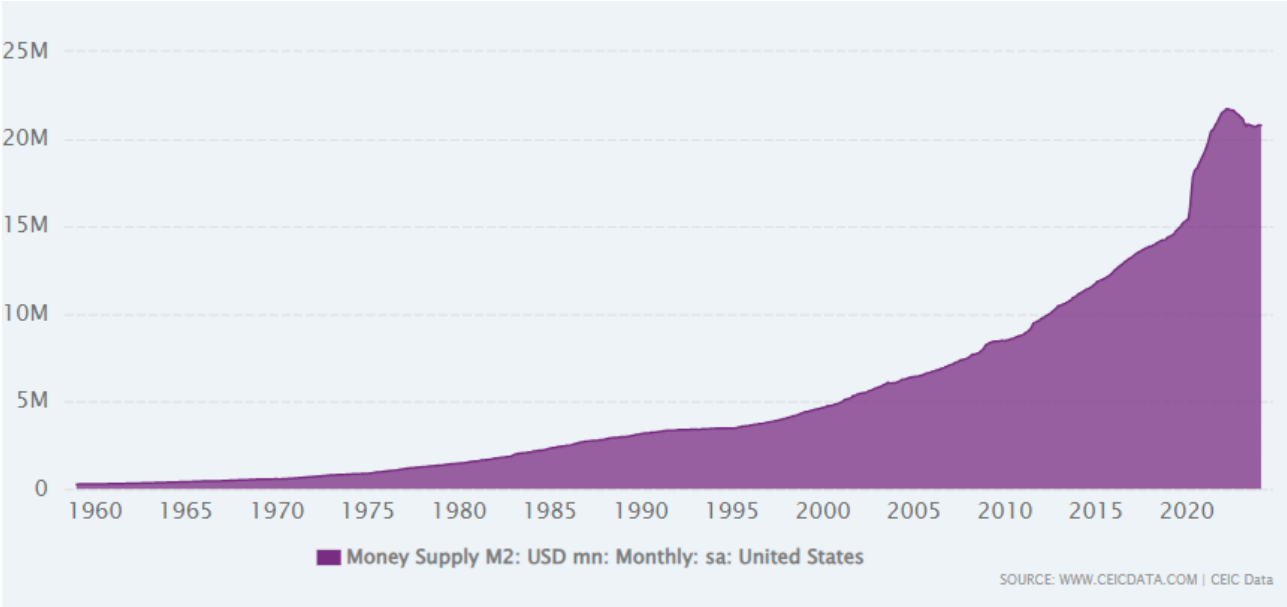


Abbildung 2: Umlaufende Geldmenge des US-Dollars M2

Beginnen wir mir der umlaufenden Geldmenge M2 des US-Dollars. Diese lag im Jahre 1971 etwa bei 610 Milliarden Dollar. 1960 lag sie noch bei zirka 290 Milliarden Dollar und hat sich also in diesen 11 Jahren etwa verdoppelt, aber wenn wir uns die Zahl heute anschauen, die bei fast 22 Billionen liegt, dann sehen wir, dass mit der Aufhebung der Bindung an Gold die Ausweitung exponentiell vorangetrieben wurde, oder man kann auch sagen, dass alle Hemmungen abgelegt wurden. In dieser Zeit hat sich die Geldmenge ver-35-facht. Oder andersherum gesprochen; ein Dollar heute ist nur noch 2,8 Cent von damals wert. Während der weltweit grassierenden Erkrankung von 2019 bis 2021 wurden fast 30% aller jemals erschaffenen US-Dollar in Umlauf gebracht. Ein Trend, der jetzt mit extremen Aufwand wieder eingefangen werden soll. Ein Blick auf den rechten Teil des Graphen zeigt, dass nachdem die Ferderal Reserve[15] die Zinsen nach dem Ende der grassierenden Krankheit angehoben hat, sich die Geldmenge leicht verringert hat. Derzeit liegt das Niveau knapp unter 21 Billionen US-Dollar. Dieser Rückgang der Geldmenge wurde sehr teuer erkauft, da durch die Zinsanhebung sich Kredite verteuern und der amerikanische Staat heute etwa 800 Millarden[16] US-Dollar jährlich aufbringen muss, nur um den Zinsdienst zu leisten. Aber auch Unternehmen und private Kreditnehmer leiden massiv unter den anfangs zu billig herausgegebenen Krediten, die sich durch die Anhebung des Leitzinses etwa verachtfacht haben. Das es in der Eurozone[17] nicht besser ist, zeigt der untenstehende Graph. Hier ist der Rückgang geringer ausgefallen, obwohl die Zinssätze ähnlich hoch sind.

15 Ferderal Reserve, kurz FED wird als Zentralbank der USA gesehen, ist aber in Wirklichkeit ein Zusammenschluss aus 12 privaten Banken, die einer besonderen Rechtsprechung unterstehen.

16 Quelle - https://www.usdebtclock.org/index.html

17 Quelle - https://de.statista.com/statistik/daten/studie/241824/umfrage/entwicklung-der-geldmenge-m2-in-der-euro-zone/

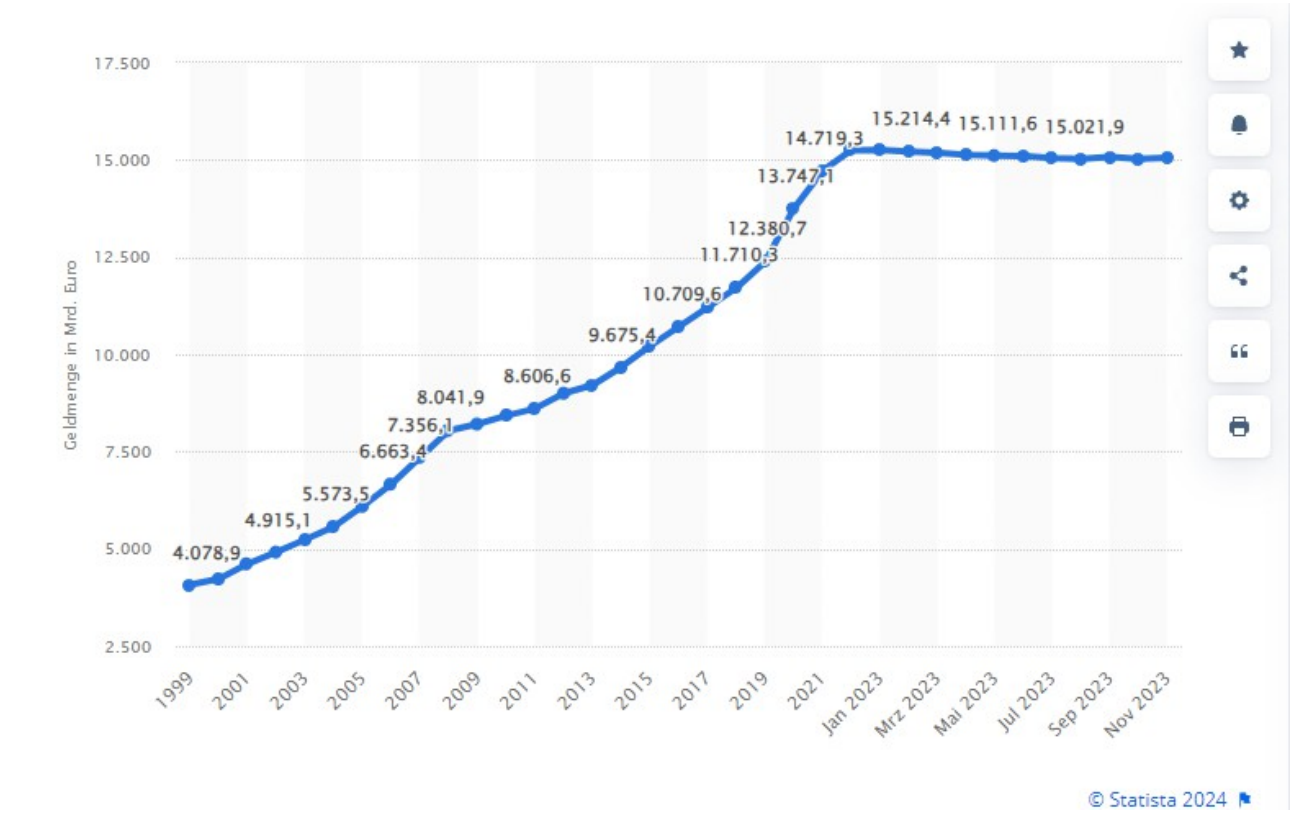


Abbildung 3: Umlaufende Geldmenge des Euro M2

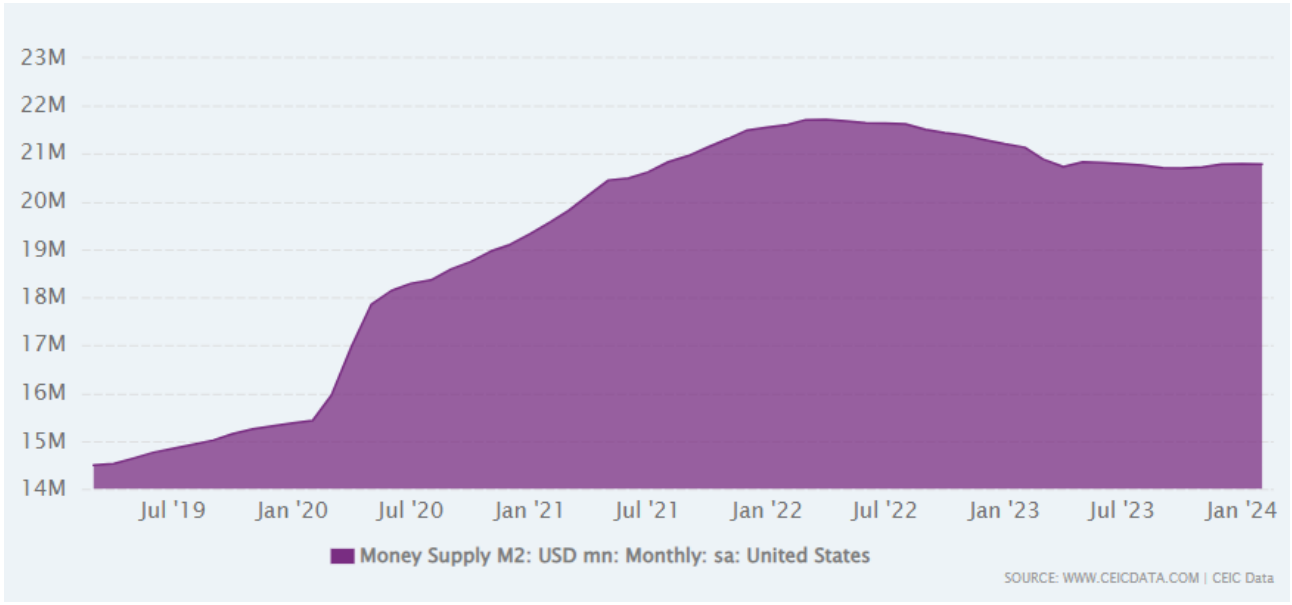


Abbildung 4: Umlaufende Geldmenge M2 des US-Dollars in den letzten 5 Jahren

Wenn wir uns die den Goldpreis anschauen, dann ist klar, bis 1971 war dieser nahezu fix. 35 US-Dollar pro Feinunze[18] Gold. Und dieser Zustand hielt, mit kleinen Korrekturen vor dem Bretton

18 Unze, lat unica – der 12. Teil. Eine Unze entspricht einem Gewicht von 28,35 Gramm

Woods Abkommen seit dem ausgehenden 18. Jahrhundert. Schauen wir uns heute den Goldpreis an, so kostet eine Unze Gold weit über 2.000 Dollar, also das mehr als 60-fache von damals, Tendenz stark steigend. Wenn wir dazu noch wissen, dass die größten Mengen an Gold die gehandelt werden gar nicht physisch vorliegen, sonder in Form von Zertifikaten und die Menge an Zertifikaten, wir erinnern uns, ein Zertifikat ist eine Beglaubigung, dass die nominal angegebene Menge an Gold auch physikalisch hinterlegt ist, den physikalischen Bestand um das 122-fache[19] übersteigt, so müsste der Goldpreis heute bei über 144.000 $ liegen. Tut er aber nicht und was mich dabei immer sprachlos zurück lässt ist, dass alle Händler das wissen und sich niemand darüber wundert, wie es sein kann, dass die Emittenten der Zertifikate derart dreist lügen dürfen und nie dafür zur Rechenschaft gezogen werden. Es ist ja so, dass diese Beglaubigungen von verschiedenen Institutionen wie Zentralbanken, Geschäftsbanken und Händlern ausgegeben werden. Früher nannte man so etwas noch bandenmäßigen Betrug, aber heute ist diese Praxis Usus und weithin akzeptiert. Darin begründet sich mein ärgster Kritikpunkt an Gold, denn durch diese extreme Manipulation ist Gold kein reelles Handelsgut mehr. Nichts desto trotz sollte Gold in jedem guten Portfolio sein.

19 Quelle - https://www.usdebtclock.org/index.html

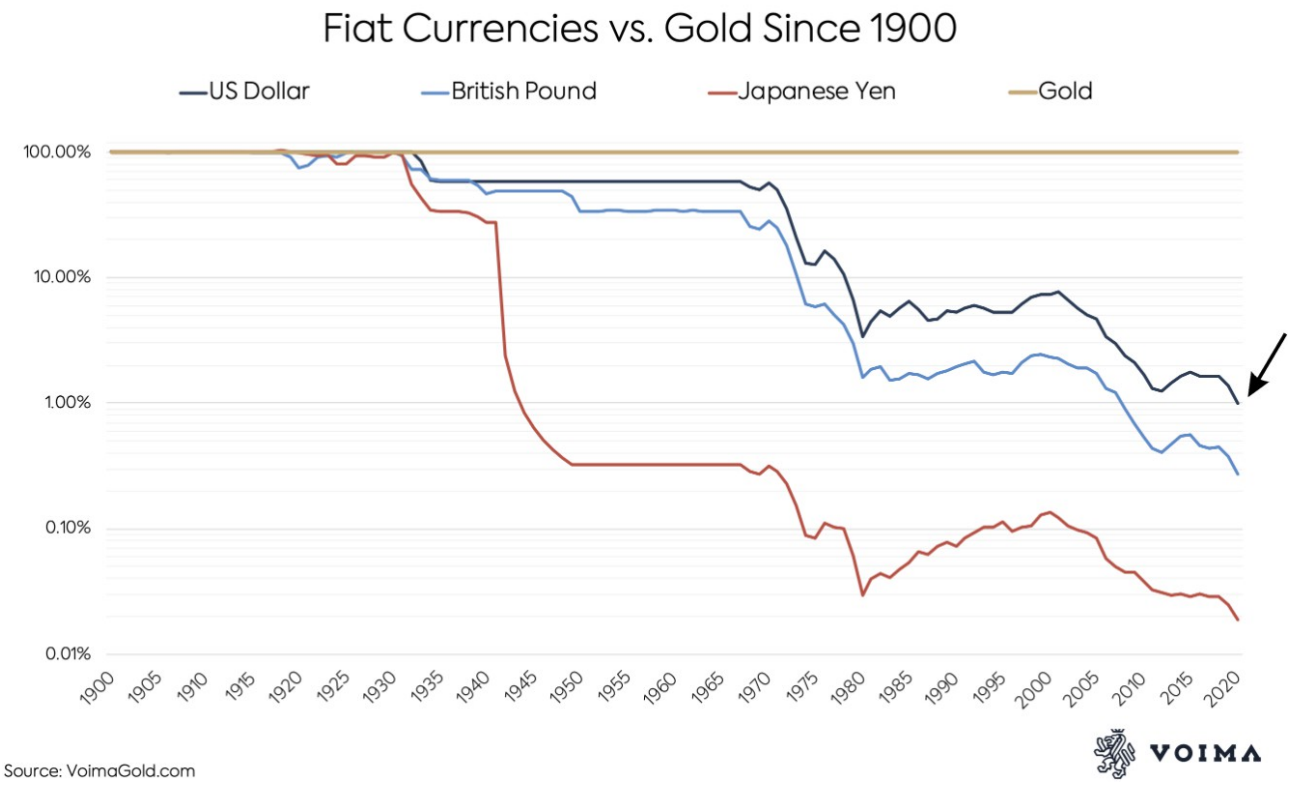


Abbildung 5: Preisentwicklung von Fiatwährungen gegenüber Gold

Kommen wir zum nächsten abenteuerlichen Aspekt, den uns die Aufhebung des Goldstandards gebracht hat. Wir haben ja schon festgestellt, dass der US-Dollar stark an Wert verloren hat. Vergleichen wir nicht nur den Dollar, sondern auch noch andere Währungen mit dem Goldpreis der letzten Hundert Jahre, dann stellen wir fest, dass der Dollar auf etwa 1% seines Wertes gesungen ist. Schlimmer hat es das britische Pfund erwischt welches noch bei 0,4% seines Wertes von vor 100 Jahren rangiert. Spitzenreiter der Wertlosigkeit ist der japanische Yen, der aufgrund des verlorenen Weltkrieges schon wesentlich schlechtere Startbedingungen hatte, heute noch 0,02% seines Wertes erhalten konnte. Und für alle drei Währungen gilt, dass mit der Aufhebung des Goldstandards der freie Fall eingesetzt hat.

Nicht verwunderlich ist demzufolge die Preissteigerung bei Konsumgütern. Bis 1971 gab es, und das wird jetzt einige überraschen, inflationäre **und** deflationäre Phasen, und über die Zeit gesehen, haben sich die Konsumgüter nur minimal verteuert. Es gab sowohl Preisanstiege und auch die Gegenbewegung, die Preissenkungen. Je weiter die Industrialisierung voranschritt, desto stärke war allerdings die Inflation. Ab dem Jahr 1971 explodiert allerdings der Konsumpreisindex und liegt heute bei dem etwa 10-fachen von 1971. Sprich ein Brötchen von 1971 kostet heute das 10-fache, schade nur, dass die Menschen nicht im selben Maße Lohnerhöhungen bekommen haben.

Es gibt einen schönen Chart zur Preisentwicklung von Campbell's Tomatensuppe, die auch schon von Andy Warhol in seinen Bildern verewigt wurde, da diese Suppe über 130 Jahre nach dem selben Rezept zu immer gleichen Konditionen hergestellt wird. Auch hier sehen wir, dass im Jahr 1974 die Preisexplosion begonnen hat. Die Verzögerung erklärt sich aus dem Umstand, dass bis dahin noch eine staatlicher Preisregulierung[20] existierte, die auf Druck aus der Wirtschaft 1974 aufgehoben werden musste um den Inflationsdruck der Unternehmen zu lindern.

20 Der Economic Stabilization Act (Lebensmittelpreisbindung) wurde 1970 eingeführt um inflationäre Tendenzen einzuhegen.

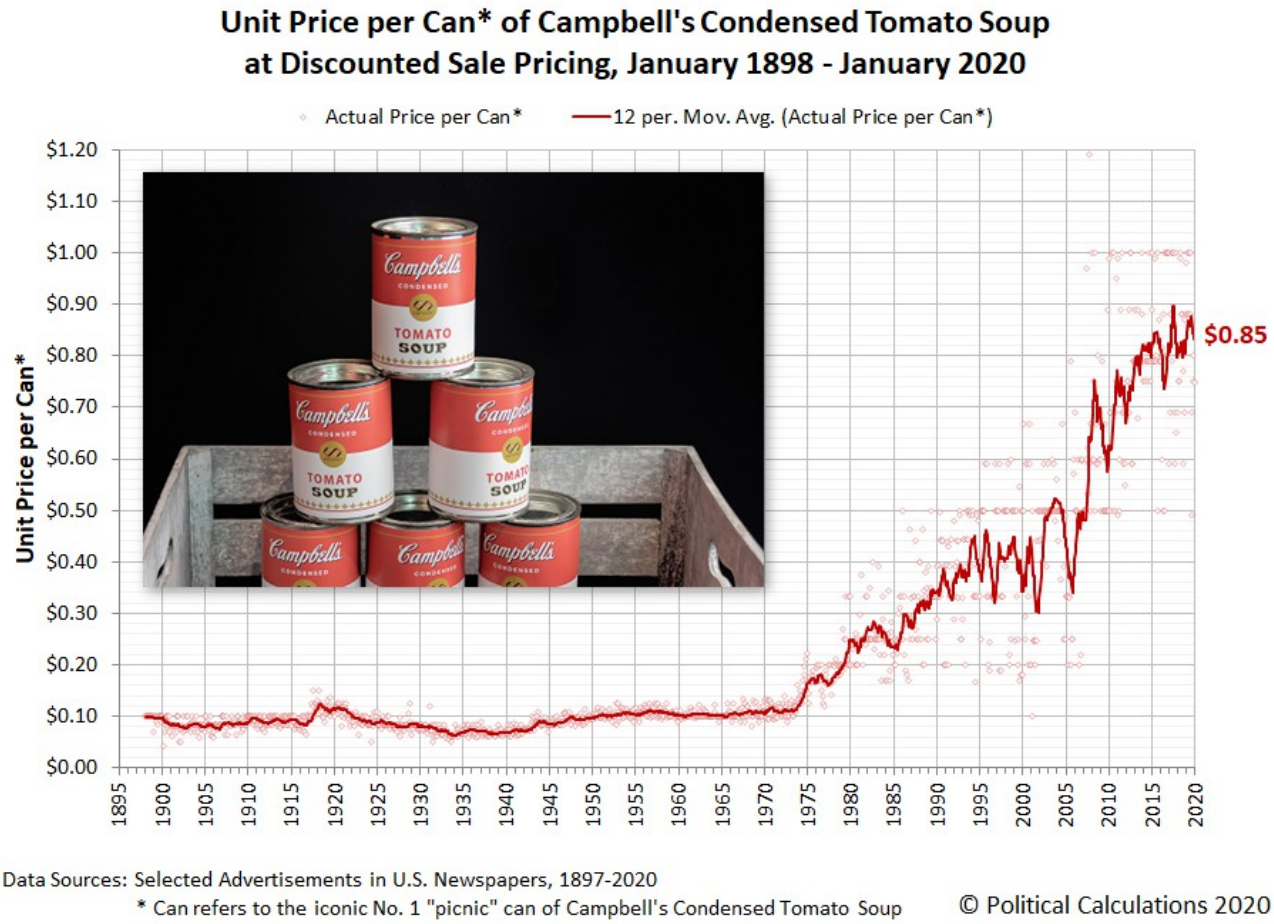


Abbildung 6: Preisentwicklung von Campbell's Tomatensuppe seit 1898

Jetzt ist ein Einwand eigentlich unabdingbar: Wir haben gesehen, dass der Dollar nur noch 1% seines Wertes behalten hat, aber der Konsumindex „nur“ um das 10-fache gestiegen ist. Wie kann das sein? Ganz einfach. Die Art und Weise, wie die Preissteigerung heute gerechnet wird, im Vergleich zu von 100 Jahren, ist extrem anders. Damals, als Inflation kein großes Thema war, wurden die Waren des täglichen Bedarfs in einen Warenkorb gelegt und daraus der Index errechnet. Heute ist das schon eine Wissenschaft für sich und nicht nur, dass der Warenkorb[21] mit unsinnigen, aber preisstabilen Dingen überfrachtet wird, sondern die Aspekte, die wirkliche Preistreiber sind, sind marginalisiert, oder fehlen komplett. Ich denke nirgends stimmt der Satz von Winston Churchill: „Traue keiner Statistik, die Du nicht selbst gefälscht hast.“ mehr als bei der Inflationsberechnung.

21 Quelle – Statistisches Bundesamt, Verbraucherpreisindex, Wägungsschema | https://www.destatis.de/DE/Themen/Wirtschaft/Preise/Verbraucherpreisindex/Methoden/Downloads/waegungsschema-2020.pdf?__blob=publicationFile

Verbraucherpreisindex für Deutschland - Wägungsschema
Consumer price index for Germany - weighting pattern
Basisjahr / base year 2020

SEA-VPI / SEA-CPI*	Bezeichnung / item		Gewicht in Promille / Weighting in per mill
	Verbraucherpreisindex insgesamt	Consumer price index, total	1000
01	Nahrungsmittel und alkoholfreie Getränke	Food and non-alcoholic beverages	119,04
02	Alkoholische Getränke und Tabakwaren	Alcoholic beverages and tobacco	35,26
03	Bekleidung und Schuhe	Clothing and footwear	42,25
04	Wohnung, Wasser, Strom, Gas und andere Brennstoffe	Housing, water, electricity, gas and other fuels	259,25
05	Möbel, Leuchten, Geräte u.a. Haushaltszubehör	Furniture, lighting equipment, appliances and other household equipment	67,78
06	Gesundheit	Health	55,49
07	Verkehr	Transport	138,22
08	Post und Telekommunikation	Communication	23,35
09	Freizeit, Unterhaltung und Kultur	Recreation, entertainment and culture	104,23
10	Bildungswesen	Education	9,06
11	Gaststätten- und Beherbergungsdienstleistungen	Restaurant and accommodation services	47,20
12	Andere Waren und Dienstleistungen	Miscellaneous goods and services	98,87

Abbildung 7: Wägungsschema des Verbraucherpreisindexes

Wenn wir die Gewichtung der Lebensbereiche für Deutschland anschauen, dann fallen zwei Bereiche besonders auf. Zum einen der Bereich 04 – Wohnung, Wasser, Strom, Gas und andere Brennstoffe, der mit 25,9% augenscheinlich am stärksten vertreten ist. Schaut man sich aber die Einzelpositionen an, so kann man durchaus enttäuscht sein, wenn man feststellt, dass die Kaltmiete mit sage und schreibe 7,55% veranschlagt ist. Das bedeutet also, dass bei einem Netto-Einkommen von 3000 € die Kaltmiete 226,50 € ausmacht. Ein andres Beispiel: Wenn die durchschnittliche Kaltmiete von 700 € um 100 € auf 800 € steigt, und leider ist das kein übertriebener Wert, dann ist das nicht eine Steigerung / Inflation von 12,5%, oder eben 100€, sondern es fließen lediglich 52,85 € in die Inflationsberechnung ein. Das das Geld dennoch nicht mehr im Portemonnaie ist, ist trotz des geringen Inflationsanstieges wohl einfach Pech für den Bürger. Energie und Brennstoffe, das heißt Strom, Gas, Öl, Kohle und Holz, schlagen mit stolzen 4,34% in der Berechnung zu Buche. Ein Blick auf die letzte Nebenkostenabrechnung macht jedem klar, dass diese Gewichtung alles andere als ehrlich ist.

Der zweit größte Bereich ist der Punkt 07 – Verkehr. Dafür werden 13,82 % veranschlagt, mehr also als für Lebensmittel oder Bekleidung oder sonstiges. Die heutige Realität sieht folgendermaßen aus. Diese ganzen neuen Autos, die über die Straßen rollen, gehören den Banken, sei es als Leasing oder als Finanzierung und diese Verträge sind in den meisten Fällen statisch. Autos werden nicht mit einer 100 jährigen Annuität und flexiblem Zins verkauft, sondern zum Festpreis für 3, 5 oder 10 Jahre. Für die Anschaffung eines Fahrzeuges werden 4,6% im Warenkorb veranschlagt, für den Betrieb, das Tanken, sage und schreibe 3,07% und der Urlaubsflug liegt bei 0,49% der Rest verteilt sich auf Instandhaltung und den Öffentlichen Verkehr. Diese Zahlen zeigen sehr deutlich, wie die Verhältnisse so verschoben werden, auf dass eine satte Verteuerung der Benzinpreise nur zu einem minimalen Anstieg der Inflation führen und dennoch waren die Verwerfungen 2022/2023 so extrem, dass es nicht mehr so leicht wegdiskutiert werden konnte. In Deutschland wurde für einen Liter Diesel locker 2,50 € bezahlt und das waren nun einmal mehr als die zugegebenen 10% Inflation. Wer heizen musste, hatte Pech und wohnen - na wer muss schon wohnen.

Was gar nicht in dieser Inflationsberechnung auftaucht, sind Immobilienpreise, die sich ähnlich wie

die Konsumgüter exponentiell verteuert haben und somit natürlich auf die Mieten direkten Einfluss haben. Auch die Argumentation, die Einkommen seien im Median stark gestiegen ist faktisch gesehen einfach nicht wahr. Heute ist es selbst für gut ausgebildete Menschen sehr schwer bis unmöglich aus eigener Kraft sich eine Immobilie zu kaufen. Die folgende Grafik zeigt, wie es Jahrzehnte lang immer leichter wurde ein eigenes Haus zu kaufen bis 1971 der Trend stagnierte und Anfang der 2000er Jahre das Verhältnis zwischen Gelderwerb und Immobilienpreis sich nach oben entkoppelt hat.

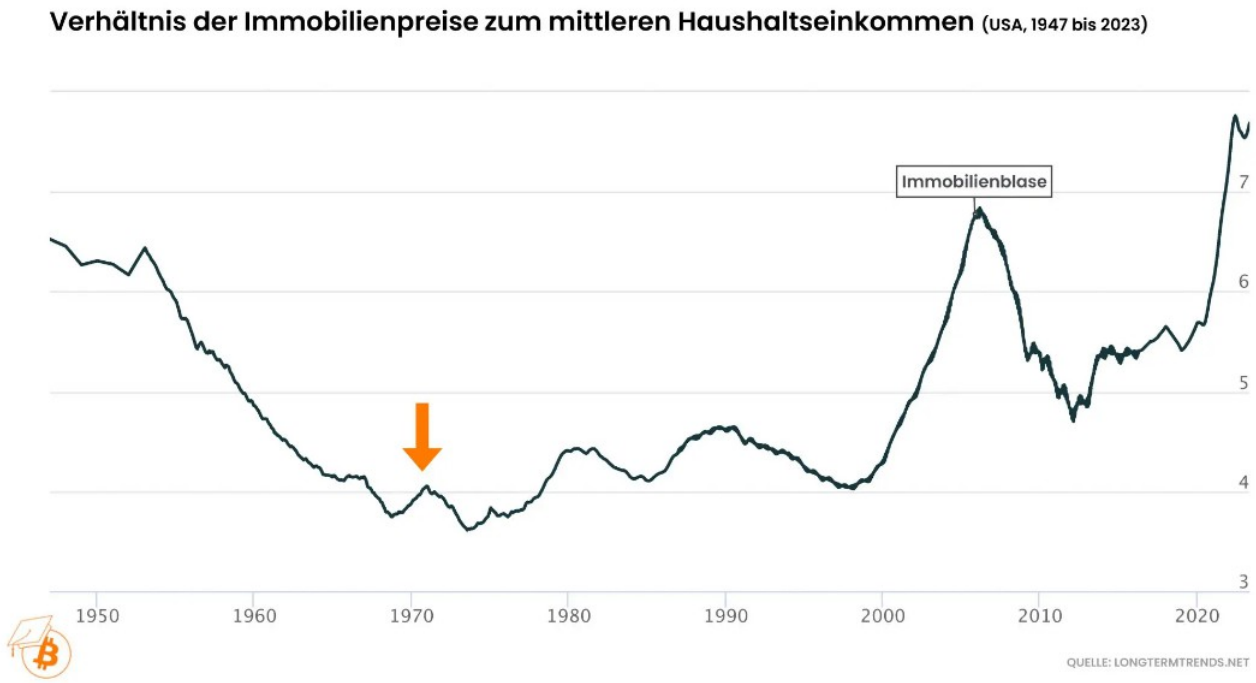


Abbildung 8: Verhältnis der Immobilienpreise zum Haushaltseinkommen

Noch eindrucksvoller sieht man diese Entwicklung, wenn wir nicht nur die Relation anschauen, sondern die explizite Entwicklung. Während sich der Immobilienpreis stetig verteuert, abgesehen von der heftigen Delle 2008 als die US-Immobilienblase platzte und die gesamte Weltwirtschaft mit sich nach unten riss, hat sich das Medianeinkommen nur sehr moderat gesteigert und mit jeder noch so kleinen Krise fällt es überproportional, um sich dann ganz langsam wieder ein wenig nach oben zu kämpfen. Im Vergleich dazu steigen die Immobilienpreise rasant und der Wunsch ein Eigenheim zu kaufen, bleibt für die Meisten ein Wunsch.

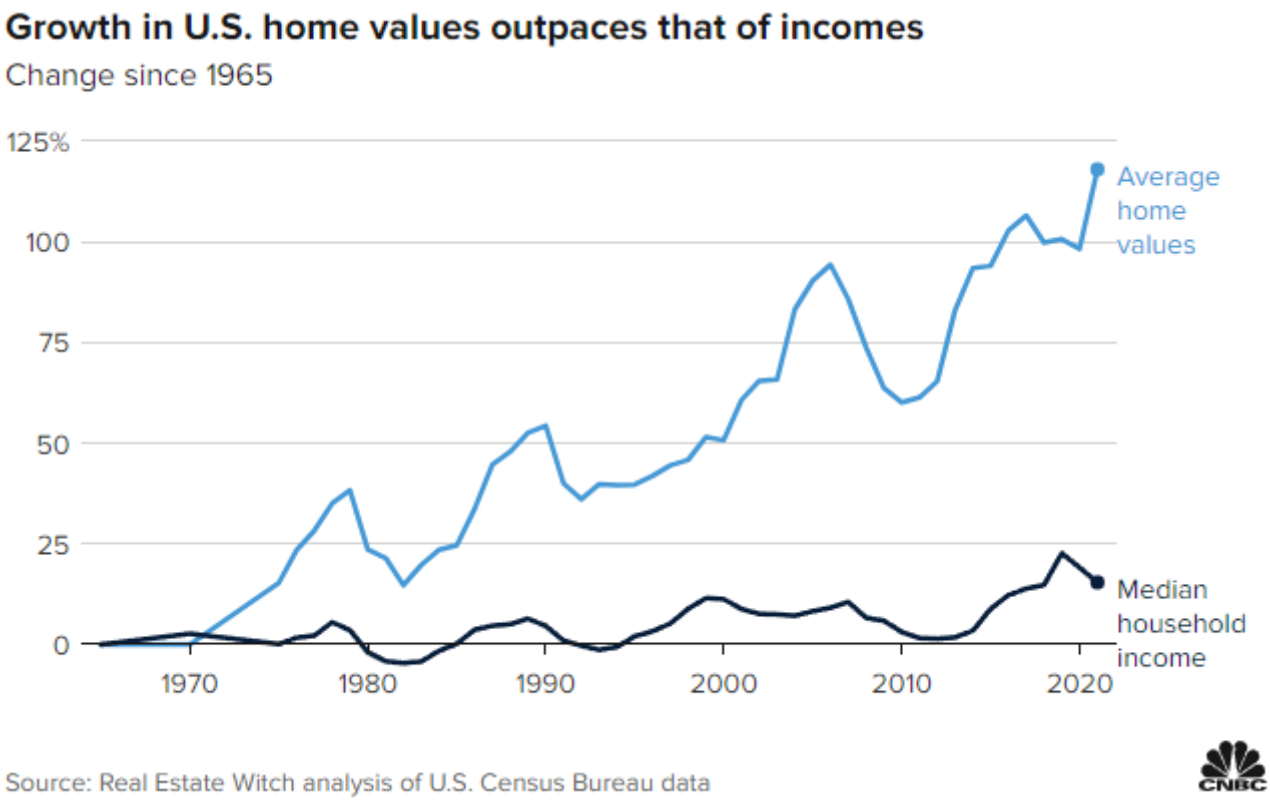


Abbildung 9: Entwicklung des Median-Einkommens im Verhältnis zum durchschnittlichen Immobilienpreis

Einen letzten Punkt sollten wir noch kurz besprechen, der auch in gar keiner Weise in die Geldentwertung nach 1971 einfließt. Die Vermögenssicherung durch Aktien und andere Wertpapiere. So wie die Immobilien wurden diese Anlagen eigentlich zum Sparen verwendet, da alles andere gegen die Inflation keinen Bestand hat. Wenn wir uns das durchschnittliche Kurs-Gewinn-Verhältnis (KGV) im S&P 500[22] anschauen, so sehen wir, dass das Bewertungsniveau sehr deutlich über dem Durchschnitt liegt. Die Krux an der Sache ist nur, dass Investitionen, insbesondere in den Aktienmarkt, mit diversen Risiken verbunden sind und ein hohes KGV signalisiert nicht gerade hohe Gewinnchancen. Aktien sind im Verhältnis zur erwartbaren Rendite im Durchschnitt einfach zu teuer.

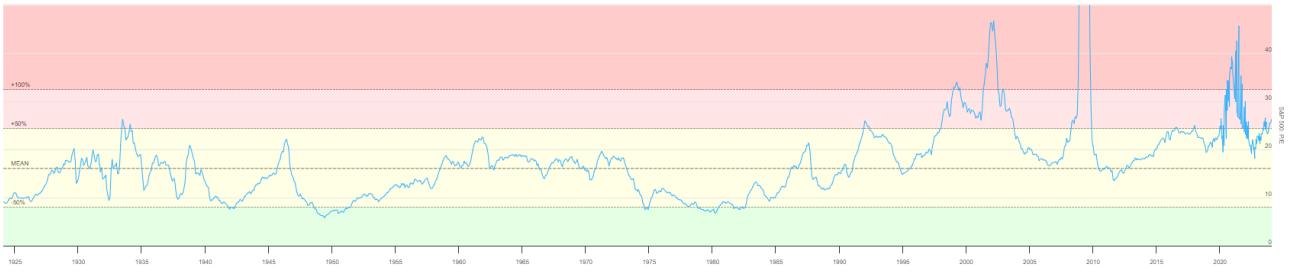


Abbildung 10: Kurs-Gewinn-Verhältnis im S&P 500 für die letzten 100 Jahre

Wir halten also erst mal fest. Nach der Aufhebung der Goldbindung zur Weltleitwährung US-Dollar wurde die Geldmenge extrem ausgeweitet und die Inflation schritt mit großen Schritten voran. Das

22 S&P 500 – Aktienindex, der die größten börsennotierten Unternehmen in der Vereinigten Staaten abbildet.

bedeutet also in der Konsequenz nichts anderes, als dass wir unsere Arbeitsleistung, mit anderen Worten unsere Lebenszeit, nicht mehr adäquat speichern können, da der Wertspeicher Geld immer weiter entwertet. Weiterhin haben wir gesehen, dass auch die alternativen Wertspeicher wie Aktien und Immobilen sich extrem verteuert haben und anscheinend viel des frisch erzeugten Geldes in diese Anlageklassen geflossen ist. Und dennoch bleiben die Wertsteigerungen im Normal immer noch hinter der Inflation zurück. Kurz gesagt, der normale Bürger wird im Übermaß um seine Leistung und Lebenszeit betrogen und die, die schon im Reichtum leben können sehr leicht, insbesondere mit Immobilien, ihr Vermögen noch weiter ausweiten. Die Geldfunktion Wertespeicher ist heute vollkommen abhanden gekommen. Jetzt ist eine berechtigte Frage, warum man in Bitcoin anstatt in Betongold investieren, wenn doch die Immobilien die Reichen immer reicher machen. Zum einen sind Immobilien, wie der Name ja schon sagt, immobil, der Wert ist also fest mit dem Grund verwachsen und jeder staatlichen Willkür ausgesetzt. Zum anderen ist in den letzten Jahren schon so viel Geld in diesen Sektor geflossen, dass ein Einstieg sehr schwer ist und die Steigerungen von früher nicht mehr erreicht werden können, beziehungsweise sogar massiver Verlust beim Platzen von Immobilienblasen droht. Als drittes und vielleicht bestes Argument gegen Immobilien ist ihr Unteilbarkeit. Man kann nicht 0,136 Stück Haus kaufen, maximal noch eine Ein- oder Zweizimmerwohnung, aber man benötigt sehr viel Kapital um einzusteigen und Banken sind heute sehr vorsichtig, was die Finanzierung angeht, zumal die Zinsentwicklung der letzten Jahre alles andere als einladend für Bauherren sind.

„Du kommst hier ned rein!“ Warum alle willkommen sind.

Jetzt kommen wir zu einer Eigenschaft von Bitcoin, für die die Obrigkeit dieses kleine Wunderwerk wirklich hasst und zwar ist Bitcoin maximal inklusiv. Wir haben in der kurzen technischen Einführung ja gesehen, dass niemand Bitcoin als zentrale Einheit steuert und das gilt natürlich auch für die Nutzung. Aber der Reihe nach.

Nach Schätzungen der Weltbank[23] haben zirka 1,7 Millarden Menschen keinen Zugang zu einem Bankkonto und dies vor allem im globalen Süden. Jetzt ist allerdings die Frage warum diese Menschen keine Konten bei Banken haben und die Antwort ist so einfach wie erschreckend. Es gibt in all diesen Ländern Banken und die Menschen haben in der überwältigenden Mehrheit Handys, mit denen sie Bankgeschäfte tätigen könnten, aber sie haben in der Vergangenheit derartig schlechte Erfahrungen mit Inflation, Enteignungen und so weiter gemacht, dass sie den Banken nicht vertrauen. Insbesondere in den Regionen der Welt, die infrastrukturell schlecht erschlossen sind, benehmen sich Banken wie die Cowboys einst im wilden Westen. Für Transaktionen werden teilweise Gebühren erhoben, die den Tageslohn eines „Bankkunden“ weit übersteigen. Und so haben sich die Menschen derart eingerichtet, dass alle Geschäfte in bar und persönlich abgewickelt werden. Für uns Menschen aus der so genannten entwickelten Welt, was immer das auch bedeuten mag, ist sofort klar, dass diese Art des Geldtransfers nicht effizient ist. Hier kann Bitcoin einen massiven Beitrag leisten, um lokale Infrastrukturen leistungsfähiger zu machen, denn mit Bitcoin, oder besser gesagt mit den Geldadaptionen von Bitcoin, wie zum Beispiel Lightning[24], kann Geld in Sekunden weltweit zu extrem niedrigen bis gar keinen Gebühren, sicher versendet werden und niemand kann diesen Vorgang stoppen oder verhindern. Dies ist, wie nicht schwer zu verstehen, natürlich nicht im Sinne derjenigen, die Bankdienstleistungen anbieten, aber es wird noch viel schlimmer, denn was für eine Privatperson gilt, gilt auch für Unternehmen und ganze Staaten.

Wir haben erfahren, dass der US-Dollar die Weltleitwährung/Weltreservewährung ist, in der die

23 Quelle - https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows

24 Lightning ist eine sogenannte "Second Layer"-Lösung für das Bitcoin-Netzwerk, die entwickelt wurde, um einige der Herausforderungen von Bitcoin zu bewältigen, wie z.B. Skalierbarkeit und Transaktionsgeschwindigkeit.

meisten internationalen Geschäfte abgewickelt werden. Insbesondere das am meisten gehandelte Gut, Erdöl, wird in US-Dollar bezahlt, aber im Grunde auch alle anderen Waren, die weltweit gehandelt werden, und so muss jeder Händler und auch die Staaten diesen Dollar vorhalten. Damit dies weltweit funktioniert, wurde das so genannte SWIFT[25] System etabliert, dass, wer hätte es gedacht, durch die USA kontrolliert wird. Und genau dieses SWIFT System ist die so oft beschworene Macht des Dollars, denn wer aus SWIFT ausgeschlossen, oder auch nur eingeschränkt wird, der hat keinen Zugang mehr zum internationalen Zahlungsverkehr. In der Vergangenheit haben die USA diesen Hebel immer öfter und immer rigoroser ausgenutzt um Banken, Konzerne oder Staaten auf Linie zu zwingen. 2022 wurden sieben Banken der Russischen Föderation aus SWIFT ausgeschlossen, was als finanzielle Atombombe in den Medien dargestellt wurde, aber auch Banken in Ländern wie Venezuela, Nord Korea, Cuba und dem Iran unterliegen Restriktionen, mit denen die (meist) völkerrechtswidrigen Sanktionen gegen diese Länder durchgesetzt werden sollen. Die Ironie an dieser Geschichte ist, je mehr Restriktionen durch das internationale Zahlungssystem ausgeübt wird, desto sicherer wird Bitcoin, da alle Ausgeschlossenen sich diesen Weg der einfachen und universellen Zahlung offen halten, auch wenn dies nicht offiziell so verlautbart wird. Die BRICS-Staaten, das sind Brasilien, Russland, Indien, China und Südafrika, harmonisieren bereits auf traditionelle Art ihre Zahlungen untereinander mit dem CIPS[26], dem fast 100 weitere Länder bereits angeschlossen sind, darunter zum Beispiel auch der NATO-Staat Türkei. Auf diese Weise wird die hegemoniale Macht der USA massiv untergraben was aber leider zu einer immer instabileren Weltordnung führt. Wir erinnern uns noch lebhaft an den völkerrechtswidrigen Überfall der NATO-Staaten auf das nordafrikanische Libyen, nachdem der damalige Staatspräsident Muammar al-Gaddafi sich mit anderen afrikanischen Staaten über die Einführung einer neuen Währung, dem Gold-Dinar, verständigt hatte. Dies wurde von Seiten der USA als direkter Angriff gesehen und im Rahmen des arabischen Frühlings wurde Libyen buchstäblich von einem modernen und wirtschaftlich prosperierenden Staat ins Mittelalter gebombt. Für seinen Frefel wurde Muammar al-Gaddafi tatsächlich gepfählt.

Ein zunehmend besorgniserregender Umstand in der so genannten westlichen Welt ist die Tatsache, welche man bis dato nur aus autoritären Systemen kannte, dass Regierungskritiker wirtschaftlich zerstört werden und dies geht sehr einfach durch die Kündigung von Bankkonten. In diesen Fällen übt der Staat, beziehungsweise vom Staat abhängige Organisationen, die in westlichen Ländern immer häufiger Nichtregierungsorganisationen genannt werden, Druck auf Banken aus, um die, durch Mikrospenden finanzierten Nachrichtenportale und Meinungsplattformen, aber auch Privatpersonen mit Reichweite, von der Finanzierung abzuschneiden. Auch hier ist Bitcoin eine wasserdichte Methode, um dies zu verhindern, denn wie bereits erfahren, kann Bitcoin nicht zensiert werden. Man darf das jetzt aber nicht falsch verstehen. Bitcoin soll nicht helfen Menschen zu finanzieren, die mit ihren Portalen Straftaten wie Beleidigung und Verleumdung vorantreiben, nein. Alles was nach gesellschaftlichem Konsens strafbar ist, wird durch die Justiz geahndet, aber was die modernen westlichen Staaten derzeit forciert betreiben ist Meinungsunterdrückung weit unter der Strafbarkeitsgrenze. Opposition und Kritik wird immer weniger geduldet. Uneinigkeit mit der herrschenden Macht wird als Deligitimation gebrandmarkt. Dieser Trend, der in der gesamten westlichen Welt zu sehen ist, ist aus demokratischer Sicht äußerst bedenklich und Bitcoin kann hier ein probates Mittel sein um den Machthabern die Möglichkeit zu nehmen verdeckt und diskret seine Oppositionellen wirtschaftlich zu zerstören.

An dieser Stelle muss natürlich noch ein viel geliebtes Vorurteil gegen Bitcoin demaskiert werden. Es wird immer behauptet, dass Bitcoin von Kriminellen verwendet wird und es nur ein Zahlungsmittel für zwielichtige Gestalten und Drogendealer ist. Es stimmt, dass Bitcoin auch für

25 SWIFT - SWIFT steht für "Society for Worldwide Interbank Financial Telecommunication". Es handelt sich um eine kooperative Organisation, die ein Netzwerk für Finanzinstitute betreibt, um den sicheren und standardisierten Austausch von finanziellen Transaktionen zu ermöglichen.

26 CIPS - Cross-Border Interbank Payment System, zu deutsch Grenzüberschreitendes Interbanken Zahlungssystem

Straftaten benutzt wird, aber eine Analyse der Europäischen Beobachtungsstelle für Drogen und Drogensucht hat festgestellt, dass sage und schreibe 0,4% aller Transaktionen im Zusammenhang mit illegalen Machenschaften stehen. Das alles überwältigende Gros an illegaler Finanzierung wird mit Fiatgeld gemacht und zwar Tag täglich und vor den Augen der Behörden. Also falls nochmals jemand Bitcoin verbieten will, weil es von Verbrechern benutzt wird, dann muss der Dollar, Euro, Yen und alle anderen Währungen auch weg! Diese Anschuldigung gegen Bitcoin ist so dermaßen dumm und dreist, dass es nahezu schmerzt. Aber den Mächtigen ist nicht zu doof, um mit Dreck nach der Konkurrenz zu werfen.

Wir fassen zusammen: Bitcoin ist ein Wertespeicher und vielleicht auch ein Geld, welches vollkommen inklusive ist. Niemand kann von Bitcoin ausgeschlossen werden, niemand kann Bitcoin zensieren. Und jetzt kommt noch eine Sache dazu, mit der man jeden Zöllner zum Wahnsinn treiben kann.

Wenn man seine eigene Wallet[27], also Brieftasche, betreibt, dann hat man alle seine Schlüssel zum Empfangen als auch Versenden von Bitcoins in der eigenen Verwahrung. Das ist einerseits toll, denn damit ist man sozusagen seine eigene Bank und muss niemanden fragen und bemühen wenn man Geldgeschäfte machen will, aber es birgt natürlich auch die große Verantwortung, dass man selbst und zwar nur man selbst, für die sichere Aufbewahrung zuständig ist. Wenn die Schlüssel einmal verloren gehen, sind sie für immer weg und alle Werte, die hinter den Adressen liegen sind verloren. Das klingt jetzt allerdings dramatischer als es in Wirklichkeit ist, denn um auf den Zöllner vom Anfang zurückzukommen, kann man sich diese Schlüssel in Form von 12 oder 24 Wörtern speichern und egal wo auf dieser Welt, nur mit einem Internetzugang seine Wallet/Brieftasche wieder herstellen. Diese Wörter in der richtigen Reihenfolge führen immer wieder zum eigenen Vermögen. Etwas so geniales gab es in der Menschheitsgeschichte noch nicht!

Man kann also mit Millionen beladen durch den Zoll gehen, denkt an seine Wörter und niemand auf der Welt kann einen stoppen. Wir alle haben schon gehört was Menschen passieren kann, wenn sie Geldbeträge aktuell größer 10.000 € über EU-Grenzen bringen wollen. Das muss angemeldet und deklariert werden, da müssen Formulare ausgefüllt und Beamte angebettelt werden, nur damit man sein eigenes Geld von dem Verdacht der Geldwäsche befreit. Und wir wissen auch alle, um an das vorherige Thema nochmals anzuknüpfen, dass es nicht um Geldwäsche geht, sondern darum, Kontrolle über das Vermögen der Bürger zu haben. Es blitzt immer wieder mal in den Medien auf das die größten Geldwäscher und Terrorismusfinanzierer die Staaten selbst sind. Erinnern Sie sich noch an den Fall Barschel? Oder wer hat Al Quaida ins Leben gerufen? Wohin gehen die aberhunderte Millionen aus Katar und wo sind die 6 Millarden Dollar geblieben, die Donald Rumpsfeld nicht mehr finden konnte? Der Staat und die Banken wollen Kontrolle und da braucht sich niemand etwas vormachen und eben genau das ist mit Bitcoin nicht möglich. Aber wir dürfen uns auch nicht zu früh freuen, denn Bitcoin ist auch nicht anonym wie wir im Kapitel „Kontrolle – Ihre Papiere bitte“ noch sehen werden und was wieder die Anschuldigung es sei nur ein Verbrechergeld widerlegt.

Damit beenden wir den ersten Überblick über Bitcoin und besprechen in den nächsten Kapiteln einzelne Themen, die lose, nach Interesse, gelesen werden können. Wer bis hierher schon durchgehalten hat, der hat auf jeden Fall schon mal ein sehr viel tieferes Verständnis für Bitcoin entwickelt, als die aller meisten Wirtschaftjournalisten, die sich allenthalben aufschwingen ihre Hetzkommentare und ihr gefährliches Halbwissen in den Gazetten zu verbreiten oder auch anderorts medial unter das Volk zu steuern. Ich für meinen Teil bedaure diese Menschen, die krampfhaft an etwas, von dem sie selbst wissen müssen, dass es zum Scheitern verurteilt ist, festhalten, nur weil sie ihre eigene kleine Welt bewahren wollen, oder sich einen relativen Vorteil versprechen.

27 Wallet, eng. Brieftasche ist die digitale Geldbörse, in der die öffentlichen und privaten Schlüssel verwahrt werden.

Wer ist der Samurai Satoshi Nakamoto?

Die Bitcoin interessierten Menschen rätseln seit Anbeginn, wer der Erfinder von Bitcoin, dieser Satoshi Nakamoto sein könnte. Und warum steht in der Überschrift Samurai? Ein Samurai war im alten Japan ein Ritter, der analog zur mitteleuropäischen Tradition, ein Sinnbild für Ehrlichkeit, Können, Mut und Selbstlosigkeit war. Und genau das verkörpert dieser Name im Sinne von Bitcoin. Bitcoin ist so konzipiert und in die Welt gebracht worden, dass ganz eindeutig gesagt werden kann, dies geschah nicht zum eigenen Vorteil, dies geschah nicht zur eigenen Bereicherung, sondern zum Wohle der gesamten Menschheit ohne jede Ausnahme. Bitcoin ist so konzipiert, dass es ohne jedes Ansehen der Person, ohne jede Wertung daher kommt und jeden Menschen als das annimmt was er oder sie ist. Ein reines Geschöpf.

Um es vorweg zu sagen, niemand weiß wer Satoshi Nakamoto ist, nicht mal ob es ein Mann, eine Frau oder eine Gruppe ist. Der/die geniale/n Erfinder/in haben es von Anfang an konsequent vermieden die eigene Identität offen zu legen. Und für mich ist das, wenn wir uns die Geltungssucht diverser Personen anschauen, schon fast nicht mehr von dieser Welt. Aber genug Lob gehudelt.

Wie der Mensch nun mal so ist, er strebt nach Wissen und so sind ein paar Leute mit den Jahren ins Fadenkreuz der Satoshi-Jäger geraten. Das sind...

- **Hal Finney** - Er hat aktiv an der Entwicklung von Bitcoin mit programmiert und hat die erste Transaktion erhalten. Auch das Proof-of-Work-Prinzip geht auf ihn zurück. Er wird als wohl wichtigste Figur in der frühen Entwicklung von Bitcoin angesehen und wer weiß, vielleicht hat er eine zweite Identität.
- **Nick Szabo** – Auch ein Pionier der Kryptowährungen, Computerwissenschaftler, Kryptograph und Rechtswissenschaftler. Er ist der Vater der „Smart Contracts“ die er bereits in den 1990er Jahren entwickelte. Sein Aufsatz „Bit Gold“ aus dem Jahr 1998 beschreibt ein digitales Wertaufbewahrungssystem, das viele Ähnlichkeiten zu Bitcoin aufweist.
- **Wei Dei** – Ebenfalls Kryptograph und Computerwissenschaftler, der mit seinem Aufsatz „B-Money“ 1998 das Konzept von dezentralen, elektronischen Währungen vorstellte. Er war auch ein lautstarker Cipher-Punk, der sich schon sehr früh für den Schutz der Privatsphäre im Internet einsetzte. Auf seinen Überlegungen beruht die Sicherung der Transaktionen durch Kryptographie.
- **Craig Wright** – Er war früh als Entwickler für Bitcoin dabei und behauptet selbst von sich Satoshi Nakamoto zu sein. Allerdings tut er lauter Dinge, die dem Geist von Satoshi Nakamoto absolut zuwider laufen und im Jahre 2024 verlor er vor Gericht[28] den Anspruch gegen die Crypto Open Patent Alliance (COPA). Der Richter Justice Mellor urteilte, dass Wright nicht Satoshi Nakamoto ist. Das führte auch dazu, dass Wright keine Patente auf die bis heute konsequent Open Source gehaltenen Dokumente und Konzepte legen konnte.
- **Dorian Satoshi Nakamoto** – Das ist ein Mensch und Computerwissenschaftler, der einfach den selben Namen hat und in der Nähe von Hal Finney wohnte. Er wurde von Reportern belagert, nachdem Newsweek[29] einen Artikel veröffentlicht hatte, in dem er als Erfinder des Bitcoin bezeichnet wurde. Er hat dies zeit Lebens abgestritten... Verdächtig.
- **Elon Musk und Steve Jobs** werden auch noch gehandelt, aber das ist dann eher Personenkult als Substanz.

Abschließend lässt sich also nicht sagen, wer Satoshi Nakamoto ist oder zumindest wie viele. Was so außergewöhnlich daran ist, ist der Umstand, dass Bitcoin, das ganz klar als Verteidigung gegen

28 Quelle - https://en.wikipedia.org/wiki/Craig_Steven_Wright
29 Quelle - https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

die Ausbeutung durch das konventionelle Fiatgeldsystem erfunden wurde, keine zentrale Figur hat. Es gibt niemanden, den man anhimmeln kann und auch niemanden, der die Macht hätte auf staatlichen oder anderen institutionellen Druck hin das Wesen von Bitcoin zu verändern. Die Machthaber haben kein Gesicht, so wie zum Beispiel bei Julian Assange, der als Gründer von WikiLeaks für das Aufdecken der schmutzigen Machenschaften der Machthaber eingekerkert wurde. Durch seine selbst gewählte Anonymität hat sich Satoshi Nakamoto nicht nur sein eigenes normales Leben gerettet, sondern er hat eine mehr oder weniger Kunstfigur als Märtyrer an den Anfang des Projektes gestellt. Und dies ist einer der genialsten Schachzüge im Entstehungsprozess von Bitcoin.

Wieso kommen die Plebejer zurück?

Die Plebs[30], abgeleitet aus dem alten Rom, sind ein Teil der Bitcoingemeinde, die es wirklich ernst meinen. Die Plebs versuchen nach Idealen zu leben, so wie sie durch die frühe Bitcoingemeinde und Satoshi Nakamoto selbst postuliert, oder besser vorgelebt, wurden. Dazu gehören Tugenden wie Demut, Genügsamkeit, Wertschätzung, Achtung vor sich selbst und vor der Schöpfung als solche und natürlich eine hohe Technikaffinität. Natürlich ist dies eine generelle und vereinfachte Beschreibung und man sollte niemals vom Einzelnen auf die Gruppe schließen, doch es gibt wirklich Charaktaristika, die etwas Universelles haben.

In der Regel sind es Menschen, die eine eher kritische Haltung zu Staat und Obrigkeit haben. Ganz zentral ist Ihnen das Thema Unabhängigkeit, das sehr leicht durch Bitcoin erreicht werden kann, denn wenn man mal genau darüber nachdenkt, so sind extrem viele Bereiche unseres Lebens direkt oder indirekt von Geld abhängig. Dadurch das Bitcoin deflationär ist und die Kaufkraft erhält oder sogar steigert, haben ganz einfache und normale Menschen auf einmal wieder die Möglichkeit die Früchte der eigenen Arbeit zu genießen. Dort wo sonst Unmengen an Wert, oder mit anderen Worten Lebenszeit, durch das System in Form von Inflation und sinnlosen Gebühren abgesaugt wird, freut sich der Bitcoiner, da er daran einfach nicht teil nimmt. Auch andere Effekte der modernen westlichen Welt treffen auf den Plebejer nicht zu. Diese Verschwendungssucht, die uns allen schon in die Wiege gelegt wurde kämpft im Geiste des Bitcoiners mit dem Gedanken, dass wenn man sein Geld nicht sinnlos für Firlefanz ausgibt, sondern in Bitcoin spart dieses Geld immer mehr wert wird, hingegen der Firlefanz irgendwo in der Ecke liegt. Das wird oft mit Geiz verwechselt, ist aber eine rationale Form der Bedürfnisbefriedigung, die dem Rest der Gesellschaft durch das System aberzogen wurde. Bitcoiner leben den Geist, vor dem Nobelpreisträger für Ökonomie immer warnen. Die Deflation sei der Tod der Wirtschaft, doch ist es in Wahrheit so, dass diese Menschen auch essen, trinken und konsumieren müssen und wollen, sie wollen aber ein gutes und faires Angebot und nicht den Industriemüll, der heutzutage für den Durchschnittsmensch hergestellt wird. Mit dem Slogan „Billig, will ich!“ kann man keinen Bitcoiner mehr hinter dem Ofen hervorlocken.

Durch seinen ungebundenen Besitz ist der Bitcoiner sehr leicht in der Lage sein Wohnort irgendwo auf der Erde zu wählen, an dem auch das Steuermodel und sonstige staatlichen Strukturen angenehm sind. Viele Bitcoiner sind Kosmopoliten, was natürlich nicht zwingend ist, aber für viele eine logische Fortsetzung der Erkenntniskette. Wer sich mit Bitcoin beschäftigt, erfährt so viele Dinge über diese Welt, die Systeme und deren Probleme, dass die alte, enge Welt oft nicht ausreicht. Ein Zitat von Mark Twain lautet „Reisen ist tödlich für Vorurteile, Bigotterie und engstirnigen Nationalismus.“ und das ist es auch, was viele Bitcoiner an- und umtreibt – die Welt sehen und wirklich erkennen, Chancen aktiv suchen als auf sie zu warten.

Derzeit gibt es den Trend nach El Salvador zu gehen, dem ersten Land der Welt in dem Bitcoin offizielles Zahlungsmittel neben dem Dollar ist. Zugegeben der Weg nach El Salavdor ist eher

30 Plebs, lat. Das gemeine Volk

etwas für junge und gesunde Menschen, da das mittelamerikanische Land sich gerade von einem der gefährlichsten Orte auf der Welt mit einer astronomischen Mordrate zu einem der sichersten Orte entwickelt und dieser Weg ist noch lange nicht abgeschlossen. Und wie es nun mal so ist, kann das Gesundheitswesen in einem Land des globalen Südens, von einigen auch despektierlich die Dritten Welt genannt, nicht als das Beste angesehen werden. Der Präsident von El Salvador, Nayib Bukele, hat mit rigorosen Gesetzen und bis dato in El Salvador nicht gekannter Härte gegen Kriminalität und Korruption eine Nation geschaffen, die zum ersten mal seit der Kolonialzeit Anfang des 19. Jahrhunderts eine wirkliche Perspektive hat. Kritiker werfen ihm autoritären Führungsstil vor, doch bei den einfachen Menschen ist der Präsident sehr beliebt. El Salvador entwickelt sich zusehends von einem düsteren Entwicklungsland zu einem offenen und modernen Staat. Dabei hilft natürlich das eigene staatliche Schürfen von Bitcoin mit vulkanischer Energie, ein Potenzial, welches das Land schon sein Jahrmillionen hat, aber heute erst ausschöpfen kann.

Aber weiter von den Plebs. Viele Bitcoiner verstehen sich als Widerständige gegen das Establishment. Sie lehnen die Bevormundung und Gängelung ab und berufen sich auf so etwas ähnliches wie ihre Naturrechte. Das traditionelle Fiatgeldsystem wird natürlich in Frage gestellt und sie benennen offen die herrschende Oligarchie. Da diese Menschen oft die Mechanismen der Macht intensiv studiert haben, wissen was der Cantillon-Effekt ist und da sie die Machtpyramide sehr deutlich sehen können bleibt ihnen nichts anderes übrig als sich angewidert abzuwenden, denn auch sehr verbindend bei den Plebs ist die Gewaltlosigkeit. Sie haben verstanden, dass mit Gewalt nichts gelöst werden kann, sondern nur durch den Entzug von Energie; eine der elementaren Gesetzmäßigkeiten. Alles beruht auf Energie und der effektivste Weg etwas zu bekämpfen ist der Entzug der Energie. Wie schon erwähnt, der Bitcoiner kann seine Sachen packen und ist dann mal weg.

Ein nicht zu verachtender Nebeneffekt des „hodlns“, also des Ansammelns von Bitcoin ist auch, dass man viel entspannter wird. Die wirtschaftliche Position verbessert sich im Grunde ständig und so fallen sehr viele Stressfaktoren ganz einfach vom Bitcoiner ab. Geld macht nicht glücklich, aber es beruhigt schon sehr. Anders sieht es selbstverständlich bei den (selbsternannten) Händlern aus, die teilweise mit gehebelten Positionen versuchen schnell reich zu werden. Bei den Kursschwankungen kann das gut gehen, tut es aber oft nicht.

Ein weiteres verbreitetes charakteristisches Element der Bitcoiner ist die Ablehnung von Hierarchie im Allgemeinen oder besser der Hang zum Egalitarismus. Die Gemeinschaft aus Gleichen ist ein ganz zentraler Gedanke und angestrebtes Ziel. Diese Gemeinschaft wird auch nach Kräften gelebt und gefördert. Jetzt darf auf keinen Fall der Eindruck entstehen, dass diese Menschen die verordnete Gender- und Inklusionspolitik befürworten oder leben, eher im Gegenteil, aber die Plebs sind sehr liberal und jeder, egal wie man aussieht, welche Religion man hat, welches Geschlecht man hat, woher man kommt ist gleich viel wert. Die Plebs sind wirklich liberal.

Mittlerweile gibt es zig Treffen und Messen, Kongresse und Vorträge und andere Events rund um Bitcoin. Es hat sich eine sehr rege Bewegung gebildet, die ausfällig wenige „Stars“ hat. Natürlich gibt es wie überall exponierte Personen, aber die überzeugen in der Regel durch Intelligenz, Wissen, Witz, Geist und nicht durch Besitz oder Macht.

Was aber so gut wie allen Bitcoinern zu eigen ist ist die starke Technikaffinität. Sie können mit Ihren Computern und Handys schon sehr gut umgehen, kennen X Wege um dieses und jenes Problem zu lösen. Doch das muss den zukünftigen Plebejer nicht abschrecken, der nicht mit den ganzen technischen Geräten aufgewachsen ist. Zum einen wird der Umgang mit Bitcoin immer anwenderfreundlicher und zum anderen bewegen sich die Menschen, die sich dem Thema widmen unweigerlich auf die Technik zu, sodass nach kurzer Zeit die anfänglichen Hürden überwunden sind. Dieses Buch leistet dazu auch einen Betrag.

Also doch Flaschen sammeln

Eins gibt es noch, was sehr viele Bitcoiner verbindet und zwar der Gedanke, oder besser schon die Gewissheit, dass die staatlichen Systeme im Alter nicht mehr funktionieren werden und die einzige wirkliche Alternative zur ausgefallenen Rente die angesammelten Bitcoins, das Portfolio, ist. Die Plebejer vertrauen, wie schon erwähnt, dem Staat nicht über den Weg und wenn wir uns die gängigen Rentensysteme in der EU anschauen, dann sehen wir ganz schnell, dass dies bei der aktuellen Demographie zum Scheitern verurteilt ist. In Deutschland alleine muss das Rentensystem jährlich mit über 87 Milliarden Euro[31] quer finanziert werden, damit es nicht schon heute kollabiert. Aktuell gehen die Baby Boomer, also die erste Generation die nach dem 2. Weltkrieg geboren wurde, in Rente und da dies eine riesige Volksgruppe ist, verschiebt sich die Menge derjenigen die Leistungen erbringen und die derjenigen die Leistungen empfangen immer weiter und ein heute 20 oder 30 jähriger Mensch kann sich leicht ausrechnen, dass dies unter normalen Umständen nicht zu leisten ist. In Europa wird diesem Trend massiv mit vermehrter Einwanderung begegnet, doch, mal ganz abgesehen von den kulturellen Herausforderungen, wandern zu viele der Neuankömmlinge in die Sozialsysteme ein. Die Blaupause der Gastarbeiter aus Italien und der Türkei in den 1970er und 1980er Jahren funktioniert heute nicht mehr, da die modernen Gesellschaften ein viel höheres Maß an Spezialisierung haben und einfache Arbeiten immer weiter mechanisiert werden. Und auch damals dauerte es mindestens eine Generation bis die türkischstämmigen Menschen in Deutschland wirklich Fuß gefasst haben. Leider sieht es in den anderen EU-Ländern auch nicht viel besser aus.

Den Bitcoinern ist völlig klar, dass sie im Alter nichts mehr von den Staaten zu erwarten haben und deshalb nehmen sie ihr Schicksal selbst in die Hand.

Abbildung 11: Rentenatlas Deutschland 2022

Durch den deflationären Charakter von Bitcoin ist es auch wirklich möglich mit relativ wenig

31 Quelle - https://www.deutsche-rentenversicherung.de/SharedDocs/Downloads/DE/Statistiken-und-Berichte/Rentenatlas/2023/rentenatlas-2023-download.pdf?__blob=publicationFile&v=7

eingesetzter Lebenszeit, sprich eingesetztem Geld, eine hohe Wertsteigerung zu erreichen und so sein Leben im Alter auch finanzieren zu können. Selbst mit monatlichen Kleinstbeträgen kann über die Zeit ein ansehnliches Vermögen aufgebaut werden. Es gibt relativ viele Menschen, die frühzeitig auf Bitcoin gesetzt haben und bereits heute die Früchte daraus ernten. Junge Menschen, die zu Spottkursen eingestiegen sind und deren Vermögen sich ver-10, ver-50, ver-100facht hat. Allerdings hatten diese Menschen auch das größte Risiko, denn vor 8, 10, 12 Jahren wusste niemand wirklich, ob Bitcoin sich durchsetzen würde. Und das Beste daran ist, dass Bitcoin dieses Potential nie verliert, da durch seine Konzeption ein ewiger Wertzuwachs nicht garantiert, aber sehr wahrscheinlich ist.

Wie funktioniert Bitcoin und was ist die Blockchain?

In diesem Kapitel erkläre ich den technischen Ansatz von Bitcoin so, dass auch Nichtinformatiker dies verstehen können. Leider ist es aber immer noch ein technisches Thema und wem das zu viel ist, der kann dieses Kapitel auch einfach überspringen. Um Bitcoin anwenden zu können muss man nicht wissen, wie es technisch funktioniert. Genau so wie man nicht wissen muss, wie ein Motor wirklich funktioniert um Auto fahren zu können. Für das Gesamtverständnis ist es allerdings sehr gut, wenn man auch eine Ahnung vom technischen Ansatz hat, denn aus der technischen Konzeption ergeben sich einge Eigenschaften von Bitcoin, die ihn absolut einzigartig machen. Gehen wir los...

Das Wort Blockchain, dass mittlerweile wirklich jeder kennt, aber nur wenige etwas damit anfangen können, beschreibt nichts anderes als eine Datenbank. Auf Deutsch bedeutet es einfach nur Blockkette. Im Falle von Bitcoin ist es im Grunde ein Kassenbuch. Ein sehr großes Kassenbuch.

Klassische Datenbanken, man nennt die auch relationale Datenbanken, organisieren ihre Daten in Form von Tabellen, die aus Zeilen und Spalten bestehen und verwenden Zeiger und Indizes um Daten schnell finden und manipulieren zu können. Relationale Datenbanken werden für Geschäftsvorgänge, Kundendaten, Buchhaltung und alle möglichen anderen Daten genutzt, wenn es nur darum geht Informationen zu speichern und schnell zur Verfügung zu stellen. Relationale Datenbanken funktionieren nach dem Server-Client-Prinzip, das bedeutet, ein Computer, der Server, führt die Datenbank aus und viele andere Computer, die Clients, rufen Daten ab oder senden Daten zur Speicherung und Löschung.

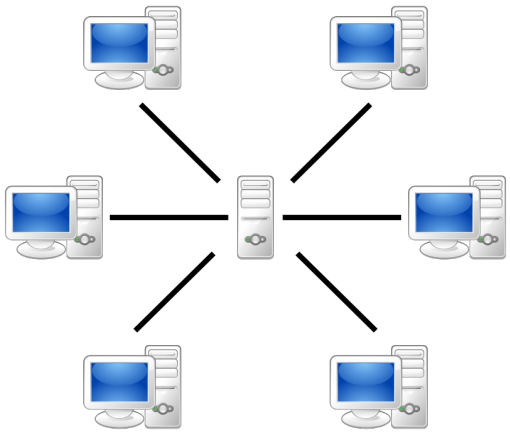


Abbildung 12: Schema für ein Server-Client-Sysetem. Quelle: Wikipedia

Der Server untersteht in diesem Netzwerk der Autorität, die die volle Kontrolle über die Daten hat. Es handelt sich also um eine zentralistische Struktur.

ID / Zeiger	Vorname	Nachname	Status
1	Maria	Haber	Mitarbeiter
2	Herbert	Müller	Kunde
3	Ali	Salam	Kunde
4	Corinna	Maier	Mitarbeiter

Tabelle 1: Beispiel für den Aufbau von Datensätzen in einer relationalen Datenbank

Im Gegensatz dazu ist eine Blockchain eine dezentralisierte, verteilte Datenstruktur, die Informationen in einem kontinuierlichen Protokoll von Blöcken speichert. Jeder Block enthält eine Reihe von Transaktionen, die durch kryptografische Methoden gesichert sind. Der Erfinder der Blockchain, Satoshi Nakamoto, hat diese so konzipiert, dass Daten nicht nachträglich verändert werden können, was sie zu einem verlässlichen und transparenten Aufzeichnungssystem macht. Die einzelnen Computer in einer Blockchain werden Knoten (Nodes) genannt, wobei jeder Konten im Netzwerk gleichberechtigt ist und es keine Kontrollinstanz oder Autorität gibt. In diesem Fall spricht man von einem Peer-to-Peer-Netzwerk.

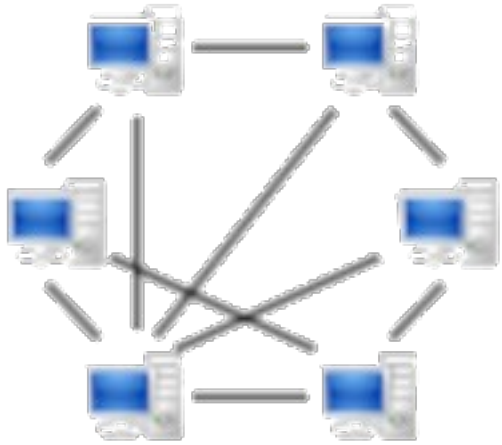


Abbildung 13: Darstellung eines verteilten Netzwerks (Peer-to-Peer), Quelle: Wikipedia

Die Speicherung der Daten funktioniert nicht wie bei relationalen Datenbanken in Form von Zeilen und Spalten, sonder linear in Blöcken, was bedeutet, dass die Blöcke chronologisch aneinander gereiht und durch einen kryptografischen Hashwert verknüpft werden. Ein Hash ist eine spezielle Art der Datentransformation, die in der Computertechnik und Kryptographie weit verbreitet ist. Es handelt sich um ein mathematisches Verfahren, bei dem aus einer beliebigen Eingabemenge (z.B. Text, Bild, Datei) ein eindeutiger, fest definierter Wert erzeugt wird.

Eine Relationale Datenbank speichert die Daten in einzelnen Datensätzen, die je nach Anforderung neu erstellt, geändert oder gelöscht werden können. Somit kann eine Abfrage erstellt werden, die den aktuellen Zustand des Datensatzes, also der Tabellenzeile, ergibt. Die Datenbank kennt den Werdegang der Daten nicht. Bei einer Blockchain ergibt sich der aktuelle Datenbestand aus der Betrachtung aller Blöcke. Ein Beispiel: Eine Bitcoinadresse wurde am Tag X_1 neu erstellt und ein Betrag von einem Bitcoin auf der Adresse XY hinterlegt. Wenn jetzt nach 14 Tagen ein halber Bitcoin ausgegeben wird, sprich auf eine andere Adresse transferiert wird, dann speichert die Bitcoin-Blockchain in einem weiteren Block diese Transaktion mit dem Wert 0,5 Bitcoin am Tag X_2 von der Adresse XY auf die Adresse YZ. In der Betrachtung ergeben sich dann zwei Einträge, die nacheinander ausgewertet werden und somit den Zustand der Adresse XY anzeigen, nämlich 0,5 Bitcoin per Stand jetzt. Das bedeutet logischerweise natürlich, dass kein Datensatz, also keine Transaktion, gelöscht werden darf.

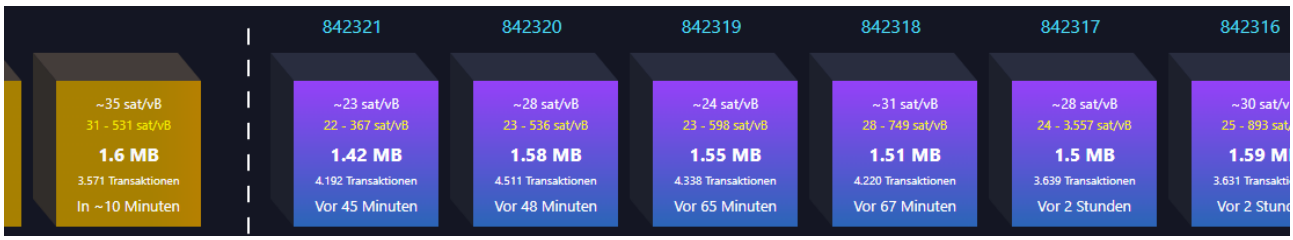


Abbildung 14: Screenshot aus dem Mempool mit der Darstellung von einzelnen Blöcken

Eine Besonderheit bei der Blockchain ist, dass alle Teilnehmer auf alle öffentlichen Daten zugreifen können und natürlich auch müssen, da der aktuelle Datenstand ja nur durch die chronologische Reihenfolge offenbar wird. Bei herkömmlichen Datenbanken nach dem Client-Server-Model werden Daten durch den Server limitiert und über ein ausgefeiltes Berechtigungssystem an den Client gesendet. Damit die Daten von bereits angehängten Blöcke der Kette nicht nachträglich manipuliert werden können, werden kryptografische Verfahren eingesetzt die selbst bei der kleinsten Veränderung der Daten zu komplett anderen Ergebnissen führen und so anzeigen, dass der manipulierte Block nicht valide ist. Um die Kette einwandfrei nachverfolgen zu können gibt es neben dem Zeitstempel auch in jedem Block immer eine Referenz auf den vorherigen.

Betrachtet man beide Modelle nebeneinander, so kann man sehr schnell feststellen, dass eine Blockchain zwar ein sicheres System, aber kein schnelles und auch nicht besonders effizientes System ist. Auch kann die Blockchain nicht gut skaliert werden, da immer nur neue Daten im System aufgenommen werden, wenn es einen neuen Block gibt und bei Bitcoin dauert dies in der Regel immer 10 Minuten, daraus ergibt sich bei einer durchschnittlichen Transaktionsgröße von 300 Bytes das nur etwa 7 Transaktionen pro Sekunde eingetragen werden können. Für Kundendaten, Ersatzteilverwaltungen, Produktlisten und wer weiß was für Datensätze ist eine Blockchain nicht geeignet. Nur wenn wirklich die Evolution der Daten im Vordergrund steht ist diese Art einer Datenbank überhaupt sinnvoll. Und genau das ist es warum Bitcoin die Blockchain braucht. Durch die Transparenz löst Bitcoin das Drittparteien-Problem, soll heißen, dass keine zusätzliche Institution oder Struktur benötigt wird, die bezeugen muss dass diese oder jene Transaktion rechtes ist. Auch gibt es keine zentrale Instanz bei der der Nutzer sich anmelden kann und sagen das er mitmachen möchte. Keine zentrale Instanz kann für den Einzelnen irgendetwas machen. Die Blockchain von Bitcoin verwaltet sich, so komisch das auch klingen mag, vollkommen selbst aufgrund von frei zugänglichen Protokollen und Konventionen. Niemand kann ausgeschlossen werden und jeder ist willkommen. Der gesamte Quelltext für die Kernanwendungen ist quelloffen und durch kein Patent oder irgendwas geschützt. Es steht jedem frei selbst Computerprogramme zu schreiben, die die Funktion von Bitcoin in jedweder Form beinhaltet.

Jetzt schauen wir uns mal einen Block[32] selbst an.

32 Quelle - https://mempool.space/de/

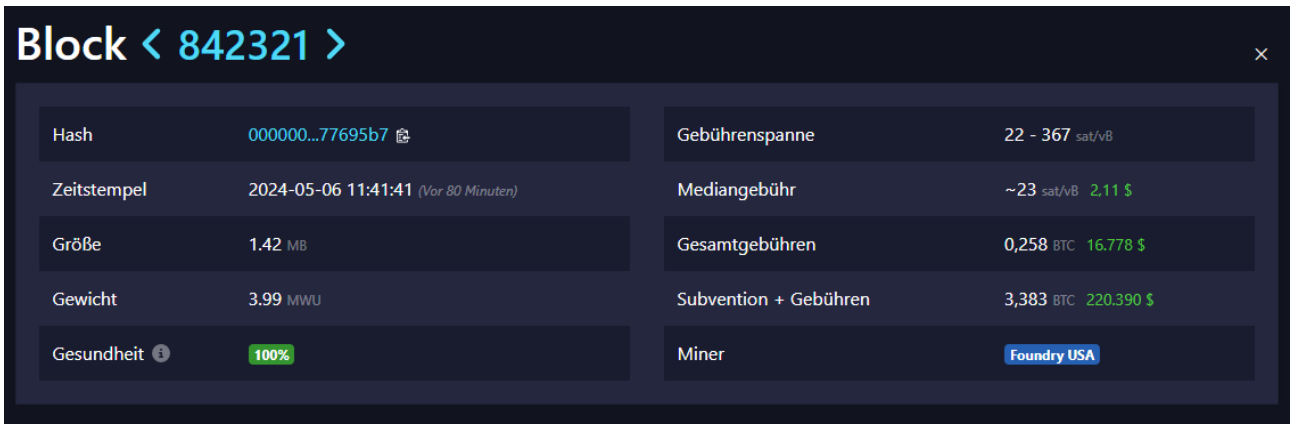


Abbildung 15: Headerdaten eines Blocks der Blockchain

Ganz oben sehen wir die Nummer des Blocks, oder die Blockhöhe. In diesem Fall 842.321.

Links sehen wir...

- Hash : 0000000000000000000018e3416e46fa9be0e9da6cbf44eae4331efb0577695b7 – dies ist die kryptografische Zeichenkette, die aus allen Daten des Blocks gebildet wird.
- Zeitstempel : Die genaue Zeit, zu der der Block angehängt wurde.
- Größe : Datenmenge in Megabytes, aus der der Block besteht.
- Gewicht : Die maximale Datenmenge die aufgenommen werden könnte. (Anfangs waren das 1 Megabyte und nach dem SegWit-Update wurde dies auf maximal 4 Megabyte erweitert)
- Gesundheit : Damit ist die Integrität der Daten gemeint. Sprich die Blockdaten sind fehlerfrei.

Auf der rechten Seite werden folgende Werte angezeigt:

- Gebührenspanne : Die Spanne der Transaktionsgebühren
- Mediangebühr : Die Transaktionsgebühr im Median
- Gesamtgebühren : Summe aller Gebühren in diesem Block
- Subvention + Gebühren : Das ist die Summe aus den Gebühren und der Belohnung in Form von neuen Bitcoins für das Finden des Blocks.
- Miner : Name des Miners / Miningpools der den Block gefunden hat.

Der einzelne Block sieht dann in etwas so aus. Jedes Quadrat steht für eine Transaktion und die Farben zeigen an, welche Priorität die Eintragung hat und damit auch welche Gebühren verlangt werden. Grundsätzlich

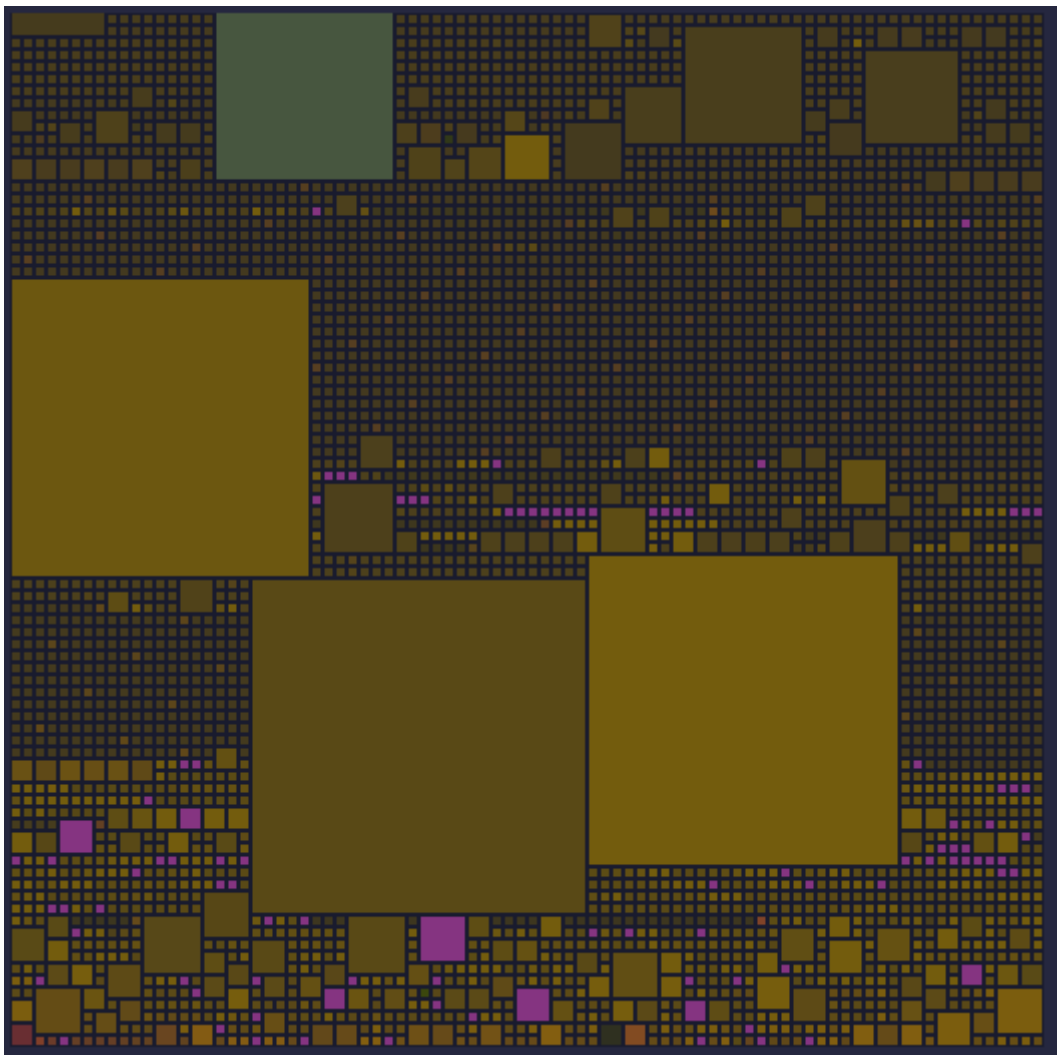


Abbildung 16: Visualisierung eines Blocks mit seinen Transaktionen, Quelle: Scan Mempool.space

Abschließend kann man sagen, dass dieses Verfahren Daten zu speichern und miteinander zu verknüpfen nicht besonders schnell ist, aber den unschlagbaren Vorteil hat, dass alle Daten transparent gehalten werden können und durch die Dezentralität der einzelnen Kontenpunkte ist das Netzwerk mit seinen unzähligen Redundanzen maximal gegen Angriffe und Manipulationen geschützt. Was wir noch klären müssen, ist was nun eigentlich ein Bitcoin ist. Die ganze Zeit ist vom Netzwerk und Transaktionen und jede Menge mehr die Rede, aber was ist es denn am Schluss, was sich jeder auf der Börse kaufen kann und nebenher gesagt sehr viel Geld dafür bezahlen soll.

Ein Bitcoin, offiziell Abgekürzt als BTC, ist eine Phantasieeinheit, die im Grunde auf nichts begründet ist. Man spricht in diesem Zusammenhang von einem Token, aus dem Englischen für Zeichen oder Merkmal. Diese Einheit wird dazu verwendet, das Netzwerk zu finanzieren, also die Energie und den menschlichen Aufwand zu begleichen und dient als Recheneinheit. Der Wert dieser Recheneinheit ergibt sich aus der zugrundeliegenden Datenbank und Infrastruktur und, ganz entscheidend, der Akzeptanz der Nutzer. Bei Bitcoin sind, wie wir ja schon gesehen haben, die Eigenschaften und Funktionen dergestalt, dass es sich um ein richtiges Geld handel kann, wenn die Menschen es wollen. Geld ist, man darf das nicht vergessen, eine gesellschaftliche Übereinkunft. Sonst nichts. Das klingt jetzt etwas nüchtern und es stellt sich automatisch die Frage, ob die ganzen Kritiker recht haben, wenn sie sagen das es sich nur um eine Spekulationsblase handelt. Kurz um, haben sie nicht und im Kapitel „Nur ein Schneeballsystem – Warum Bitcoin seine Kritiker Lügen

straft“ erkläre ich sehr genau warum das so ist. Bitcoin ist ein Ökosystem, welches es so noch nie gab und es ermöglicht uns ungeahnte Chancen diese Welt in einen besseren Ort zu verwandeln dabei ist BTC die Währungseinheit auf die wir uns einigen können und mit der wir dies erreichen können.

Von der Schwierigkeit ein Puzzle zu lösen. Was ist Mining?

Bitcoin ist eine dezentrale Kryptowährung, was bedeutet, dass es keine zentrale Instanz wie eine Zentralbank oder ein Unternehmen gibt, die Bitcoin kontrolliert oder verwaltet. Die Fortschreibung im Bitcoin-Netzwerk wird stattdessen von vielen Teilnehmern - den sogenannten "Minern", zu deutsch Schürfern, betrieben und aufrechterhalten. Das Mining ist der Prozess, bei dem neue Bitcoins in Umlauf gebracht und Transaktionen im Bitcoin-Netzwerk verifiziert werden. Miner verwenden hochleistungsfähige Computer, um komplexe mathematische Rätsel zu lösen, die mit dem Verifizieren von Bitcoin-Transaktionen in Zusammenhang stehen. Wenn ein Miner eines dieser Rätsel löst, wird er mit einer Belohnung in Form von neu geschaffenen Bitcoins und Transaktionsgebühren belohnt.

Der Prozess teilt sich in mehrere Einzelschritte. Zuerst werden ausstehende Bitcoin-Transaktionen gesammelt und in einem Block, das ist eine Datenmenge von maximal 4 Megabyte nach dem neuen Segregated Witness Standard, gebündelt. Die Transaktionen werden also quasi in einem Warteraum aufbewahrt, bis sie in die Datenbank aufgenommen werden können. Wir haben ja bereits festgestellt, die Blockchain nichts anderes ist als ein riesiges Kassenbuch, welches hauptsächlich aus Transaktionen besteht.

Im zweiten Schritt wird mit dem sogenannten Proof-of-Work-Verfahren ermittelt, wer die weitere Bearbeitung des Blockes durchführen darf. Proof-of-Work bedeutet, dass immens viel Rechenleistung aufgewendet werden muss, um einem festen Algorithmus folgend, ein mathematisches Puzzle zu lösen. Dieser Nachweis von Arbeit, denn nichts anderes bedeutet Poof-of-Work, sichert, dass neue Datenblöcke nicht einfach aus dem Nichts erzeugt werden können und es eine Kraftanstrengung ist die Blockchain fortzuschreiben. Dies ist einer der Hauptunterschiede zum herkömmlichen Fiatgeldsystem. Der Schürfer, der das Puzzle zuerst löst erhält den Zuschlag den neuen Block anzufügen und ihm werden auch die Belohnung und die Transaktionsgebühren zugeschlagen.

Nach erfolgreichem Erbringen des Arbeitsnachweises (Proof-of-Work) wird der Datenblock aus dem ersten Schritt an die Blockchain angehängt und alle anderen Teilnehmer des Netzwerkes, dazu gehören auch die Nutzer welche einen Knotenpunkt im Netzwerk betreiben (Full-Nodes), überprüfen den Block und die darin enthaltenen Transaktionen, damit sichergestellt wird, dass alles in Ordnung ist. Dieser Vorgang nennt sich Validierung und zieht sich über mehrere Blocks. Nach etwa sechs weiteren Blöcken gilt eine Transaktion als sicher, da der Aufwand einen Block nachträglich zu ändern derartig groß wäre, dass dies fast nicht leistbar ist. Je mehr Blöcke angehängt werden, desto unfälschbarer wird eine Transaktion. Dieser Miningprozess ist das Fundament des demokratischsten Geldsystem seit Menschen Gedenken. Wir dürfen nie außer Acht lassen, dass sich jeder an diesem Miningprozess beteiligen kann. Das unterscheidet Bitcoin kolossal von Fiatwährungen, bei denen selber Geld drucken schwer bestraft wird, was wiederum zeigt, wie das Machtgefälle ist. Wenn ein Zentralbänker Milliarden erschafft, dann ist das gut und wichtig für die Stabilität und all die salbungsvollen Geschichten, die erzählt werden, aber wenn ein Bürger ein paar Scheine zuhause kopiert, gibt es Gefängnis.

Zuletzt wird die Belohnung in Form von neuen Bitcoins und den Gebühren aus den Transaktionen an den Miner ausgeschüttet, der den Proof-of-Work für sich entschieden hat. Meisten sind dies sogenannte Minig-Pools, also Zusammenschlüsse aus vielen Minern um die Chance zu erhöhen einen validen Block zu finden. Bei den heutigen Rechenleistungen ist es nur noch theoretisch

möglich als Einzelperson regelmäßig Blöcke zu finden. Aber jeder kann sich einem Mining-Pool anschließen und erhält dann relativ zu seinem Beitrag eine Vergütung für gefundene Blöcke.

Mit der Zeit werden die Blköcke validiert

Für das lösen dieser Rätsel gibt es ein paar Regeln. Je mehr Computer, das heißt Miner, am Proof-of-Work beteiligt sind, gemessen an Rechenleistung und ausgedrückt in der Hashrate, desto schwerer wird die Aufgabe einen validen Block zu finden. Es ist klar, dass ein Rätsel schneller gelöst wird, wenn sich mehr Menschen/Maschinen an die Lösung machen. Dafür gibt es den „Regler“ der Schwierigkeit (Difficulty), der entsprechend der eingebrachten Rechenleistung automatisch alle 2016 Blöcke, das entspricht etwa 14 Tagen, angepasst wird und so auch gewährleistet, dass die Blockzeit, also die Zeitspanne zwischen dem Finden von zwei Blöcken, im Mittel bei 10 Minuten bleibt. Man kann sagen, dass Bitcoin einen Herzschlag von 6 pro Stunde hat. Es ist aber auch nicht ungewöhnlich, dass die Zeiten sehr viel kürzer oder länger sind. Diese 10 Minuten stellen nur ein Durchschnitt dar.

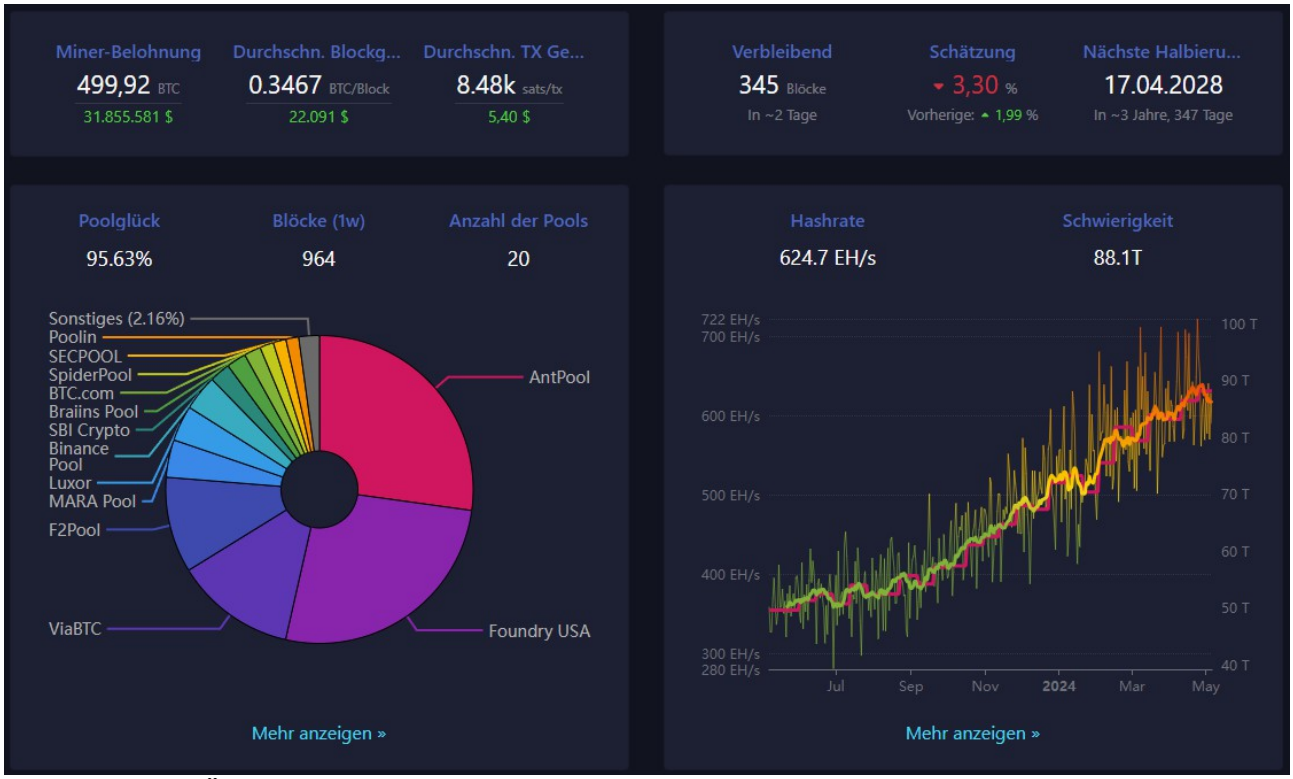


Abbildung 17: Übersicht über die aktuelle Hashrate und die beteiligten Minig-Pools

Aus dem Aufgezähltem resultiert der einfache Schluss, dass es sehr schwer bis nahezu unmöglich ist diesen Mechanismus des Proof-of-Work zum Beispiel durch Großunternehmen oder gar Staaten zu manipulieren. Ein potenzieller Angreifer müsste mehr Rechenleistung aufbringen als bereits im Netzwerk besteht und dies ist alleine schon durch die Hardwareressourcen, als auch durch die aufzuwendende Energie schier unmöglich. Es gibt nicht so viele leistungsfähige Miningcomputer und schon gar nicht neben eigens dafür betriebenen Kraftwerken. Aber nichts desto Trotz ist diese sogenannte 51% Attacke ein theoretisches Problem, welches von den Entwicklern, auch in Hinblick auf Quantencomputern im Auge behalten werden muss.

In der Grafik sieht man die Hashrate, die derzeit bei 624,7 EH/s liegt. Das bedeutet, dass 624,7 Quintillionen (1 mit 18 Nullen) Hashberechnung pro Sekunde ausgeführt werden und man kann schon sagen, dass das extrem viel Rechenleistung ist.

Dieses Mining-Verfahren ist der Schlüssel zur Funktionsweise und Sicherheit des Bitcoin-

Netzwerks. Durch den Wettbewerb zwischen Minern, die um die Lösung des Proof-of-Work-Rätsels konkurrieren, wird die Integrität und Dezentralisierung des Netzwerks gewährleistet. Je mehr Rechenleistung ins Netzwerk eingebracht wird, desto sicherer ist es, da es immer schwieriger wird, das Netzwerk zu manipulieren oder anzugreifen. Allerdings erfordert das Mining auch enorme Mengen an Energie und Hardware-Ressourcen. Die Miner müssen leistungsfähige, energieeffiziente Computer betreiben, um im Wettbewerb um neue Blöcke erfolgreich zu sein. Daher ist das Mining-Geschäft sehr wettbewerbsintensiv und wird von großen, spezialisierten Mining-Pools dominiert. Zum viel diskutierten Thema des Energieverbrauchs gibt es ein eigenes Kapitel in dem ich nochmals ganz genau auf das Thema eingehe.

Es wird oft diskutiert, ob ein Ökosystem wie Bitcoin, vielleicht in verbesserter Form, nochmals entstehen könnte und ich bin der festen Überzeugung, dass dies unmöglich ist, denn am Anfang, als sich noch niemand für Bitcoin interessiert hat, war das Projekt sehr angreif- und verwundbar. Damals hätten Staaten, denen das Projekt ein Dorn im Auge ist, es einfach auslöschen können und das würden sie auch mit einem designierten Nachfolger machen. Heute mit der immensen Verbreitung und der Dezantralität ist Bitcoin praktisch nicht mehr angreifbar.

Insgesamt ist das Bitcoin-Mining ein komplexer, aber faszinierender Prozess, der das Rückgrat des Bitcoin-Netzwerks bildet. Durch das Zusammenwirken vieler Miner wird die Sicherheit und Dezentralisierung des Netzwerks gewährleistet und neue Bitcoins in Umlauf gebracht.

Wenn sich die Wege trennen.

Ein Geld- und Wertesystem steht immer vor den Herausforderungen, dass sich unsere Welt sehr schnell ändert und manchmal auch Anpassungen notwendig sind. Bitcoin ist da natürlich keine Ausnahme. Da Bitcoin keine zentrale Instanz kennt, die entscheiden kann, welche Änderungen wichtig und / oder notwendig sind läuft das Verfahren komplett basisdemokratisch ab. Und auch substanziell - niemand wir zu irgendetwas gezwungen. Jeder entscheidet selbst welche Entwicklung eingeschlagen werden soll, oder eben auch nicht. Derartige Gedanken sind aus dem Fiatsystem gänzlich fremd und man muss darüber erst einmal gründlich nachdenken und zu verstehen, welche bahnbrechende Neuerung gegenüber der alten Welt das ist.

Wichtig bei der Entwicklung von Bitcoin zu verstehen ist, dass wirklich jeder, der gute Programmierkenntnisse hat und das Interesse mitbringt, sich an der Evolution beteiligen kann. Alle Programmierer sind dezentral auf der ganzen Welt verteilt und tauschen sich in geeigneten Foren und Chats aus. Auch diese Gremien sind vollkommen demokratisch gehalten, also es gibt nicht den Chefprogrammierer und den Projektdesigner, die sagen wohin die Reise gehen soll. Jeder hat so viel Stimmrecht wie kluge Ideen eingebracht werden.

Um das Protokoll auf veränderte Gegebenheiten anpassen zu können gibt es verschiedene Mechanismen. Schauen wir uns diese einmal genauer an.

Die Weiterentwicklung des Bitcoin-Protokolls erfolgt über einen sorgfältigen und transparenten Prozess der gemeinschaftlichen Diskussion und Konsensfindung innerhalb der Bitcoin-Community. Änderungen am Programmcode und wichtige Protokoll-Upgrades werden von den Bitcoin-Entwicklern sehr gründlich geprüft und debattiert, bevor sie umgesetzt werden. Dabei wird großer Wert darauf gelegt, die Stabilität und Vertrauenswürdigkeit von Bitcoin nicht zu gefährden. Ein beschleunigter "Speedy Trial"-Ansatz, wie er etwa in Rechtssystemen Verwendung findet, ist im Kontext von Bitcoin komplett irrelevant. Stattdessen folgt die Bitcoin-Entwicklung einem bedachtsamen Vorgehen, bei dem die gesamte Community eingebunden wird. Wichtige Upgrades wie SegWit oder Taproot wurden so über einen längeren Zeitraum breit diskutiert und schrittweise eingeführt, ohne eine schnelle, übergangene Konsensfindung zuzulassen. Dieser umsichtige Prozess ist essentiell, um das Vertrauen in das Bitcoin-Netzwerk zu erhalten und kontinuierlich

weiterzuentwickeln.

Wenn nach reiflicher Überlegung und offener Diskussion eine Änderung implementiert werden soll, so gibt es den sogenannten Soft Fork, englisch für weiche Gabelung, was eine rückwärtskompatible Änderung des Bitcoinnetzwerks ist. Das bedeutet, dass nach der Einführung eines Soft Forks ältere Bitcoin-Knoten (Nodes) die neuen Regeln weiterhin akzeptieren können, ohne dass sie ein Upgrade durchführen müssen. Durch die Rückwärtskompatibilität eines Soft Forks können also ältere Kontenpunkte weiterhin am Netzwerk teilnehmen, ohne ein Upgrade durchführen zu müssen. Dies erhöht die Stabilität und Akzeptanz von Änderungen im Bitcoinnetzwerk. Mit diesem Verfahren wurde zum Beispiel 2012 das Pay-to-Script-Hash eingeführt, was komplexere Transaktionen ermöglicht.

Und dann gibt es noch den sogenannten Hard Fork, zu deutsch dann die harte Gabelung. Das ist eine nicht rückwärtskompatible Änderung des Bitcoinnetzwerks, was bedeutet, dass nach der Einführung eines Hard Forks ältere Bitcoin-Knoten die neuen Regeln nicht mehr akzeptieren können und daher ein Upgrade durchführen müssen, um am Netzwerk teilnehmen zu können. Im Gegensatz zur weichen Variante führt ein Hard Fork also zur Aufspaltung des Bitcoinnetzwerks in zwei separate Kryptowährungen. Dies kann manchmal notwendig sein, um grundlegende Änderungen am Protokoll vorzunehmen, birgt aber auch Risiken für die Stabilität und Einheit des Gesamtsystems. Als Folge von Hard Forks sind Bitcoin Cash und Ethereum als eigenständige Kryprowährungen entstanden. Ein Hard Fork ist immer nur die letzte Wahl, denn mit jeder Änderung das Netzwerk potentiell geschwächt wird. Bitcoin möchte niemanden auf seinem Siegeszug verlieren.

Wir sehen also, dass es verschiedene Möglichkeiten gibt Bitcoin erfolgreich in die Zukunft zu bringen, gleichgültig welche Herausforderungen dort warten.

Steht am Ende des Minings die Arbeitslosigkeit?

Wir haben jetzt schon mehrfach gehört, dass die Schürfer, die Miner, für jeden neuen Block neu geschaffene Bitcoins bekommen. Aber was geschieht, wenn im Jahr 2140 keine neuen Bitcoin mehr ausgegeben werden und auch davor die Menge so gering ist, dass die Kosten für die Energie nicht erwirtschaftet werden können? Hören die dann einfach auf und bricht das Netzwerk damit zusammen?
Die Haupteinnahmequelle der Schürfer ist heute die Belohnung für neu gefundene Blöcke, aber bereits jetzt kommen etwa noch einmal 5% bis 10% des Erlöses durch die Transaktionsgebühren oben drauf, was einem Erlös in der Größenordnung 0,15 – 0,3 BTC entspricht. Vor dem letzten Halving, also der Halbierung der Belohnung pro Block, im April 2024, als es für einen neuen Block noch 6,25 BTC gab, waren es nur 2% - 5%, ergo etwa die selbe Menge, doch ist der Wechselkurs in dieser Zeit auch massiv angestiegen. Wir sollten uns nochmals vor Augen halten, dass Bitcoin massiv deflationär ist und was heute einen Bitcoin kostet, wie zum Beispiel ein Mittelklasse BMW, kostet in 5 Jahren wahrscheinlich nur noch 0,5 Bitcoin oder noch weniger. In der Tendenz wird die Akzeptanz von Bitcoin steigen und es wird auch viel Geld aus alternativen Kryptowährungen in das Netzwerk fließen, sobald die Anleger merken, dass diese Projekte nicht wirklich halten, was sie versprechen. Insbesondere die Einführung von ETFs, die institutionellen Anlegern die Möglichkeit bieten in Bitcoin zu investieren, was auch sehr stark genutzt wird, hilft mit, den Wechselkurs zu Fiatwährungen weiter zu steigern. In der Folge sind die Schürfer in der Lage ihre Kosten immer mehr aus den Gebühren zu bestreiten, die gegebenenfalls auch angehoben werden können, respektive der Gegenwert steigt. Das bedeutet also, dass es weiterhin ein lohnendes Geschäftsmodel ist, Mining zu betreiben.

Ein Gedanke zu den Gebühren soll hier auch noch eingestreut werden, denn man kann sich ja

ehrlicher weise fragen, wozu es diese überhaupt gibt, solange es eine Belohnung für das Finden ausgezahlt wird. Dabei geht es hauptsächlich darum, dass kein Spam in der Blockchain gespeichert wird, der die Datenmenge nur unnötig aufbläht. Je geringer die Datenmenge, desto leichter ist es die komplette Blockchain selber als sogenannter Full-Node (Knotenpunkt) zuhause zu haben, was wiederum die Verteilung und damit die Sicherheit der gesamten Blockchain erhöht.

Derzeit sind auch die Datenmengen pro Block noch lange nicht ausgereizt, bedeutet also, dass noch einiges mehr an Gebühren möglich ist. Mit jedem neuen Nutzer werden mehr Transaktionen notwendig, was schließlich zur besseren Auslastung der Blöcke und damit zu mehr Transaktionsgebühren führ. Damit dies aber für den einzelnen Nutzer nicht zu einem finanziellen Fiasko wird, was natürlich die Akzeptanz von Bitcoin massiv schmälern würde werden mit der Zeit mehr und mehr Anwendungen zum Einsatz kommen, die zum Beispiel Technologien wie das Lightning-Netzwerk nutzen. Sobald der Bedarf in ausreichender Menge vorhanden ist, werden auch Lösungen angeboten werden. Und durch Lightning zum Beispiel sind Zahlungen von Kleinstbeträgen sehr einfach möglich. Das wäre dann der Punkt, an dem Bitcoin anfängt wirklich Geld zu werden. An diesem Punkt tragen dann die Betreiber der Lightning Kanäle die Hauptlast der Gebühren wodurch die Gebührenlast im Allgemeinen gegenüber heute fallen würde und doch alle Beteiligten ausreichend entlohnt würden. In der Informatik sind Entwicklungen sehr schnell und bisweilen auch bahnbrechend möglich und man kann sicher davon ausgehen, dass ein Asset wie Bitcoin mit einer Marktkapitalisierung von heute über einer Billion Dollar nicht aufgegeben wird. Das wäre so, als wenn alle Anleger einen Konzern wie Google oder Apple aufgeben würden.

Die Notwendigkeit weiter Blocks zu schürfen und die Sicherheit des gesamten Netzwerkes zu erhalten wird also eher anhalten und durch das Gebührenmodel kann dies auch recht leicht finanziert werden.

Gläsern

Jeder hat es schon gehört und jeder weiß im Hinterkopf auch, dass wir alle für Unternehmen und Behörden gläsern sind. Gläsern im Sinne, dass diese Institutionen wissen was wir kaufen, wo wir uns aufhalten, welche Vorlieben wir haben, was wir so im allgemeinen machen. Sie sammeln ständig Daten und im Falle des Staates ist dies wirkliche Überwachung. - Nur weil Daten nicht sofort gegen einen Bürger ausgespielt werden, heißt das noch lange nicht, dass man dies nicht mit denen tun kann, die sich unbotmäßig verhalten. - Wir haben uns daran gewöhnt auf Schritt und Tritt informativ verfolgt zu werden. Aber hat sich schon mal jemand die Frage gestellt, warum die, die so viel über jeden einzelnen wissen so ungern von sich selbst erzählen? Nehmen wir einmal die Staaten, in diesem Beispiel den deutschen Staat. Der Sicherheitsapparat filmt ständig im öffentlichen Raum und natürlich auf Autobahnen, die anlasslose Überwachung ist für die Geheimdienste, zum Beispiel mit dem sogenannten Saatstrojaner, auf dem Papier wohl nicht zulässig, beziehungsweise mit Hürden versehen, in der Praxis kann aber jeder, der sich nicht konform verhält digital vollkommen ausspioniert werden; und unser Leben heute ist einfach digital, ob wir das nun wollen oder nicht. Aber wenn der Bürger zum Staat geht und nachfragt, was mit all diesen Daten passiert oder ob er seine eigenen Daten einsehen darf, dann werden diese Behörden sehr schmallippig. Auf einmal gibt es Datenschutz, also der Bürger wird vor seinen eigenen Daten geschützt, und wenn es dann doch irgendwo steht, dass Unterlagen herausgegeben werden müssen, dann wird geschwärzt was das Zeug hält. Wenn man zu den Internetriesen geht ist es genau das selbe. Die haben zwar eine gewisse Auskunftspflicht, aber die erstreckt sich auf Banalitäten. Die Rohdaten, die man bekommen muss sind für den ungeübten nichts wert. Erst wenn diese Daten in den Kontext, zum Beispiel zu anderen Menschen, gestellt werden, ergeben diese erst wirklich Sinn, erst dann können Muster erkannt werden. Das kann der Kunde aber nicht und so kann Google und Facebook und wie sie alle heißen auch Daten herausgeben. Man wundert sich bisweilen, was da so

alles gespeichert wird und fragt sich, ob das rechtens ist, aber wir wissen ja auch, nur wer allen Datenschutzbestimmungen, die nicht umsonst zig Seiten lang sind, zustimmt, der kann diese „Dienste“ auch nutzen. Wir haben heute einen Zustand erreicht, den man sich eigentlich gar nicht ausdenken kann. Spionage, Überwachung, Gängleung, Zensur, Verleumdung wird uns heute insbesondere im Gewand der sozialen Medien, als Service verkauft. Wir werden durch die Internetgiganten gedrillt, wie in einem nordkoreanischen Umerziehungslager, aber der Clou daran ist, dass wir das Gefühl haben, endlich sagen zu dürfen, was wir wollen. Dabei blenden wir komplett aus, dass unsere Meinung unter einem der unzähligen unbedeutenden Posts so absolut gar keine Wirkmacht hat und wenn doch jemand Reichweite generiert, dann wird eingeschränkt, zensiert, gelöscht, verunglimpft, die Polizei und Staatsanwaltschaft geschickt, das Konto gekündigt, der Arbeitgeber angerufen und wer weiß was für nicht so nette Formen der (in)direkten Gewalt angewendet. Das Internet ist heute schon lange kein freier Raum mehr, es ist ein Ort der Meinung und zwar der Mainstream Meinung. Wer da nicht mitspielt, dem blüht das gerade Beschriebene. Die Menschen werden durch diese Medien zu vollkommen Unmündigen degradiert, was dann darin gipfelt, dass diese Menschen wenn sie zum Beispiel brutale Polizeigewalt sehen nicht etwas dem Opfer zu Hilfe kommen, sondern die Szene mit ihrem Handy Filmen um es dann bei Facebook und Instagram, oder wo auch immer, hochzuladen. Diesen zustand konnte sich nicht einmal George Owell in seinem Buch 1984 ausdenken und da stehen schon sehr bizarre Dinge drin.

Das nächste sind die ganzen Programmcodes, seinen sie jetzt von den Staaten oder von Unternehmen, sind alle geheim. Es ist ein sehr verbreitetes und wirksames Machtinstrument Wissen vorzuenthalten. Stellen wir uns einfach einmal vor, die Regierung würde ihren Bürgern alles sagen wie es um das Land so bestellt ist. Wenn sie ihr Herrschaftswissen wirklich teilen würden wäre noch vor dem Mittagstee Revolution und all die Lügen und Verdrehungen, die falschen Anschuldigungen und miserablen Rechtfertigungen würden den Politikern und Behördenmitarbeitern ins Gesicht geschleudert werden. Das System funktioniert nur so gut, weil wir nicht wissen was wirklich los ist und in der Struktur selbst gilt auch das „Need-to-Know-Prinzip“ also jeder weiß nur so viel, wie für seine Tätigkeit unbedingt erforderlich ist. Deshalb ist es auch nicht richtig den normalen Beamten, oder den Mitarbeiter in einem Unternehmen für die Zustände verantwortlich zu machen.

Bitcoin ist da etwas anders. Bitcoin speichert natürlich auch jede Transaktion. Das muss sein, weil wir ja schon gesehen haben, dass die Hauptkette, das Kassenbuch, so weitergeführt wird. Aber Bitcoin speichert keine Namen, keine Geburtsdaten oder sonstigen persönlichen Daten – nichts. Lediglich die beiden Adressen von Sender und Empfänger werden in kryptografisch verschlüsselter Form gespeichert und ein paar zusätzliche Daten zur Transaktion und **nur** wenn man selbst als Individuum den eigenen Namen mit einer Adresse verbindet, dann kann nachvollzogen werden, wer welchen Betrag an wen (wenn diese Adresse auch bereits bekannt ist) geschickt hat. Bitcoin ist also nicht anonym, denn wir werden noch sehen, wie die Staaten mittlerweile versuchen Adressen mit Namen zu verbinden und wir werden sehen, wie man sich dagegen schützen kann. Aber was fundamental anders ist bei Bitcoin ist, dass der Programmtext des Kerns und auch der allermeisten Anwendungen offengelegt ist. Wer also möchte und das entsprechende Verständnis mitbringt kann jeden einzelnen Schritt den die Software macht minuziös nachverfolgen und prüfen, ob irgendwo Daten abgegriffen werden, ob irgendwelcher Missbrauch betrieben wird. So etwas gibt es bei Microsoft, Meta, Google oder Apple nicht und wird es nie geben. Und bei Bitcoin kann man jede Transaktion anschauen, also jeder kann jede Transaktion anschauen. Man stelle sich das mal bei einer Bank vor, die übrigens auch jede Menge Daten sammelt und nichts herausgibt, wenn es darum geht. Wenn die Deutsch Bank alle Kontoauszüge von allen Kunden transparent ausstellen würde, wäre ganz schnell für jeden klar, dass diese Bank nicht nur am Rande des Abgrundes steht, sondern schon meilenweit darüber. Aber das müssen sie nicht und mit den heutigen Bilanzierungstricks bleiben die Geheimnisse der Deutschen Bank auch deren Geheimnisse. Das gilt für die allermeisten

anderen Banken übrigens auch. Früher gab es noch so etwas wie das Bankgeheimnis, welches naiv und vordergründig betrachtet den Kunden und seinen Wohlstand schützen sollte. Denkt man etwas länger über dieses Geheimnis nach, kommt man unter Umständen auf den Gedanken, dass durch die Geheimniskrämerei eher die Bank geschützt wurde, denn der Kunde. Bei Bitcoin bewirkt diese totale und kompromisslose Transparenz, dass wir niemanden mehr vertrauen müssen. Wenn wir anzweifeln ob die eine oder andere Transaktion korrekt ist, na dann schauen wir eben nach und zum Beispiel sind die Adressen der ETFs[33] der großen Vermögensverwalter mittlerweile fast alle bekannt und jeder kann sehen, ob die Menge an ETF Emmisionen zu der gehaltenen Menge an Bitcoin passen. So eine Überprüfung ist bei allen anderen Fonds nicht möglich und man kann nur hoffen, dass dort die Verwahrer nicht die größten Gauner sind.

Und was diese Transparenz von Bitcoin noch bewirkt ist, dass jeder sehen kann wie Bitcoin verteilt ist. Durch den Umstand, dass die allermeisten Bitcoins bereits geschürft wurden und die Gruppe derer, die in der Anfangszeit sich überhaupt mit Bitcoin befasst haben sehr klein war ist die Verteilung logischerweise sehr ungleich, selbst im Verhältnis zum Fiatgeld, welches schon extrem ungleich verteilt ist. Die nachfolgende Grafik zeigt, wie die Verteilung aktuell ist.

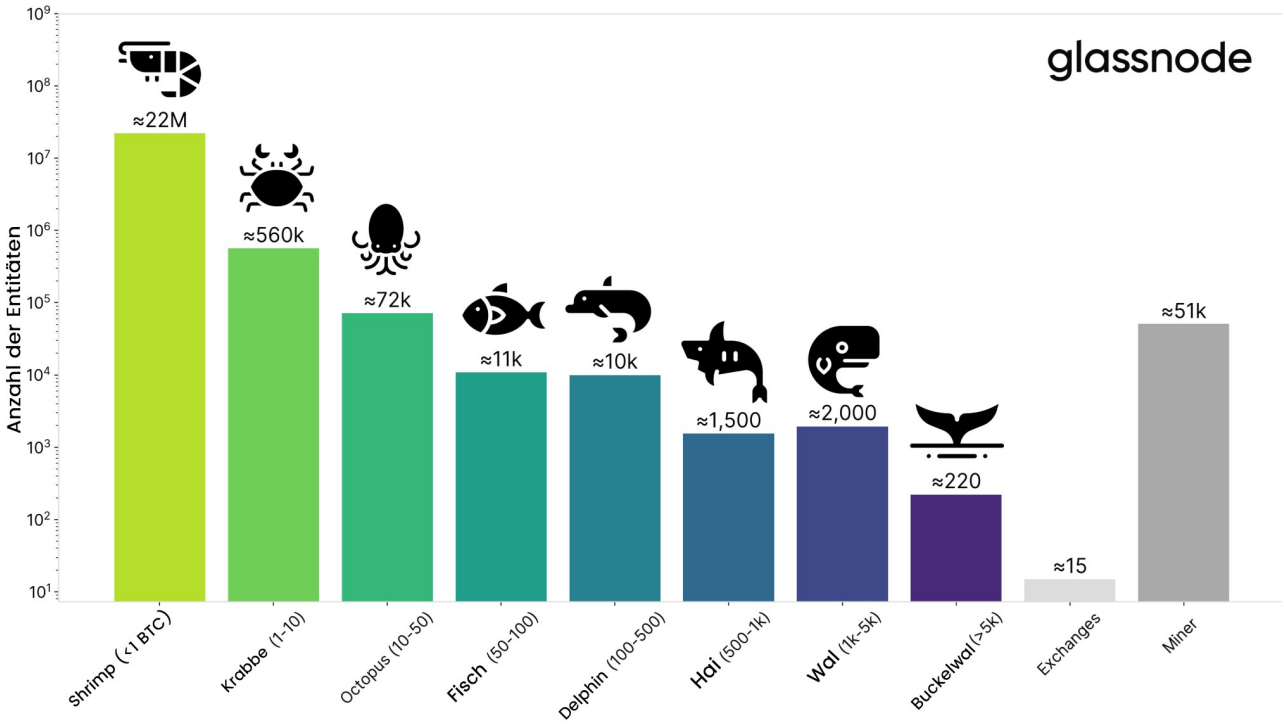


Abbildung 18: Verteilung von Bitcoin nach Klassifikationen. Quelle Glassnode.com

Bei Bitcoin hat es sich eingebürgert, dass die einzelnen Adressen in Abhängigkeit zu ihrem Wert in Meerestiere zu gruppiert werden um in der Analogie der Körpergröße den Wert, beziehungsweise die Anzahl, der gehaltenen Bitcoins zu veranschaulichen. In einem frühen Bitcoin-White-Paper von Satoshi Nakamoto aus dem Jahr 2008 findet sich folgende Passage, in der er die Bitcoin-Technologie mit Meerestieren vergleicht: „[Die Bitcoin] sind wie Muscheln im Meer, die von Wellen an Land gespült werden - eine zufällige, aber vorhersehbare Verteilung.“ Nakamoto nutzt in diesem Vergleich die Analogie, dass so wie Muscheln und andere Meerestiere von den Wellen an Land gespült werden, auch neue Bitcoins "zufällig, aber vorhersehbar" durch den Mining-Prozess in Umlauf gebracht werden. Diese bildhafte Analogie sollte veranschaulichen, wie der dezentrale und algorithmisch gesteuerte Bitcoin-Mechanismus funktioniert. Nakamoto griff damit auf ein einfaches Naturbeispiel zurück, um das neuartige Konzept von Bitcoin verständlicher zu machen.

33 ETF - Exchange Traded Funds

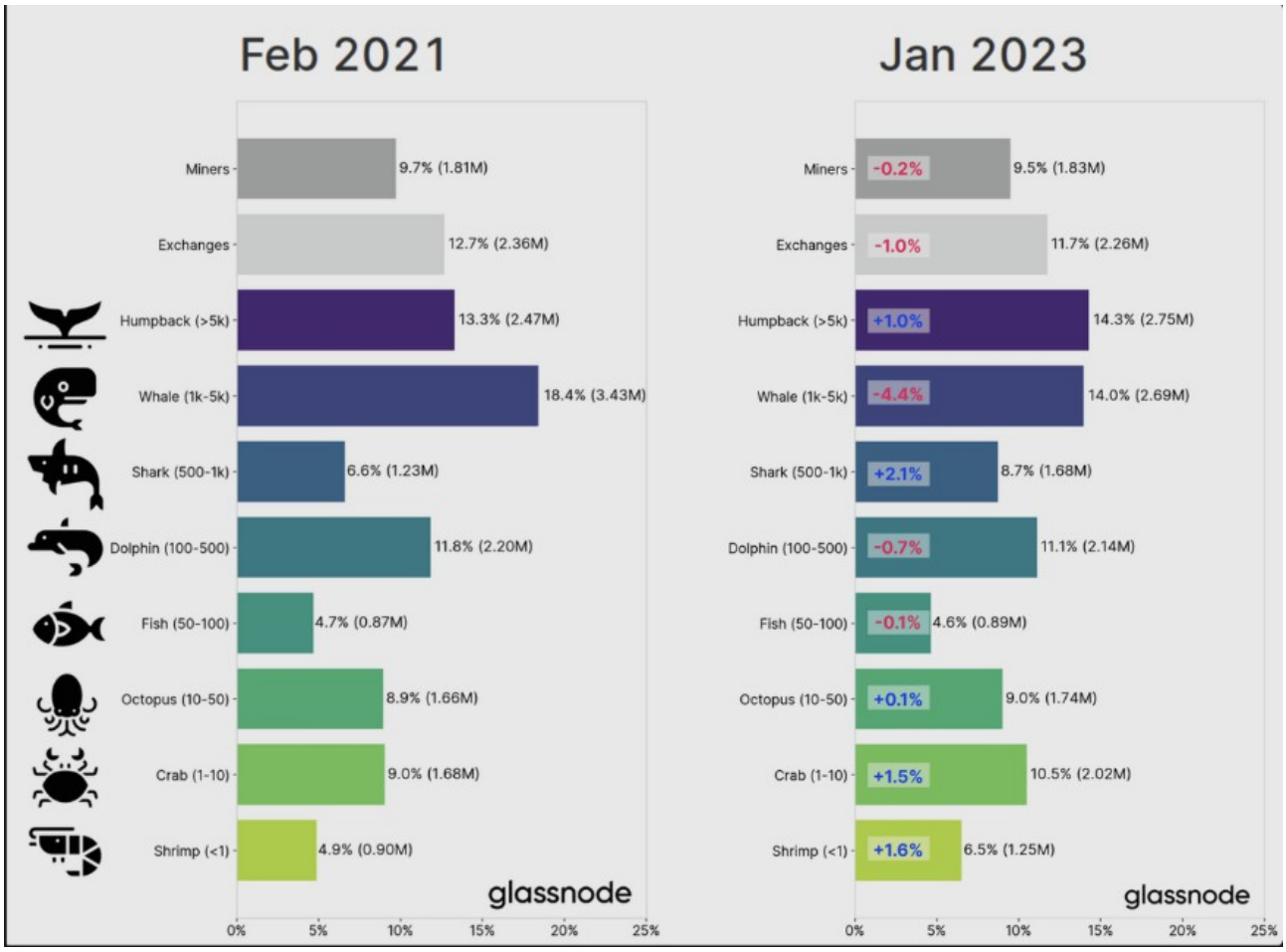


Abbildung 19: Veränderung der Verteilung von Bitcoin. Quelle Glassnode.com

Diese Grafik zeigt, wie sich Bitcoin langsam in die Gesellschaft verteilt. Dieser Prozess ist unglücklicherweise sehr verhalten, da zum einen der Wert von Bitcoin schon extrem hoch ist und zum anderen durch die permanente Wertsteigerung ein starker Anreiz gegeben ist die Bitcoin, die man hat, zu halten. Aber man kann den Trend ablesen, dass die Verteilung besser wird und sobald die Umlaufgeschwindigkeit steigt wird sich Bitcoin sehr viel gerechter als Fiatgeld verteilen. Und der Grund dafür ist recht einfach, nämlich durch die deflationäre Natur und den ständigen Wertzuwachs erhält man nominal immer weniger Bitcoin für sein Fiatgeld, seine Arbeit oder Ware, obwohl der Wert der kleineren Menge durchaus gleich oder sogar größer ist als vorher. Das bedeutet, wenn heute ein Wal ein Haus kauft für sagen wir 5 BTC wird dies in 10 Jahren vielleicht durch die Wertsteigerung der Immobilie selbst, aber insbesondere auch durch die Steigerung bei Bitcoin selbst nur noch 2 BTC wert sein. In Fiatwährung mag es aber der selbe Preis oder sogar mehr sein, doch in BTC gemessen sinkt der Verkaufspreis. Real haben sich also in unserem Beispiel bei einem Verkauf 3 BTC verteilt. Dieser Prozess ist wie schon gesagt sehr langwierig, aber die Verteilung wird unaufhaltsam voranschreiten und auf lange Sicht ein sehr viel gerechteres System schaffen. Zu den Buckelwalen (Humbacks) muss noch gesagt werden, dass dazu auch die Verwahrer der Vermögensverwalter dazu gezählt werden müssen. Das sind also teilweise riesige Bestände, die aber unzählige Besitzer haben.

Was man bei dieser Betrachtung nicht außer Acht lassen darf ist auch, dass viele Adressen, insgesamt etwa 19% oder zirka 4 Millionen Stück des gesamten Bestandes, bereits für immer verlorene Bitcoin sind. Diese können nicht mehr umverteilt werden. Wir kommen noch dazu, wie so etwas passieren kann, aber als Bitcoin noch ganz am Anfang stand wurde es auch von Menschen,

die sich für das Konzept interessierten und damals zu Witzpreisen Coins gekauft haben, natürlich nicht richtig ernst genommen. Es gibt hanebüchene Geschichten in denen Müllhalden durchforstet wurden um eine Festplatte zu finden, auf der die Schlüssel zu zig Bitcoin gespeichert waren. Heute wird sehr viel besser auf die Schlüssel aufgepasst, aber die Bitcoin, die bereits verloren sind, werden das auch für immer bleiben. Satoshi Nakamoto hat dies als Spende an das Netzwerk bezeichnet.

Was wir auf jeden Fall für uns mitnehmen ist, dass Bitcoin durch seine vollkommene Transparenz jedes Drittparteienrisiko ausschließt, sei es bezüglich des Bestandes, der Verteilung oder auch der Datensicherheit. Diese Form der Anlage ist absolut einmalig.

Wozu braucht man Wallets und wieso können die heiß und kalt sein?

Im Zusammenhang mit Kryptowährungen taucht immer wieder diese ominöse Wort „Wallet“ auf, was nichts anderes heißt als Brieftasche, oder Geldbörse. Und dann hält sich der Mythos, dass in dieser Wallet die Kryptos aufgestapelt liegen und man die mit sich herumtragen kann. Die Wirklichkeit ist so viel nüchterner... Die Bitcoins liegen immer und zu jeder Zeit auf der Blockchain. Diese werden niemals heruntergeladen oder von Anwender zu Anwender gesendet. Alles was passiert ist, dass in dem zentralen Kassenbuch, der Blockchain, Einträge stehen, die bestätigen, dass so und so viele Bitcoins auf dieser und jener Adresse liegen. Das ist alles.

Diese elektronische Geldbörse ist eine Softwareanwendung, die nichts anderes tut, als einen privaten Schlüssel zu verwalten. Der private Schlüssel ist eine zufällig generierte, extrem große Zahl. Und es ist diese große Zahl, die den Zugang zu den eigenen Vermögenswerten schützt. Aus ihr wird der öffentliche Schlüssel über ein mathematische Verfahren, dass sich Elliptische-Kurven-Kryptografie nennt, abgeleitet. Wichtig dabei ist zu wissen, dass vom öffentlichen Schlüssel nicht rückwärts auf den privaten Schlüssel geschlossen werden kann, was bedeutet, dass man seinen öffentlichen Schlüssel kommunizieren kann und muss und nur wenn man den privaten dazu auch hat eine Transaktion möglich wird.

Was eine Wallet noch tut ist die Bitcoin-Adressen ebenfalls nach einem kryptographischen Verfahren aus dem privaten Schlüssel ableiten[34]. Dabei wird aus dem privaten Schlüssel der öffentlichen abgeleitet welcher dann mit einer SHA-256 Funktion verschlüsselt wird um dann mit der RIPEMD-160 Funktion weiter verarbeitet zu werden. Das Ergebnis wird mit der Versions-Nummer und einer Prüfsumme versehen und dann als Base58-codierte Zeichenfolge dargestellt. Mit diesem Verfahren werden die Formate P2PKH (Pay-to-Public-Key-Hash) oder P2SH (Pay-ToScript-Hash) erzeugt. Diese Adressen beginnen immer mit 1 (P2PKH) beziehungsweise mit 3 (P2SH). Das modernere SegWit-Format[35] verwendet für die Adresse die Bech32-Kodierung und produziert Bitcoinadressen, die immer mit bc1 beginnen.

Aber genug von diesem technischen Kram. Wir merken uns, dass aus dem privaten Schlüssel alles abgeleitet, aber der Vorgang niemals umgekehrt werden kann. Mehr braucht der normal Sterbliche eigentlich nicht zu wissen.

Die Adressen kann man am ehesten mit Kontonummern vergleichen auf die Bitcoin gesendet werden können. Und das führt uns gleich zur nächsten Implikation. Diese Wallets kann man sich

34 Mnemonic Code Converter – Website, bei der man die Schlüssel- und Adressableitung sehr gut nachverfolgen kann. - https://iancoleman.io/bip39/

35 Segregated Witness ist eine technische Verbesserung des Bitcoin-Netzwerks, die 2017 eingeführt wurde.

einfach runterladen oder kaufen und damit erstellt man im Netzwerk selbst seinen Zugang. Man muss also nicht beim Bankberater sitzen und sich nackig machen, sondern man entscheidet für sich das man Bitcoin haben will und wird in diesem Augenblick auch zu seiner eigenen Bank. Niemand kann ausschließen, niemand kann zensieren, niemand weiß wer hinter der neu erzeugten Adresse steht und es gibt auch keinen Kredit. Banken hassen Bitcoin!

Jetzt ist es wichtig zu wissen wer diesen privaten Schlüssel besitzt. Bislang war immer nur die Rede davon, dass man dies selbst ist und man auch die Verantwortung für die sichere Aufbewahrung hat. Aber es gibt Wallet-Modelle, bei denen eine dritte Partei die privaten schlüssel besitzt, die sogenannten Custodian Wallets. Ein Custodian, aus dem Englischen der Hüter, ist also der Verwalter den Schlüssel. Nun darf man sich das nicht wie bei Harry Potter und Hagrid vorstellen, denn die normalen Hüter sind in der Regel Kryptobörsen und wenn wir uns an Mt. Gox[36] erinnern, bei denen durch einen Hackerangriff Milliardenwerte gestohlen wurden, oder Quadriga CX[37], bei der der Gründer überraschend verstarb, der als einziger Zugriff auf die zentral gelagerten Schlüssel hatte und über 200 Millionen an Kundengeldern verloren gingen. Ganz bekannt auch in der letzten Zeit die Kryptobörse FTX[38] mit Ihrem Chef Sam Bankmann-Fried, der gerichtlich bestätigt, Kundengelder veruntreut hat und so seinen Anlegern einen Schaden von rund 8 Milliarden US-Dollar bescherte. Solche Dinge gibt es sofort, sobald Geld in einer relevanten Größenordnung im Spiel ist und deshalb gibt es bei Bitcoineren, aber auch bei Altcoinern, den immer wieder zitierten Satz „Not your keys, not your coins!“, was übersetzt nichts anderes heißt, als Nicht Deine Schlüssel, also auch nicht Deine Bitcoin. Man muss diesem Hüter zu 100% vertrauen und das macht die Sache schwierig. Da sitzen keinen Hagrids!
Das nächste Problem ist natürlich auch, dass solche Institutionen wie Börsen eine große Menge an Kryprowährungen aller Art halten und damit auch ein lohnendes Ziel für Hacker und sonstige Kriminelle sind. Doch es gibt eine sehr einfache Möglichkeit das alles zu vermeiden.

Es gibt wie schon ein paar mal angedeutet die Möglichkeit eine sogenannte Hardware-Wallet oder auch Cold-Wallet zu kaufen. Das macht zwar für den Minianleger, der nur 200-300 Euro angelegt hat keinen Sinn, aber ab einer gewissen Menge wird dies fast schon zu einem Muss. Diese Wallets sind nichts anderes als ein USB-Stick und eine Software, die auf dem Computer oder dem Smartphone ausgeführt wird und, leicht nachzuvollziehen, wenn der USB-Stick nicht im Rechner steckt, kann ihn auch keiner knacken, zumal erst mal bekannt sein muss, dass man überhaupt so etwas besitzt und auch die Menge die zu stehlen wäre sich überhaupt lohnt. Das Cold meint in diesem Falle einfach, das die Hardware nicht mit dem Internet verbunden ist. Diese Wallets werden, wenn sie mit dem Computer oder Smartphone verbunden sind und es einen Zugang zum Internet gibt zu sogenannten Hot-Wallets, heiße Wallets, also zu diesem Zeitpunkt sind sie angreifbar und es gibt verschiedenen Verfahren wie die Hersteller sichergestellt haben, dass auch dann keine Daten gestohlen werden können.

Wer kein zusätzliches Geld ausgeben möchte, aber seine Schlüssel dennoch selbst verwalten will, der kann sich eine Software-Wallet installieren, die im Grunde das selbe tut wir die Hardware-Variante, nur, dass es sich eben um eine Software handelt, die sich auf einem Computer oder Smartphone befindet, welches ständig mit dem Internet verbunden ist. Das sind also von Haus aus Hot-Wallets. Dieses Sicherheitsrisiko muss man eingehen wollen, aber es ist auf jeden Fall eine gute Lösung gerade für Klein- und Kleinstsparer, die sich die Bitcoinwelt einmal anschauen wollen.

Jetzt gibt es noch einen wichtigen Aspekt, den wir im Zusammenhang mit den Schlüsseln und deren

36 Quelle - https://en.wikipedia.org/wiki/Mt._Gox
37 Quelle - https://en.wikipedia.org/wiki/Quadriga_Fintech_Solutions
38 Quelle - https://en.wikipedia.org/wiki/FTX

Aufbewahrung besprechen müssen. Einen privaten Schlüssel kann sich niemand merken. Jetzt kommt es aber vor, dass egal welches, jedes technische Gerät oder Software kaputt gehen kann, verloren wird oder sonst irgendwie nicht zugänglich ist. In dem Falle, weil man ja zum Beispiel bei einer Hardware-Wallet selbst für seine Zugangsdaten verantwortlich ist, sind die ganzen schönen Bitcoins weg, beziehungsweise man kommt nicht mehr dran. Hier kommen die Seeds ins Spiel. Seed bedeutet auf deutsch Samen und ist ein Begriff aus der Softwareentwicklung wenn es um Zufallsgeneratoren geht. Ein Seed ist also ein Produkt einer echten Zufälligkeit.Dabei handelt es sich um 12, 18 oder 24 Worte aus einer definierten Wortmenge, die in der richtigen Reihenfolge den privaten Schlüssel repräsentieren. Was bedeutet das? Ganz einfach. Selbst wenn die Wallet kaputt oder gestohlen oder sonst irgendwas ist, kann man mit diesen Worten seinen Wert wieder herstellen und im Falle eines Diebstahls zum Beispiel die Bitcoins auf einen andere, sichere Adresse übertragen, bevor der Dieb dies tut. Was man aber auch berücksichtigen muss ist, mit diesen Worten kann das jeder! Oder wenn bei einem Brand die Hardware-Wallet zerstört wurde, sollte der Zettel mit den Worten nicht daneben gelegen haben. Es gibt Anbieter, die Lösungen verkaufen, mit denen man seine Seeds, die geheimen Worte, auf Stahl stanzen kann. Das sieht toll aus, ist aber auch nicht gerade sehr preiswert. Es gibt auch die Möglichkeit die Liste der Worte in Bankschließfächer zu legen oder sie verteilt an Freunde oder Verwandte zu geben. Ein Aspekt, den man bei den Worten nicht außer Acht lassen darf, ist der Umstand, dass nur alle Worte in der richtigen Reihenfolge zum Erfolg führen. Gibt man seinen Eltern 12 der insgesamt 24 Worte und nochmal 12 dem Steuerberater, so können beide Parteien damit nichts anfangen, bis an dem Tag, an dem sie sich zusammenschließen.

Wie auch schon erwähnt ermöglicht dieses System es auch, sein Vermögen an jeder Kontrolle vorbeizuschmuggeln, was mit Bargeld, Giralgeld, Gold, Häusern, und so weiter absolut unmöglich ist. Man kann als nackter Mensch am Flughafen durch die Kontrolle gehen und kennt einfach seine 24 Worte auswendig. Ein geniales System!

Wenn die Wallet gesperrt, weg oder zerstört ist[39] heißt es übrigens ganz ruhig bleiben und alles was man tut mit Bedacht und konzentriert zu tun.

Kontrolle – Ihre Papiere bitte

Bitcoin ist ein sehr junges Ding und wie es mit so jungen Dingern nun mal so ist, sind die auch sehr wild. In den Anfangsjahren, als alle Kryptowährungen von den staatlichen Stellen entweder gar nicht wahr genommen wurden oder nur müde belächelt, konnte man wirklich alles machen. Es gab keinerlei Regulierung. Dann wurde nach und nach immer mehr Geld in Bitcoin investiert, man bedenke, dass wir heute von einem Investitionsvolumen nur alleine bei Bitcoin von weit über 1 Billion US-Dollar sprechen, und die ersten Ausfälle durch Börsen und Abzocker wurden publik. Es fing also an wie in jedem anderen Finanzsektor, dass sich Betrüger und andere Kriminelle einfanden um dem Gutgläubigen sein Geld aus der Tasche zu ziehen. Gleichzeitig nahmen die Staaten die wachsende Bedeutung von Bitcoin wahr und sahen darin eine absolut reale Gefahr für die eigenen Währungen. Einige schlaue Köpfe in der Administrationen, ja die gibt es wirklich, wenn auch nicht so oft, erkannten das Potenzial der Kryptowährungen und auch wie sie diese steuerlich ausschlachten konnten. Am Anfang stand das Thema Geldwäscheprävention im Fokus der staatlichen Eingriffe und die Europäische Bankenaufsichtsbehöre (EBA) und die Europäische Wertpapier- und Marktaufsicht veröffentlichten erste Warnungen und Empfehlungen zu Kryptowährungen. Ab 2018 stieg mit dem rapiden Wachstum des Kryptomarktes auch der Regulierungsdruck. Zu dieser Zeit wurde der Aktionsplan für Finanztechnologie entwickelt, der auch Kryprowährungen addressiert. Im Jahre 2020 präsentiert die Europäische Kommission den

39 Wallet wiederherstellen - https://relai.app/de/blog/bitcoin-wallet-wiederherstellen/

Legislativvorschlag für die Verordnung über Märkte für Krypto-Vermögenswerte (MiCA)[40]. Ziel ist es, einheitliche Regeln für Kryptowährungen in der EU zu schaffen. MiCA wurde bereits durch das Europäische Parlament und den Rat verabschiedet und tritt sukzessive in Kraft.

In den USA verlief die Entwicklung der Regulierung etwas fragmentierter. Dort sind die SEC, die CFTC[41] und das Finanzministerium für die Regulierung verantwortlich. Es gibt im Grunde noch keine einheitliche Gesetzgebung auf Bundesebene, sondern nur in den Bundesstaaten selbst, aber es wird angestrebt eine einheitliche Rechtsgrundlage in den kommenden Jahren zu schaffen. Bemerkenswert ist, dass die SEC Bitcoin entgegen allen anderen Kryptowährungen als Rohstoff betrachtet und die anderen Kryptoprojekte an Geldanlagen, wie auch Aktien oder dergleichen. Das Bedeutet natürlich auch, dass die US-Aufsichtsbehörden verstanden haben, welches Potential in Bitcoin liegt und, so wird gemunkelt, werden sie die ersten sein, die Bitcoin im großen Stil adaptieren um ihre exorbitante Verschuldung abzubauen.

Jetzt bietet Bitcoin, auch durch seine teilweise Anonymität und natürlich durch die Dezentralität, keinen wirklichen Angriffspunkt für die Staaten zur Regulierung. Wir haben ja bereits gesehen wie man sich selbst ohne jede dritte Instanz einen eigenen Zugang zum Netzwerk erstellen kann, also es keinen richtigen Hebel gibt, an dem der Staat ansetzen kann. Aus diesem Grund, und einfach weil sie es können, regulieren die Staaten die Schnittstellen zwischen der Fiatgeldwelt und den Kryptowährungen. Insbesondere die Börsen sind hier im Fokus, da über sie die größten Kundengelder in oder aus dem Universum der Kryptowährungen transferiert werden. Regulierte Anbieter müssen mittlerweile das sogenannte Know-Your-Customer-Prinzip (KYC) anwenden, in dem, analog zur Kontoeröffnung bei der Bank, vor Ort geprüft wird, wer eine Wallet bei der Börse eröffnen möchte. Normalerweise wird dies durch einen Videotelefonanruf gemacht und dabei müssen Ausweisdokumente vorgelegt werden. Wahre Bitcoin Enthusiasten lehnen diese Art der Reglementierung rundweg ab und versuchen auf die immer noch vorhanden Möglichkeiten auszuweichen Bitcoin anonym zu erwerben. So gibt es zum Beispiel Bitcoin-ATMs, also so etwas wie Bitcoin Bankomaten, an denen man Bargeld gegen Bitcoin tauschen kann. Auch einige Mining-Pools, also Menschen, die direkt an der Quelle sitzen, verkaufen Bitcoin direkt an Anleger. Wie man allerdings an die Kontakte kommt ist dem Autor nicht bekannt. Eine weitere Möglichkeit die Nachverfolgbarkeit zu verschleiern, oder besser die Anonymität wieder besser herzustellen, ist, nachdem man ganz offiziell Bitcoins auf einer Börse gekauft hat diese durch einen sogenannte Bitcoin-Mixer zu schicken. Ein Bitcoin-Mixer, auch als Tumbler bezeichnet, ist ein Service, der sich in der Grauzone der Legalität befindet, welcher dazu dient, die Rückverfolgbarkeit von Bitcoin-Transaktionen zu erschweren. Auch beliebt sind CoinJoin Services, also Dienste, die die Bitcoins mit denen von anderen Nutzern verschmelzen und so die Zahlungsstöme verschleiern. Dabei muss man immer im Blick behalten, dass Legalität für Bitcoin im klassischen Sinne kein ernstzunehmender Begriff ist. Sobald ein Server, oder eben so ein Mixer, in einem Land steht, in dem es keine entsprechende Regulierung gibt, kann es folglich auch keine legalen Probleme geben. Bitcoin ist zu 100% kosmopolitisch und kann nicht von einem Land, einem Länderbund oder sonst einem Konstrukt eingefangen werden. Das ist schlicht unmöglich. Aber das ist nur eines der möglichen Konzepte um es den Staaten sehr viel schwerer zu machen das Eigentum eines Bürgers mit seinem Namen zu verknüpfen. Es sind, wie bereits erwähnt, die Ein- und Ausgänge, der Übergang von Fiatgeld zu Bitcoin und von Bitcoin in Fiatgeld, die wirklich kontrolliert werden können. Und ohne jetzt Anregungen geben zu wollen, aber wer sagt, dass das Grundstück, das ich kaufen will, nicht wirklich für 1000 Euro angeboten wird? Oder das schöne Auto wirklich nur 500 US-Dollar kostet. Kann doch sein, oder nicht?

40 MiCA - https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2305_Mica.html

41 CFTC - Die CFTC (Commodity Futures Trading Commission) ist eine unabhängige Bundesbehörde in den Vereinigten Staaten, die für die Regulierung und Überwachung des Terminhandelsmarktes für Rohstoffe und Finanzinstrumente zuständig ist.

Was auch noch in diesen Themenkomplex gehört ist der feuchte Traum eines jeden Zentralbankers – CBDC. Central Bank Digital Currencies, zu deutsch, Digitales Zentralbankgeld. Die Idee hinter der digitalen Zentralbankwährung ist die absolute Kontrolle des Staates über seine Bürger auch wenn dies immer sehr anders formuliert wird und kritische Geister werfen Bitcoin und den anderen Kryptowährungsprojekten vor, sie würden den gesellschaftlichen Konsens und die Akzeptanz in der Bevölkerung dafür schaffen. Es ist richtig, dass durch die Überlegungen von Satoshi Nakamoto und der frühen Bitcoin-Entwicklern überhaupt erst die Grundlagen die die digitalen Zentralbankwährungen gelegt wurden, selbst hätten die Zentralbänker und deren Handlanger das niemals geschafft, doch ist die Absicht, der Geist und die Ethik, die hinter diesen Entwicklern stand und steht absolut diametral den Kontrollphantasien der Zentralbanken entgegengesetzt. Gegensätzlicher könnte es nicht sein. Noch gibt es nur sehr wenige digitalen Zentralbankwährungen doch nahezu alle Zentralbanken sind in der Entwicklung und wollen in den nächsten Jahren dieses Konzept etablieren. Die Frage muss aber gestellt werden. Was ist so schrecklich an dieser Geldform, was läuft da anders? Um diese Frage zu beantworten müssen wir uns nochmal ins Gedächtnis rufen, dass es diese Smart Contracts gibt, also diese programmierbaren Verträge, die auf dem Wenn-Dann-Prinzip aufbauen. Mit diesen programmierbaren Verträgen kann eine Zentralbankwährung ausgestattet werden und das bedeutet dann nichts anderes mehr, als dass die Geldregulierer, als in letzter Konsequenz die Regierungen, direkt auf die Bürger durch das Geld einwirken können. Darüber, dass unsere Daten bei jedem Einkauf mit EC-Karte, Handy oder Kreditkarte von allen möglichen Unternehmen gespeichert werden und der Discounter um die Ecke genau weiß wie unser Leben aussieht, daran haben wir uns gewöhnt und nehmen es einfach nur hin. Der Versandhändler Amazon rühmt sich sogar vorher zu wissen ob eine Frau schwanger ist, alleine nur an ihrem Kaufverhalten. Alle die da sensitiv sind bezahlen mit Bargeld und verzichten auf diese lächerlichen Paybackpunkte. Aber CBDCs gehen noch viel weiter. Zum einen machen sie die normalen Geschäftsbanken überflüssig, da die Konten direkt bei der Zentralbank geführt werden, und der Staat, die Regierung, die Behörden sofort alles wissenswerte über jeden Bürger zur Verfügung haben. Und wir vergegenwärtigen uns, dass es nicht nur wohlmeinende Regierungen gibt - eigentlich gibt es gar keine wohlmeinende Regierung, aber das kann ja noch kommen. Zum anderen kann dieses Geld programmiert werden, bedeutet, es können Smart Contracs einprogrammiert werden, die bewirken wenn zu Beispiel ein Diabetiskranker sich einen Schokoriegel kaufen will, dies einfach mit dem zur Verfügung stehenden Geld nicht bezahlt werde kann, oder wenn das CO_2-Kontingent aufgebraucht ist, man nicht mehr in den Urlaub fahren darf, oder das Geld außerhalb eines gesteckten örtlichen Rahmens keine Gültigkeit mehr hat oder es ganz einfach am Ende des Monats gelöscht wird. So etwas ist alles denkbar und wurde bereits gedacht. Die Liste der automatisierbaren Verbote, Gebote und Gängeleien, die der Staat im Handumdrehen hätte ist unendlich lang und einmal diese Tür aufgestoßen, gleitet jeder Staat in ein totalitäres System ab. Die Zeit der grassierenden Seuche hat uns gezeigt, wie dünn der Firn der Demokratien ist und wie schnell Kritiker ausgegrenzt wurden bis hin zur Vernichtung der wirtschaftlichen Existenz, oder wie im Fall von Michael Ballweg[42], unliebsame Geister Monate lang in Stammheim einsaßen. Die Zeit von Menschenrechten und Freiheiten ist vorbei, das sollte jeder mittlerweile verstanden haben und ja es geht noch schlimmer. Auch das stimmt, beruhigt aber nicht so richtig.

Abschließend können wir sagen, dass der Staat in all seinen Facetten immer übergriffiger wird und auch (erfolglos) versucht Bitcoin zu regulieren. Noch sind die Methoden relativ plump aber die Geschichte zeigt, dass diese Techniken immer weiter verfeinert werden.

Was wir aber auch nicht außer Acht lassen dürfen, ist der Umstand, dass durch eine gewisse Regulierung auch das Vertrauen der normalen Menschen und Unternehmen in Bitcoin wächst und damit auch ein Zustrom an Einlagegeldern generiert wird. So wären zum Beispiel die Bitcoin-

42 Michael Ballweg in Untersuchungshaft - https://www.nzz.ch/international/michael-ballweg-sass-er-zu-lange-in-untersuchungshaft-ld.1733221

ETFs, die von fast allen großen Vermögensverwaltern heute angeboten werden, ohne die entsprechende Regulierung gar nicht möglich gewesen. Diese Medaille hat eben auch zwei Seiten.

21 - Der Tanz um die heilige Kuh.

In der Welt von Bitcoin dreht sich sehr viel um die Zahl 21 und man fragt sich, warum dem so ist. In den meisten Fällen ist das erste, was Menschen spezifisch von Bitcoin mitbekommen, dass dieser auf 21.000.000 Stück limitiert ist. Das ist mal eine Ansage im Vergleich zu den allermeisten anderen Kryptowährungsprojekten und vor allem im Vergleich zu den normalen, den Fiatwährungen wie Dollar, Euro, Yen oder Rupie. Bitcoin hat also ein Limit und kann nicht inflationiert werden. Das stimmt aber so nicht wirklich, denn es gibt nicht nur Bitcoin als Einheit, sondern so wie es beim Euro oder Dollar die Cent gibt, gibt es bei Bitcoin Satoshi. Hundert Millionen (100.000.000) Satoshi bilden einen Bitcoin, bedeutet also, dass es 2 Trilliarden, 100 Milliarden (2.100.000.000.000.000) Währungseinheiten gibt. Damit ist auch gleich die Frage beantwortet, was passiert, wenn mal mehr als 21 Millionen Menschen Bitcoin benutzen wollen. Doch bei dieser Zahl und das ist eben dann doch der Clou an Bitcoin ist die Schöpfung von frischem Geld beendet. Dies wird zirka im Jahr 2140 passieren nach der letzten Halbierung der Schürfgewinne, da dann die Belohnung für das Finden eines neuen Blocks kleiner als 1 Satoshi wäre.

Die Formel beschreibt das Prinzip des sogenannten Halvings, also der kontinuierlichen Halbierung der Ausschüttung für einen neu gefundenen Block. Was steht da?

$$\sum_{i=0}^{32} 210{,}000\,\frac{50}{2^i}$$

Abbildung 20: Summenformel zur Berechnung der Gesamtmenge

Die Formel besagt, dass die Summe aller möglichen Bitcoin einem Algorithmus unterliegt, der in 32 Zyklen, alle 210.000 gefundenen Blocks die Belohnung, beginnend mit 50 Stück, mit jeder Iteration durch 2 dividiert. Für normale Menschen gesprochen: Am Anfang gab es 50 Bitcoins pro gefundenem Block, oder 50% aller Bitcoin, nach 210.000 geschürften Blocks oder zirka 4 Jahren später waren es 25 Stück pro Block, dann 12,5 Stück, dann 6,25 Stück und aktuell nach dem 4. Halving, sind es nur noch 3,125 Stück pro Block. Und wenn wir jetzt die Liste bis in die 32 Iteration durchspielen, dann erhalten wir die maximale Menge von 20.999.999,9769 Bitcoin.

Wenn wir schon beim Rechnen sind, hier ist eine vereinfachte Formel, wie man die Gesamtmenge an Bitcoin auch errechnen kann.

[Ausschüttung pro Block] x [Blocks bis zum Halving] x 2

50 BTC x 210.000 x 2 = 21.000.000 BTC

Satoshi Nakamoto hat sich niemals dazu erklärt, warum es eben 210.000 Blocks pro Halbierung sind, oder warum er nicht mit 100 Stück pro Block angefangen, sprich die 42[43] - die Antwort auf das Leben, das Universum und alles anderen - gewählt hat. Vielleicht ist/war 21 seine/ihre Glückszahl, oder der Preis für eine Büchse Bier. Vielleicht mochte er auch Douglas Adams nicht. Man weiß es einfach nicht. Es bleibt festzuhalten, dass die Halbierung alle 210.000 Blöcke statt findet und durch die maximale Iteration von 32 dadurch 21.000.000 Stück erstellt werden können. Im Grunde ist es auch unwichtig, auf wie viele Stück die Gesamtmenge festgelegt wurde, wichtig ist, dass es diese Festlegung gibt und dass keine zentrale Partei in irgendeiner Form die Möglichkeit hat diese Maximalmenge zu verändern.

43 Quelle - https://de.wikipedia.org/wiki/42_(Antwort)

Auf jeden Fall ist die Bitcoingemeinde sehr fokussiert auf diese Zahl und jede Menge Firmen und Webseiten tragen die 21 im Namen. Um die Zahl wird ein regelrechter Kult gemacht und im Grunde genommen weiß niemand warum.

Aber bei der Betrachtung drängt sich noch ein Gedanke auf, nämlich was passiert, wenn Bitcoin wirklich das universale Zahlungsmittel der gesamten Welt wird, oder noch schräger gedacht, wenn der Mensch in den Weltraum geht und es mehrere Welten gibt? Die Antwort ist ganz einfach: Wenn die Mehrheit aller Bitcoinnutzer es für sinnvoll erachtet, dann kann das Protokoll und damit die Maximalmenge zum Beispiel verdoppelt werden. Aber das entscheiden dann die Nutzer und nicht die Vorstände von Zentralbanken und genau dieser Gedanke ist eine der zentralen Säulen von Bitcoin – wenn es sinnvoll für alle ist, kann sich das Netzwerk anpassen, wenn es nur dem Vorteil einer einflussreichen Clique dient wird sich das Netzwerk verweigern.

Was ist Geld?

Um Bitcoin als Geld wirklich verstehen z können, müssen wir uns einmal bewusst machen, was Geld eigentlich ist. Geld ist, wenn man es ganz abstrakt ausdrücken möchte, ein Konsens aus Fähigkeiten und Eigenschaften. Je besser dieses Geld die einzelnen Fähigkeiten und Funktionen abbildet, desto größer ist der Konsens, die Akzeptanz, in der Bevölkerung. Wie wollen uns einmal die drei wichtigsten Werte, nämlich Bitcoin natürlich, Gold und Fiatgeld in einer Tabelle anschauen um gegenüberzustellen, welches „Geld“ welche Funktionen erfüllt.

Die Geldfunktionen sind das jedem geläufige Tauschmittel, sprich Geld fungiert als Ersatz für Waren und Dienstleistungen und kann von einem zum anderen gegeben werden. Dann haben wir das Wertaufbewahrungsmittel, bedeutet wenn noch kein Tausch stattfinden soll speichert Geld den Wert bis zum Einsatz im Tausch. Als nächstes muss ein Geld eine genormte Recheneinheit sein, also die nominalen Preise für alle Waren und Dienstleistungen müssen in dem Geld ausgedrückt werden können. Eine sehr wichtige Funktion ist die Teilbarkeit, oder auch Divisibilität, soll heißen, dass das Geld in kleinere Einheiten zerlegt werden kann um Transaktionen in beliebiger Höhe zu ermöglichen. Die Portabilität ist die nächste Eigenschaft, die beschreibt, wie gut der gespeicherte Wert von Ort A nach Ort B gebracht oder transferiert werden kann. Ganz elementar ist die Homogenität, auch Fungibilität genannt, die beschreibt, dass jede Einheit gegen einen nominal gleichwertige ausgetauscht werden. Das bedeutet, dass ein Euro immer ein Euro ist, und es vollkommen egal ist welche Münze man in der Hand hat, solange die nominale Summe identisch ist. Die Dauerhaftigkeit eines Geldes beschreibt wie schnell der Stoff vergeht und zu guter Letzt die Knappheit, eine der wichtigsten Eigenschaften, beschreibt wie viel oder wenig Geld vorhanden ist.

Geldfunktion	Bitcoin	Gold	Fiatgeld
Tauschmittel	+	-	+
Wertaufbewahrungsmittel	++	++	-
Recheneinheit	o	-	+
Teilbarkeit / Divisibilität	+	+	+
Portabilität	+	-	+
Homogenität / Fungibilität	+	+	+
Dauerhaftigkeit	+	++	+
Knapphaltung	++	+	--

Tabelle 2: Gegenüberstellung der verschiedenen Geldformen nach Ihren Funktionen und Eigenschaften

Der erste Blick zeigt uns schon, dass Bitcoin fast alle Eigenschaften und Funktionen eines guten Geldes erfüllt. Die beiden beliebtesten Alternativen dies aber nur bedingt tun. Gehen wir die einzelnen Punkte durch:

Die normalen Fiatwährungen sind selbstverständlich als Tauschmittel geeignet, dies sehen wir bei jedem Einkauf im Supermarkt, aber Gold scheitert an dieser Hürde. Theoretisch ist es natürlich möglich Goldmünzen oder gar Barren zu verwenden, aber die Tauschpartner werden darüber nicht besonders glücklich sein. Gold ist in größeren Mengen schlecht transportabel und benötigt ein hohes Maß an Sicherheitsmaßnahmen. Ähnliches gilt auch für Bargeld, wir denken an Geldtransporter, hingegen Giralgeld vollkommen sicher angenommen werden kann.

Wenn wir Geld als Wertaufbewahrungsmittel sehen, so überzeugen Bitcoin und Gold ganz massiv. Gold kann auf eine 5.000jährige Geschichte der Werthaltigkeit verweisen und auch Bitcoin, obwohl sehr viel jünger, hat in der Zeit seiner Existenz nichts an Wert verloren, ganz im Gegenteil. Das Fiatgeld eignet sich so gut wie gar nicht zur Werterhaltung, wird es doch durch die gewollte Inflation immer weniger wert.

Geld als Recheneinheit ist im Grunde dem US-Dollar überlassen, da der globale Standard so ist, dass alle Waren und Dienstleistungen auf globaler Ebene in der Leitwährung ausgedrückt werden und im zweiten Schritt die Anpassung in der jeweiligen Landeswährung erfolgt. Es wäre theoretisch möglich dies in Gold oder Bitcoin zu tun, doch das ist im Endeffekt nichts anderes als die Ableitung von der Leitwährung in eine Regionalwährung. Der Konsens liegt aktuell immer noch beim Fiatgeld, sprich dem US-Dollar. Aber durch den Umstand, dass Bitcoin keiner Nation oder irgendwelcher Institution gehört ist es ein folgerichtiger Gedanke zu sagen, alle Werte sollten in Bitcoin ausgedrückt werden und danach in die Regionalwährung übertragen werden. Es ist nach meiner Meinung sehr wahrscheinlich, dass dies in Zukunft passiert, sobald die Volatilität, also die Kursschwankungen, bei Bitcoin auf ein vernünftiges Maß sinkt. Dazu muss der Bitcoin aber eine höhere Umlaufgeschwindigkeit bekommen. Auf jeden Fall hat Bitcoin dieses Potenzial, auch wenn es derzeit noch nicht angewendet wird. Für Gold kann man sagen, dass dies eigentlich nur möglich wäre, wenn eine neue Leitwährung, die einem Goldstandard folgt, wieder installiert würde. Doch dann wäre nicht das Gold die Recheneinheit, sondern die goldgedeckte Währung.

Die Divisibilität ist bei allen gegeben, am schlechtesten ausgeprägt natürlich beim Gold. Aber auch

da kann man jede Menge abbilden. Ein Beispiel dafür aus dem Bereich Silber ist das sogenannte Hacksilber. Das waren Münzfragmente, die mit der Axt aus der originalen Münze herausgeschlagen wurden um kleine Beträge zu bezahlen. Bei Gold wurde so etwas auch gemacht, aber lange nicht so häufig, da in den früheren goldgedeckten Währungen für Kleinbeträge ein Silbermünzensatz zur Verfügung stand.

Die Portabilität ist bei Gold, wie schon erwähnt, eingeschränkt, da wir es mit großen Gewichten und einem erheblichen Sicherheitsaufwand zu tun haben. Bargeld unterliegt den selben Einschränkungen, ist aber leider nicht mehr der größte Geldanteil im Fiatsystem. Dies ist eindeutig das Giralgeld, also Geld, welches von einem Konto zum anderen per Buchungssatz transportiert wird. Wie bei Bitcoin findet keine physische Bewegung statt und ist damit sehr leicht portabel.

Alle drei Geldarten sind zu 100% fungibel. Es gibt zwar einen Unterschied, ob man einen Klumpen Gold besitzt oder einen schönen Krügerrand, aber da Gold in seiner Geldfunktion per Gewicht verwendet wird, ist eine Prägung nicht relevant. Das einzige was sich durch zum Beispiel eine Münzprägung oder den Prägestempel einer anerkannten Goldscheideanstallt leichter evaluieren lässt, ist der Reinheitsgehalt, aber auch den muss man in Zweifel bei jedem Stück einzeln bestimmen. Schlussendlich ist es dennoch so, dass jede Unze Gold des selben Reinheitsgrades gleichwertig ist und beliebig ausgetauscht werden kann. Und für Bargeld gilt nämliches. Ein 10 Dollarschein ist ein 10 Dollarschein, gleichgültig in welchem Jahr er gedruckt wurde oder welche Sicherheitsmerkmale aufgebracht sind. Für Giralgeld und Bitcoin, die es in physischer Form gar nicht gibt, ist klar, dass jede Einheit gleichwertig sein muss.

Auch die Dauerhaftigkeit ist bei allen angeschauten Geldformen gegeben, ganz besonders aber natürlich bei Gold, welches durch seine chemischen Eigenschaften über Jahrtausende keinerlei Schwund hat. Dagegen sind Bitcoin und Giralgeld auf Strom angewiesen, aber auch den wird es sehr wahrscheinlich noch lange geben.

Zuletzt betrachten wir noch die Knappheit der einzelnen Geldformen. Wie bereits erklärt wird das Fiatgeld aus dem Nichts geschaffen und ist nur durch den Gemütszustand von Bankern limitiert. Es gibt zwar Regeln, die beachtet werden müssen, doch werden diese bei jeder ersten Möglichkeit ignoriert. Bei Fiatgeld kann man in gar keiner Form von Knappheit sprechen, selbst wenn es gerade keine Hyperinflation gibt. Gold ist ein knappes Gut, aber leider weiß niemand wie viel Gold es wirklich gibt, denn der Bestand wird ja von Vertrauensparteien bezeugt und wir wissen, dass der tatsächliche physische Goldbestand nur ein 120igstel des weltweit gehandelten Goldes ist. Nichts desto trotz ist Gold knapp und neues physisches Gold kommt nur durch sehr viel Energieaufwand in den Markt. Bei Bitcoin ist es selbstredend so, dass es das einzige wirklich limitierte und dadurch knappe Gut auf der Welt ist, wenn wir von Kunstwerken und dergleichen absehen. Diese Eigenschaft ist sehr oft die erste Information die Menschen von Bitcoin hören, dass es nur 21 Millionen davon gibt.

Neben den allgemeingültigen Eigenschaften eines Geldes gibt es auch noch weitere wichtige, die wir auch noch kurz betrachten wollen. Zum einen ist da der Zentralisierungsgrad und zum anderen die gesellschaftliche Akzeptanz. Bitcoin ist vollkommen dezentral und Gold im weitesten Sinne auch, da die Goldminen in verschiedenen Händen liegen und der Handel auch abseits der Börse getätigt werden kann. Fiatgeld ist komplett zentralisiert und wird von sehr wenigen Menschen kontrolliert. Der Einwand, dass es sehr viele Zentralbanken gibt, die alle ihre eigene Geldpolitik betreiben ist nur bedingt zulässig, da sich alle Zentralbanken an der Weltleitwährung Dollar ausrichten.

Die gesellschaftliche Akzeptanz ist im Grunde keine Eigenschaft oder Funktion von Geld, sondern eine Folge aus allen Eigenschaften und Funktionen. Sie ist sehr stark abhängig vom gesellschaftlichen und politischen Klima in einem Land. Gold und Bitcoin werden von den Menschen immer frei gewählt, meistens in der Funktion als Wertaufbewahrungsmittel, doch wie

sieht es mit Fiatgeld aus?

In den sogenannten westlichen Ländern wird das Geld von der Bevölkerung klaglos akzeptiert und das ist, obwohl diese Geldform nichts anderes ist als täglicher Raub, durch die Indoktrination zu erklären. Die Europäer,die Nordamerikaner, die Australier und Neuseeländer werden in dem Geist erzogen, dass ihre Gesellschaftsform besonders erstrebenswert sei und alle ihrem Beispiel folgen müssen. Das ist die klassische Hybris der eigenen Überlegenheit. Seit der Kolonialzeit wurden derartig viele Werte in diese Länder verschleppt, dass sich unermessliche Reichtümer dort in den Händen Weniger angehäuft haben. Aufbauend auf diesem Reichtum wird nach außen gesendet, die ganzen Gesellschaften seien besonders reich und allen ginge es überdurchschnittlich gut. Dem ist aber ganz und gar nicht so. Ja im Westen gibt es die offene Armut, wie wir sie aus den Ländern der abfällig Dritten Welt genannten Regionen der Erde kennen, so nicht, aber der durch Raub und Unterdrückung erreichte materielle Wohlstand lässt ganze Völker von leeren, Konsum gesteuerten Menschen im ewigen Hamsterrad zurück und die, die da nicht mitmachen wollen, die sind genauso arm und mittellos wie in Asien, Afrika oder Südamerika. Es wird nur etwas besser verdeckt. Die Staaten der westlichen Welt betreiben eine unvorstellbare Propagandamaschine um die eigenen Systeme als die besten, schönsten und erstrebenswertesten darzustellen und immer mit ihnen auch ihre Währungen. Die Indoktrination beginnt bereits im Kindergarten, geht über Schule und gegebenenfalls Universität direkt ins Berufsleben. Alles ist immer das Beste, das Erstrebenswerteste und Schönste, was es je in der Menschheitsgeschichte gab. Und wenn der Mensch dann im Rentenalter angekommen ist, merkt dieser auf einmal, dass das Versprechen von der schönen bunten Welt gravierende Mängel aufweist, doch bis dahin haben die Mächtigen bereits Unmengen an Lebenszeit aus dem Individuum geraubt. Aber lassen wir das.

Die Staaten haben ihre Währungen als verbindlich erklärt und zwingen ihre Bevölkerung so diese zu verwenden, entweder durch Indoktrination in Schulen und Medien – Soft Power, oder durch rohe Gewalt durch Polizei und Militär – Hard Power. Die Benutzung einer Zweitwährung oder der direkte Tausch ist, bis in ein paar wenigen Ausnahmefällen, schlicht nicht möglich, beziehungsweise wird sogar bestraft. Ein Beispiel: A möchte ein Haus bauen. Wenn ihm B und C dabei helfen geraten sie in den Verdacht der Schwarzarbeit und müssen sich vor den Zoll fürchten. Gerade in südlichen Kulturen ist es hingegen vollkommen normal, dass die ganze Familie mithilft ein Haus zu bauen und wenn das fertig ist kommt der nächste Verwandte dran. Und so weiter, und so weiter. In Deutschland geht so etwas nur sehr bedingt, was mit ein Punkt ist, warum manche Deutsche missgünstig auf ihre türkischen, bulgarischen oder rumänischen Nachbarn schauen. Der Deutsche wurde dazu erzogen, dass alles von irgendeiner Fachfirma gemacht werden muss und die will eben Geld. Auch gibt es eine Flut an Vorschriften, die einzuhalten sind und jedes mal durch irgendwen bezeugt werden muss, dass diese oder jene Vorschrift auch eingehalten wurde und damit diese geforderte Unterschrift geleistet werden kann, muss eben Geld fließen, da damit auch eine Haftung einhergeht. Das Prinzip ist recht einfach, aber wirklich effektiv. Durch ein Dschungel von Vorschriften und einzuholender Genehmigungen, die natürlich nur erteilt werden können, wenn noch mehr Vorschriften eingehalten wurden, werden unzählige Parteien in jeden Prozess integriert und der Staat, in Form des Finanzamtes, hält bei jeder „Wertschöpfung“ die Hand auf. Die Raubritter des Mittelalters hätten das nicht besser gestalten können.

Doch es geht noch brachialer. Aus Österreich gibt es drastisches Beispiel aus den Jahren 1931 bis 1933 wie in der Gemeinde Wörgel im Inntal, die wie viele andere Ortschaften von der Weltwirtschaftskrise stark in Mitleidenschaft gezogen wurde, ein Regionalgeldexperiment[44] auf Basis von Schwundgeld, durch die Wiener Zentralverwaltung verboten und unter Androhung von Waffengewalt beendet wurde. Das im Volksmund „Wunder von Wörgel“ genannte Experiment, ins Leben gerufen vom damaligen Bürgermeister Michael Unterguggenberger, führte neben dem Schilling ein regional begrenztes, auf dem Freigeld von Silvio Gesell aufbauendes, Schwundgeld

44 Quelle - https://de.wikipedia.org/wiki/Wörgler_Schwundgeld

ein. Das bedeutet, dass das Geld mit der Zeit immer mehr an Wert verliert und es einen hohen Anreiz gab, dieses Geld schnell auszugeben.

Ab Juli 1932 gab die Gemeindeverwaltung als Lohn für kommunale Arbeiten, die von Arbeitslosen verrichtet wurden, sogenannte Arbeitswertscheine aus. Diese gab es in verschiedenen Nennwerten von 1, 5 und 10 Schilling. Monatlich musste zu einem festen Prozentsatz von 1% eine Marke gekauft und aufgeklebt werden, damit der Nennwert erhalten blieb; also klassisches Schwundgeld. Dieses Geld galt in der gesamten Gemeinde und konnte auch zur Zahlung von Abgaben verwendet werden, was eine extrem hohe Akzeptanz zur Folge hatte. Durch dieses Prinzip wurde die Umlaufgeschwindigkeit des Geldes derart erhöht, dass die Gemeinde Wörgel eine sehr beachtliche Entwicklung nahm. Der Erfolg und das damit verbundene Prinzip wurde sehr schnell in anderen Gemeinden bekannt und einige adaptierten den Ansatz. Es reichte selbst bis zum französischen Finanzminister Édouard Daladier, der persönlich nach Wörgel reiste um sich über das Projekt vor Ort zu informieren. Mit zunehmender Aufmerksamkeit wurden die Repressalien durch die österreichische Zentralbank immer stärker bis diese im November 1933 die gerichtliche Beendigung des Experiments erwirkte, was die vorher aufstrebende Gemeinde wieder in die Krise stürze.

Heute existieren mehrere Regionalwährungen, welche von den Zentralbanken geduldet werden, da sie in der Regel sich eben auf eine Region beziehen, freiwillig sind und, ganz wichtig, einen festen Wechselkurs zum Euro von 1 zu 1 haben. Die heutigen Regionalwährung haben alle das selbe Problem. Der einzige wirkliche Mehrwert stellt sich in Form der Wertschöpfung und des Werterhaltes in und für die Region dar. Dies ist im Zeitalter von Onlinehandel und Schnäppchenjagd aber nur bedingt für die breite Masse von Interesse. Aber der Aufwand eines parallel geführten Geldes ist aber recht hoch. Damit ist die Idee von einem aktiven Geld für die Menschen, so wie es das Freigeld ursprünglich beschreibt, zu einem gerade einmal bedingt die Region förderndes Zahlungsmittel degradiert worden.

Wir halten fest, dass der Staat auf dem Monopol der Geldschöpfung besteht und sich diese für ihn so bequeme Möglichkeit sich zu finanzieren nicht ohne weiteres aus der Hand gibt.

Warum Bitcoin kein Geld ist und was das mit Blitzen zu tun hat

Jetzt wollen wir uns aber wieder freundlicheren Themen zuwenden und anschauen, warum Bitcoin heute noch kein Geld ist und der Weg zu einem praktikablen Lösung noch sehr lang sein wird. Die Antwort darauf ist im Grunde sehr einfach. Bitcoin ist zu langsam. Wenn wir uns nochmals vergegenwärtigen, dass die Blockchain immer nur zirka alle 10 Minuten um einen Block erweitert werden kann und die Datenmenge im Block sehr begrenzt ist, dann ist auch vollkommen klar, dass Bitcoin bereits im Betrieb eines größeren Einkaufszentrum scheitern würde. Zu viele Transaktionen in zu kurzer Zeit. Die Hauptkette ist nicht wirklich skalierbar. Dafür ist das System nicht gemacht. Wenn wir uns das bildlich vorstellen wollen dann wäre es so, als wenn alle 10 Minuten ein Geldtransporter zu diesem Einkaufszentrum kommt und sich, sagen wir 2 Minuten Zeit nimmt um Gelder in Empfang zu nehmen und auszugeben und nach Ablauf der Zeit einfach wieder wegfährt. Die Schlangen an den Kassen wären unendlich lange, und niemand wollte in diesem Zentrum einkaufen.

Um dieses Problem zu lösen und Bitcoin wirklich zu einem aktiven Tauschmittel zu machen gibt es zwei populäre Ansätze. Der eine war im Jahr 2017 als sich durch eine Abspaltung, man nennt so etwas Hard Fork, Bitcoin Cash bildete. Bei dieser neuen Blockchain wurde die Datenmenge pro Block auf 8 Megabyte erhöht um mehr Transaktionen pro Blockzyklus speichern zu können und 2018 wurde diese Grenze nochmals auf 32 Megabyte erweitert. Bitcoin Cash hat nie die Akzeptanz der Schürfer und der Nutzer gefunden, da durch diese Änderung eines der grundlegenden Prinzipien

von Bitcoin, nämlich die Transparenz durch kleine Datenmengen, welche jeder im Netzwerk mit geringem Aufwand selbst herstellen kann, massiv beeinträchtigt wurde. Die meisten anderen Regeln gelten für diese Blockchain weiterhin, doch erzwingt ein so fundamentaler Eingriff und damit der Akzeptanzverlust bei den Bitcoin Cash Schürfern immer weitere Änderungen. Heute ist diese Blockchain zwar noch in Betrieb, aber völlig marginalisiert. Die Marktkapitalisierung liegt im Vergleich zu Bitcoin bei weniger als 8 Promille.

Ein vielversprechender Ansatz, der auch von der überwältigenden Mehrheit der Nutzer von Bitcoin getragen wird ist das sogenannte Lightning Netzwerk[45]. Lightning heiß aus dem Englischen übersetzt nicht anderes als Blitz und genau so funktioniert das auch – Blitz schnell. Während im Hauptnetzwerk maximal 7 Transaktionen pro Sekunde möglich sind, kann durch Lightning eine fast unendliche Geschwindigkeit erreicht werden. Das ermöglicht schnelles und einfaches Bezahlen und da keine Transaktionsgebühren anfallen ist es auch perfekt für Kleinstbeträge geeignet.

Bei Lightning[46] wird zwischen zwei Teilnehmern ein Kanal über eine Transaktion auf der Hauptkette vereinbart, über den dann bis zu 500 Transaktionen pro Sekunde getätigt werden können. Bei der Eröffnung wird ein gewisser Betrag von beiden Seiten hinterlegt und was folgt ist im Grunde nichts anderes als ein Kontokorrent im herkömmlichen Buchungswesen. Keine der Transaktionen wird, solange der Kanal besteht, auf der Hauptkette von Bitcoin eingetragen, was natürlich auch bedeutet, dass keinerlei Gebühren anfallen und die Aktion extrem schnell stattfinden kann. Erst wenn der Kanal geschlossen wird, wird das Ergebnis aller Buchungen in der Hauptkette von Bitcoin wieder geschrieben und endgültig finalisiert. Dies ermöglicht Finanzdienstleistern enorme Möglichkeiten. Lightning rein zwischen Privatanwender zu nutzen ist gut möglich, aber einfach zu kompliziert und wenn nicht professionell gehandhabt nicht wirklich praktikabel.

Ich möchte ein Beispiel machen, damit man sich das vorstellen kann. Nehmen wir an wir haben einen Dienstleister wie PayPal, Visa, Mastercard, was auch immer. Damit wir mit dem Service Geschäfte machen können, eröffnen wir einen solchen Lightning-Kanal und zahlen eine Summe ein. So lange jetzt Guthaben auf unserer Seite ist, können wir nach Herzenslust einkaufen und der Dienstleister protokolliert alles schön mit. Wichtig dabei ist, dass wir nur bei denen Händlern einkaufen können, die ebenfalls den Service nutzen. Nach sagen wir einem Monat wird dann Kassensturz gemacht und der Kanal abgerechnet oder besser geschlossen. Der Dienstleister verteilt alle Beträge, die wir ausgegeben haben auf die bestehenden Kanäle unserer Geschäftspartner mit diesem Diensleister und das Ergebnis wird in die Blockchain geschrieben. Für einen zentralisierten Dienstleister ist dies ein gutes Geschäftsmodel, aber für Privatpersonen ist dieses System nur sehr bedingt sinnvoll, zumal für jeden Eintrag in der Hauptkette Gebühren fällig werden.

Jetzt kam das Wort zentralisierter Dienstleister vor und da, so geht es mir übrigens auch, bekommt ein Bitcoiner Pickel. Wir müssen uns fragen, welche Macht so ein Dienstleister aus seiner Stellung ableiten kann und ja, die ist nicht unbeträchtlich und das noch größere Problem ist, dass so ein Dienstleister Zensur betreiben könnte, also auch ein ganz fundamentales Element von Bitcoin außer Kraft setzen. An dieser Stelle muss sich ein jeder fragen, in wie weit er bereit ist, sich mit einem Dienstleister einzulassen, der übrigens jederzeit auch gewechselt werden kann. Aber grundsätzlich ist das Bezahlen von Klein- und Kleinstbeträgen in der ersten Ebene von Bitcoin weder sinnvoll noch ökonomisch möglich. Ich gehe auch stark davon aus, dass die Lösungen, die noch erarbeitet werden (müssen), um Lightning besser im Hauptnetzwerk zu verankern mit zunehmender Akzeptanz von Bitcoin und damit unweigerlich steigenden Gebühren schneller auf den Markt kommen. Und wenn wir uns die Alternative anschauen, die da Digiale Zentralbankwährung – Central Bank Digital Currency (CBDC) heißt, ist alles besser als diese. Da gibt es nicht das Luxusproblem, dass Aspekte des Geldes leicht beeinträchtigt sein könnten, oder die

45 Lightning Network - https://lightning.network
46 Lightning White Paper - https://lightning.network/lightning-network-paper.pdf

Geschwindigkeit nicht reicht. CBDCs sind reiner Zwang und Kontrolle.

Aber zurück. In Lightning gibt es einen Mechanismus um Betrug oder anderweitig unfaire Methoden zu sanktionieren. Bei der Eröffnung geben beide Parteien einen gewissen Betrag in den zu eröffnenden Kanal und sobald eine Seite versucht zu betrügen, kann die andere dies durch das Bitcoin-Netzwerk prüfen lassen und das „Opfer“ erhält den gesamte Wert des Kanals. Dazu ist kein Richter und keine Schiedsstelle notwendig. Sobald festgestellt wird, dass sich eine Seite nicht an die verabredeten Regeln gehalten hat, kommt die Sanktion. Wenn wir uns also nochmal die Geschichte mit dem Dienstleister vor Augen halten, so müssen die sehr genau aufpassen, was sie machen und wie sie mit ihren Kunden agieren, ansonsten wird deren Einsatz einfach dem Kunden zugeschlagen. Dieser Gedanke ist in der heutigen Bankenwelt so absurd, dass man den gar nicht richtig zu Ende denken kann.

Lightning ist zur Zeit noch in der Entwicklungsphase und es müssen noch einige Hindernisse und Risiken aus dem Weg geräumt werden, bis diese Technologie für alle Nutzer sicher zur Verfügung steht. Es gibt schon einige Anbieter für Lightning-Wallets, die mit unter auch sehr einfach in der Handhabung sind, doch der Weg für Bitcoin bis zu einem richtigen Geld ist noch weit, aber wir gehen jeden Tag weiter voran.

Alle sind mehr oder weniger Gleich – der Cantillon Effekt

Haben Sie auch das Gefühl, dass diese Geschichte von der Gleichwertigkeit Aller irgendwie heftige Risse aufweist? Erleben wir nicht permanent, wie die einen ständig verkünden, dass sie noch reicher geworden sind, selbst in tiefsten Kriesen wie der grassierenden Seuche Anfang der 2020er Jahre, während man selbst nicht vorwärts kommt, egal wie sehr man sich anstrengt. Und nach ein paar Gesprächen mit der Familie, Freunden und Bekannten stellt man fest, dass es denen im Grunde auch so geht. Das liegt daran, dass wir die falschen Freunde haben und aus den falschen Familien stammen. Wir, die Normalos, sind ganz einfach zu weit weg von der Geldschöpfung und profitieren überhaupt nicht oder wenn nur minimal vom sogenannten Cantillon Effekt.

Der Cantillon-Effekt beschreibt ein ökonomisches Phänomen, bei dem Veränderungen in der Geldmenge ungleichmäßige Auswirkungen auf die Preise und die Vermögensverteilung in einer Volkswirtschaft haben. Dieser Effekt wurde erstmals von dem französischen Ökonomen Richard Cantillon im 18. Jahrhundert beschrieben. Der Kern des Cantillon-Effekts ist, dass nicht alle Wirtschaftsakteure gleichzeitig und in gleichem Maße von einer Geldmengenausweitung profitieren. Stattdessen profitieren diejenigen, die das neue Geld als Erste erhalten, am meisten. Diese Akteure können die zusätzliche Kaufkraft nutzen, bevor es zu einem Anstieg der Preise kommt. Jene, die das Geld erst später erhalten, sehen sich dann mit höheren Preisen konfrontiert, ohne von der Geldmengenausweitung profitiert zu haben. Bildlich kann man sich das wie eine Champagner-Pyramiede vorstellen, bei der die obersten Gläser überlaufen und dadurch die unteren leidlich füllen. Je weiter oben ein Gals ist, desto schneller ist es voll.

Ein Beispiel verdeutlicht den Mechanismus: Wenn eine Zentralbank die Geldmenge erhöht, indem sie Staatsanleihen kauft, profitieren zunächst die Inhaber dieser Anleihen, da der Wert ihrer Papiere steigt. In einem nächsten Schritt können diese Anleihenbesitzer ihre zusätzlichen Mittel für Konsum- oder Investitionszwecke verwenden. Dadurch steigt die Nachfrage nach Gütern und Dienstleistungen, was zu Preissteigerungen führt. Die Arbeitnehmer, Rentner und andere Gruppen, die das Geld erst in einem späteren Stadium erhalten, müssen dann die höheren Preise bezahlen, ohne zuvor von der Geldmengenausweitung profitiert zu haben. Somit kommt es zu Umverteilungseffekten, die die Einkommens- und Vermögensungleichheit in der Gesellschaft vergrößert. Deshalb werden die – heute sagt man nicht mehr Oligarchen, sondern Philanthropen – ständig in perverser Manier reicher, während der Normalbürger einen stetigen Rückgang seiner

Kaufkraft feststellt.

Der Cantillon-Effekt zeigt, dass Geldpolitik nicht neutral ist, sondern reale Auswirkungen auf die Wirtschaft hat. Ökonomen diskutieren den Cantillon-Effekt bis heute intensiv und sehen darin eine wichtige Ergänzung zur klassischen Quantitätstheorie des Geldes. Das ist einer der wichtigsten Faktoren der extremen Geldakkumulation bei den Superreichen, die in der Folge zu heftigen Verwerfungen der politischen Systeme führen können und führen, da Geld bekanntlich Macht bedeutet.

Das Bitcoin-Netzwerk weist im Vergleich zu herkömmlichen, Zentralbank-gesteuerten Währungen einen fundamentalen Unterschied auf, der dazu führt, dass der Cantillon-Effekt hier nicht zum Tragen kommt. Dieser Unterschied liegt in der Natur der Bitcoin-Geldschöpfung, die dezentral und nicht von einer zentralen Instanz kontrolliert erfolgt. Bei Bitcoin erfolgt die Geldschöpfung nicht durch eine Zentralbank, sondern dezentral über das gesamte Netzwerk. Neue Bitcoin-Einheiten werden durch das Mining-Verfahren geschaffen, an dem theoretisch jeder Teilnehmer gleichberechtigt teilnehmen kann. Es gibt somit keine bevorzugten Akteure, die als Erste von der Geldmengenausweitung profitieren würden. Darüber hinaus sind die Regeln der Bitcoin-Geldschöpfung transparent und öffentlich einsehbar. Es gibt keine geheimen oder diskretionären geldpolitischen Entscheidungen, die bestimmte Marktteilnehmer begünstigen könnten. Stattdessen folgt die Ausweitung der Bitcoin-Geldmenge einem vorab definierten und deterministischen Zeitplan, wodurch es keine plötzlichen oder unerwarteten Änderungen der Geldpolitik gibt.

Die Geldverteilung bei Bitcoin ist im Vergleich zu herkömmlichen Fiatwährungen relativ konzentriert, weist aber im Laufe der Zeit eine zunehmende Dezentralisierung auf. Zu Beginn des Bitcoin-Netzwerks wurden die meisten Bitcoins durch den Schöpfer Satoshi Nakamoto und frühe Mitwirkende geschürft, was zu einer anfänglichen Konzentration des Bitcoinbesitzes bei wenigen Akteuren führte. Im Laufe der Jahre hat sich die Geldverteilung bei Bitcoin dennoch zunehmend dezentralisiert, da mehr Nutzer Bitcoins erwerben und halten. Laut Schätzungen besitzen mittlerweile über 100 Millionen Menschen weltweit Bitcoins.

Statistische Maße wie der Gini-Koeffizient[47] zeigen, dass die Bitcoinverteilung zwar immer noch konzentrierter ist als bei Fiatwährungen, sich aber in Richtung einer gleichmäßigeren Verteilung entwickelt. In jüngster Zeit gewinnen auch institutionelle Investoren wie Fonds und Unternehmen an Bedeutung im Bitcoin-Ökosystem, was die Konzentration des Bitcoinbesitzes zukünftig wieder erhöhen könnte.

Zusammengefasst führen die dezentrale Struktur, die Transparenz und die fixierte Geldmengenausweitung dazu, dass der Cantillon-Effekt bei Bitcoin nicht auftritt. Alle Teilnehmer haben einen gleichberechtigten Zugang zur Geldschöpfung, sodass es keine systematische Umverteilung von Vermögen und Einkommen gibt, wie es bei herkömmlichen, Zentralbank-gesteuerten Währungen der Fall ist. Natürlich unterliegt die Geldverteilung sehr vielen Kriterien, wie zum Beispiel auch der Leistungsfähigkeit und Leistungsbereitschaft jedes Einzelnen und ganz besonders natürlich des bereits vorhandenen Reichtums, den man in Bitcoin investieren kann, doch kann man sagen, dass durch Bitcoin auf die lange Sicht sich das Geld eher gleichmäßig verteilt.

In God We Trust – Einfach, diskret, vertrauenslos

Wir haben jetzt schon mehrfach gesehen, dass Bitcoin vollkommen dezentral ist und es absolut keine Person, Stelle, Institution oder sonst irgendwen gibt, der/die für Bitcoin verantwortlich zeichnen. Nicht einmal die Programmierer haben einen wirklichen Einfluss darauf. Alle Prozesse zeichnen sich durch vollkommene Transparenz und Basisdemokratie aus und beweisen dabei nebenher bemerkt, dass unser jetziges System mit all seinen Geheimnissen und zentralen

47 Gini-Koeffizient ist ein Index, der die Vermögensverteilung in einer Zahl veranschaulicht.

Entscheidungen unglaublich viel Dreck am Stecken haben muss, denn der Aufwand der für dieses kaputte System betrieben wird ist gigantisch und das würde nicht gemacht werden, wenn die Nutznießer des Systems dies nicht bräuchten. Aber das ist wiederum ein anderes Thema.

Die Transparenz bewirkt, dass Bitcoin ohne jedes äußere Vertrauen auskommt, es keine Notare und Clearingstellen geben muss und dadurch wird das komplette System sehr einfach. Es bedarf nur noch der Übereinkunft zweier Parteien für einen Tausch oder Kauf und schon kann alles abschließend geregelt werden. Es wird keine Bank benötigt und kein Kreditkartenunternehmen.

Durch die Pseudoanonymität und die Mittel, die man hat um mit Hilfe von Verschleierungstechniken die eigenen Adresse zu anonymisieren ist Bitcoin auch bei aller Überwachung und Kontrolle, die Staaten ausüben können, ein relativ diskretes Geld. Natürlich nicht so anonym wie Bargeld, aber fast und dabei weltweit einsetzbar. Auf den von der Federal Reserve ausgegebenen US-Dollar Noten steht „In god we trust“. Eigentlich ganz putzig, ist die Ferderal Reserve nur keine kirchliche Einrichtung. Aber dieser Satz repräsentiert wie nichts anderes worum es in dem aktuellen Fiatsystem geht. Es ist ein von oben aufoktroyiertes System, das nur der Oberschicht nützt und auch nur solange funktioniert, solange die Masse der Menschen nicht versteht, wie die Strukturen wirklich laufen. Kurzum, solange geglaubt und vertraut wird, werden die Reichen reicher und die Armen ärmer. Henry Ford hat mal gesagt: „Wenn die Menschen das Geldsystem verstehen würden, hätten wir eine Revolution morgen“ und so schlimm das auch klingt, es ist leider wahr. Es ist sehr bemerkenswert, dass so unglaublich viele „Gesetze“ die zur Stabilität und zur Sicherung von Währungen geschaffen wurden, mit einem Federstrich, oder besser noch durch einfaches Ignorieren außer Kraft gesetzt werden können. Die Maastricht-Kriterien zur Stabilität des Euros sind zwar alle auf dem Papier noch da, doch es interessiert sich niemand dafür. Auch die Aufhebung des Goldstandards durch Präsident Nixon 1971 ist nur vorübergehend. Der Mann ist nur schon lange Tod, ohne dass die Aufhebung zurückgenommen wurde und hier ist wohl die alte Weisheit angebracht, dass nichts so lange hält wie das Provisorium. Aber lassen wir auch dieses Thema, denn das wäre ein Thema, zu dem man noch ein ganzes Buch verfassen müsste, wollte man dem Missbrauch des Geldsystems und der dazugehörenden Verschleierung gerecht werden. Alles sehr unappetitlich...

Bitcoin ist heute sehr einfach geworden und kann selbst von Menschen, die nicht mit einem Handy in der Wiege aufgewachsen sind, problemlos verwendet werden. Aber Bitcoin kann noch ein bisschen mehr. Bitcoin ist grenzenlos. Dadurch, dass man nur seine winzige Hardware-Wallet in der Tasche hat, seine Software-Wallet auf dem Handy oder im äußersten Fall 12 bis 24 Wörter im Kopf kann man sein Geld an jeden Ort der Welt unbegrenzt mitnehmen. Man versuche dies einmal mit Gold, oder Bargeld. Bitcoin kann, wie schon mehrfach gesagt, einfach nicht reguliert und begrenzt werden und jeder Versuch dies zu tun ist von vornherein zum Scheitern verurteilt. Daher auch die staatlichen Restriktionsversuche beim monetären Zugang zu Bitcoin, also bei den den Börsen. Wenn man diesen Gedanken erst einmal zugelassen hat und in seiner Tiefe versteht, dann wird ganz schnell klar, dass es bei Bitcoin nicht um den Kurswert in Euro oder Dollar geht, sondern der eigentliche Sinn und Zweck ist sie Ablösung des bestehenden Systems und zwar nicht durch Revolution, Kampf und Geschrei, nein ganz im Gegenteil, durch Evolution. Bitcoin wird sich durchsetzen, da jedem früher oder später auffallen wird, dass das aktuelle System nicht lebensfähig ist. Und egal welches Nachfolgemodel eingeführt werden wird, denn eines ist klar, es wird eine wie auch immer geartete Währungsreform in der nahen Zukunft geben, dieses neue System wird wieder mit den selben Unzulänglichkeiten und Ungerechtigkeiten ausgestattet sein, denn die herrschende Klasse, die das System bestimmt, will weiter profitieren. Bitcoin ist der Ausweg, so wie es keine andere Geldform auch nur im Ansatz kann. Und Bitcoin ist die ultimative Antwort auf die propagierten CBDCs, also das digitale Zentralbankgeld. Dieser Übergang wird aber wie gesagt recht leise ablaufen und über einen sehr langen Zeitraum und auf diese Weise werden die Schäden, die unweigerlich durch einen Umsturz entstehen würden, stark abgefedert, oder gar komplett

vermieden.

Dieser Gedanke sollte also selbst bei denen, die sehr wohlhabend sind, keine Befürchtungen aufkommen lassen und damit natürlich eine größere Akzeptanz und damit auch eine verstärkte Wirkmacht auslösen. Aber das werden wir erst noch sehen. Ich denke, dass sich der Prozess an sich nicht mehr aufhalten lässt, die Frage ist einzig und alleine wie schnell und wie intelligent die Umsetzung erfolgen wird.

Nur ein Schneeballsystem – Warum Bitcoin seine Kritiker Lügen straft

Die Anwürfe, dass Bitcoin nur ein Schneeballsystem sei trifft auf fast alle Altcoins zu. Warum ist Bitcoin anders?

Mit die beliebteste Kritik an Bitcoin ist, es sei ein reines Schneeballsystem, oder in der Sprache der Ökonomen ein Ponzi Scheme[48]. Zuerst müssen wir mal klären, was das denn genau ist.

Ein Schneeballsystem zeichnet sich durch folgende Punkte aus:

1. Keine echte Investitionstätigkeit: Es gibt keine tatsächlichen Geschäftsaktivitäten oder Investitionen, die Gewinne erwirtschaften. Die Auszahlungen an Investoren stammen ausschließlich aus den Einlagen neuer Teilnehmer.
2. Hohe Renditeversprechen: Um neue Investoren anzulocken, werden unrealistisch hohe Renditen von 20% oder mehr pro Jahr versprochen.
3. Intransparenz: Die genauen Geschäftsaktivitäten und Finanzen werden vor den Investoren verheimlicht.
4. Schnelles Wachstum: Um neue Gelder zu akquirieren, wird das Schema aggressiv beworben und expandiert rasch.
5. Frühe Investoren werden bevorzugt: Die ersten Teilnehmer erhalten hohe Auszahlungen, um andere anzulocken.

Irgendwann bricht das System unweigerlich zusammen, sobald nicht mehr genug neue Investoren hinzukommen, um die alten auszuzahlen. Dann verlieren die letzten Investoren ihr gesamtes Geld. Historisch haben wir die Klassiker mit Charles Ponzi in den 1920ern, nachdem dieses betrügerische Verfahren auch benannt wurde, oder in den 2000er Jahren Bernhard Madoff[49], die solche Systeme betrieben haben.

Wenn wir uns die 5 Punkte oben mal anschauen und uns fragen, was davon auf Bitcoin zutrifft, dann stellt sich innerhalb eines Wimpernschlages heraus, dass dieser Vergleich vollkommener Schwachsinn ist. Jeder weiß, dass es keine Geschäftstätigkeit bei Bitcoin gibt und der einzige wertsteigernde Aspekt seine Knappheit und die steigende Akzeptanz ist. Bitcoin verspricht genau wie ein Klumpen Gold gar keine Rendite. Bitcoin ist so transparent wie kein anderes Asset auf dieser Welt. Niemand weiß wie die Unternehmenszahlen von Firma XY wirklich aussehen, oder wie viel Platin physisch hinterlegt ist. Das sind alles Firmengeheimnisse, oder Bezeugungen von Vertrauenspersonen, doch bei Bitcoin kann alles von Jedermann selbständig eingesehen und kontrolliert werden. Es stimmt, dass es ein bescheidenes Maß an Werbung gibt in Bitcoin zu investieren, meistens von Börsen oder ETF-Händlern[50], aber niemand gibt wirklich viel Geld für aggressive Werbung für Bitcoin aus. Es gibt keine „Auszahlungen“ bei Bitcoin, sondern lediglich

48 Ponzi scheme – Benannt in den 1920er Jahren nach Charles Ponzi, der ein betrügerischen Schneeballsystem betrieb. - https://de.wikipedia.org/wiki/Charles_Ponzi

49 Bernhard L. Madoff - https://de.wikipedia.org/wiki/Bernard_L._Madoff

50 ETF - Exchange Traded Fund, also börsengehandelter Fonds.

die Kursentwicklung und die kann natürlich auch zum Nachteil des Investors sein. Wir sehen, ein Ponzi scheme kann auf ein Gut wie Bitcoin gar nicht angewendet werden.

Aber warum wird dieser Vorwurf dann immer wieder vorgebracht und verfängt bei den Lesern der Gazetten und Magazine? Ganz einfach. Ich sag jetzt mal die „Medien mit Interesse“ verknüpfen Bitcoin entgegen der Wahrheit mit den unzähligen anderen Kryptoprojekten und diese sind zum überwiegenden Teil wirklich Schneeballsysteme, oder dem ähnlich. Dadurch, dass Eigenschaften wie die Dezentralität, die numerische Limitation auf 21 Millionen Stück und der Schürfprozess mit dem Proof-of-Work weggelassen werden wird Bitcoin mit dem gleichen Kamm gebürstet wie all die teilweise betrügerisch angelegten Altcoin Projekte. Auf diese Weise schaffen es die „interessierten“ Journalisten und sprechenden Köpfe aus Verwaltung und Politik eine Verklammerung herzustellen zwischen Betrug und Kyrpto und vor allem der bekanntesten Kryptowährung dem Bitcoin.

Angriff auf den Energieverschwender

Da ich Jahre lang als Energieberater gearbeitet habe ist mir dieses Thema irgendwie sehr wichtig und, wer hätte es gedacht, auch etwas ausführlicher.

Bei Bitcoin steht immer der sehr hohe Energiebedarf im Raum, der dem Schürfen von Bitcoin geschuldet ist. Dabei wird immer behauptet, dass Bitcoin die Energie verschwenden würde, voraussetzend, dass Bitcoin nur so ein Spielzeug sei, oder eine Art Casino und man könne damit einfach nur spekulieren. Wir haben ja schon festgestellt, das Bitcoin alles andere als eine Spielerei ist und einen wirklich wichtigen Beitrag zur heutigen und vor allem zukünftigen Gesellschaft leisten wird und bedingt heute schon leistet. Weiter sollte man mal den Gedanken zulassen, wie viel Energie durch Streamingdienste und Onlinevideospiele verbraucht wird. Das sind wirkliche Spielereien, allerdings gesellschaftlich anerkannt. Aber das ist schon wiederein ganz anderes Thema.

Es ist wirklich essenziell zu verstehen, dass die Integrität von Bitcoin darin begründet ist, dass Leistung in einer gewissen Zeit erbracht werden muss. Bitcoin kann nicht einfach einen neuen Block „erfinden“ und an die Kette anhängen. Es gibt keine Fiat-Blöcke! Nur wer nachweisen kann, dass Energie in Form von Rechenleistung aufgewendet wurde, der erhält das Recht Daten anzufügen. Dieses Prinzip ist so elementar und wichtig, dass es immer und immer wieder gesagt werden muss. Bitcoin verschwendet nicht, so wie seine Kritiker immer glauben machen wollen, die Energie, sondern diese wird umgewandelt. Das Fundament von Bitcoin ist Energie und Zeit. Das sind zwei Größen, die nicht manipuliert werden können und dies macht Bitcoin zum sichersten Asset[51] der Menschheitsgeschichte. Man kann also sagen, dass Bitcoin Energie und Zeit in Definitheit und Sicherheit umwandelt.

Im Grunde ist es so wie bei einem Bauern. Kein Bauer kann Samen in die Erde geben und danach gleich mit der Erntemaschine kommen. Bei den Pflanzen ist es die Energie der Sonne und Zeit, die die Feldfrüchte gedeihen lassen, bei Bitcoin ist es die Energie des Stromes und Zeit, aber im Grunde sind beide Prozesse gleich. Der einzige Unterschied ist der, dass in Bitcoin, also in der erschaffenen Einheit, die Energie nicht gespeichert wird, hingegen in der Karotte schon. Sie hat die Energie in Masse umgewandelt. Bei Bitcoin dient die aufgewendete Energie als ultimative und durch niemanden manipulierbare Versicherung, dass die Blockchain nicht mit willkürlichen Daten ex nihilo[52] bestückt werden kann. Es ist also analog so wie beim Goldabbau. Es gibt nur neues Gold, wenn in den Stollen gefahren wird und unter Mühen das Gestein geöffnet wird. Und auch im Gold ist die geleistete Energie nicht mehr enthalten. Der Barren, die Münze, der Ring speichert selbst die

51 Asset – engl. Vermögenswert
52 Ex nihilo, lat. Aus dem Nichts

aufgewendete Energie nicht.

Aus der „alten“ Finanzwelt und von diversen Journalisten wird immer wieder vorgebracht, dass Bitcoin Energie verschwenden würde und einen Gesamtenergiebedarf habe, der größer sei als manche Staaten. Das klingt dann immer sehr abschreckend und eingedenk der Diskussion zum Thema Klima ist das eigentlich schon das Aus für eine Anlageklasse. Genau darauf zielen solche totschlagargumente auch ab, aber wir sollten uns erst einmal fragen wer solche Anschuldigungen erhebt und zu welchem Zweck, bevor wir dann klären, dass Bitcoin der am besten gehbare Weg ist unsere Natur auf lange Sicht zu schützen und zu bewahren.

Jeder Mensch hat Interessen und das ist auch in gar keiner Weise verwerflich, nur sollten diese Menschen auch sagen, aus welcher Motivation heraus sie sich zu einem Thema äußern. Es gibt auch Menschen, die keine Ahnung haben und nur Dinge wiederkäuen, die man ihnen eingeträufelt hat, wer weiß. Wirtschaftsjournalisten sind einfach als Teil ihres Berufes mit Unternehmen verbandelt und zum Beispiel für den klassischen Aktienmarkt ist es einfach nicht gut, wenn Investitionen nicht in die Aktien, sondern in Kryprowährungen gehen. Das ist schlicht schlecht fürs Geschäft. Menschen, die in politischen oder wirtschaftlichen Verhältnissen zu Banken, oder gar Zentralbanken stehen können dem schärfsten Konkurrenten selbstverständlich auch nichts abgewinnen, wie sollten sie auch. In den vorangegangenen Kapiteln haben wir ja überdeutlich gesehen, dass das Establishment gar kein Interesse an Bitcoin haben kann und so ist es nicht verwunderlich, wenn diese Kreise ihre wirtschaftliche und auch politische Macht nutzen um Bitcoin schlecht zu machen und wie gesagt, Klima ist ein Totschlagargument. Damit kann man alles vom Tisch bügeln.

Aber wie verhält es sich wirklich? Beim Schürfen von neuen Böcken wird wirklich sehr viel Energie in Form von Strom angefordert, doch das bedeutet ja nicht zwingend, dass diese Energie nicht weiter verwendet werden kann. Es gibt Schürfunternehmen, die die Abwärme, die durch die Computer produziert wird, als Direkt- oder Fernwärme nutzbar machen. So produziert zum Beispiel Hashlabs Mining Fernwärme[53] in Finnland. Oder die Firma 21Energy[54] produziert Heizungen für den Endverbraucher, die neben der Heizung Bitcoin schürfen. Solche Lösungen werden fast täglich neu angeboten und die Vielfalt der dualen Energienutzung steigt ständig an. Natürlich darf man das auch nicht überbewerten, aber der Weg weist definitiv in die richtige Richtung und dies ist auch ganz logisch, denn in Mitteleuropa ist Energie, insbesondere Strom, derart teuer, dass dem Einzelnen gar nichts anderes übrig bleibt, als Wege zu suchen Kosten zu optimieren. Bitcoin bietet sich da wirklich an auch für den normalen Bürger eine duale Lösung aus heizen und schürfen bei sich zu installieren und so die horrenden Nebenkosten gegen Null zu bringen.

Der zweite Bereich, in dem Bitcoin einen sehr großen Beitrag zur Stabilisierung des Stromnetzes leistet, ist in der Überproduktion, insbesondere von volatilen Energieträgern wie Wind und Solar. Dazu ein kleiner Exkurs in die Welt des Stromes. Strom muss in dem Moment, in dem er benötigt wird auch produziert werden, es sei denn man verfügt über Speicher, die aber im globalen Maßstab nicht zur Verfügung stehen. Das bedeutet, dass die Kraftwerks- und Netzbetreiber ständig schauen müssen, das immer genau die richtige Menge Strom zur Verfügung steht. Bei uns in Mitteleuropa hat der Strom eine Frequenz von 50 Herz, heißt er schwingt 50 mal pro Sekunde. Diese stabile Frequenz ist extrem wichtig für die Leistungsverteilung im gesamten Netz. Steigt oder sinkt die Frequenz zu stark droht das Stromnetz komplett zu kollabieren und wir sprechen dabei von einer Toleranz von einem halben Herz nach oben und unten. Das führt dann zu einem Stromausfall. Es ist also wichtig, dass nicht zu wenig und nicht zu viel Strom produziert wird. Derzeit ist insbesondere in Deutschland, aber auch in der ganzen EU, der Trend hin zu Wind- und Sonnenenergie, die sehr volatil sind. Nachts scheint keine Sonne und wenn der Wind nicht weht, dreht sich auch kein

53 Quelle - https://cryptonews.com/news/project-in-finland-uses-bitcoin-mining-to-heat-homes.htm
54 Quelle - https://21energy.com/?sca_ref=5419545.wMbFU8rzuo

Windrad, aber im Sommer sonntags um 16:00, wenn die Sonne auf den Grill scheint, oder in einer stürmischen Nacht braucht niemand den Strom. Daraus folgt, dass die Netzbetreiber nicht nur genügend grundlastfähige Stromquellen haben müssen wie Atom-, Kohle, Öl- und Gaskraftwerke, letztere können auch zur Feinregulierung eingesetzt werden, da sie schnell an und abgeschalten werden können, was bei Kohle- und Atomstrom nicht möglich ist, sondern sie brauchen auch Abnehmer für Überproduktionen. Bei Unterdeckungen wird Strom in der Regel aus dem benachbarten Ausland zu horrenden Kosten eingekauft. Aber es sind diese Überproduktionen in denen an der Strombörse für die Abnahme von Strom Geld bezahlt wird. Das ist ein zunehmendes Paradoxon und eben genau hier kann Bitcoin wieder einspringen. Bitcoinmining lohnt sich nur, wenn der Strom sehr preiswert ist und das ist eben genau dieser über produzierte Strom. Um aktuell Überproduktionen zu vermeiden, werden volatile Kraftwerke, zu förderst die Windparks, einfach abgeschalten und für den Ausfall werden die Betreiber entschädigt. Der Betrag beläuft sich alleine in Deutschland auf etwa eine Milliarde Euro pro Jahr, die durch die staatlich garantierte Förderung einfach verschenkt wird und vom Steuerzahler bezahlt werden müssen. Das dies kein zukunftsweisenden System ist sollte jedem bereits klar sein. Ein Umstand, der auch noch hinzu kommt, ist das durch die ständigen Eingriffe ins Netz der Stromfluss, sprich die Frequenz, an sich instabil wird. Man spricht hier auch von Flatterstrom.

Nun gibt es Lösungen Miningparks, das sind in der Regel Container, vollgestopft mit Computern, in die Nähe von diesen volatilen Kraftwerken zu stellen und anstatt die Kraftwerke bei einer Überproduktion abzuschalten, wird die Energie für das Schürfen von Bitcoin benutzt. Sobald die Überproduktion vorbei ist, schalten sich die Computer wieder ab und der Strom wird wieder an Industrie und Haushalte geliefert. Der US-Bundesstaat Texas[55] wendet dieses System bereits großflächig an und das Stromnetz konnte auf diese Weise ganz extrem stabilisiert werden. Ein Gewinn für die Kraftwerksbetreiber, ein Gewinn für die Bitcoin Schürfer und für die Netzbetreiber und damit für die Endkunden, da es keinen Flatterstrom mehr gibt. Es gibt noch viele andere Lösungsansätze wie Bitcoin im großen Maßstab zur Stabilisierung eingesetzt werden kann. In Norwegen wird Strom zum Beispiel fast ausschließlich aus Wasserkraft[56] erzeugt und wegen der anfallenden Wassermengen kann auch hier der Strom nicht wirklich in den Stauwehren gespeichert werden. Auch hier kann das Bitcoin Schürfen sehr kostengünstig erfolgen, da die Menge an Strom die produziert werden kann von der norwegischen Industrie und den Haushalten gar nicht abgenommen werden können. Auch sind Übertragungswege in diesem doch recht großen Land nicht effizient zu handhaben. Die Lösung besteht wieder darin am Ort der Produktion die Schürfinfrastruktur aufzubauen.

Aber wie kann man sich das vorstellen, dass diese Computer ständig an und ausgeschaltet werden. Warum bricht dann der Bitcoin selbst nicht zusammen? Gäbe es nur einen Kontenpunkt im Bitcoinnetzwerk, dann wäre dies natürlich auch nicht möglich, aber da es sich um ein riesiges Peer-to-Peer-Netzwerk[57] handelt, welches sich über die gesamte Welt erstreckt, sind immer genug Computer angeschlossen um die sogenannte Hashrate[58] so weit oben zu halten, dass die Sicherheit nicht leidet. Es sind diese phänomenalen Eigenschaften von Bitcoin, die es möglich machen ganz neue und unkonventionelle Wege in der Datenverarbeitung zu gehen. Das eben beschriebene Verfahren, die Computer neben dem Windpark aufzustellen und einfach abzuschalten, wenn kein Wind weht, ist mit einem normalen Server von Banken, Kreditkartenfirmen oder was auch immer unmöglich. Diese verbrauchen ganz konsequent den Strom aus der Steckdose, egal ob Sonne, Wind, Kohle, Atom oder Gas. Die konventionelle Finanzwelt ist absolut indifferent woher der Strom kommt, Hauptsache er kommt. Und nebenher haben wir gleich noch etwas gelernt, nämlich die

55 Quelle - https://www.blocktrainer.de/blog/bitcoin-mining-kann-stromnetze-und-strompreise-stabilisieren
56 Quelle - https://de.statista.com/statistik/daten/studie/1292636/umfrage/struktur-der-stromerzeugung-in-norwegen/
57 Peer-to-Peer-Netzwerk – Dezentrales Netzwerk, in dem alle Teilnehmer gleichberechtigt verbunden sind.
58 Hashrate – Beschreibt die Leistungsfähigkeit eines Rechners oder eines Netzwerks von Computern bei der Berechnung kryptografischer Prozesse

immer wieder vorgetragene Mähr was passiert wenn der Strom ausfällt. Es passiert eben nichts, außer er fällt auf der ganzen Welt aus, aber dann haben wir alle ganz andere Probleme als uns um Vermögenswerte zu kümmern. Und wenn der Strom wieder da ist, dann ist auch die Bitcoin Blockchain wieder da und zwar um ein Vielfaches schneller als Banken und Kreditkartenfirmen ihre Zentralrechner wieder am Netz haben.

Kritiker wenden ja immer ein, dass Bitcoin keine sinnvolle Anwendung für die Energie sei, sich also der Verbrauch nicht durch einen wirklichen Nutzen rechtfertigen lässt. Rechnen wir den Stromverbrauch von den ganzen Sozialen Netzwerken wie Facebook, Instagram, X (Twitter) und Co. zusammen, kommen wir auf etwa 90 Terra Watt Stunden (TWh), das ist so viel wie der Verbrauch von Kolumbien. Oder die verschiedenen Streamingdienste verbrauchen auch Unmengen an Energie, wohlgemerkt ständig und indifferent, und auch hier stellt sich doch eindeutig die Frage, ob der Nutzen den Energiebedarf wirklich rechtfertigt.

Jetzt kommen wir aber zu einem Aspekt, den die Kritiker seltsamerweise nie thematisieren, sprechen sie doch auch Bitcoin ab, ein wirkliches Geld sein zu können. Der Energieverbrauch für das aktuelle Geldsystem liegt geschätzt bei 100-300 TWh[59] hingegen Bitcoin bei 50-150 TWh. Sicher ist der Bitcoin-Verbrauch sehr hoch, doch mit dem reinen Stromverbrauch ist es beim traditionellen Finanzsystem auch noch nicht erledigt. Wir hatten schon besprochen, dass der US-Dollar die Weltreservewährung ist, doch wie wird die Reservewährung besichert? Bislang haben wir uns nur damit beschäftigt, welche Werte, nämlich vornehmlich Öl, den Wert vom US-Dollar stützen, aber das alleine ist es leider nicht. Die Vereinigten Staaten haben mit weitem Abstand das größte Militär und dies existiert zum Löwenanteil dazu die hegemoniale Macht zu sichern, oder sprich den US-Dollar und damit den Reichtum der USA zu erhalten. Es gibt keine verlässlichen Zahlen zum Energieverbrauch des US-Militärs, da diese aus „Sicherheitsgründen“ nicht veröffentlicht werden, aber Schätzungen gehen davon aus, dass das US-Miltär einer der größten Verbraucher weltweit ist. In anderen Staaten und Staatenverbünden, wie zum Beispiel die Europäische Union, ist es auch nicht anders. Das Geldsystem wird durch Militärische Macht geschützt und wenn wir uns die miserablen Leistungszahlen der ganzen Fiat-Währungen anschauen, dann ist auch schnell klar, warum das so sein muss. Das Sprichwort „Geld regiert die Welt“ stimmt ganz einfach und wenn dem so ist, bleibt die Frage wer regiert das Geld? Ich will hier jetzt keine Theorien diskutieren, aber eines ist sicher, ohne militärische Macht, ohne rohe Gewalt, hält sich kein zentrales, aufgezwungenes Geldsystem.

Und jetzt spinnen wir der Gedanken mal weiter. Der Einfachheit halber sagen wir Bitcoin benötigt nur die Hälfte an Energie wie das bestehende Geldsystem und der evolutionäre Prozess geht immer weiter, Bitcoin wird von immer mehr Menschen angenommen und mittels innovativer Adaptionen und Anwendungen im Alltag eingesetzt, dadurch verringert sich der Energieverbrauch des klassischen Geldsystems sukzessive, da immer mehr Institutionen des traditionellen Geldsystems unnötig werden. Das klingt jetzt vielleicht etwas weit gedacht, ist es aber gar nicht. Wenn Bitcoin alleine nur im Interbankenverkehr eingesetzt wird und damit das externe Clearing, also die zusätzliche Vertrauesinstanz wegfällt, werden Unmengen an Resourcen und damit auch Energie frei. Und noch weiter gesponnen verringert sich der Energieverbrauch mit dem vollständigen Wegfall des klassischen Finanzsystems auf 50%. Man fragt sich wirklich, warum so etwas nicht in den Magazinen und Zeitungen diskutiert wird.

Es ist also einfach sehr verkürzt zu behaupten Bitcoin würde als Spekulationsobjekt einfach nur Energie verschwenden, ganz im Gegenteil. Durch innovative Lösungen wird Energie mehrfach und effizient eingesetzt. Durch die Inklusivität, die Portabilität, die Unzensierbarkeit und all die anderen Vorteile von Bitcoin muss dieses neue Geld auch nicht durch Gewalt aufgezwungen werden, jeder vernünftige Mensch möchte so ein Geld, so einen Wertespeicher.

59 TWh – Terra Watt Stunden

Und jetzt kommen wir zu einem Thema, dass überhaupt von niemanden öffentlich besprochen wird. Und zwar das Thema Umweltschutz und Ressourcenschonung. Aus den uns bekannten Fakten können wir ableiten, dass Bitcoin ein deflationäres Geldsystem ist und dies bedeutet, dass der Wert der Währungseinheit kontinuierlich steigt, oder in den Alltag übersetzt, man bekommt morgen mehr für sein Geld als heute. Wir kennen dieses Phänomen aus der Computertechnik. Der Preis für Geräte und Komponenten bleibt im Grunde immer gleich oder steigt nur sehr moderat, aber die Leistung steigt kontinuierlich stark an. In diesem Segment wird der technologische Fortschritt, der Produktivitätszugewinn und die Leistungssteigerung, an den Kunden weitergegeben. Es gibt also für den Kunden einen wirklichen Anreiz die Kaufentscheidung wirklich zu durchdenken und gegebenenfalls abzuwarten und dennoch floriert der Wirtschaftszweig wie fast kein anderer. In so ziemlich allen anderen Branchen ist dem nicht so. Wir werden jeden Tag mit allem möglichen Firlefanz belästigt was wir alles kaufen sollen, den nur heute ist es noch so billig und nur jetzt gibt es dieses und jenes. Wir werden also ständig getrieben jetzt unser Geld auszugeben und die aktuellen Inflationszahlen, die sich in der gesamten westlichen Welt hartnäckig hoch halten, bestärken uns in diesem Verhalten, denn morgen ist das Geld einfach weniger wert. Mit einem Bitcoin Geldsystem müssten die Firmen wieder Produkte und Dienstleistungen anbieten, die wirklich überzeugen, Waren die keine geplante Obsoleszenz[60] haben. Alle, und das wären sehr viele Unternehmen, die versuchen mit minderwertiger Ware am Markt zu bestehen würden in kürzester Zeit pleite gehen. Das bedeutet also auch, dass die Unmengen an vollkommen überflüssigen Produkten, die heute durch Firmen produziert werden, die ständig neue Kredite aufnehmen können um sich zu halten, gar nicht mehr hergestellt würden, dass die Rohstoffe nicht mehr vergeudet würden, dass sinnlose Dienstleistungen, die ja auch ein gewisses Umfeld brauchen, eingestellt würden. Die Liste der „Überflüssigen“ ist unendlich lang! Aber die Menschen würden dennoch weiter konsumieren, auch wenn die Mehrheit der Ökonomen dies vehement bestreiten werden. Warum sollte man sich denn nicht ein neues Handy kaufen? Natürlich möchte man so etwas haben, aber eben nicht jedes Jahr und nur, wenn das neue auch mehr kann oder das alte wirklich kaputt ist. Man würde im Supermarkt immer noch sein Essen einkaufen, aber nicht mehr die minderwertigen Füllstoffe, deren Hersteller oft Worte wie Lebensmitteln verwenden. Auch die fast schon Sucht viel zu viel einzukaufen, eben weil irgendetwas gerade billig ist würde aufhören, denn morgen ist zwar das Produkt nicht mehr im Sonderangebot, aber das Geld ist mehr wert. Das ist ein bahnbrechender Gedanke, oder wie der Engländer sagen würde – Mind blowing!

Die Deflation, und das widerspricht auch schon wieder der Lehrmeinung, zwingt die Marktteilnehmer dazu effizient und hochwertig zu produzieren und verbessert gleichzeitig die Stellung des Kunden, der ja überzeugt werden muss sich von seinem wertvollen Geld zu trennen, was unter Umständen auch der Grund ist, warum dies keine Lehrmeinung ist. Aber egal wie, Bitcoin als universales Geld würde den größten Beitrag leisten diesen unseren Planeten zu schützen und den Raubbau zu beenden und zwar nicht durch Verbote, komische Gesetze, oberlehrerhafte Belehrungen, hirnlose Ideologien, nein einfach weil die Menschen sich vernünftiger verhalten würden. Es ist nur der einfache Gedanke, dass alles was ich heute nicht verkonsumiere morgen mehr wert ist. Mehr ist es gar nicht. Ein Blick auf die Hyperinflation in Deutschland von Sommer 1922 bis November 1923 zeigt uns ganz drastisch die Gegenbewegung, als alles, und zwar wirklich alles, wertvoller war als die damalige Reichsmark. Die Menschen haben mit den Geldscheinen ihre Öfen betrieben, denn Holz war viel wertvoller. Sobald der Lohn ausgezahlt wurde, wurde der sofort in die Läden getragen, denn am nächsten Tag waren die Waren viel teurer.

Wenn heute die Menschen in großen Mengen sich gewahr würden, dass ihr Geld im Wert steigt und nicht gegen Firlefanz und unsinnige Dinge eingetauscht werden sollte, wären morgen die Müllberge sehr viel kleiner, würde man wieder mit dem Fahrrad zum Bäcker fahren und die Kinder mit dem Bus zur Schule. Der ganze völlig aus den Fugen geratenen und nur durch Kredit ermöglichte

60 Geplante Obsoleszenz bezeichnet eine gewollte Verkürzung der Lebensdauer von Produkten durch den Hersteller.

Konsum, der für jeden sichtbar unseren Planeten nachhaltig schädigt, würde aufhören, aber die Menschen würden dennoch nicht in Höhlen wohnen. Wir bräuchten keine Verbote und keinen Oberlehrer, der uns sagt, auf was wir alles verzichten sollen zum Wohle des Klimas und des Planeten. Das wüssten die Menschen sehr schnell und sehr genau selbst.

Damit möchte ich dieses Kapitel auch abschließen und nochmals festhalten, dass Bitcoin, entgegen all der Anwürfe, einen wichtigen und wertvollen Beitrag zur Erhaltung unseres Planeten leisten kann.

Lieber Gott mach mich reich – Anlagestrategien

Wer träumt nicht davon über Nacht reich zu werden und das ohne etwas dafür zu tun. Mit Bitcoin bleibt das auch weiterhin ein Traum, denn dieser Gedanke ist einfach unrealistisch. Aber Bitcoin kann natürlich helfen seinen eigenen Wohlstand aufzubauen, beziehungsweise abzusichern.

Eines muss beim Anlegen in Bitcoin erwähnt werden. Wer das nur macht, damit er oder sie am Schluss mehr Fiatgeld hat kann das natürlich gerne tun, aber dies ist die unterste Stufe von dem was Bitcoin ist und kann. Die Spekulation war nie die Intension von Satoshi Nakamoto, sondern der gesellschaftliche und politische Nutzen. Wer Bitcoin nur als Spekulationsobjekt sieht, kann dieses Buch auch gerne zur Seite legen, denn dafür gibt es unzählige andere, die von Finanzfachleuten geschrieben wurden und viel besser vermitteln können wie man noch mehr von diesem kaputten System partizipieren kann. Wer aber bereits schon die unzähligen Vorteile und Implikationen versteht oder zumindest erahnt, der ist in diesem Kapitel vollkommen richtig.

Wenn es um Anlagestrategien geht, dann scheiden sich die Geister sehr schnell und viele sind von diesem oder jenem, aber auf jeden Fall vom eigenen Weg überzeugt und propagieren diesen auch. Ich möchte hier eigentlich nur einen Weg aufzeigen, der insbesondere für Anfänger, sowohl bei Bitcoin, als auch bei Investitionen an sich, leicht nachvollziehbar und vielversprechend ist. Die anderen Möglichkeiten werden nur kurz angesprochen.

Vorab muss ich noch sagen, dies hier ist keine Finanzberatung und ich möchte niemanden dazu verleiten egal in welche Anlagen zu investieren. Dieses Kapitel versteht sich als rein theoretische Betrachtung.

Die sinnvollste und sicherste Methode sein Geld in Bitcoin anzulegen ist der tot langweilige Sparplan. Das heißt man kauft in regelmäßigen Abständen, zum Beispiel monatlich, immer zum gleichen Betrag Bitcoin ein und hält diese dann für mehrere Jahre. Eben langweilig. Aber bei dieser Technik, die im Englischen Dollar-Cost Averaging (DCA) genannt wird, glättet man durch den regelmäßigen Kauf die Kursschwankungen und unterliegt dann nur noch dem generellen Trend, der bei Bitcoin stark nach oben zeigt. In der Kryptogemeinde hat sich der Begriff „hodln“ dafür eingebürgert, ein Meme, dass für das Halten (hold) der Werte steht.

Abbildung 21: Kursentwicklung von Bitcoin der letzten 13 Jahre

Wenn wir uns den Kurs anschauen, dann sehen wir eine periodische Entwicklung. Immer zu den Zeiten des Halvings, also immer wenn die Menge an neuen Bitcoins pro gefundenen Block für die Miner halbiert wurde, steigt der Kurs etwas zeitverzögert stark an. Am Anfang waren es nur wenige Cent, beziehungsweise Dollar, aber relativ waren die Sprünge vergleichbar hoch. Und eine Weile später fällt der Kurs dann wieder heftig, liegt aber nicht dauerhaft unter dem Allzeithoch der Vorperiode. Das ist natürlich nur eine Betrachtung der Vergangenheit und bedeutet nicht, dass es in Zukunft auch so sein wird, aber die Tendenz lässt sich dennoch ableiten. Aus dem Kurs kann man schlussendlich eine Treppe ableiten, die kontinuierlich nach oben führt. Also die langfristige Strategie ist bei Bitcoin bislang extrem erfolgreich.

Was auch sehr wichtig beim investieren ist, ist dass man nur so viel einsetzt, wie man sich auch leisten kann. Es gibt Möglichkeiten Bitcoin gehebelt zu kaufen, also durch Aufnahme von Krediten, doch kann ich nur dringend davon abraten. Wir haben in der Vergangenheit sehr lange Bärenmärkte gesehen, also Zeiten, in denen Bitcoin entweder im Kurs gefallen oder sich nur seitwärts bewegt hat, und wenn dann Kredite bedient werden müssen, kann das in den Ruin führen.

Ganz beliebt ist auch die „Buy the Dip“ Methode (Die Delle kaufen), bei der in einer Phase des Kursrückgangs gekauft und dann nach einem Kursgewinn wieder verkauft wird. Es wird also die „Delle“ gekauft. Das ist, was man unter dem normalen Trading versteht. Vor dieser Methode muss insbesondere in Deutschland gewarnt werden, da solche Gewinne und Verluste zum normalen Einkommenssteuersatz versteuert werden müssen, allerdings der Verlust bis dato auf 20.000 Euro gedeckelt ist. Das bedeutet, dass wenn zum Beispiel innerhalb eines Jahres ein Gewinn von 50.000 € erwirtschaftet wurde und ebenso viel Verlust gemacht, sprich am Ende eine Null-auf-Null-Rechnung raus kommt, dann würde das Finanzamt nur 20.000 Euro Verlustvortrag akzeptieren und es müssten 30.000 € zum Einkommensteuersatz versteuert werden, obwohl das Geld nicht da ist. Das kann ganz hässliche Auswirkungen haben. Aber dazu bitte unbedingt mit einem Steuerberater sprechen, dieses Buch gibt auch in gar keiner Weise steuerlich Beratung. Im Gegensatz dazu sind Erträge aus einem Verkauf nach der Mindesthaltefrist von einem Jahr in Deutschland steuerfrei. Wer also hodelt und nach frühestens einem Jahr verkauft, ist (noch) auf der sicheren Seite und bezahlt keine Steuer.

Ganz wichtig zu beachten ist, dass man nicht nur einseitig investiert und alle Eier in einen Korb legt. Wenn Vermögen aufgebaut werden soll, so ist es sehr zu empfehlen in verschiedene Anlageklassen zu investieren. Als komplementäre Anlage biete sich zum Beispiel physische Gold,

Silber oder Platin an. Von sogenanntem Papiergold, also Gold, das durch Wertpapiere oder Derivate gehandelt wird, rate ich grundsätzlich ab. Auch Aktien oder Rohstoffminen können gute Ergänzungen im Portfolio sein. Dazu bitte ich aber dringend sich mit einem Anlageberater, vielleicht nicht gerade dem von der Hausbank, der nur die eigenen Fonds verkaufen darf, zu unterhalten und so eine individuelle Anlagestrategie zu erarbeiten.

Was auch noch geht, sind Investitionen in Exchange Traded Funds (ETF) und Exchange Traded Notes (ETN). ETFs sind börsengehandelte Investmentfonds, die einem bestimmten Index oder Basiswert folgen. In diesem Fall dem Bitcoin. ETFs können Aktien, Anleihen, Rohstoffe oder andere Anlageklassen abbilden und sind für Privatanleger sehr beliebt, da sie kostengünstig, transparent und in der Regel liquide sind. Bitcoin ETFs wurden jetzt in den USA und Hong Kong zugelassen und werden früher oder später auch in der EU zur Verfügung stehen. Im Falle von Bitcoin ist dies die Anlage, wenn Unternehmen und Gesellschaften investieren wollen, da die ETFs das Problem der Schlüsselverwahrung lösen. Als Privatanleger gibt es keinen wirklichen Anreiz Bitcoin ETFs zu erwerben.

Im Gegensatz dazu sind ETNs börsengehandelte Schuldverschreibungen, die ebenfalls einem Index oder Basiswert folgen. ETNs werden direkt vom Emittenten, meist einer Bank, ausgegeben und sind damit keine kollektiven Investmentvehikel wie ETFs. ETNs bieten Anlegern Zugang zu Anlageklassen, die über traditionelle Fondsstrukturen schwer zu replizieren sind, wie beispielsweise Rohstoffe oder Volatilitätsindizes. Allerdings tragen Anleger beim Kauf eines ETN auch das Ausfallrisiko des Emittenten. Diese Möglichkeit Bitcoin über ETNs zu kaufen existiert in der EU bereits, aber auch ETNs sind für private Menschen keine wirkliche Alternative zum Erwerb von eigenen Bitcoins.

Sowohl ETFs als auch ETNs haben ihre Vor- und Nachteile, die es im Einzelfall sorgfältig abzuwägen gilt. Grundsätzlich bieten beide Produktformen Anlegern eine einfache und kostengünstige Möglichkeit, an der Entwicklung bestimmter Basiswerte zu partizipieren. Anleger sollten sich vor einer Investition jedoch eingehend mit den Charakteristika und Risiken der jeweiligen Produkte vertraut machen.

Auch wenn Bitcoin oft nur als solches gesehen wird, Bitcoin ist keine Anlage oder Spekulationsobjekt nur um seiner selbst willen. Bitcoin hat einen reellen Nutzen, der sich in mannigfacher Form zeigt und vor allem schützt Bitcoin vor der schleichenden Enteignung durch die Inflation. Wer seit 4 Jahren in Bitcoin im Rahmen eines Sparplans investiert hat, auch zu den Zeiten als das letzte All-Time-High war, der ist heute mit sehr hohen Prozentzahlen im Plus und muss beim Verkauf keine Steuern bezahlen. So ist es in der Geschichte von Bitcoin seit Anbeginn. Bitcoin wurde nicht erfunden um schnellen Reichtum zu generieren, sondern um finanzielle Autarkie zu erlangen und Sand ins Getriebe der Geldoligarchie zu streuen.
Aber mal ganz egal wie man investiert und egal was man macht, aber eines sollte man immer beherzigen. Man muss seine Entscheidungen selber treffen und mit denen auch ein gutes Gefühl haben. Ich warne davor sich auf „Expertenmeinungen“ zu verlassen selber aber das volle Risiko zu tragen, insbesondere, wenn sich diese Experten aufdrängen. Es gibt eine Heerschar von Beratern, neudeutsch Influencer, die sehr viel Geld damit verdienen, Andere davon zu überzeugen etwas zu tun, was sie selbst nie machen würden. Augen auf beim Hamsterkauf! Das gilt immer noch uneingeschränkt.
Bitte fragen Sie sich immer und zu jeder Zeit, warum Sie jemand mit irgendeiner Nachricht, Botschaft, Meinung behelligt. Was hat der Gegenüber davon, wenn er sagt, was er sagt und anpreist, was er anpreist. Diese Influencer zum Beispiel bewerben sehr oft alternative Projekte und stellen die Welt in einer Form dar, die es schlicht nicht gibt. Sie werden in den Coins dieser Projekte für

diese Werbung bezahlt und verursachen durch ihre positive Berichterstattung eine künstliche Nachfrage. Sobald der Kurs entsprechend ist, verkaufen die Projektentwickler und Influencer, der Kurs stürzt ab und den Schaden tragen die, die das zu spät mitbekommen haben.
Das heißt aber nicht, dass man nicht in irgendwelche Projekte investieren kann, ganz und gar nicht. Es bedeutet nur, dass die alte Weisheit angewendet werden sollte und kein Geld in Dinge investiert werden soll, die man nicht versteht. Das gilt nicht nur bei Kryptowährungen, sondern bei allen anderen Anlagen auch. Keine Ahnung von Gold – Finger weg von Gold; keine Ahnung von Optionsscheinen – Finger weg von Optionsscheinen. Ganz einfach.
Auch ein sonderbares Phänomen ist, wenn bekannte Personen, wie zum Beispiel Elon Musk, immer mal wieder reichster Mensch der Welt und Gründer von Tesla und Space X, sich zu Kryptowährungen äußern und damit heftige Kursbewegungen erzeugen. Von Derartigem sollte man sich einfach frei machen. Zum einen sind das auch nur Menschen und zum anderen haben diese eben auch Interessen. Ich kann es nur betonen. Wenn man sich eine Strategie zurecht gelegt hat und zum Beispiel in einen Sparplan investiert, dann sollte man dies einfach so weitermachen, egal was die Welt ringsherum so alles sagt und meint.
Und jetzt muss natürlich die Frage beantwortet werden, was der Autor für ein Motiv hat, dieses Buch zu schreiben. Ganz einfach. Ich bin selbst von Bitcoin überzeugt und glaube daran, dass viele Menschen diese Vorteile sehen sollten. Je mehr verstehen, wie kaputt und korrupt das derzeitige Geldsystem und damit unweigerlich auch das gesellschaftliche und politische System ist, desto schneller kann in diesen Gebieten eine Heilung einsetzten. Wie die aussieht weiß ich nicht und will ich auch gar nicht postulieren, aber ich weiß, dass alles auf Geld und Wert beruht und das bedeutet, dass wir das Fundament reformieren müssen, bevor wir uns mit irgendwelchen anderen Dingen beschäftigen können. Und eine Technologie zu verstehen, sie vielleicht sogar erklären zu können, ist auf jeden Fall auch ein guter Einstieg um sein Lebensunterhalt zu verdienen.

Ich hodle!

Es gibt eine interssante und humorvolle Anekdote aus den frühen Tagen des Bitcoin-Booms wie der Begriff „Hodl“ geprägt wurde.

Im Jahr 2013 schrieb ein anonymer Bitcoin-Nutzer mit dem Pseudonym "GameKyuubi"[61] in dem Bitcoin-Forum Bitcointalk einen legendären Beitrag mit dem Titel "I AM HODLING". Darin beschrieb er, wie er betrunken am Wochenende Bitcoin-Transaktionen tätigte und dann am Montag beschloss, seine Bitcoins einfach zu "halten".

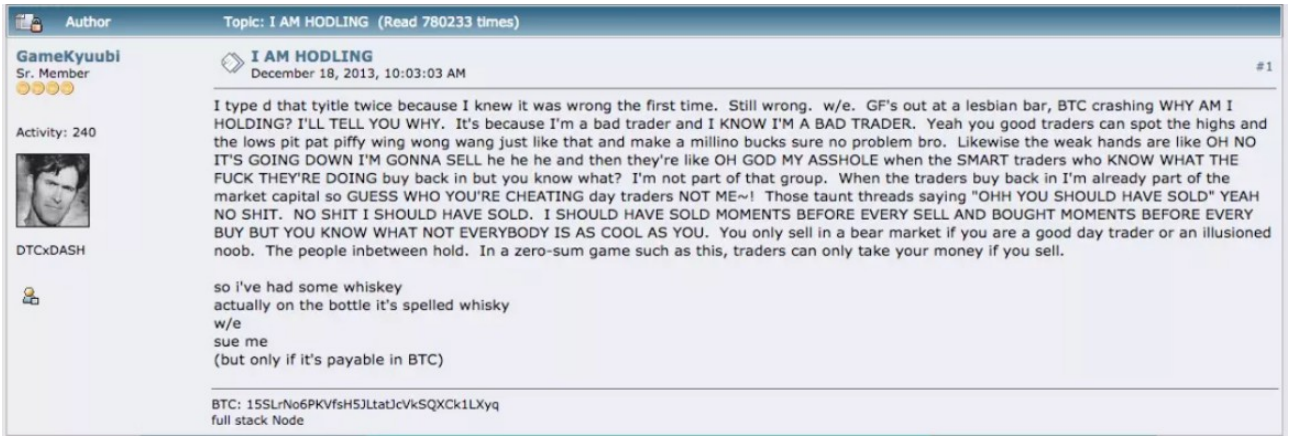
Der Beitrag war voller Rechtschreib- und Grammatikfehler, was dem Ganzen eine noch humorvollere Note verlieh. Das Wort "HODL" war zunächst nur ein Tippfehler für "HOLD" (englisch: to hold - halten), wurde aber schnell zu einem festen Begriff in der Kryptowelt.

Der anonyme Autor erklärte, dass er bewusst "HODLING" schrieb, da er nicht verkaufen wollte, egal wie stark der Preis schwankte. Für ihn war es wichtiger, seine Bitcoins langfristig zu halten, anstatt auf kurzfristige Gewinne zu spekulieren.

Dieser einfache, aber prägnante Beitrag traf einen Nerv in der Krypto-Community. "HODL" wurde schnell zu einem Mantra für Investoren, die an den langfristigen Erfolg von Kryptowährungen glaubten. Der Begriff steht seitdem für geduldiges, emotionsloses Halten von Kryptowerten, unabhängig von Kursschwankungen.

Obwohl der Verfasser des Beitrags anonym blieb, wurde "HODL" zu einem festen Bestandteil der Krypto-Kultur und erinnert Anleger bis heute daran, in stürmischen Zeiten Ruhe zu bewahren.

61 GameKyuubi am 18.12.13 um 10:03 Uhr auf bitcointalk.org


Author | Topic: I AM HODLING (Read 780233 times)

GameKyuubi
Sr. Member
Activity: 240
DTCxDASH

I AM HODLING
December 18, 2013, 10:03:03 AM
#1

I type d that tyitle twice because I knew it was wrong the first time. Still wrong. w/e. GF's out at a lesbian bar, BTC crashing WHY AM I HOLDING? I'LL TELL YOU WHY. It's because I'm a bad trader and I KNOW I'M A BAD TRADER. Yeah you good traders can spot the highs and the lows pit pat piffy wing wong wang just like that and make a millino bucks sure no problem bro. Likewise the weak hands are like OH NO IT'S GOING DOWN I'M GONNA SELL he he he and then they're like OH GOD MY ASSHOLE when the SMART traders who KNOW WHAT THE FUCK THEY'RE DOING buy back in but you know what? I'm not part of that group. When the traders buy back in I'm already part of the market capital so GUESS WHO YOU'RE CHEATING day traders NOT ME~! Those taunt threads saying "OHH YOU SHOULD HAVE SOLD" YEAH NO SHIT. NO SHIT I SHOULD HAVE SOLD. I SHOULD HAVE SOLD MOMENTS BEFORE EVERY SELL AND BOUGHT MOMENTS BEFORE EVERY BUY BUT YOU KNOW WHAT NOT EVERYBODY IS AS COOL AS YOU. You only sell in a bear market if you are a good day trader or an illusioned noob. The people inbetween hold. In a zero-sum game such as this, traders can only take your money if you sell.

so i've had some whiskey
actually on the bottle it's spelled whisky
w/e
sue me
(but only if it's payable in BTC)

BTC: 15SLrNo6PKVfsH5JLtatJcVkSQXCk1LXyq
full stack Node

Abbildung 22: Screenshot der Originalnachricht zum Hodln

Die Übersetzung:

Ich Hodl

Ich habe diese Überschrift zweimal getippt, weil ich beim ersten mal wusste, dass ich mich vertippt hatte. Immer noch falsch, aber egal Wochenende.
Meine Freundin ist in einer Lesben-Bar unterwegs und der Bitcoin ist total abgestürzt.
WARUM HALTE ICH? ICH SAG EUCH WARUM. Der Grund ist ich bin ein schlechter Händler und ich weiß, dass ich ein schlechter Händler bin. Ja, ihr tollen Händler, könnt einfach so mir nichts dir nichts erkennen wann wir uns auf einem Hoch- und wann in einem Tiefpunkt befinden und einfach so ne' Million machen – kein Problem Bruder.
Die sogenannten „Schwachen Hände" agieren auf die gleiche Weise und machen sich ständig Gedanken wie „OH MEIN GOTT, ALLES FÄLLT, ICH MUSS VERKAUFEN". Hihihi… und wenn dann die KLUGEN Händler, DIE WISSEN WAS SIE TUN, wieder beginnen einzusteigen und zu kaufen, brennt den schwachen Händen wieder das Arschloch.
Ich gehöre nicht zu dieser Gruppe. Wenn die Händler anfangen einzukaufen bin ich bereits ein Teil des Marktes also ratet mal WEN DIESE ECHTZEITHÄNDLER DANN ABZOCKEN? MICH NICHT!
Diese höhnischen Kommentare á la "OHH DU HÄTTEST VERKAUFEN SOLLEN". JA, ACH WAS? KEIN SCHEISS, ICH HÄTTE VERKAUFEN SOLLEN. ABER ICH WEISS, DASS NICHT JEDER SO COOL IST WIE DU".
Während eines Bärenmarktes verkaufst du nur, wenn du ein guter Händler oder ein desillusionierter Neuling bist. Alle Leute dazwischen halten ihre Bitcoins einfach. In einem Nullsummenspiel wie diesem, können dir die Händler nur dann dein Geld wegnehmen, wenn du auch tatsächlich verkaufst.

Ja ich hatte einige Gläser Whiskey.
Eigentlich steht auf der Flasche sogar Whisky. Wochenende eben. Verklagt mich doch.
(Aber nur wenn in BTC bezahlt werden kann).

Bitcoin vs. Altcoins

Satoshi Nakamoto hat Bitcoin und damit die Technologie der Blockchain erfunden. Aus dieser Erfindung ergeben sich sensationelle Vorteile, aber auch Limitierungen. Damit eben die Nachteile „ausgemerzt" werden und alles viel besser und schöner wird, haben mittlerweile unzählige eifrige Menschen Alternativen zu Bitcoin entwickelt und tun dies jeden Tag. Die genaue Zahl der Projekte

kennt niemand mehr. Schätzungen gehen von über 20.000 aus. Bei CoinMarketCap[62] werden derzeit fast 10.000 gelistet und hier kann nicht und soll auch gar nicht auf die einzelnen Projekte eingegangen werden. Um es gleich vorweg sehr klar zu sagen, die allermeisten der alternativen Projekte/Coins haben keinen Nutzen, machen nichts besser und sind schlicht Betrug. Aber es gibt auch Projekte, die wirklich einen Mehrwert schaffen wollen und dies teilweise auch tun. Und es sind diese Projekte, die bis weilen gute Ideen entwickeln, welche dann von Bitcoin adaptiert werden könnten um technische Grenzen, die Bitcoin fraglos noch hat, zu überwinden. Es stellt sich also für mich nicht die Frage welches Projekt, welches Netzwerk das beste ist und was gar nicht geht, sondern wir können einer Evolution, einer Entwicklung, zuschauen und am Schluss, davon bin ich fest überzeugt, wird Bitcoin als die erste und bekannteste Krytowährung alle anderen Projekte weit hinter sich lassen, beziehungsweise deren Untergang verursachen. Ein Beispiel sind die Smart Contracts, also die deterministischen Verträge, die einem Wenn-Dann-Prinzip folgen. In der Urversion von Bitcoin waren diese nicht vorgesehen, wurden aber ab 2014 durch Erweiterungen in rudimentärer Form in den Code aufgenommen. Bitcoins stärkster Konkurrent, Ethereum, hat diese Technologie viel stärker implementiert und stellt mit das ausgeprägteste Smart Contract System zur Verfügung. In letzter Zeit ist das Projekt Solana, das auf Smart Contracts spezialisiert ist und eine breite Programmiersprachenbasis unterstützt, modern geworden. Gerade dieses Thema ist für Unternehmen in der Zukunft wirklich ein Feld, welches es auszuloten gilt. Sollte es in Zukunft tatsächlich einen breiten Markt für diese Art der Anwendung geben, wird dies in Bitcoin, vielleicht auch über eine weitere Schicht, facettenreicher implementiert werden, aber mit dem Vorteil, dass Bitcoin im Gegensatz zu seinen Mitbewerbern, auf dem Proof-of-Work-Prinzip beruht und eine absolut integre Datenstruktur aufweist. Es ist geradezu verrückt, was alle machbar sein könnte, wenn es nur den wirklichen Bedarf dafür gibt, denn eines muss uns klar sein. Auch durch sein Gebührenmodel, aber eben hauptsächlich durch gewollte technische Beschränkungen, kann man Bitcoin nicht mit unsinnigem Müll verstopfen und die Datenbank überfrachten. Die Anwendungsfälle, die wirklich in die „Königsklasse“ aufgenommen werden wollen, müssen einen tatsächlichen Nutzen haben und leider gibt es den bei sehr vielen Projekten nicht, oder besser nicht so, als es sich dafür wirklich lohnt wertvolle Ressourcen zu verbrauchen.

Aber jedem ist es natürlich selbst anheim gestellt, sich mit anderen Projekten und deren Fähigkeiten zu befassen und ganz ehrlich, der eine oder andere Altcoin hat auch kurzfristig eine bessere Performance an der Börse. Auf die lange Sicht aber wird es nach meiner festen Überzeugung nur ein lebensfähiges Projekt geben und das wird Bitcoin sein. Die Bitcoiner sprechen bei den alternativen Projekten auch oft von Shitcoins, also „scheiß Coins“. Abgesehen von den auf Betrug angelegten Projekten ist das aber keine, wie ich finde, zulässige Bezeichnung. Das sind andere Gedanken und andere Ziele und nur die Gesellschaft an sich und der Markt werden zeigen wessen Ideen gut und wessen Ideen nicht so gut sind. Absolut basisdemokratisch.

Bitcoin in der (Geo)politik

Politik und vor allem Geopolitik impliziert immer den Krieg, also das Szenario, dass sich wie kein anderes gegen die einzelnen Menschen richtet. Mit Krieg kommt Hunger, Vertreibung, Vergewaltigung, Zerstörung, Tod und Verderben. Nicht umsonst ist Krieg das schlimmste Verbrechen, dass die Weltgemeinschaft in Form der UN Charta kennt. Und sonderbarerweise schwadronieren die, die die meisten Kriege führen immer am lautesten vom Frieden, oder in der letzten Pervertierung von Sinn, vom letzten Krieg damit es Frieden geben kann. In einem Kriegsszenario werden alle sogenannten menschlichen Werte durch die Regierungen der kriegführenden Staaten aufgehoben und ins Gegenteil verkehrt. Auf einmal wird es richtig und erstrebenswert zu töten, zu verstümmeln und es ist gerechtfertigt Bomben auf Kinder, Frauen, Alte

62 CoinMarketCap -https://coinmarketcap.com

und Kranke zu werfen. Die Perversion dieses Zustandes ist gar nicht in Worte zu fassen und spiegelt den mentalen Zustand von Staatschefs und ihrer Generäle wieder.

„Stell Dir vor es ist Krieg und niemand geht hin.“ Dieser Spruch stammt aus der Friedensbewegung der 80er Jahre und ist heute leider wieder sehr akut geworden. Richtiger Krieg ist im Grunde nur in einer Fiat-Welt möglich, da Krieg derartig viele Ressourcen verschlingt, dass so etwas nur durch das Gelddrucken finanzierbar ist. In einer Bitcoinwelt müsste dieser Spruch heißen: „Stell Dir vor jemand will Krieg und kann ihn nicht bezahlen.“ Das gilt aber auch für das Militär an sich. Wenn wir uns heute anschauen, wie viel Geld in die Rüstung und Militär im Allgemeinen gesteckt wird, ohne dass irgendein substanzieller Nutzen entsteht. Um in der Welt von Bitcoin Krieg zu führen oder diesen vorzubereiten muss das Volk ausgequetscht werden, denn erst muss das Geld da sein und dann können Waffen und Soldaten bezahlt werden. Und diese einfache Umkehrung würde bewirken, dass es keine Erweiterung der NATO so gegeben hätte, dass kein nukleares Wettrüsten jemals möglich gewesen wäre. All diese widerlichen Zustände, die uns als normalen Bürger als so etwas wie Gott gegeben verkauft werden, sind mit Bitcoin nicht machbar, denn diese Bürger wären schon längst auf den Barrikaden, müssten sie diese menschenfeindlichen Dinge wirklich bezahlen. Das geht nur, in de man die Bürger durch Geldmengenausweitung und damit Inflation heimlich beraubt und Reichtümer aus anderen Teilen der Welt durch das Geldsystem abzapft. Übrigens in der Grafik sind die jährlichen Militärausgaben aufgezeigt, nicht die seit dem 2. Weltkrieg oder so. Unvorstellbare Summen werden von einer skrupellosen und maximal korrupten Schicht zum eigenen Vorteil missbraucht. Dabei ist Krieg nur die drastischste und menschenverachtenste Art und Weise das Geld und damit die Leistung der Bürger in die Taschen der Reichen und Superreichen umzuverteilen. Mit der grassierenden Krankheit haben wir gesehen, dass dies auch durch die Pharmaindustrie gut bewerkstelligt werden kann. Beliebt sind auch alle Public Private Parntership-Projekte (PPP) in denen staatliche, hoheitliche Leistungen durch die Mitfinanzierung von Unternehmen in gewinnorientierte Projekte verwandeln, die dann, einem Schaufelrad gleich, Geld von Fleißig nach Reich transportieren. Das Muster ist immer Angst und der vermeintliche Schutz, den der Staat zur Verfügung stellt oder die Dringlichkeit und die höhere Kompetenz der Privatunternehmen. Auf jeden Fall wird dem Bürger, dem Wähler, dem Untertan immer ein Zustand der Entscheidungsnot vorgegaukelt, der keinen Aufschub duldet. All das ist durch Bitcoin nicht möglich.

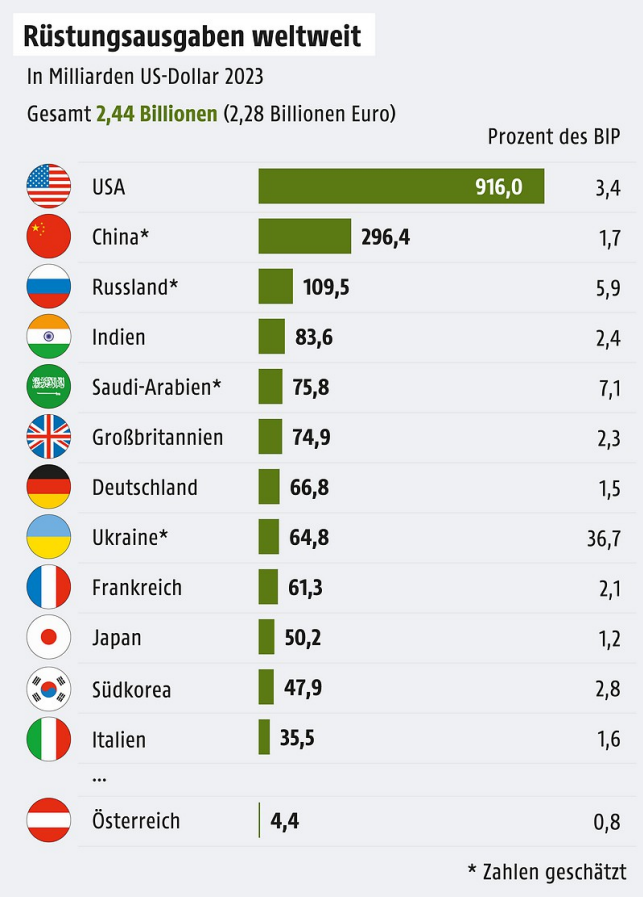


Abbildung 23: Militärausgaben im Vergleich der Nationen. Quelle orf.at

Wie sähe ein Staat aus, in dem der Bitcoinstandard gelten würde? Ganz einfach. Der Staat würde sich auf seine Kernaufgaben beschränken und alles andere unterliegt einem freien Markt. Vielleicht nicht ganz so radikal wie sich das der eine oder andere Libertäre wünschen würde, aber dieser

aufgeblähte und überbordende Staatsapparat würde durch die Bürger nicht finanziert werden, oder wäre gar nicht zu leisten. Wolfang Schäuble hat 1982 zum ersten mal den Ausspruch getan, „Was eine schwäbische Hausfrau mit den Staatsfinanzen machen würde, sollte auch für die Bundesregierung gelten.“ Nun ist er niemand, der sich selbst je daran gehalten hätte und schon gar nicht in seiner Zeit als Finanzminister, aber genau das wäre dann das Programm des Staates. Man kann nur so viel ausgeben, wie man einnimmt und man kann nur soviel einnehmen, wie die Bürger bereit sind zu bezahlen. Wahlgeschenke die durch Kredite finanziert werden müssen, wie die Rentenerhöhungen oder dieses sogenannte Bürgergeld in Deutschland sind dann einfach nicht mehr machbar. Ein Land, in dem Bitcoin das Zahlungsmittel ist, in dem kann es keinen ausufernden Sozialstaat geben, schlicht weil die anderen Bürger das nicht tragen wollen. In einem so geartetem Staat haben die Bürger wieder Verantwortung für sich selbst und Generationen, die sich auf Sozialleistungen ausruhen, sind nicht denkbar. Das heißt aber nicht, dass Kranken und Schwachen nicht geholfen werden würde. Ich glaube niemand würde sich bei wirklich Bedürftigen ausnehmen. Nur der Missbrauch wäre extrem schwer. Übrigens das Argument, dass man die Bürger dazu zwingen kann überproportionale Steuern abzugeben funktioniert mit Bitcoin auch nicht so richtig. Klar wird es immer einen Sockel von Menschen geben, die ihren Heimatort nicht verlassen wollen, aber mit Bitcoin kommt ein ähnliches Steuersystem wie in der Schweiz, in der jeder Kanton seine Rahmenbedingungen selbst festlegt und um Einwohner mit den anderen Kantonen konkurriert. Bei Menschen mag das nicht so ausgeprägt sein, aber bei Unternehmen, die eine sehr viel höhere Steuerlast tragen sehr wohl.

Wir sehen also, dass es für heutige Politiker herzlich wenig Anreiz gibt sich mit Bitcoin zu befassen, ist dieses System doch so fundamental gegensätzlich zu dem, was diese Damen und Herren in ihren Parteikarrieren so alles gelernt haben. Man stelle sich einmal vor, was Politiker wie Joe Biden, Olaf Scholz, Rishi Sunak, Giorgia Meloni oder Emmanuel Macron ohne die Modern Money Theory (MMT), also das ungebremste Gelddrucken machen würden. Wenn es nicht mehr reicht die dummen Bubenspiele weiterzutreiben und ganze Volkswirtschaften durch Inkompetenz zu versenken. Mit einem harten Geld wie Bitcoin, sind solche Scharlatane über Nacht bloß gestellt und müssten sich für ihre Unfähigkeit rechtfertigen. Aber sehr wahrscheinlich wären solche Menschen auch nicht so weit nach oben auf der politischen Karriereleiter gekommen, wären die Maßstäbe vernünftig angelegt.

Auch das gesellschaftlich Bild wird sich mit der breiten Akzeptanz von Bitcoin stark verändern. Dadurch, dass die Bürger nicht mehr „durch die Hintertür“ jeden Tag bestohlen werden, fällt auch die Notwendigkeit weg, dass zum Beispiel in einer Familie beide Ehepartner arbeiten müssen und Kinder wieder von ihren Eltern, insbesondere von ihren Mütter betreut werden können. Das darf man bitte nicht falsch verstehen. Ich propagiere nicht, dass die Frau an Heim und Herd gehört, ganz im Gegenteil, aber was heutzutage unter der Überschrift Emanzipation verkauft wird, ist nichts anderes als Sklaverei. Heutige Familien sind, ohne zu pauschal werden zu wollen, ist einer wirklich beklagenswerten Situation, sind sie doch überproportional von Armut bedroht. Wenn eine Frau Karriere machen möchte, dann nur zu und die besten Wünsche, aber wenn sie es muss, oder schlimmer noch wenn sie gezwungen wird mitzuverdienen, damit es über den Monat reicht, so hat das rein gar nichts mit Emanzipation zu tun; das ist dann Ausbeutung. Und es ist auch vollkommen gleichgültig, wer sich um die Kinder kümmert, ob Mutter oder Vater, Hauptsache es ist nicht die staatliche Betreuung in der Krippe und Kindergarten oder die Kinder müssen ständig zu Omas und Tanten abgeschoben werden. Ich finde, dass das Aufziehen seiner Kindern eine persönliche und gesellschaftliche Herkulesaufgabe ist und dafür muss man jedem und jeder, die diesen Weg gehen höchsten Respekt zollen. Diese Eltern erbringen mit den größten gesellschaftlichen Nutzen.

Wenn der massive ökonomische Druck von Familien genommen wird, können wieder glückliche und gesunde Kinder aufwachsen, die Halt und Sicherheit im Leben haben. Die Verhaltensforschung

hat unzählige Studien[63] [64]veröffentlicht, in denen sehr klar beschrieben wird, wie wichtig eine feste Bindung zwischen Eltern und Kindern und in der Familie an sich ist. Wir dürfen uns nichts vormachen, die Zerschlagung der Familien hat den Staaten erst diesen immensen Einfluss in den Köpfen der Menschen gebracht. Spätestens seit den 1980er und 1990er Jahren, als es geradezu Pflicht wurde seine Kinder unter einem Jahr schon in die Fremdbetreuung zu geben, ist die Flut an leicht manipulierbaren Kindern extrem angeschwollen[65]. Nur so kann man wirklich erklären, wie die Normopathie[66] in unseren Gesellschaften derartig Einzug gehalten hat. Und dieser Effekt verstärkt sich durch sich selbst. Für die Obrigkeit ist das wohl sehr erstrebenswert, aber die Individuen zerbrechen über kurz oder lang an einem solchen System, wie die Sowjetunion zum Beispiel deutlich zeigt. Und das ist keine übertriebene Parallele. Erziehungs- und gesellschaftspolitisch hat sich zumindest Westeuropa und Nordamerika genau so entwickelt, wie die UdSSR. Bitcoin kann hier eben auch durch den Wegfall des ökonomischen Drucks mehr Menschen dazu bringen wieder in sozial gesunden Strukturen zu leben und so auf die lange Sicht die Gesellschaft zu heilen.

Wir müssen noch einen Punkt ansprechen, der sich mit Politik und Bitcoin befasst, nämlich die Adaptionsgeschwindigkeit. Durch die heutige technische Limitierung können sich nicht alle Menschen über Nacht eine Bitcoin-Wallet holen. Aktuell können im Hauptnetzwerk zwischen 5 bis 7 Transaktionen pro Sekunde gemacht werden. Bei gerechnet 7 Milliarden Menschen dauert dieser Prozess des Onbordings, also der Aufnahme ins System, zirka 50 bis 100 Jahre, je nachdem wie viele Anfragen pro Block zugelassen werden und an der Stelle, an der Andere dies kritisieren und als Problem aufbauschen, sage ich, dass es ein Segen ist, denn nur so ist gewährleistet, dass die Geschwindigkeit der Umstellung auch von den Menschen angenommen und verstanden werden kann. Nichts wäre schlimmer als eine Revolution, was uns die bereits erlebten Revolutionen mehr als drastisch vor Augen halten. Auch wenn der Gedanke verlockend ist und wir immer alles gleich und sofort haben möchten, aber auf dem Weg in ein wirklich neues System müssen alle mitgenommen werden und dieser Prozess bedarf sehr viel Zeit, gerechnet in Generationen. Insbesondere die westlichen Gesellschaften sind heute dermaßen von der Politik und politischen Prozessen entfernt, entfremdet und auch ausgeschlossen, dass es wirklich eine Herkulesaufgabe wird, sie zu bilden und das Verständnis für den heutigen falschen Weg zu schaffen. Und nur wenn dies gelingt, und ja, es wird gelingen, ist es nachhaltig sinnvoll politische Zustände aufzulösen und durch neue, bessere Systeme zu ersetzen. Alle großen politischen Umwälzungen, die wir in den letzten 300 Jahren gesehen haben wurden von diversen Rädelsführern angeführt und vorgedacht. Der einzelne Mensch wurde immer als zu dumm und zu phlegmatisch postuliert und aus den gesamten politischen Prozessen ausgeschlossen. Diese Revolutionen in Frankreich, Deutschland, Iran, Mexiko, Chile, Russland, Haiti, Cuba, China, Bolivien und sonst irgendwo auf der Welt sind gescheitert. Das ist ein Fakt und der Grund liegt einzig und alleine darin, dass es den Menschen aufgezwungen wurde. Eine wirkliche Revolution kann, so bin ich fest überzeugt, nur aus der Gesellschaft selbst heraus erwachsen und muss sich zwingend in den Köpfen der Menschen selbst bilden. Nur wer versteht, wie heute manipuliert und betrogen wird, wird den Sinn und die Notwendigkeit für Veränderungen auch langfristig mittragen. Und wer versteht, mit welchen Methoden heute gegen die Menschen gearbeitet wird, wird neue Wege finden, wie ein gedeihliches Miteinander überhaupt möglich ist und der Rückfall in die alte Struktur in neuem Gewand

63 "The Importance of Early Attachment: Security of Attachment at Age 1 Predicts Children's Mental Health at Age 15" Autoren: Sroufe, L. A., Egeland, B., Carlson, E. A., & Collins, W. A.

64 "The Long-Term Effects of Early Childhood Relationships on Developmental Outcomes" Autoren: Sroufe, L. A., Carlson, E. A., Levy, A. K., & Egeland, B.

65 "The Effects of Early Childcare Attendance on Child Cognitive and Socio-Emotional Outcomes" Autoren: Belsky, J., Vandell, D. L., Burchinal, M., Clarke-Stewart, K. A., McCartney, K., Owen, M. T. & the NICHD Early Child Care Research Network

66 Normopathie bezeichnet eine übertriebene Anpassung an gesellschaftliche Normen und Erwartungen, die zwar Stabilität und Ordnung fördern, jedoch die individuelle Entfaltung und den gesellschaftlichen Wandel behindert.

verhindert werden kann. Dieser Prozess kann nur durch Aufklärung und Wissensvermittlung, ohne ideologische Beschränkungen erfolgen. Die beste Art zu lernen ist, ein Angebot in Form von neutraler Information zu machen und die absolut freie Entscheidung beim Lernenden zu belassen, ob und wie die Information aufgenommen wird. Heute wird nur durch Zwang gelernt, beziehungsweise indoktriniert. Wer nicht nachbetet, was ein Lehrer in der Schule, ein Professor in der Universität sagt, wird umgehend dafür abgestraft. Wer in der Öffentlichkeit eine andere als die Regierungsmeinung vertritt, wird sozial und wirtschaftlich vernichtet. Das konfuzianische Sprichwort „Strafe einen, um tausend zu belehren.“ wurde nicht nur im maoistischen China sehr wörtlich genommen, sonder ist heute eines der meistverwendeten direkten Machtmittel weltweit. Die erste Lektion, die ein jeder erst mal wieder lernen sollte, ist dass es richtig und gut ist zu lernen und Wissen wertvoll ist.

Wenn wir nochmals den unsäglichen Gedanken an Krieg aufnehmen wollen, dann ist auch klar, dass ein Staat, der schon auf Bitcoin umgestellt hätte und sich einem anderen gegenübersieht, in dem das Fiatsystem weiter vorherrscht, das Bitcoin basierte System dramatisch unterlegen wäre und dieses System könnte sich nur, durch Zusammenschluss mit anderen Staaten und unter Aufbietung wirklich aller Reserven der Bevölkerung, wehren. Das Bitcoin System könnte nur durch immense Abgaben und durch heftige Kreditaufnahme in fremder Fiatwährung seinen Überlebenskampf ausfechten. Dies ist ein Grund mehr, warum die offizielle Umstellung so behutsam und langsam wie möglich durchgeführt werden muss. Im besten Fall parallel auf der ganzen Welt, respektive in den großen Wirtschaftsnationen. Je breiter die mentale Basis, desto größer sind die Chancen, dass die Welt ein wirklich besserer Ort wird.

Man kann sich das heute vielleicht noch nicht so konkret vorstellen, aber durch das Verstehen von Bitcoin werden sich die Menschen fundamental ändern und daraus folgt unweigerlich, dass sich auch die politischen Verhältnisse ändern werden. Dabei bleibt wirklich zu betonen, dass dieser Prozess langsam und in der Breite geschehen muss, denn wir alle wollen nicht im Chaos enden, wir wollen keine Konfrontation, keine sinnlose Zerstörung. Wir wollen keinen Krieg.

Gedanken

Wenn wir ein Fazit aus dem bisher gesagten ziehen wollen, so ist es vielleicht, dass Bitcoin nicht alles, aber sehr vieles besser machen kann und es an jedem Einzelnen liegt, ob und wie er oder sie sich entscheidet. Es gibt für niemanden einen immanenten Druck jetzt und sofort eine Entscheidung für heute und immerdar zu fällen. Jeder kann sich wirklich so viel Zeit nehmen, wie gebraucht wird, um die Zustände heute zu erkennen, zu verstehen und für sich den besten Weg zu finden. Dabei ist es vollkommen gleichgültig wer Bitcoin propagiert oder sich dagegen stellt. Bitcoin wird dies alles überstehen und braucht auch keine Unterstützer und Steigbügelhalter. Das Ökosystem ist mittlerweile so groß geworden, dass es nach menschlichem Ermessen unmöglich ist Bitcoin zu stoppen und die einzige Entscheidung, die ein jeder für sich treffen muss, ist nur wann er oder sie dazustößt.

Bitcoin hat fantastische und einzigartige Eigenschaften was ihn zu einem wirklich neuen und für die Menschheit an sich wegweisenden Hilfsmittel macht die Fehlstellungen, die sich im Laufe der Geschichte angesammelt haben und die immer wieder in schlimmen oder gar desaströsen Szenarien endeten, zu heilen und den Teufelskreis von Unterdrückung und Gewalt, Ausgrenzung und Verelendung endlich zu durchbrechen. Bitcoin ist und macht frei. Bitcoin ist fair und intrinsisch gerecht. Bitcoin ist vollkommen neutral. Bitcoin nimmt jeden an und mit. Mit Bitcoin wird ein seriöser und nachhaltiger Umgang mit dem Planeten geradezu erzwungen, da alles andere nicht ökonomisch ist und auf lange Sicht dem Untergang geweiht. Auch zeigt Bitcoin den zwingenden Umstand auf, die Welt wieder zu regionalisieren, da globale Strukturen nicht effizient sind und wiederum einen massiven ökonomischen Nachteil in sich bergen. Das Subsidiaritätsprinzip,

welches bereits in vielen Verfassungen der Nationen verankert ist, aber immer und überall ausgehebelt wird, besagt, dass die kleinste Einheit die größte Entscheidungsmacht haben sollte und Bitcoin zeigt auf, wie ein vollkommen globales System die Menschen genau darin unterstützt in regionalen Kreisen und Strukturen zu denken und zu handeln, dabei aber einen globalen Ansatz zu bewahren und für jeden Punkt eine Anbindung an die gesamte Welt zu schaffen. Bitcoin kann von jeder Denkschule angenommen werden, denn es gibt keine Vorbehalte was Religion, Geografie, Nationalität, ethnische Herkunft oder sonstiges, was sich die Menschen über Jahrtausende ausgedacht haben um zu spalten, anbelangt. Jeder, mit jeder Hautfarbe, jedem Glauben, an jedem Ort in jeder Sprache kann ein Teil von Bitcoin werden und wird es früher oder später auch werden.

Bitcoin wird weiter wachsen und sich ausbreiten, Menschen begeistern und Existenzen sichern. Das ist nach meinem dafürhalten unabdingbar. Keine Macht der Welt kann Bitcoin mehr aufhalten. Und je restriktiver die Machtsysteme werden, desto schneller werden die Menschen, nicht vielleicht im sogenannten Wertewesten, aber die globale Mehrheit sehr wohl, die Vorteile von Bitcoin für sich nutzen. Bitcoin ist sehr resilient, wie seine erst nur 16-jährige Geschichte sehr eindrücklich zeigt und die Gefahr, dass ein Billionenwert irgendwie verboten oder abgeschaltet werden könnte ist absurd. Es mag vielleicht noch sehr lange dauern und wer weiß ob Sie und ich den Tag des endgültigen Durchbruchs von Bitcoin noch erleben werden, aber dieser Tag wird kommen. Und bis dahin versuchen wir unsere Kaufkraft zu sichern und jedem der offen dafür ist von diesem tollen Ding zu erzählen, das sich da Bitcoin nennt.

Eins ganz zum Schluss noch. Das sind alles meine Gedanken, die ich mir gemacht habe, basierend auf den mir zur Verfügung stehenden Quellen und die können natürlich auch falsch sein. Ich beschwöre also jeden selbst zu prüfen, zu hinterfragen und den Fehler von Bitcoin zu suchen und falls es einen gibt, mir umgehend Bescheid zu sagen.

In diesem Sinne – Venceremos!

Übersetzungen

Hier beginnt nun das Nachschlagewerk, um dieses ganze Fachchinesisch welches Bitcoin unweigerlich mitbringt alphabetisch einsehen zu können. Bitcoin selbst ist schon schwer genug zu verstehen und daher muss über die ganzen Fachbegriffe Klarheit herrschen, wenn wir Bitcoin wirklich verstehen wollen. Die meisten der aufgeführten Worte kommen in diesem Buch gar nicht vor, aber wer sich mit Bitcoin beschäftigt wird unweigerlich auf diese Begriffe und Redewendungen stoßen und dann ist es gut zu wissen, was das alles bedeutet.

2FA -2FA (Two Factor Authentification), zu deutsch Zwei Faktor Authentifkation, ist eine zusätzliche Sicherheitsmaßnahme, die neben Ihrem Benutzernamen und Passwort noch einen zweiten Authentifizierungsschritt erfordert. Dadurch wird Ihr Konto deutlich besser vor unbefugtem Zugriff geschützt. Dieses Verfahren wird von den meisten Börsen verlangt.
Der Ablauf ist wie folgt:

- Anmeldung mit Benutzernamen und Passwort
- Zusätzlich wird ein einmaliger Bestätigungscode angefordert, den Sie über ein zweites Gerät, wie Ihr Smartphone, erhalten.
- Eingabe des Bestätigungscodes, um die Anmeldung abzuschließen.

Dieser zweite Verifizierungsschritt kann auf verschiedene Arten erfolgen:

- Per SMS oder Anruf auf Ihr Mobiltelefon
- Über eine spezielle 2FA-App wie Google Authenticator oder Microsoft Authenticator
- Mit einem Hardware-Sicherheitsschlüssel

Per Push-Benachrichtigung auf Ihrem Smartphone

Der Vorteil liegt auf der Hand: Selbst wenn jemand Ihr Passwort knackt, kann er ohne den zusätzlichen Code nicht auf Ihr Konto zugreifen. 2FA erhöht also die Sicherheit Ihrer Konten enorm.
Die meisten Online-Dienste, wie E-Mail-Konten, Bankkonten oder Social-Media-Plattformen, bieten mittlerweile 2FA an.
Aber wo Licht ist, ist auch Schatten. Die Nachteile von 2FA liegen auf der Hand.

- Zusätzlicher Aufwand: Die Verwendung von 2FA erfordert einen zusätzlichen Schritt im Anmeldeprozess, was für manche Nutzer als lästig empfunden werden kann. Das kann die Benutzererfahrung beeinträchtigen.
- Verlust des zweiten Faktors: Wenn der Nutzer den zweiten Faktor, wie z.B. das Mobiltelefon, verliert oder beschädigt, kann er u.U. nicht auf sein Konto zugreifen. Das kann sehr frustrierend sein.
- Komplexität: Für weniger technikaffine Nutzer kann die Einrichtung und Verwendung von 2FA eine Herausforderung darstellen. Das kann zu Problemen und Frust führen.
- Abhängigkeit von Mobilfunknetzen: Wenn der zweite Faktor über eine Mobilfunk-App funktioniert, kann der Nutzer im Falle eines Netzausfalls oder Roamings Probleme beim Anmelden haben.
- Datenschutzbedenken: Einige Nutzer sorgen sich um die Sicherheit und Datenschutzaspekte, wenn sie persönliche Informationen wie Telefonnummern mit Diensten teilen müssen.
- Kosten: Für Unternehmen kann die Implementierung von 2FA zusätzliche Kosten verursachen, z.B. für spezielle Hardware-Token.

51% Attack - Eine 51%-Attacke bei Bitcoin ist ein sehr ernsthaftes und riskantes Sicherheitsproblem im Bitcoin-Netzwerk.
Bitcoin funktioniert auf Basis eines dezentralen Peer to Peer Netzwerk, in dem Transaktionen von einem Netzwerk von Knoten (Nodes) verifiziert und bestätigt werden. Das sogenannte "Mining" ist der Prozess, bei dem neue Blöcke zur Blockchain hinzugefügt werden. Miner verwenden ihre Rechenleistung, um komplexe kryptografische Rätsel zu lösen, um neue Blöcke zu validieren und dem Netzwerk hinzuzufügen.
Eine 51%-Attacke tritt dann auf, wenn ein einzelner Miner oder eine Gruppe von Minern mehr als 50% der gesamten Rechenleistung des Bitcoin-Netzwerks kontrollieren. In einer solchen Situation hätte diese Mehrheit die Kontrolle über das Netzwerk und könnte folgende Dinge tun:
Transaktionen rückgängig machen: Sie könnten ihre eigenen Transaktionen wieder rückgängig machen, indem sie eine alternative Blockchain-Geschichte erstellen und dem Netzwerk präsentieren. Dies würde es ihnen ermöglichen, Bitcoins doppelt auszugeben.
Neue Transaktionen blockieren: Die Mehrheit könnte auch neue Transaktionen blockieren und so verhindern, dass sie in die Blockchain aufgenommen werden.
Den Konsens manipulieren: Mit mehr als 50% der Rechenleistung könnten die Angreifer den Konsens im Netzwerk kontrollieren und so die Regeln und Protokolle nach ihren Vorstellungen ändern.
Eine erfolgreiche 51%-Attacke würde also das gesamte Vertrauen in das Bitcoin-System untergraben und die Integrität und Sicherheit des Netzwerks massiv gefährden. Aus diesem Grund ist die Wahrscheinlichkeit einer solchen Attacke extrem gering, da die Kosten und der Aufwand dafür sehr hoch wären. Dennoch ist es ein wichtiges theoretisches Risiko, das die Entwickler des Bitcoin-Netzwerks ständig im Blick haben müssen.

Airdrop - Bei Bitcoin und anderen Kryptowährungen werden Airdrops, zu deutsch

Helikoptergeld, verwendet, um neue Nutzer für das Netzwerk zu gewinnen und die Adoption der Kryptowährung zu fördern. Es handelt sich dabei um eine reine Marketingstrategie.
Im Falle von Bitcoin funktioniert ein Airdrop in der Regel so:
Das Bitcoin-Projekt oder eine damit verbundene Organisation verteilt kostenlos eine bestimmte Menge an Bitcoin-Einheiten (Satoshis) an qualifizierte Nutzer.
Um für den Airdrop berechtigt zu sein, müssen Nutzer oft bestimmte Bedingungen erfüllen, wie z.B. das Erstellen eines Bitcoin-Wallets, das Teilen von Social-Media-Posts oder das Teilnehmen an einer Umfrage.
Die verteilten Bitcoin-Einheiten sind für die Empfänger kostenlos. Die Idee ist es, diese Nutzer für das Bitcoin-Netzwerk zu interessieren und sie zum Halten und Verwenden von Bitcoin zu motivieren.
Airdrops können auch dazu dienen, neue Bitcoin-Funktionen oder Dienste bekannt zu machen und die Nutzerbasis dafür zu erweitern. Normalerweise wird für die Transaktionen der Airdrops das Lightningg-Netzwerk verwendet. Im Gegensatz zu den ganzen anderen Altcoins, die diese Technik ebenfalls einsetzen und beliebig Ihre Token erstellen können, sind alle Satoshis, die auf diesem Weg in Umlauf gebracht werden Teil der maximalen Summe von 21.000.000 Bitcoins und alles was bei solchen Werbemaßnahmen verloren geht, ist auch für immer verloren.
Insgesamt sollen Bitcoin-Airdrops also dazu beitragen, die Akzeptanz und Verbreitung von Bitcoin zu fördern, indem Nutzer kostenlos in das Ökosystem eingebunden werden. Allerdings müssen Airdrops sorgfältig geplant werden, um Betrug und Missbrauch zu vermeiden. Insgesamt stellen sie eine interessante Marketingstrategie dar, die von vielen innovativen Startups genutzt wird.

Altcoin - Altcoins sind alle Kryptowährungen, die nicht Bitcoin sind. Der Begriff "Altcoin" leitet sich von "alternative coin" ab und bezeichnet alle Kryptowährungen, die nach Bitcoin entwickelt wurden. Sie sind Konkurrenzprodukte zu Bitcoin und versuchen, bestimmte Funktionen und Eigenschaften von Bitcoin zu verbessern oder zu erweitern. Zu den Altcoins gehören bekannte Kryptowährungen wie Ethereum, Litecoin, Ripple, Monero, Dogecoin und viele andere. Insgesamt gibt es mehr als 11.000 verschiedene Projekte.
Altcoins versuchen, sich durch unterschiedliche technologische Ansätze, Funktionen oder Zielgruppen von Bitcoin abzuheben. Sie sind im Vergleich zu Bitcoin deutlich jünger, haben deutlich geringere Marktkapitalisierungen und sind tendenziell volatiler.
Viele Anleger sehen in Altcoins Potenzial für höhere Renditen, aber auch ein höheres Risiko im Vergleich zu Bitcoin.
Der Begriff "Shitcoin" wird oftmals für Altcoins verwendet, die als qualitativ minderwertig oder riskant eingestuft werden.
Bis zum heutigen Tage haben wir noch kein einziges Altcoin Projekt kennengelernt, dass wirklich eine Verbesserung zu Bitcoin darstellt oder eine Funktionalität anbietet, die nicht mit Bitcoin, zum Beispiel über eine Second-Layer-Technologie, sprich einen Aufsatz, ebenfalls abgebildet werden könnte. Was aber alle Altcoins eint, ist der Umstand, dass eigene Token ausgegeben werden und im Grunde nichts anderes gemacht wird, als legal Geld gedruckt. Nach Ansicht der Amerikanischen Börsenaufsicht (SEC) sind alle Kryptowährungen außer Bitcoin wie hoch riskante Wertpapiere zu behandeln. Bitcoin hingegen wird als Rohstoff, ähnlich wie Gold, Platin oder Silber behandelt.

ALM - AML steht für Anti Money Laundering, zu deutsch Anti Geldwäsche, und steht im engen Zusammenhang mit dem KYC-Prinzip (Know Your Customer).
Das Grundprinzip der Geldwäscheprävention ist es, den illegalen Kreislauf von Geldern oder anderen Vermögenswerten, die durch Straftaten erlangt wurden, zu unterbrechen. Dieser Prozess der Geldwäsche hat üblicherweise drei Stufen:

- Placement (Einführung): In dieser ersten Phase werden die illegal erworbenen Gelder in das legale Finanzsystem eingebracht, z.B. durch Bareinzahlungen auf Bankkonten.

- Layering (Verschleierung): Anschließend werden die Gelder durch komplexe Finanztransaktionen und -transfers verschleiert, um ihre illegale Herkunft zu verbergen.
- Integration (Ausführung): Schließlich werden die Gelder in den legalen Wirtschaftskreislauf eingebracht, z.B. durch den Kauf von Immobilien oder Investitionen.

Um diesen Kreislauf zu durchbrechen, haben Staaten umfangreiche gesetzliche Regelungen zur Geldwäscheprävention erlassen. Die Kernelemente sind:

- Identifizierungspflicht: Finanzinstitute und andere beteiligte Unternehmen müssen ihre Kunden eindeutig identifizieren und verifizieren. So soll verhindert werden, dass anonyme oder fiktive Personen am Prozess beteiligt sind.
- Sorgfaltspflichten: Die Unternehmen müssen die Herkunft der Gelder und den Zweck der Geschäftsbeziehung überprüfen und dokumentieren. Bei Verdachtsfällen sind sie zur Meldung an die zuständigen Behörden verpflichtet.
- Compliance-Maßnahmen: Die Unternehmen müssen interne Kontrollen, Richtlinien und Schulungen für Mitarbeiter etablieren, um Geldwäsche in ihren Abläufen zu verhindern.
- Beschränkungen/Verbote: Es gibt gesetzliche Limits für Barzahlungen und ein generelles Verbot, Gelder oder Vermögenswerte zu verschieben, die durch Straftaten erlangt wurden.

Durch diese umfassenden Maßnahmen soll der illegale Finanzkreislauf unterbrochen und verhindert werden, dass Kriminelle ihre Erträge in den legalen Wirtschaftskreislauf einschleusen können.
Im Alltag, also außerhalb der Bitcoinwelt, durchlaufen wir ständig diese Prozesse, ohne dass wir dies noch wirklich wahrnehmen. Wenn Bankkonten eröffnet, Autos von Händlern gekauft, Geld über Grenzen gebracht oder das Eigenheim gekauft werden soll. Ständig werden die Regeln der Geldwäscheprävention auf uns als Bürger angewendet.
Es gibt einen nicht unerheblichen Teil der Bitcoingemeinde, die diese Art der Überwachung durch den Staat sehr kritisch sehen, oder gar gänzlich ablehnen. Allerdings muss man sagen, dass nach den heutigen Verhältnissen ein gewisses Maß an Regulierung gar nicht mehr ausgeschlossen werden kann und sinnvolle Regulierung den Weg für Bitcoin in die Breite ebnet. Anonymität ist ein sehr hohes Gut, kann aber auch zu einer unüberwindlichen Hürde werden.

Apeing - Sich in Bitcoin "reinzuaffen" bedeutet, eine größere Menge als üblich zu kaufen, aufgrund des (vermeintlichen) Vertrauens oder bullisher Gefühle in Bezug auf die derzeitigen Marktbedingungen, oder auf Deutsch - richtig zu zocken.
Der Begriff stammt aus den Finanzwelt und wurde von der breiteren Kryptowährungsgemeinschaft übernommen. In ursprünglichen Kontext bedeutet er, die übliche Sorgfaltspflicht und den gesunden Menschenverstand beim Investieren zu umgehen. "Reinaffen" heißt also, dass jemand ein Token kurz nach dem Start des Token-Projekts, NFT- oder DeFi-Projekts kauft, ohne eine gründliche Recherche durchzuführen.

„Reinaffen“ kann sich auch darauf beziehen, dass der Preis von Bitcoin oder eines Altcoin erheblich steigt, ohne dass es dafür einen konkreten Grund gibt, also nur als reine Spekulation.

„So viele Leute affen sich gerade rein.“
„Affen spielen heute auf dem Markt ihre Spiele.“

ASIC - ASIC steht für "Application Specific Integrated Circuit". Das bedeutet, dass es sich um einen integrierten Schaltkreis handelt, der speziell für eine bestimmte Anwendung entwickelt wurde. Im Falle des Bitcoin-Minings sind ASICs Computerchips, die speziell dafür konzipiert sind, die komplexen mathematischen Berechnungen durchzuführen, die für das Bitcoin-Mining

erforderlich sind. Im Vergleich zu normalen Computerprozessoren oder Grafikkarten (GPU) sind ASICs deutlich effizienter und leistungsfähiger, wenn es darum geht, Bitcoin-Transaktionen zu verarbeiten und neue Blöcke im Blockchain-Netzwerk zu generieren.
Der Grund dafür ist, dass ASICs eine dedizierte Hardware-Architektur haben, die ausschließlich auf diese eine Aufgabe - das Bitcoin-Mining - ausgerichtet ist. Normale Computer-Hardware ist dagegen eher für allgemeine Zwecke konzipiert.
Der Einsatz von ASICs hat das Bitcoin-Mining deutlich professionalisiert und zentralisiert, da nur noch Miner mit dieser spezialisierten Hardware konkurrenzfähig sind.

Asset - Assets sind wirtschaftliche Güter, die einem Unternehmen oder einer Person gehören und einen Vermögenswert darstellen. In Bezug auf Bitcoin lassen sich verschiedene Arten von Krypto-Assets identifizieren. Die wohl bekannteste Form ist Bitcoin selbst - die führende Kryptowährung, die als digitales Zahlungsmittel und Wertaufbewahrungsmittel dient. Bitcoin kann als Finanzvermögen betrachtet werden, da es einen Marktwert hat und wie andere Währungen gehandelt wird. Darüber hinaus existieren viele weitere Krypto-Assets wie Altcoins, Token und digitale Vermögenswerte, die ebenfalls als Assets gelten können.
Diese Krypto-Assets haben für Besitzer diverse Funktionen: Sie können als Investitionsobjekt dienen, zur Diversifizierung eines Portfolios beitragen oder für Transaktionen und Zahlungen verwendet werden. Ähnlich wie traditionelle Finanzanlagen unterliegen auch Krypto-Assets Wertschwankungen, die von Faktoren wie Angebot, Nachfrage, Regulierung und Technologieentwicklung beeinflusst werden.

Der Wert eines Krypto-Assets hängt von verschiedenen Aspekten ab, beispielsweise der Marktkapitalisierung, der Liquidität, der Akzeptanz und den technischen Eigenschaften. Um den aktuellen Vermögenswert zu erfassen, müssen Krypto-Assets regelmäßig bewertet werden. Sie stellen daher einen wichtigen Teil des digitalen Vermögens von Privatpersonen und Unternehmen dar, die sich im Kryptomarkt engagieren.

ATH - ATH steht für "All Time High" oder zu deutsch Allzeithoch. In Bezug auf Bitcoin bezeichnet es den höchsten Preis, den Bitcoin jemals in Relation zu einer Fiatwährung erreicht hat. Das bedeutet konkret:
Der Bitcoin-Kurs hat im Laufe seiner Geschichte einen Höchststand erreicht, der bis zu diesem Zeitpunkt noch nie zuvor übertroffen wurde.
Dieser Höchststand ist der absolute Spitzenwert in der gesamten Kursgeschichte des Bitcoins.
Sobald der Bitcoin-Kurs diesen Höchststand überschreitet, wird ein neues All-Time-High erreicht.
All-Time-Highs sind ein wichtiger Indikator für die langfristige Preisentwicklung und Wertschöpfung von Bitcoin.
Sie werden von vielen Anlegern und Analysten genau beobachtet, da sie Aufschluss über die Leistungsfähigkeit und das weitere Potenzial der Kryptowährung geben können.
Zusammengefasst bezeichnet ein "All-Time-High" also den historischen Höchststand des Bitcoin-Kurses, der bisher noch nie übertroffen wurde.
Wichtig beim All Time High ist, dass es in jeder Landeswährung unterschiedlich ist und selbst wenn sich der Marktwert weltweit nicht verändert, der Wert von Bitcoin in einer spezifischen Landeswährung durch Inflation der Währung sich verändern kann. Drastisch kann man das in der Türkei und in Japan sehen.

BaFin - Die Bundesanstalt für Finanzdienstleistungsaufsicht, kurz BaFin, ist die zuständige Behörde für die Beaufsichtigung des Finanzmarktes in Deutschland. Sie wurde im Jahr 2002 gegründet und hat ihren Sitz in Bonn und Frankfurt am Main. Zu den Hauptaufgaben der BaFin

gehört die Überwachung und Regulierung von Banken, Versicherungen, Wertpapierfirmen und anderen Finanzinstituten. Dazu prüft sie die Einhaltung von geltenden Gesetzen und Vorschriften. Darüber hinaus hat die BaFin den Auftrag, Verbraucher vor unlauteren Geschäftspraktiken in der Finanzbranche zu schützen. Sie stellt sicher, dass Finanzprodukte und -dienstleistungen transparent und verantwortungsvoll angeboten werden. Eine weitere zentrale Aufgabe ist die Sicherstellung der Stabilität und Integrität des gesamten Finanzsystems in Deutschland. Hierbei überwacht die BaFin potenzielle Risiken, die vom Finanzsektor für die Gesamtwirtschaft ausgehen können. Neben der allgemeinen Finanzmarktaufsicht ist die Behörde auch für Spezialaufgaben wie die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuständig. Die BaFin arbeitet eng mit anderen nationalen und internationalen Aufsichtsbehörden zusammen. Sie ist eine unabhängige Bundesoberbehörde, die dem Bundesministerium der Finanzen untersteht, wobei ihre Entscheidungen gerichtlich überprüft werden können.

Banana Bread - Seit etwa 2021 tauchen in den Sozialen Netzwerken wie X (vormals Twitter) oder Reddit immer wieder Posts auf, die in Beiträgen über Bitcoin von "Banana Bread", zu deutsch Bananenbrot handeln und man wundert sich, was das zu bedeuten hat.
Der Trend hat seinen Ursprung in den Menschen, die Bitcoin als toxisch ansehen und um diese Menschen zu besänftigen wurde der Euphemismus Bananenbrot erfunden, damit sich keine weiteren Beschwerden anhäufen.
Anstelle von Bitcoin erwähnten die Leute in ihren Kommentaren stattdessen Bananenbrot. Sie fügten clevere Wortspiele hinzu und nutzten die Eigenschaften von Bitcoin.

Bear Market - Ein Bear Market, auch Baissemarkt oder Bärenmarkt genannt, ist eine Phase am Finanzmarkt, in der die Preise von Vermögenswerten wie Aktien, Rohstoffe oder Kryptowährungen über einen längeren Zeitraum kontinuierlich fallen.
Typische Merkmale eines Bärenmarktes sind:

- Rückgang der Aktienkurse um mindestens 20% über einen Zeitraum von mehreren Monaten oder Jahren.
- Wachsende Unsicherheit und Pessimismus unter Anlegern.
- Niedrigere Investitionen und Konsumausgaben in der Wirtschaft.
- Höhere Volatilität an den Märkten.

Im Gegensatz dazu steht der Bull Market, also ein Bullenmarkt, in dem die Preise aufgrund einer optimistischen Stimmung steigen.
Bärenmärkte werden oft durch schwache Konjunktur, steigende Inflation, Rezessionsängste oder geopolitische Krisen ausgelöst. Sie stellen eine Herausforderung für Anleger dar, bieten aber auch Chancen für langfristig orientierte Investoren, die antizyklisch in unterbewertete Werte investieren.

Block - Bei Bitcoin und anderen Kryptowährungen basiert die Aufzeichnung und Verwaltung aller Transaktionen auf einer Datenstruktur namens Blockchain. Die Blockchain besteht aus einer Reihe von Blöcken, die diese Transaktionen enthalten und chronologisch miteinander verknüpft sind.
Ein Block ist also ein Bauteil der Blockchain und beinhaltet mehrere Transaktionen, die in einem bestimmten Zeitraum durchgeführt wurden. Jeder Block enthält zusätzlich zu den Transaktionsdaten auch einige Metadaten, die für die Funktionsweise des Bitcoin-Netzwerks wichtig sind.
Zu diesen Metadaten gehören:
Blockheader: Dieser enthält wichtige Informationen wie die Referenz zum vorherigen Block

(Hashwert), den Zeitstempel, die Schwierigkeit des Proof of Work- Algorithmus sowie den Hashwert aller Transaktionen im Block.
Transaktionen: Der Hauptteil eines Blocks besteht aus den eigentlichen Transaktionsdaten, die in diesem Zeitraum verbucht wurden. Dies können Hunderte oder Tausende von Einzeltransaktionen sein.
Nonce: Dies ist ein Zählerwert, der für das Lösen des Proof-of-Work-Rätsels verwendet wird, um den Block zu validieren und in die Blockchain aufzunehmen.
Der Prozess, bei dem neue Blöcke zur Blockchain hinzugefügt werden, wird als "Mining" bezeichnet. Miner verwenden leistungsstarke Computer, sogenannte ASICs, um den Proof-of-Work-Algorithmus zu lösen, indem sie eine gültige Nonce finden. Sobald ein Miner einen neuen gültigen Block erzeugt hat, wird dieser an die Blockchain angefügt und alle in ihm enthaltenen Transaktionen als bestätigt betrachtet.
Jeder neue Block, der an die Blockchain angefügt wird, baut direkt auf dem vorherigen auf, da er dessen Hashwert beinhaltet. Dadurch entsteht eine unveränderbare Kette von Blöcken, die die gesamte Transaktionshistorie des Bitcoin-Netzwerks abbildet. Dies ist der Grund, warum die Blockchain als dezentrale, transparente und sichere Datenstruktur zum Aufzeichnen von Transaktionen dient.
Zusammengefasst ist ein Block also ein eigenständiges Element innerhalb der Blockchain, das eine Reihe von Transaktionen beinhaltet und durch spezifische Metadaten definiert ist. Die fortwährende Erweiterung der Blockchain durch neue Blöcke ist der Schlüsselprozess, der die Integrität und Funktionalität des gesamten Bitcoin-Netzwerks aufrechterhält.

Blockcain - Eine Blockchain ist eine Art dezentrale Datenbank, die Informationen in Form von Blöcken speichert und diese miteinander verknüpft, um eine sichere und transparente Aufzeichnung von Transaktionen oder anderen Daten zu gewährleisten. Im Gegensatz zu einer herkömmlichen zentralisierten Datenbank, bei der eine zentrale Instanz die Kontrolle über die gespeicherten Informationen hat, wird eine Blockchain von einem verteilten Netzwerk von Computern verwaltet, die als Nodes bezeichnet werden. Jeder Node im Netzwerk speichert eine Kopie der gesamten Blockchain, was bedeutet, dass alle Nodes über alle bisherigen Transaktionen informiert sind.
Die Funktionsweise einer Blockchain basiert auf mehreren grundlegenden Konzepten. Wenn eine Transaktion getätigt wird, wird sie an das Netzwerk gesendet und von den Nodes verbreitet. Die Transaktionen oder Daten werden in Blöcken gruppiert, die miteinander verknüpft sind, indem jeder Block einen eindeutigen Hash-Wert des vorherigen Blocks enthält. Dieser Prozess schafft eine unveränderliche und chronologische Kette von Blöcken, wodurch die Integrität der gespeicherten Informationen gewährleistet wird.
Ein weiterer wichtiger Aspekt der Blockchain ist das Peer-to-Peer Netzwerk, das die Kommunikation und den Datenaustausch zwischen den Nodes ermöglicht. Jeder Node im Bitcoin-Netzwerk ist mit anderen Nodes verbunden, wodurch ein dezentrales Netzwerk entsteht. Dieser dezentrale Ansatz trägt zur Sicherheit und Robustheit des Netzwerks bei, da es keine Single-Point-of-Failure gibt und das Netzwerk widerstandsfähiger gegen Angriffe oder Ausfälle ist. Die Peer-to-Peer-Architektur ermöglicht es, dass Transaktionen und Blöcke von einem Node zum anderen übertragen werden, ohne dass eine zentrale Autorität oder Vermittlungsstelle erforderlich ist.
Die Vorteile einer Blockchain gegenüber einer herkömmlichen Datenbank liegen in ihrer Sicherheit, Transparenz und Dezentralisierung. Da die Daten in Blöcken gespeichert und kryptografisch miteinander verknüpft sind, ist es äußerst schwierig, die gespeicherten Informationen zu manipulieren. Darüber hinaus ermöglicht die Dezentralisierung, dass keine zentrale Instanz die Kontrolle über das Netzwerk hat, was das Vertrauen in die Integrität der Daten stärkt. Die Transparenz einer Blockchain bedeutet, dass alle Transaktionen für alle Teilnehmer sichtbar sind, was die Nachverfolgbarkeit und Verifizierbarkeit von Informationen erleichtert.

Die Funktionsweise einer Blockchain basiert auf mehreren grundlegenden Konzepten. Zunächst werden die Transaktionen oder Daten in Blöcken gruppiert, die miteinander verknüpft sind, indem jeder Block einen eindeutigen Hash-Wert des vorherigen Blocks enthält. Dieser Prozess schafft eine unveränderliche und chronologische Kette von Blöcken, wodurch die Integrität der gespeicherten Informationen gewährleistet wird.
Ein weiterer wichtiger Aspekt der Blockchain ist die Konsensmechanismus, der verwendet wird, um sicherzustellen, dass alle Teilnehmer des Netzwerks über die Gültigkeit der Transaktionen einig sind. Dies kann durch verschiedene Methoden wie Poof of Work, Proof of Stake oder andere Mechanismen erreicht werden.
Die Vorteile einer Blockchain gegenüber einer herkömmlichen Datenbank liegen in ihrer Sicherheit, Transparenz und Dezentralisierung. Da die Daten in Blöcken gespeichert und kryptografisch miteinander verknüpft sind, ist es äußerst schwierig, oder nahezu unmöglich, die gespeicherten Informationen zu manipulieren. Darüber hinaus ermöglicht die Dezentralisierung, dass keine zentrale Instanz die Kontrolle über das Netzwerk hat, was das Vertrauen in die Integrität der Daten stärkt. Die Transparenz einer Blockchain bedeutet, dass alle Transaktionen für alle Teilnehmer sichtbar sind, was die Nachverfolgbarkeit und Verifizierbarkeit von Informationen erleichtert.
Allerdings gibt es auch Nachteile, die mit der Verwendung einer Blockchain verbunden sind. Dazu gehören die Skalierbarkeit, die Energieeffizienz und die Geschwindigkeit. Aufgrund der Art und Weise, wie eine Blockchain aufgebaut ist, kann sie in einigen Fällen langsamer sein als herkömmliche Datenbanken. Außerdem erfordert der Prozess des "Mining" in einigen Konsensmechanismen eine beträchtliche Menge an Energie, was zu Bedenken hinsichtlich der Umweltauswirkungen führt.
Insgesamt bietet die Blockchain-Technologie jedoch eine innovative Möglichkeit, Daten sicher und transparent zu speichern und Transaktionen ohne die Notwendigkeit einer vertrauenswürdigen Mittelsperson durchzuführen.

Blockhöhe - Die Blockhöhe bei Bitcoin bezeichnet die Nummer oder Position des aktuellen Blocks in der Blockchain. Der erste Block, also der Genesis Block, hat die Nummer 0. Jeder nachfolgende Block erhält dann eine fortlaufende Nummer, so dass der zweite Block die Nummer 1 hat, der dritte Block die Nummer 2 usw.
Die Blockhöhe ist eine wichtige Information, da sie den Fortschritt und die Entwicklung der Bitcoin-Blockchain anzeigt. Je höher die Blockhöhe, desto mehr Blöcke wurden insgesamt geschürft und in die Blockchain aufgenommen.
Zu jedem Zeitpunkt gibt es genau eine aktuelle Blockhöhe, die dem zuletzt hinzugefügten Block entspricht. Diese Blockhöhe wird im Bitcoin-Netzwerk ständig aktualisiert, da alle 10 Minuten im Durchschnitt ein neuer Block geschürft und hinzugefügt wird.
Die Blockhöhe ist auch wichtig für verschiedene Bitcoin-Funktionen und -Regeln. Zum Beispiel hängt die Blockbelohnung, also die Menge an neu geschaffenen Bitcoins, von der aktuellen Blockhöhe ab. Außerdem werden bestimmte Protokoll-Upgrades oder -Änderungen an einer bestimmten Blockhöhe aktiviert.
Insgesamt ist die Blockhöhe ein essentieller Wert, um den aktuellen Stand und die Entwicklung der Bitcoin-Blockchain zu verfolgen.

Block Reward - Der Block Reward ist eine der Grundlagen des Bitcoin-Systems. Er ist die Belohnung, die Miner dafür erhalten, dass sie erfolgreich einen neuen Block zur Blockchain hinzufügen.
Der Blockreward funktioniert folgendermaßen:
Jedes Mal, wenn ein neuer Block zur Blockchain hinzugefügt wird, erhalten die Miner, die diesen Block geschürft haben, eine bestimmte Menge an neu geschaffenen Bitcoins als Belohnung.

Der Anfangswert des Blockrewards betrug 50 BTC pro Block. Dieser Wert halbiert sich alle 210.000 Blöcke, was etwa alle 4 Jahre passiert (Halving).
Derzeit (Stand 2024) beträgt der Blockreward 3,125 BTC pro Block. Nach dem nächsten Halving im Jahr 2028 wird er auf 1,5625 BTC sinken.
Der Blockreward ist eine wichtige Motivation für die Miner, das Bitcoin-Netzwerk am Laufen zu halten und neue Blöcke zu schürfen. So werden neue Bitcoins in Umlauf gebracht.
Langfristig soll der Blockreward wegfallen, sodass die Miner ihre Einnahmen hauptsächlich über Transaktionsgebühren erzielen.
Der Blockreward ist somit ein zentraler Bestandteil des Bitcoin-Ökosystems und trägt zur Aufrechterhaltung und Sicherheit des Netzwerks bei.

BTC - BTC steht für Bitcoin, die bekannteste und erste digitale Kryptowährung der Welt und Inhalt dieses Buches. Bitcoin wurde 2009 von einer unbekannten Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto entwickelt.
Bitcoin ist eine dezentralisierte, peer to peer-basierte digitale Währung, bei der Transaktionen direkt zwischen Nutzern ohne einen zentralen Vermittler stattfinden. Das bedeutet, dass es keine Zentralbank oder andere Autorität gibt, die Bitcoin kontrolliert oder reguliert.
Stattdessen basiert Bitcoin auf einer Technologie namens Blockchain. In dieser Blockchain werden alle Bitcoin-Transaktionen aufgezeichnet und von einem dezentralen Netzwerk von Computern, den sogenannten "Minern", verifiziert und bestätigt.
Bitcoins können digital gehalten, versendet und empfangen werden. Sie können für den Kauf von Waren und Dienstleistungen verwendet werden, ähnlich wie herkömmliche Währungen. Der Wert von Bitcoin wird durch Angebot und Nachfrage auf den Kryptowährungsmärkten bestimmt und kann stark schwanken.
Bitcoin gilt als revolutionär, da es eine neue Form des digitalen Geldes und dezentralen Finanzsystems darstellt. Viele sehen in Bitcoin eine Alternative zu traditionellen Währungen und Finanzsystemen.

Bubble - Eine Blase, englisch Bubble, entsteht häufig bei neuen, innovativen Technologien oder Anlageklassen, wenn die Preise in kurzer Zeit stark ansteigen, ohne dass die zugrunde liegenden fundamentalen Werte dies rechtfertigen würden. Dies war auch bei Bitcoin der Fall.
Zu Beginn war Bitcoin vor allem bei Krypto-Enthusiasten beliebt, da es als innovative Digitalwährung galt, die ohne Kontrolle durch Zentralbanken oder Regierungen auskam. In den Jahren 2017 und 2018 erlebte der Bitcoinkurs dann einen massiven Preisanstieg von unter 1.000 US-Dollar auf fast 20.000 US-Dollar. Viele Anleger sprangen darauf auf, in der Hoffnung auf schnelle Gewinne.
Allerdings fehlten Bitcoin damals noch viele Anwendungsfälle und die Akzeptanz als Zahlungsmittel blieb gering. Der Preis stieg also deutlich über den "fairen Wert" hinaus, was typisch für eine Blase ist. Letztlich platzte diese Blase Ende 2017/Anfang 2018, der Kurs stürzte stark ab.
Seitdem hat sich der Bitcoinmarkt zwar stabilisiert, er unterliegt aber weiterhin starken Kursschwankungen. Es ist unausweichlich, dass Bitcoin auf die Dauer einen ewigen Wertzuwachs relativ zu allen Fiatwährungen erfahren wird, aber die geringe Umlaufgeschwindigkeit von Bitcoin und die Psychologie bei Anlegern (FOMO) führen immer wieder zu heftigen Blasen.

Bull Market - Bei Bitcoin und anderen Kryptowährungen bezeichnet man eine Aufwärtsentwicklung der Preise als Bull Market, zu deutsch Bullenmarkt oder auch Hausse genannt. In einem solchen Bullenmarkt zeigen sich ähnliche Eigenschaften wie bei Aktienmärkten:

- Steigende Preise: Der Bitcoinkurs verzeichnet über einen längeren Zeitraum (meist mehrere Monate) kontinuierliche Kurszuwächse von mindestens 20%.
- Hohes Investoreninteresse: Die Nachfrage nach Bitcoin steigt, da Anleger zuversichtlich sind und verstärkt Kryptowährungen kaufen.
- Positive Stimmung: Die Marktteilnehmer sind optimistisch und gehen von weiter steigenden Kursen aus, was die Dynamik des Bullmarktes verstärkt.
- Steigendes Handelsvolumen: Das Handelsvolumen an Kryptobörsen nimmt in einem Bullmarkt deutlich zu, da mehr Käufer am Markt sind.
- Mediale Aufmerksamkeit: Steigende Bitcoin-Kurse ziehen häufig verstärkte mediale Berichterstattung und öffentliches Interesse auf sich.

Ein Bitcoin-Bullenmarkt kann Monate oder sogar Jahre andauern und wird oft von hoher Volatilität begleitet. Anleger versuchen dann, von den steigenden Kursen zu profitieren, müssen aber auch größere Preisschwankungen einkalkulieren.
Wichtig ist, dass ein Bullenmarkt bei Bitcoin genauso wie an Aktienmärkten irgendwann endet und in eine Phase rückläufiger Kurse, also einen Bärenmarkt (Bear Market), übergehen kann. Anleger sollten dies bei ihren Investitionsentscheidungen berücksichtigen.

Buy the Dip - "Buy the Dip", zu deutsch so viel wie kaufe die Delle, ist eine Investitionsstrategie, die oft bei Kryptowährungen wie Bitcoin angewendet wird. Dabei geht es darum, Kryptowährungen zu kaufen, wenn der Preis vorübergehend gefallen ist (also "im Dip"). Das Ziel ist es, von dem erwarteten Preisanstieg zu profitieren, wenn der Preis wieder steigt.
Der Hintergedanke ist, dass Kursrückgänge bei Kryptowährungen oft nur vorübergehend sind und der Preis langfristig wieder ansteigt. Investoren, die zu solchen Dips kaufen, hoffen darauf, beim nächsten Preisanstieg einen Gewinn erzielen zu können.
Allerdings ist es schwierig, den richtigen Zeitpunkt für den Einstieg zu finden. Kursrückgänge können sich auch verlängern oder noch tiefer fallen, als erwartet. Daher ist "Buy the Dip" eine riskante Strategie, die nur mit Vorsicht angewendet werden sollte.
Insgesamt ist es wichtig, stets die Risiken im Hinterkopf zu behalten und nur so viel Geld zu investieren, wie man sich leisten kann zu verlieren. Eine diversifizierte Anlagestrategie kann hier sinnvoll sein, um das Risiko zu minimieren.

CBDC - Zentralbank-Digitalwährungen (CBDC) sind digitale Formen der nationalen Währungen, die von Zentralbanken ausgegeben und verwaltet werden. Im Wesentlichen handelt es sich um eine digitale Version des physischen Geldes, das von einer Zentralbank emittiert wird. Im Gegensatz zu Kryptowährungen wie Bitcoin, die dezentralisiert und unabhängig von einer zentralen Autorität sind, wird eine CBDC von einer staatlichen oder nationalen Zentralbank kontrolliert.
Die Ausgabe und Verwaltung von CBDC liegt in der Verantwortung der jeweiligen Zentralbank eines Landes. Die Zentralbanken haben die Aufgabe, die Geldpolitik des Landes zu steuern und die Stabilität der nationalen Währung zu gewährleisten. Die Einführung einer CBDC würde es den Zentralbanken ermöglichen, direkten Einfluss auf die Geldmenge und die Geldpolitik auszuüben, da sie die digitale Währung emittieren und kontrollieren.
Die Einführung von CBDC birgt verschiedene potenzielle Risiken und Implikationen. Zu den Risiken gehören Datenschutz- und Sicherheitsbedenken, da die Zentralbanken sensible Finanzdaten der Bürgerinnen und Bürger verwalten würden. Darüber hinaus könnten CBDC die traditionellen Banken und Finanzinstitute beeinflussen, da sie direkte Konkurrenz zu ihren Dienstleistungen darstellen könnten. Die Einführung von CBDC könnte auch Auswirkungen auf die finanzielle Privatsphäre haben, da Transaktionen möglicherweise leichter nachverfolgbar sind.

In Bezug auf die Auswirkungen auf die Bevölkerung könnten CBDC eine breitere finanzielle Inklusion fördern, indem sie den Zugang zu Finanzdienstleistungen für Menschen in ländlichen Gebieten oder mit begrenztem Zugang zu traditionellen Banken erleichtern. Gleichzeitig könnten CBDC die Effizienz von Zahlungen verbessern und Transaktionskosten senken.
Bitcoin könnte dazu beitragen, indem es als Gegenpol zu CBDC fungiert. Als dezentralisierte Kryptowährung, die unabhängig von staatlichen Institutionen oder Zentralbanken ist, bietet Bitcoin finanzielle Souveränität und Unabhängigkeit. Bitcoin ermöglicht es den Menschen, ihre eigenen Vermögenswerte zu verwalten und Transaktionen ohne die Notwendigkeit einer zentralen Autorität durchzuführen. In einer Welt, in der CBDC an Bedeutung gewinnen, könnte Bitcoin als alternative Wertaufbewahrungsmethode und Zahlungssystem dienen, das den Benutzern mehr Kontrolle über ihre Finanzen bietet.

CFTC - Die CFTC (Commodity Futures Trading Commission) ist eine unabhängige Bundesbehörde in den Vereinigten Staaten, die für die Regulierung und Überwachung des Terminhandelsmarktes für Rohstoffe und Finanzinstrumente zuständig ist. Zu ihren Hauptaufgaben gehört zunächst die Regulierung des Terminhandels, indem sie Vorschriften und Regeln für den Handel mit Rohstoffen, Finanzprodukten und Kryptowerten erlässt sowie Terminbörsen, Clearinghäuser und Marktteilnehmer zulässt und registriert. Darüber hinaus überwacht die CFTC den Markt, beobachtet und analysiert die Marktaktivitäten, um Unregelmäßigkeiten und Manipulationen aufzudecken, und führt bei Verdacht auf Gesetzesverstöße Untersuchungen durch. Zudem ist die Behörde für die Durchsetzung der Terminhandelsvorschriften verantwortlich, verhängt Sanktionen und Strafen bei Regelverstößen und kann Gerichtsverfahren gegen Marktteilnehmer einleiten, die gegen Gesetze verstoßen. Nicht zuletzt hat die CFTC die Aufgabe, die Integrität und Transparenz des Terminhandelsmarktes sicherzustellen und faire Handelspraktiken zum Schutz von Händlern und Anlegern zu fördern. Insgesamt spielt die CFTC eine wichtige Rolle bei der Regulierung und Überwachung des Terminhandels in den USA, insbesondere auch im aufstrebenden Kryptomarkt, und ihre Entscheidungen und Maßnahmen haben erheblichen Einfluss auf die Entwicklung und Stabilität dieses Marktsegments.

CIPS - Das Cross-Border Interbank Payment System (CIPS) ist ein international genutztes Zahlungssystem, das von den BRICS-Ländern (Brasilien, Russland, Indien, China und Südafrika) als Alternative zum US-dominierten SWIFT-System entwickelt wurde. CIPS wurde im Jahr 2015 von der Volksbank von China eingeführt, mit dem Ziel, grenzüberschreitende Bankgeschäfte und Zahlungen effizienter und unabhängiger vom US-Dollar abwickeln zu können. Im Gegensatz zu SWIFT, das vor allem in US-Dollar denominiert ist, ermöglicht CIPS den Zahlungsverkehr in Lokalwährungen wie dem chinesischen Renminbi. Durch dieses System sollen Transaktionen zwischen den BRICS-Ländern und ihren Handelspartnern schneller, kostengünstiger und unabhängiger vom westlichen Finanzsystem erfolgen können. Es ist Teil der Bemühungen der aufstrebenden Volkswirtschaften, ihre Abhängigkeit vom US-Dollar und dem von den USA dominierten SWIFT-System zu reduzieren. Aktuell sind über 1.100 Banken und Finanzinstitute aus mehr als 100 Ländern an CIPS angeschlossen. Neben den fünf Gründungsmitgliedern Brasilien, Russland, Indien, China und Südafrika haben sich in den letzten Jahren auch weitere Länder wie Argentinien, Iran, Saudi-Arabien, die Vereinigten Arabischen Emirate und die Türkei dem CIPS-Netzwerk angeschlossen oder befinden sich in Gesprächen darüber. Das CIPS-System soll den Handel und Zahlungsverkehr zwischen den beteiligten Ländern erleichtern und ihre finanzielle Souveränität stärken. Es ist Teil einer umfassenderen Strategie der BRICS-Länder, ein alternatives, von den USA unabhängiges globales Finanzsystem aufzubauen, um ihre geopolitische und ökonomische Macht auszubauen. Insgesamt stellt CIPS einen wichtigen Schritt der BRICS-Länder dar, ihre Unabhängigkeit vom US-dominierten Finanzsystem zu erhöhen und ihre eigenen Interessen auf der globalen Bühne besser durchsetzen zu können.

Clearing - Das Clearing ist ein zentraler Bestandteil des modernen Finanzsystems und beschreibt den Prozess, bei dem Finanztransaktionen zwischen verschiedenen Marktteilnehmern abgewickelt und ausgeglichen werden. Im Clearing werden alle relevanten Informationen über eine Finanztransaktion gesammelt, verarbeitet und abgeglichen. Dazu gehören beispielsweise die Identität der beteiligten Parteien, die genauen Transaktionsdetails sowie der Zeitpunkt und die Art der Transaktion. Dieser Prozess stellt sicher, dass alle Beteiligten ihre Verpflichtungen erfüllen und die Transaktion erfolgreich abgewickelt wird. Die Bedeutung des Clearing liegt in der Erhöhung der Effizienz und Sicherheit des Finanzsystems. Durch die zentrale Abwicklung und Verrechnung von Transaktionen werden Risiken minimiert und Fehler vermieden. Zudem ermöglicht das Clearing eine zeitnahe Erfüllung der Geschäfte, was für die Liquidität des Marktes und die Funktionsfähigkeit der Finanzmärkte von entscheidender Bedeutung ist. Clearing-Systeme übernehmen auch wichtige Aufgaben wie die Risikoüberwachung, das Margening und die Sicherheitsleistungen. Auf diese Weise tragen sie dazu bei, die Stabilität des gesamten Finanzsystems zu gewährleisten und systemische Risiken zu begrenzen.
Insgesamt ist das Clearing ein essenzieller Bestandteil der modernen Finanzwelt, der für reibungslose Transaktionen, Risikominimierung und die Funktionsfähigkeit der Märkte soll. Durch seinen vollkommene Transparenz kann Bitcoin vollkommen auf dieses Mechanismus verzichten, der in der Vergangenheit unzählige Male dafür verantwortlich war, dass Währungen in massiver Form manipuliert wurden.

CoinJoin - Coinjoin, übersetzt so viel wie Münzenverschmelzung, ist eine Technik, die dazu dient, die Privatsphäre und Anonymität bei Bitcoin-Transaktionen zu verbessern. Dabei werden mehrere Transaktionen zu einer einzigen zusammengefasst, sodass es schwieriger wird, die einzelnen Zahlungsströme zu verfolgen.
Hier ist der Ablauf im Detail:
Mehrere Personen, die Bitcoin-Zahlungen tätigen möchten, schließen sich zusammen.
Alle Teilnehmer senden ihre Bitcoin-Beträge in einen gemeinsamen "Pool".
Aus diesem Pool werden dann neue Transaktionen generiert, bei denen die Herkunft der einzelnen Beträge nicht mehr rückverfolgbar ist.
Die neue, zusammengefasste Transaktion wird dann von allen Teilnehmern signiert und in das Bitcoin-Netzwerk gesendet.
Durch dieses Vorgehen wird es deutlich schwieriger, die ursprünglichen Zahlungsbeziehungen nachzuvollziehen. Coinjoin trägt somit zu einer erhöhten Anonymität und Privatsphäre bei Bitcoin-Überweisungen bei.
Es gibt verschiedene Projekte und Dienstleistungen, die Coinjoin-Funktionalität anbieten, wie zum Beispiel JoinMarket, Tornado Cash oder Mixing-Services. Der Einsatz von Coinjoin ist ein wichtiges Tool für alle, denen Datenschutz und Anonymität im Bitcoin-Netzwerk wichtig sind.

Coin Mixer – Siehe Tumbler

Confirmation - Das Bestätigungsprinzip (Confirmation) ist Teil des Transaktionsprozesses. Das Bitcoin-Netzwerk basiert auf der Blockchain-Technologie, bei der jede Transaktion in einem Block zusammengefasst und in die Blockchain eingetragen wird. Damit eine Transaktion als vollständig bestätigt gilt, muss sie in mehrere nachfolgende Blöcke aufgenommen werden. Jeder dieser Blöcke wird von Minern mittels komplexer kryptographischer Berechnungen erzeugt. Sobald eine Transaktion in einem Block enthalten ist, gilt sie als einmal bestätigt. Je mehr nachfolgende Blöcke hinzukommen, desto sicherer ist die Transaktion. Die erste Bestätigung ist zwar schon ein

gutes Indiz dafür, dass die Transaktion gültig ist, aber für einen hohen Sicherheitsstandard empfiehlt es sich, mindestens 6 Bestätigungen abzuwarten. Je mehr Bestätigungen, desto unwahrscheinlicher wird es, dass eine Transaktion rückgängig gemacht werden kann. Dieses Bestätigungsprinzip ist ein zentraler Aspekt der Sicherheit und Unveränderbarkeit des Bitcoin-Netzwerks. Es verhindert Betrug und sorgt dafür, dass Transaktionen endgültig und unumkehrbar sind. Das Warten auf mehrere Bestätigungen ist daher ein wichtiger Teil jeder Bitcoin-Transaktion.

Crypto - Crypto, kurz für cryptography, zu deutsch Verschlüsselung.
Die Kryptographie ist das Fundament, auf dem Bitcoin und andere Kryptowährungen aufbauen. Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen, um diese vor unbefugtem Zugriff zu schützen.
Bei Bitcoin wird Kryptographie in mehreren Schlüsselbereichen eingesetzt:

- Wallet-Schlüssel: Jeder Bitcoin-Besitzer hat ein Wallet mit öffentlichen und privaten Schlüsseln (Key). Der private Schlüssel dient als Beweis des Besitzes und ermöglicht das Senden von Bitcoins. Kryptographische Verfahren wie die elliptische Kurven-Kryptographie stellen sicher, dass die privaten Schlüssel nicht abgeleitet werden können.
- Transaktionsverifizierung: Alle Bitcoin-Transaktionen werden kryptographisch signiert. Dadurch kann das Netzwerk verifizieren, dass Transaktionen von den tatsächlichen Besitzern der Bitcoins stammen und nicht manipuliert wurden.
- Mining und Konsensfindung: Der Proof of Work-Mechanismus des Bitcoin-Netzwerks basiert auf der Lösung komplexer kryptographischer Rätsel durch die Miner. Dieser Prozess stellt sicher, dass Transaktionen nicht rückgängig gemacht oder gefälscht werden können.
- Blockchain-Integrität: Die Blockchain selbst ist eine kryptographisch verknüpfte Kette von Blöcken, in denen Transaktionen aufgezeichnet werden. Jeder Block enthält einen kryptographischen Hash des vorherigen Blocks, was die Integrität und Unveränderbarkeit der Blockchain gewährleistet.

Die Verwendung fortschrittlicher kryptographischer Verfahren wie asymmetrische Verschlüsselung, kryptographische Hashfunktionen und digitale Signaturen ist entscheidend für die Sicherheit und den Schutz von Bitcoin. Ohne diese kryptographischen Mechanismen wäre Bitcoin anfällig für Betrug und Manipulation.
Die Stärke der Bitcoin-Kryptographie zeigt sich darin, dass das Netzwerk seit seiner Einführung 2009 nie erfolgreich gehackt oder angegriffen wurde. Dies hat dazu beigetragen, dass Bitcoin als vertrauenswürdige und sichere digitale Währung wahrgenommen wird.
Insgesamt bildet die Kryptographie das technische Rückgrat von Bitcoin und ermöglicht die Dezentralisierung, Transparenz und Sicherheit, die Bitcoin so einzigartig machen. Das Verständnis der Kryptographie ist daher entscheidend, um die Funktionsweise und Leistungsfähigkeit von Bitcoin vollständig zu begreifen.
Die Bezeichnung Crypto, oder Krypto hat sich aber auch noch als Synonym für alle anderen über 10.000 Digitalwährungen etabliert, was viele in der Bitcoingemeinde erbost, da Bitcoin nicht mit diesen ganzen Projekten verglichen werden kann. Die Bitcoiner bezeichnen die anderen Projekte als Altcoins, oder Shitcoins.

DCA - Die DCA-Strategie (Dollar-Cost Averaging, oder zu deutsch Duchschnittskosteneffekt) ist eine Anlagestrategie, bei der regelmäßig und in festen Beträgen unabhängig vom aktuellen Kursniveau in ein Wertpapier investiert wird. Hier sind die wichtigsten Merkmale der DCA-Strategie:
Regelmäßige Investitionen: Statt einer einmaligen Großanlage werden über einen längeren Zeitraum hinweg in regelmäßigen Abständen (z.B. monatlich) kleinere Beträge investiert.

Fester Investitionsbetrag: Der Anlagebetrag bleibt über die Zeit konstant, unabhängig davon, ob der Kurs des Wertpapiers gerade hoch oder niedrig ist.
Glättung der Einstiegskurse: Bei fallenden Kursen können durch den fixen Anlagebetrag mehr Anteile gekauft werden, bei steigenden Kursen weniger. So werden Kursschwankungen über die Zeit geglättet.
Reduktion des Anlagerisikos: Das Risiko, zu einem ungünstigen Zeitpunkt investiert zu haben, wird durch die regelmäßigen Investitionen verringert. Langfristig kann so eine positive Rendite erzielt werden.
Die DCA-Strategie eignet sich besonders gut für Anleger, die langfristig investieren möchten und eine disziplinierte Herangehensweise an den Vermögensaufbau präferieren. Sie kann dabei helfen, die emotionalen Entscheidungen beim Investieren zu reduzieren und eine kontinuierliche Kapitalbildung zu ermöglichen.

DeFi - Eine DeFi-Anwendung, kurz für "dezentralisierte Finanzanwendung", bezieht sich auf eine Art von Finanzdienstleistung oder Anwendung, die auf Blockchain-Technologie basiert und darauf abzielt, herkömmliche Finanzintermediäre wie Banken oder Börsen zu umgehen. Diese Anwendungen ermöglichen es den Benutzern, direkt miteinander zu interagieren, ohne auf eine zentrale Autorität angewiesen zu sein.
DeFi-Anwendungen bieten eine Vielzahl von Finanzdienstleistungen, darunter Kreditvergabe, Handel, Zahlungen, Derivate und mehr. Sie basieren in der Regel auf Smart Contracts, die auf einer Blockchain ausgeführt werden, und ermöglichen es Benutzern, Vermögenswerte zu verleihen, zu leihen, zu handeln und zu investieren, ohne auf traditionelle Finanzinstitute angewiesen zu sein.
Ein Beispiel für eine DeFi-Anwendung ist ein dezentraler Kreditmarkt, auf dem Benutzer Kredite vergeben und aufnehmen können, ohne dass eine Bank als Vermittler fungiert. Ein weiteres Beispiel ist ein dezentraler Börsenmarkt, auf dem Benutzer direkt miteinander handeln können, ohne dass eine zentrale Börse erforderlich ist.
DeFi-Anwendungen haben das Potenzial, Finanzdienstleistungen für eine breitere Bevölkerungsschicht zugänglich zu machen, insbesondere für diejenigen, die keinen Zugang zu herkömmlichen Bankdienstleistungen haben. Sie bieten auch die Möglichkeit, Finanztransaktionen effizienter und kostengünstiger durchzuführen, da sie auf Blockchain-Technologie basieren, die Transparenz, Sicherheit und Unveränderlichkeit bietet.
Insgesamt können DeFi-Anwendungen als ein aufstrebender Bereich innerhalb der Kryptowährungs- und Blockchain-Branche betrachtet werden, der das Potenzial hat, die Art und Weise zu verändern, wie Finanzdienstleistungen erbracht und genutzt werden.

Degen -Degen steht für degeneriert und wird von der Bitcoingemeinde für Menschen verwendet, die einfach nur zocken. Menschen die Kredite aufnehmen und Bitcoin gehebelt zu kaufen gehen nicht nur ein hohes Risiko ein, sondern sie sind auch unter den eingefleischten Bitcoinern nicht besonders angesehen. Bitcoin ist nicht zum zocken konzipiert worden.

Difficulty - Ein wichtiger Aspekt des Bitcoin-Netzwerks ist die sogenannte "Difficulty" - der Schwierigkeitsgrad des Proof of Work-Konsensus-Mechanismus. Dieser Mechanismus ist essenziell für die Sicherheit und den Betrieb des dezentralen Bitcoin-Netzwerks, stellt aber gleichzeitig eine beachtliche technische Herausforderung dar.
Die Difficulty bestimmt, wie komplex die mathematischen Rätsel sind, die die Bitcoin-Miner lösen müssen, um neue Blöcke zu generieren und neue Bitcoins in Umlauf zu bringen. Je höher die Difficulty, desto mehr Rechenleistung und Energie müssen die Miner aufwenden, um einen gültigen Block zu finden. Dieser Schwierigkeitsgrad wird vom Bitcoin-Netzwerk automatisch angepasst, und zwar alle 2.016 Blöcke, was etwa alle zwei Wochen der Fall ist. Ziel ist es, sicherzustellen, dass

neue Blöcke im Durchschnitt alle 10 Minuten hinzugefügt werden. Wenn also mehr Rechenleistung in das Netzwerk einfließt, erhöht sich die Difficulty, um den Block-Zeitraum konstant zu halten.

Diese dynamische Anpassung der Difficulty ist notwendig, um das Gleichgewicht zwischen Transaktionsverarbeitung und Dezentralisierung des Netzwerks aufrechtzuerhalten. Je mehr Rechenleistung in das Netzwerk fließt, desto schwieriger werden die Rätsel, die die Miner lösen müssen. Die ständig steigende Difficulty ist eine der Hauptherausforderungen im Bitcoin-System. Sie führt zu einem kontinuierlich wachsenden Energieverbrauch, da immer mehr Rechenleistung benötigt wird, um neue Blöcke zu schürfen. Dies steht zunehmend in der Kritik und erschwert auch die Skalierbarkeit des Netzwerks.

Die Entwickler von Bitcoin arbeiten intensiv an Lösungen, um diese Probleme in den Griff zu bekommen und die Nachhaltigkeit des Systems zu verbessern. Allerdings stellt die Difficulty nach wie vor einen zentralen technischen Aspekt dar, der erhebliche Herausforderungen mit sich bringt.

Don't trust, verify - Das "Don't trust, verify"-Prinzip (nichts glauben, alles nachprüfen) ist ein zentraler Bestandteil der Bitcoin-Community und resultiert aus dem dezentralen und unabhängigen Charakter von Bitcoin als digitale Währung. Bitcoin-Anhänger sind generell sehr misstrauisch gegenüber Autoritäten, Institutionen und Dritten, die Kontrolle über das Finanzsystem ausüben könnten. Stattdessen legen Bitcoin-Nutzer großen Wert darauf, alles selbst zu überprüfen und zu validieren. Anstatt anderen zu vertrauen, wollen sie die Funktionsweise und Sicherheit des Bitcoin-Netzwerks durch eigene Prüfung nachvollziehen. Dazu gehört zum Beispiel:

- Den Quellcode von Bitcoin selbst zu analysieren und zu verstehen
- Die Transaktionen im öffentlichen Blockchain-Ledger eigenständig zu überprüfen
- Die Richtigkeit der Bitcoins im eigenen Wallet selbst zu kontrollieren
- Kryptografische Algorithmen und Sicherheitsmaßnahmen selbst zu überprüfen

Dieses "Don't trust, verify"-Prinzip soll sicherstellen, dass Bitcoin-Nutzer nicht auf Dritte angewiesen sind und die Kontrolle über ihre Finanzen selbst behalten. Es ist Ausdruck des tiefen Misstrauens gegenüber zentralen Autoritäten und Finanzinstituten, die für viele Bitcoin-Anhänger ein Hauptproblem des traditionellen Finanzsystems darstellen.Insgesamt zeigt sich hier eine grundsätzlich skeptische und unabhängige Haltung, die für viele Bitcoin-Enthusiasten essentiell ist, um das Prinzip der Dezentralität und Selbstbestimmung im Finanzsystem zu verwirklichen.

Double Spending - Das Double Spending Problem ist eine zentrale Herausforderung, die bei digitalen Währungen wie Bitcoin adressiert werden muss. Es beschreibt das Risiko, dass ein Nutzer digitale Münzen mehrfach ausgeben könnte. In traditionellen bargeldlosen Zahlungssystemen wird dieses Problem üblicherweise durch eine zentrale Kontrollinstanz gelöst, die sicherstellt, dass Geldtransaktionen nur einmal durchgeführt werden. Bei dezentralen Kryptowährungen wie Bitcoin gibt es jedoch keine solche zentrale Autorität. Das Double Spending Problem muss hier auf andere Weise verhindert werden. Bitcoin nutzt eine öffentliche Transaktionshistorie (Blockchain), in der alle Überweisungen verzeichnet werden. Durch das Proof-of-Work-Konzept und das Mining-Prinzip wird sichergestellt, dass jede Transaktion nur einmal in die Blockchain aufgenommen wird. Sobald eine Bitcoin-Zahlung in mehrere Blöcke tief in der Blockchain eingebunden ist, gilt sie als endgültig und nicht mehr rückgängig zu machen. Auf diese Weise löst das Bitcoin-Netzwerk das Double Spending Problem, ohne dass eine zentrale Instanz nötig ist. Die Blockchain sorgt dafür, dass jede Transaktion nur einmal ausgeführt wird. Somit ist das Double Spending Problem eine technische Herausforderung, die Bitcoin erfolgreich adressiert und einen wichtigen Beitrag zur Funktionsweise der Kryptowährung leistet.

Dust - Was ist Bitcoin-Staub / Bitcoin Dust?
Bitcoin-Staub bezieht sich auf UTXOs, die winzige Mengen von Satoshis enthalten, die von früheren Transaktionen übrig geblieben sind.
Für sich genommen würden diese winzigen BTC-Beträge mehr an Transaktionsgebühren kosten, um sie zu verarbeiten, als sie wert wären, daher liegen sie oft in Wechseladressen, bis sie zusammen mit anderen UTXOs gebündelt und ausgegeben werden.

Dusting Attack - Eine Dusting Attack, zu deutsch Staubattacke, verwenden Betrüger, die Bitcoin-Staub (Dust) an Hunderttausende verschiedener Wallet-Adressen senden. Die Idee dahinter ist, potenzielle Ziele für Social-Engineering-Attacken zu ermitteln.
Ein Betrüger wird Adressen beobachten, die den von ihm gesendeten Staub enthalten, und darauf warten, dass der Besitzer eine Transaktion tätigt, die UTXOs aus verschiedenen mit seiner Wallet verknüpften Adressen bündelt. Da Staub-UTXOs so klein sind, ist die Wahrscheinlichkeit groß, dass sie mit anderen zusammengefasst und als Eingaben verwendet werden.
Sobald dies geschieht, kann der Betrüger eine Vorstellung davon bekommen, über welche Mittel eine Person verfügt. Er kann dann entscheiden, Phishing-Nachrichten in Transaktionen einzubetten, die den Besitzer einladen, auf einen Link zu klicken, der Malware herunterlädt, oder gefälschte Websites aufzusuchen, die legitime Zielseiten imitieren und nach persönlichen Informationen fragen.

DYOR – DYOR steht für das Englische „Do your own research“, was zu deutsch heißt recherchiere selbst. In der Bitcoin-Gemeinde gilt es als eines der obersten Prinzipien, ähnlich wie „Don't trust, verify“ um sicher zu gehen, dass man selbst sich seine Informationen beschafft und sich nicht von fremden Entitäten abhängig macht und vor allem um einseitiger Beeinflussung zuvorzukommen. Wer sich in den Kaninchenbau begibt und die wirklichen Zusammenhänge versteht, der versteht auch die Notwendigkeit von Bitcoin. Diesen Prozess muss allerdings jeder selbst durchleben.

EBA - Die Europäische Bankenaufsichtsbehörde (EBA) ist eine zentrale Institution der Europäischen Union, die sich mit der Regulierung und Überwachung des Bankensektors in Europa befasst. Sie wurde im Jahr 2010 gegründet und hat ihren Sitz in Paris. Die Hauptaufgabe der EBA ist es, zur Stabilität und Sicherheit des europäischen Finanzsystems beizutragen. Dazu entwickelt sie einheitliche Regeln und Richtlinien für Banken in der EU, die von den nationalen Aufsichtsbehörden umgesetzt werden müssen. Diese Regeln betreffen beispielsweise die Eigenkapitalausstattung, Liquidität, Risikosteuerung und Transparenz von Banken. Um diese Ziele zu erreichen, führt die EBA verschiedene Aktivitäten durch. Dazu gehört die Erarbeitung technischer Standards und Leitlinien, die von den nationalen Aufsichtsbehörden angewendet werden müssen. Außerdem führt die EBA regelmäßige Stresstests durch, um die Widerstandsfähigkeit der Banken in Krisenszenarien zu testen. Darüber hinaus spielt die EBA eine wichtige Rolle bei der Koordination der Zusammenarbeit zwischen den nationalen Aufsichtsbehörden. Sie fungiert als Plattform für den Austausch von Informationen und Erfahrungen, um ein einheitliches Aufsichtsniveau in ganz Europa zu gewährleisten. Durch ihre Arbeit trägt die EBA dazu bei, Risiken im Bankensektor frühzeitig zu erkennen und Maßnahmen zu ihrer Eindämmung zu ergreifen. Damit soll ein stabiles und widerstandsfähiges Finanzsystem geschaffen werden, das Verbraucher und Unternehmen vor Finanzkrisen schützt. Insgesamt nimmt die EBA eine zentrale Rolle bei der Regulierung und Beaufsichtigung des europäischen Bankenwesens ein, um die Stabilität und Integrität des Finanzsystems sicherzustellen.

Exchange - Mit dem wachsenden Interesse an Kryptowährungen ist in den letzten Jahren eine Vielzahl von Krypto-Börsen (auch "Crypto Exchanges" genannt) entstanden. Diese Plattformen dienen als zentrale Marktplätze, an denen Anleger digitale Vermögenswerte wie Bitcoin, Ethereum oder Altcoins kaufen, verkaufen und handeln können.
Eine Crypto Exchange ist im Grunde ein online-basierter Finanzmarkt, der viele Funktionen einer traditionellen Börse erfüllt, jedoch auf dem Handel mit Kryptowährungen spezialisiert ist. Nutzer können dort Kryptowährungen gegeneinander oder gegen Fiat-Währungen wie Euro oder US-Dollar tauschen.
Der Handel auf einer Crypto Exchange läuft in der Regel folgendermaßen ab: Zunächst müssen sich Anleger auf der Plattform registrieren und ein Benutzerkonto eröffnen. Dabei müssen sie persönliche Daten wie Name, Adresse und Kontoinformationen angeben, um den Identitätsnachweis und die Kontoführung zu ermöglichen. (Siehe KYC) Nach erfolgreicher Registrierung können Nutzer Gelder auf ihr Börsenkonto einzahlen, entweder in Form von Fiat-Währungen oder bereits erworbenen Kryptowährungen.
Anschließend können sie Orders zum Kauf oder Verkauf von Kryptowährungen platzieren. Dafür stellen Crypto Exchanges verschiedene Order-Typen zur Verfügung, z.B. Marktorders, Limitorders oder Stop-Loss-Orders. Die Orders werden dann vom System der Börse ausgeführt, sobald ein passender Gegenpart gefunden wird. Jede abgewickelte Order wird auf dem Blockchain-Netzwerk der jeweiligen Kryptowährung verbucht, um die Transaktion transparent und fälschungssicher zu dokumentieren.
Neben dem reinen Handel bieten viele Crypto Exchanges ihren Nutzern auch zusätzliche Funktionen an, wie z.B. das Staking von Kryptowährungen, um passive Erträge zu erwirtschaften, oder das Verleihen von Vermögenswerten gegen Zinsen. Einige Börsen haben auch eigene Debitkarten ausgegeben, mit denen Kunden Kryptowährungen direkt im Alltag als Zahlungsmittel nutzen können.
Der große Vorteil von Crypto Exchanges ist, dass sie den Einstieg in den Kryptomarkt erheblich erleichtern und Anlegern einen einfachen und sicheren Zugang zu digitalen Vermögenswerten bieten. Allerdings sind die Plattformen aufgrund ihrer Komplexität und des hohen Risikos im Kryptomarkt auch mit gewissen Risiken behaftet, die Anleger stets im Blick haben sollten.

FED - Die Federal Reserve, auch bekannt als das Federale Reservesystem oder einfach "die Fed", ist das zentrale Bankensystem der Vereinigten Staaten. Sie wurde 1913 durch den Federal Reserve Act gegründet und ist seitdem einer der einflussreichsten Akteure in der US-Wirtschaft.
Die Hauptaufgaben der Federal Reserve sind die Aufrechterhaltung der Preisstabilität, die Förderung von Vollbeschäftigung und die Gewährleistung der Finanzmarktstabilität. Um diese Ziele zu erreichen, verfügt die Fed über verschiedene geldpolitische Instrumente, die sie einsetzt.
An der Spitze der Fed steht das Federal Reserve Board of Governors, das aus sieben Mitgliedern besteht, die vom Präsidenten der Vereinigten Staaten ernannt und vom Senat bestätigt werden. Dieses Gremium trifft die wichtigen geldpolitischen Entscheidungen und legt den Leitzins, die sogenannte Federal Funds Rate, fest. Dieser Leitzins beeinflusst maßgeblich die Kreditvergabe und Zinsen im gesamten Finanzsystem. Neben dem Federal Reserve Board gibt es noch zwölf regionale Reservebanken, die gemeinsam das Federale Reservesystem bilden. Diese Reservebanken überwachen den Bankensektor in ihren jeweiligen Regionen und stellen den Banken Kredite zur Verfügung. Sie dienen auch als Clearingstellen für den bargeldlosen Zahlungsverkehr.
Die Unabhängigkeit der Federal Reserve von der Regierung ist ein wichtiger Aspekt ihrer Struktur. Zwar ist sie dem Kongress rechenschaftspflichtig, hat aber bei der Umsetzung ihrer Geldpolitik weitgehende Autonomie. Dies soll sicherstellen, dass die Zentralbank ihre Ziele ohne politischen Einfluss verfolgen kann. Die Geldpolitik der Fed hat weitreichende Auswirkungen auf die gesamte US-Wirtschaft. Durch Zinsänderungen, den Ankauf von Wertpapieren und andere Maßnahmen kann sie die Konjunktur beeinflussen, Inflation bekämpfen und die Finanzmärkte stabilisieren. Daher

wird die Entscheidungsfindung der Fed genau beobachtet und debattiert. Insgesamt spielt die Federal Reserve eine zentrale Rolle im US-Finanzsystem und ist für die wirtschaftliche Entwicklung des Landes von großer Bedeutung. Ihre Geldpolitik hat nicht nur innerhalb der Vereinigten Staaten, sondern auch international erhebliche Auswirkungen.

Fiatgeld – Fiatgeld auch englisch fiat money, ist eine Form von Währung, die keinen inneren materiellen Wert besitzt, sondern ihren Wert durch staatliche Autorität und Akzeptanz in der Gesellschaft erhält. Im Gegensatz zu Warengeld, wie beispielsweise Gold oder Silber, hat Fiatgeld keinen eigenen intrinsischen Wert. Stattdessen wird der Wert von Fiatgeld durch die Macht des ausgebenden Staates festgelegt, der es als gesetzliches Zahlungsmittel erklärt. Dieser Prozess wird auch als "Fiat" bezeichnet, was aus dem Lateinischen stammt und "Es geschehe! Es werde!" bedeutet. Damit wird zum Ausdruck gebracht, dass der Staat den Wert und die Verwendung dieser Währung festlegt, unabhängig von einem materiellen Hintergrund. Heutzutage basieren die meisten Währungssysteme weltweit auf Fiatgeld, da die Anbindung an ein bestimmtes Wirtschaftsgut, wie es beim Goldstandard üblich war, aufgegeben wurde. Stattdessen wird der Wert einer Währungseinheit durch das Vertrauen in die staatliche Autorität und die allgemeine Akzeptanz in wirtschaftlichen Transaktionen bestimmt. Erst durch diese breite Anerkennung erlangt Fiatgeld die Eigenschaften von Geld als allgemeines Zahlungsmittel.

First Mover – Ein First Mover kann auf deutsch vielleicht am besten mit einem Pionier verglichen werden, sowohl im unternehmerischen als auch in privaten Bereich. Als erste digitale Kryptowährung, die 2009 von Satoshi Nakamoto eingeführt wurde, kann Bitcoin als klassischer First Mover in diesem Markt angesehen werden. Diese Pionierrolle bringt für Anleger sowohl Chancen als auch Risiken mit sich. Auf der Chancenseite profitieren Bitcoin-Anleger davon, dass Bitcoin als erste und bekannteste Kryptowährung eine starke Marktposition und enormen Bekanntheitsgrad aufbauen konnte. Als First Mover konnte Bitcoin die Akzeptanz und Verbreitung von Kryptowährungen insgesamt vorantreiben und ist bis heute Benchmark und Maßstab für andere Kryptowährungen. Anleger, die frühzeitig in Bitcoin investiert haben, konnten daher enorme Wertsteigerungen verbuchen. Allerdings bringt die Pionierrolle auch Risiken mit sich. Insbesondere in der Anfangsphase war die Technologie noch mit Unsicherheiten und Kinderkrankheiten behaftet. Spätere, technologisch weiterentwickelte Kryptowährungen konnten von den Erfahrungen Bitcoins lernen und Verbesserungen vornehmen. Zudem ist der Wettbewerb im Kryptomarkt inzwischen sehr hoch, sodass Bitcoin seine Vormachtstellung langfristig möglicherweise nicht wird halten können. Für Bitcoin-Anleger bedeutet dies, dass sie zwar von den Chancen des First-Mover-Vorteils profitieren konnten, aber auch die Risiken eines Pioniers berücksichtigen müssen. Eine sorgfältige Analyse der Marktentwicklungen und Wettbewerbssituation ist daher für Investoren in Bitcoin unerlässlich.

FOMO - FOMO steht für "Fear of Missing Out", zu deutsch etwas zu verpassen, und beschreibt ein psychologisches Phänomen, das oft im Zusammenhang mit Anlageentscheidungen auftritt. Konkret bedeutet FOMO, dass Anleger aus Angst, etwas Wichtiges oder Lukratives zu verpassen, impulsiv in einen Markt investieren, ohne die Risiken ausreichend zu prüfen. Dieses Gefühl der Angst, den "Zug abzupassen", führt dann dazu, dass Anleger überstürzt und emotional handeln. Bei Blasen wie der Bitcoin-Blase verstärkt sich dieser Effekt oft zusätzlich. Wenn die Kurse rasant steigen, wollen Anleger schnell noch einsteigen, um nicht den vermeintlichen "großen Gewinn" zu verpassen.
FOMO ist dabei ein sehr menschliches Verhaltensmuster, das viele Anleger an den Rand der Rationalität treibt. Stattdessen sollten Investoren systematisch und unemotional ihre Entscheidungen treffen, um langfristig erfolgreich zu sein.

Eine gesunde Portion Skepsis gegenüber Hypes und die Fähigkeit, Ruhe zu bewahren, sind daher wichtige Erfolgsfaktoren beim Investieren. FOMO kann ansonsten leicht zu unüberlegten Fehlentscheidungen führen.

FUD - FUD steht im Zusammenhang mit Bitcoin für "Fear, Uncertainty and Doubt" (Angst, Unsicherheit und Zweifel). Damit bezeichnet man verbreitete negative Berichterstattung oder Äußerungen, die darauf abzielen, Investoren oder Interessenten von Bitcoin und anderen Kryptowährungen abzuschrecken. Einige Beispiele hierfür sind Berichte über angebliche Sicherheitslücken oder Hacks von Krypto-Börsen, die Zweifel an der Sicherheit von Bitcoin säen. Auch Warnungen vor der hohen Volatilität und Preisschwankungen des Bitcoin-Kurses, die Anleger verunsichern sollen, sowie Behauptungen, Bitcoin sei eine Blase oder werde schon bald zusammenbrechen, um Investoren vom Einstieg abzuhalten, zählen dazu. Regulatorische Unsicherheiten, etwa drohende Verbote oder Einschränkungen von Kryptowährungen, die Anleger abschrecken, gehören ebenfalls zu solchen FUD-Kampagnen. Diese werden oft von etablierten Finanzinstituten, Regierungen oder Kritikern gestartet, die ein Interesse daran haben, die Akzeptanz und Verbreitung von Bitcoin zu behindern. Als Anleger ist es wichtig, solche Gerüchte kritisch zu hinterfragen und sich auf fundierte Informationen zu stützen.

Full-Node – Siehe Node.

Genesis Block - Der Genisisblock ist der erste Block in der Blockchain von Bitcoin. Er wurde am 3. Januar 2009 von Satoshi Nakamoto, dem Erfinder von Bitcoin, geschürft.
Der Genisisblock ist ein besonderer Block, da er das Fundament für die gesamte Bitcoin-Blockchain bildet. In diesem Block sind einige wichtige Informationen enthalten:
Zeitstempel: Der Zeitstempel dokumentiert den Zeitpunkt, an dem der Block erstellt wurde - nämlich am 3. Januar 2009.
Transaktionen: Der Genisisblock enthält nur eine einzige Transaktion, nämlich die Prägung der ersten 50 BTC. Diese Bitcoins wurden an die Bitcoin-Adresse von Satoshi Nakamoto gesendet.
Nonce: Die Nonce ist ein Wert, der beim Mining verändert wird, um einen gültigen Hashwert zu finden, der die Blockvorgaben erfüllt.
Hash des vorherigen Blocks: Da es keinen vorherigen Block gibt, ist dieser Wert im Genisisblock auf 0 gesetzt. Auch die Blockhöhe ist selbstverständlich 0.
Der Genisisblock ist somit der Startpunkt der gesamten Bitcoin-Blockchain und enthält die Grundlagen für das Bitcoin-Netzwerk. Er ist in den Code des Bitcoin-Clients fest einprogrammiert und kann nicht verändert werden.

Gini – Koeffizien - Der Gini-Koeffizient ist ein statistisches Maß, das zur Messung der Ungleichverteilung in einer Gesellschaft oder Volkswirtschaft verwendet wird. Er wurde vom italienischen Ökonomen Corrado Gini entwickelt und ist heutzutage ein weltweit etablierter Standard für die Analyse von Einkommens- und Vermögensverteilungen. Der Gini-Koeffizient nimmt Werte zwischen 0 und 1 an, wobei 0 eine perfekte Gleichverteilung und 1 eine absolute Ungleichverteilung bedeutet. Je höher der Gini-Koeffizient, desto ungleicher ist die Verteilung.

Konkret berechnet sich der Gini-Koeffizient aus der Fläche zwischen der Lorenz-Kurve und der Gleichverteilungslinie. Die Lorenz-Kurve zeigt grafisch den kumulierten Anteil des Gesamteinkommens oder -vermögens, den die ärmsten x% der Bevölkerung besitzen. Der Gini-Koeffizient hat den Vorteil, dass er eine präzise, einzelne Zahl zur Messung der Ungleichheit liefert. Dies ermöglicht den Vergleich zwischen verschiedenen Ländern, Zeitpunkten oder auch Vermögensarten wie Einkommen, Vermögen oder Landbesitz. In der Praxis wird der Gini-

Koeffizient häufig zur Analyse von Einkommens- und Vermögensverteilungen in Volkswirtschaften herangezogen. Er dient Politikern, Ökonomen und Sozialwissenschaftlern als wichtiger Indikator für soziale Ungleichheit und Chancengerechtigkeit in einer Gesellschaft.

Green Candle - Im Kontext von Bitcoin bezeichnet man Anleger, die an steigende Kurse glauben und daher Bitcoins kaufen, als "green candle". Dieser Begriff leitet sich von den grünen Kerzen ab, die in Kursdiagrammen einen Preisanstieg symbolisieren. Anleger, die auf steigende Kurse setzen, hoffen, dass der Preis für einen Bitcoin kontinuierlich zunimmt und sie ihre Investition später mit Gewinn wieder verkaufen können. Sie vertrauen darauf, dass die Nachfrage nach Bitcoin langfristig steigt und sich die Kryptowährung als digitales Asset am Markt etabliert.
Im Gegensatz dazu stehen "red candle"-Anleger, die auf fallende Kurse setzen und Bitcoins verkaufen, um später günstiger wieder einzusteigen. Solche Anleger, die auf Kursverluste spekulieren, werden häufig als Skeptiker oder Zweifler an der Zukunft von Bitcoin wahrgenommen.
Insgesamt spiegelt die Unterscheidung zwischen "green candle" und "red candle" Anlegern das grundsätzliche Spannungsfeld zwischen Optimismus und Pessimismus in Bezug auf die Preisentwicklung von Bitcoin wider.
Es gibt noch eine banalere Beschreibung, die nur die Kursentwicklung, grün für steigend und rot für fallend, annimmt.

Grifter – Aus den Englischen für Betrüger. Es gibt viele Böswillige in der Welt und auch in der Bitcoin-Welt haben sich Betrüger eingeschlichen. Das sind im Grunde Hochstapler, die es schaffen, die Leute durch Betrug und Lügen um ihr Geld zu bringen, anstatt mit roher Gewalt. Diese Betrüger sind in praktisch jedem Aspekt von Bitcoin zu beobachten, nehmen aber verschiedene Formen an. Die offensichtlichsten Betrüger sind Anbieter von Scheinmünzen, die versuchen, Ihre Bitcoin mit Versprechungen von höheren Gewinnen durch Abzocktechniken zu ergaunern. Allerdings gibt es auch Betrüger in der Bitcoin-Welt, die versuchen, Sie in zufällige Telegram- oder Discord-Gruppen zu locken oder Ihnen versprechen, Ihr Geld zu "verdoppeln", wenn Sie ihnen zunächst etwas Bitcoin schicken.

Denken Sie daran, dass, wenn Sie Bitcoin an eine Wallet senden, deren private Schlüssel Sie nicht besitzen, sie Ihnen nicht mehr gehören.

Wenn Sie sich tief in Bitcoin eingearbeitet haben und jeden Satoshi schätzen, werden Sie gut vorbereitet sein, um den Tricks und Taktiken der Betrüger zu entgehen.

Halving - Das Halving bei Bitcoin ist ein wichtiger und regelmäßig stattfindender Prozess, der sich auf die Belohnung für das sogenannte "Mining" von Bitcoin bezieht. Um das Halving zu verstehen, ist es zunächst wichtig zu verstehen, was Bitcoin-Mining ist.
Bitcoin-Mining ist der Prozess, bei dem neue Transaktionen verifiziert und in die Blockchain von Bitcoin aufgenommen werden. Dies geschieht, indem leistungsstarke Computer komplexe mathematische Probleme lösen. Die Personen oder Unternehmen, die ihre Rechenleistung für das Mining zur Verfügung stellen, werden als "Miner" bezeichnet. Als Belohnung für ihre Bemühungen erhalten die Miner eine bestimmte Anzahl von neuen Bitcoins sowie Transaktionsgebühren für die Transaktionen, die sie verifizieren.
Das Halving ist ein festgelegtes Ereignis, das alle 210.000 Blöcke in der Blockchain stattfindet, was ungefähr alle vier Jahre geschieht. Bei jedem Halving wird die Belohnung, die die Miner für das Hinzufügen neuer Blöcke zur Blockchain erhalten, um die Hälfte reduziert. Als Bitcoin 2009 ins Leben gerufen wurde, betrug die Belohnung 50 Bitcoins pro Block. Nach dem ersten Halving im Jahr 2012 wurde die Belohnung auf 25 Bitcoins pro Block reduziert, und nach dem zweiten Halving im Jahr 2016 wurde sie auf 12,5 Bitcoins pro Block reduziert. Das letzte Halving fand am 20. April

2024 statt, wodurch die Belohnung auf 3,125 Bitcoins pro Block halbiert wurde.
Das Halving hat mehrere Auswirkungen auf das Bitcoin-Ökosystem. Zunächst einmal führt die Reduzierung der Belohnung dazu, dass weniger neue Bitcoins in Umlauf gebracht werden, was zu einer Verlangsamung des Angebotswachstums führt. Dies kann potenziell zu einer Knappheit und einer erhöhten Nachfrage nach Bitcoin führen, was sich wiederum auf den Preis auswirken kann. Einige Marktbeobachter glauben, dass das Halving zu einem Anstieg des Bitcoin-Preises führen könnte, da das Angebot knapper wird.
Darüber hinaus kann das Halving auch Auswirkungen auf die Rentabilität des Minings haben. Da die Belohnung für das Mining halbiert wird, müssen die Miner effizienter arbeiten, um ihre Betriebskosten zu decken. Dies kann dazu führen, dass weniger effiziente Miner aus dem Markt ausscheiden, während diejenigen mit Zugang zu kostengünstigeren Energiequellen oder leistungsstärkerer Hardware einen Wettbewerbsvorteil haben.
Insgesamt ist das Halving ein wichtiger Bestandteil des Bitcoin-Protokolls und trägt zur Begrenzung des Angebots und zur langfristigen Werterhaltung von Bitcoin bei. Es ist ein Ereignis, das von der gesamten Bitcoin-Community genau verfolgt wird, da es potenziell erhebliche Auswirkungen auf den Markt und die Mining-Industrie haben kann.

Hard Fork - Ein Hard Fork, zu deutsch eine harte Gabelung, ist eine nicht rückwärtskompatible Änderung des Bitcoinnetzwerks, was bedeutet, dass nach der Einführung eines Hard Forks ältere Bitcoin-Knoten die neuen Regeln nicht mehr akzeptieren können und daher ein Upgrade durchführen müssen, um am Netzwerk teilnehmen zu können.
Die Schritte eines Hard Forks sind analog zu den des Soft Forks, nur dass eben die Spaltung erfolgt.

1. Entwicklung der neuen Regeln: Die Bitcoin-Entwickler entwerfen neue, nicht rückwärtskompatible Regeln oder Funktionen für das Bitcoinnetzwerk. Diese Änderungen können z.B. die Blockgröße, die Blockzeitspanne oder die Geldschöpfungsrate betreffen.
2. Signalisierung und Abstimmung: Die Bitcoin-Knoten signalisieren ihre Unterstützung für den Hard Fork, indem sie spezielle Nachrichten in ihren Blocks übermitteln. Sobald eine bestimmte Mehrheit der Miners (z.B. 95%) den Hard Fork unterstützt, wird er aktiviert.
3. Aktivierung des Hard Forks: Nach Erreichen der Mehrheit treten die neuen Regeln in Kraft. Ab diesem Zeitpunkt müssen alle neuen Blöcke die neuen Regeln erfüllen, um vom Netzwerk akzeptiert zu werden. Ältere Nodes, die den Hard Fork nicht unterstützen, erkennen diese neuen Blöcke nicht mehr an, da die Änderungen nicht rückwärtskompatibel sind.
4. Aufspaltung des Netzwerks: Durch den Hard Fork entsteht nun ein zweites, parallel existierendes Bitcoinnetzwerk mit jeweils eigenen Regeln. Es gibt fortan zwei unterschiedliche Kryptowährungen: Bitcoin (mit den alten Regeln) und die neue Variante (mit den neuen Regeln).
5. Migration und Adoption: Über einen gewissen Zeitraum hinweg werden immer mehr Nodes und Nutzer auf die neue Variante umstellen. Irgendwann wird die neue Variante von der überwiegenden Mehrheit des Netzwerks unterstützt.

Im Gegensatz zur weichen Variante führt ein Hard Fork also zur Aufspaltung des Bitcoinnetzwerks in zwei separate Kryptowährungen. Dies kann manchmal notwendig sein, um grundlegende Änderungen am Protokoll vorzunehmen, birgt aber auch Risiken für die Stabilität und Einheit des Gesamtsystems. Als Folge von Hard Forks sind Bitcoin Cash und Ethereum als eigenständige Kryprowährungen entstanden.

Hardware-Wallet – Siehe Wallet.

Hash - In Bitcoin und anderen Kryptowährungen bezeichnet ein Hash eine kryptografische Funktion, die Daten in eine feste Zeichenfolge von Zeichen umwandelt. Dabei haben kleine Änderungen an den Eingangsdaten stark unterschiedliche Ausgabewerte zur Folge.
Konkret bedeutet das Folgendes:
Wenn man den Block-Header eines Bitcoin-Blocks (der die Transaktionsdaten, Zeitstempel, Nonce etc. enthält) in die Hash-Funktion SHA-256 eingibt, erhält man einen 256-bit langen Hashwert. Dieser Hashwert dient als "Fingerabdruck" des Blocks und ist einzigartig. Selbst die kleinste Änderung im Block-Header würde zu einem völlig anderen Hashwert führen.
Im Bitcoin-Mining-Prozess müssen Miner einen Hashwert finden, der unter einem bestimmten Zielwert liegt. Dafür variieren sie die Nonce im Block-Header, bis ein gültiger Hashwert gefunden ist. Sobald ein Miner einen gültigen Hashwert findet, wird der Block in die Blockchain aufgenommen und der Miner erhält eine Belohnung.
Die Hash-Funktion ist also ein zentrales Konzept in Bitcoin, das eine sichere und unveränderbare Verkettung der Blöcke in der Blockchain ermöglicht. Die Eigenschaft, dass kleine Änderungen zu völlig anderen Hashwerten führen, ist für die Integrität und Sicherheit des gesamten Bitcoin-Netzwerks entscheidend.

Hashrate - Die Hashrate ist bei Bitcoin ein äußerst wichtiger und grundlegender Konzept. Sie bezeichnet die Rechenleistung, die im Bitcoin-Netzwerk zur Verfügung steht, um neue Blöcke zu schürfen und die Blockchain zu sichern. Die Hashrate wird in Hashes pro Sekunde gemessen und gibt an, wie viele Berechnungen pro Sekunde vom gesamten Netzwerk durchgeführt werden. Je höher die Hashrate, desto mehr Rechenleistung wird aufgewendet, um die Blockchain zu verarbeiten und neue Blöcke hinzuzufügen. Die Hashrate ist essentiell für die Funktionsweise und Sicherheit des Bitcoin-Netzwerks. Je höher die Hashrate, desto schwieriger wird es für Angreifer, das Netzwerk zu manipulieren oder zu übernehmen. Eine hohe Hashrate macht es praktisch unmöglich, die Blockchain zu fälschen oder zu ändern, da dies einen enormen Rechenaufwand erfordern würde. Außerdem bestimmt die Hashrate die Schwierigkeit des Schürfens neuer Blöcke. Das Bitcoin-Protokoll passt die Schwierigkeitsstufe automatisch an, so dass alle 10 Minuten ein neuer Block hinzugefügt wird. Je höher die Hashrate, desto schwieriger wird es, neue Blöcke zu schürfen, da mehr Rechenleistung erforderlich ist. Insgesamt ist die Hashrate ein zentraler Faktor für die Sicherheit, Dezentralisierung und Stabilität des Bitcoin-Netzwerks. Eine hohe und stabile Hashrate ist ein Indikator für die Gesundheit und Robustheit des Systems.

Helikpotergeld - Helikoptergeld (englisch: helicopter money) bezeichnet eine unkonventionelle geldpolitische Maßnahme, bei der die Zentralbank Bargeld direkt an die Bürger verteilt, anstatt es über Banken in das Finanzsystem zu pumpen. Der Begriff "Helikoptergeld" geht auf den Ökonomen Milton Friedman zurück, der dieses Konzept 1969 erstmals erwähnte. Er verglich die direkte Geldverteilung mit dem Bild eines Helikopters, das Geldscheine über der Bevölkerung abwirft. Theoretisch soll Helikoptergeld die Inflationsrate ankurbeln und die Konjunktur beleben, indem es die Kaufkraft der Verbraucher direkt erhöht. Im Gegensatz zu klassischen Konjunkturprogrammen, die über Staatsausgaben oder Steuersenkungen wirken, wäre Helikoptergeld eine Maßnahme der Zentralbank. Kritisch zu betrachten sind dabei allerdings einige Aspekte. So könnte die direkte Geldverteilung durch die Zentralbank deren Unabhängigkeit und Glaubwürdigkeit untergraben und langfristig das Vertrauen in die Währung und die Preisstabilität gefährden. Außerdem besteht die Gefahr unkontrollierter Preissteigerungen, sollte die Geldmenge zu stark ausgeweitet werden. Darüber hinaus hätte Helikoptergeld eine Umverteilungswirkung, da ärmere Haushalte einen größeren Anteil ihres Einkommens für den Konsum aufwenden würden, was zu sozialen Spannungen führen könnte. Auch eine mögliche Fehlallokation von Kapital, bei der ein Teil des Helikoptergelds in Spekulation und riskante Anlagen umgeleitet wird, wäre bedenklich,

da dies Blasenbildung am Finanzmarkt begünstigen könnte. Nicht zuletzt ist die tatsächliche Wirksamkeit von Helikoptergeld fraglich, da andere Maßnahmen wie Zinssenkungen oder Staatsausgaben unter Umständen effektiver sein könnten. Insgesamt ist Helikoptergeld also ein sehr kontroverses geldpolitisches Instrument, das mit Vorsicht und Umsicht eingesetzt werden müsste. Die Risiken übersteigen möglicherweise die potenziellen Vorteile, sodass eine kritische Betrachtungsweise angebracht ist.

Hodl – Siehe dazu das Kapitel Ich hodle!

Hopium - Der Begriff "Hopium" in Bezug auf Bitcoin bezieht sich auf eine übertrieben optimistische Haltung gegenüber der Zukunft von Bitcoin. Damit ist gemeint, dass Anhänger von Bitcoin manchmal dazu neigen, die positiven Aspekte von Bitcoin zu überbewerten und die möglichen Risiken oder negativen Entwicklungen zu ignorieren. Sie glauben oftmals fest an einen massiven Kursanstieg von Bitcoin in der Zukunft, ohne die realistischen Chancen und Herausforderungen ausreichend zu berücksichtigen. Diese Haltung wird als "Hopium" bezeichnet - eine Mischung aus Hoffnung (engl. „hope“) und einer suchtartigen Annahme, dass Bitcoin zwangsläufig ein enormes Kurspotenzial hat. Kritiker sehen darin eine unrealistische, fast schon berauschte Sichtweise, die die tatsächlichen Risiken und Probleme von Bitcoin ausblendet. Dies kann zu Enttäuschungen und Verlusten führen, wenn die überzogenen Erwartungen nicht eintreten. Der Begriff „Hopium“ soll also vor einer irrationalen, übertriebenen Euphorie gegenüber Bitcoin warnen und zu einer realistischeren Einschätzung der Chancen und Risiken aufrufen.

Hyperbitcoinization - Der Begriff "Hyperbitcoinization" bezieht sich auf ein hypothetisches Szenario, in dem Bitcoin die vorherrschende globale Währung wird und das traditionelle Finanzsystem vollständig ablöst. In diesem Szenario würde Bitcoin so dominant und allgegenwärtig, dass es zu einer radikalen Umwälzung des Geldsystems kommt. Anhänger dieses Konzepts glauben, dass Bitcoin aufgrund seiner Eigenschaften wie Dezentralität, Knappheit und Unveränderbarkeit letztendlich das traditionelle Finanzsystem verdrängen und zum neuen Standard werden könnte. Sie sehen in Bitcoin die Möglichkeit, sich vom bestehenden Fiat-Geldsystem und den damit verbundenen Problemen wie Inflation, Geldpolitik und Vermögensentwertung zu befreien. Durch eine zunehmende Akzeptanz und Verbreitung von Bitcoin in der Gesellschaft, sei es als Zahlungsmittel, Wertaufbewahrungsmittel oder Investitionsobjekt, könnte sich laut dieser Theorie eine "Hyperbitcoinization" ergeben. In diesem Fall würden immer mehr Menschen und Unternehmen auf Bitcoin umsteigen und das traditionelle Finanzsystem schließlich vollständig verdrängt werden. Allerdings ist dieses Szenario sehr spekulativ und unter Experten umstritten. Viele sehen Hyperbitcoinization als unwahrscheinlich an und betonen, dass Bitcoin vermutlich eher als digitales Vermögenswert neben etablierten Währungen und Finanzsystemen existieren wird, anstatt diese komplett zu ersetzen.

Key - Das Prinzip der Public und Private Keys bei Bitcoin ist von grundlegender Bedeutung für das Verständnis, wie Transaktionen durchgeführt und Bitcoin sicher gespeichert werden. Das Konzept beruht auf einem Schlüsselpaar, dem privaten und dem öffentlichen Schlüssel.

- Öffentlicher Schlüssel (Public Key): Der öffentliche Schlüssel ist ein kryptographischer Schlüssel, der verwendet wird, um Bitcoin an eine bestimmte Wallet-Adresse zu senden. Er wird aus dem privaten Schlüssel abgeleitet und kann sicher an andere Benutzer weitergegeben werden, ohne die Sicherheit der Wallet zu gefährden. Der öffentliche Schlüssel dient als Empfangsadresse, an die andere Benutzer Bitcoin senden können.
- Privater Schlüssel (Private Key): Der private Schlüssel ist äußerst vertraulich und sollte

niemals mit anderen geteilt werden. Er wird verwendet, um Transaktionen von einer Wallet zu autorisieren und ist entscheidend für den Zugriff auf die in der Wallet gespeicherten Bitcoin. Der private Schlüssel wird verwendet, um den öffentlichen Schlüssel zu erzeugen und muss daher absolut sicher aufbewahrt werden, da der Verlust des privaten Schlüssels dazu führen kann, dass die in der Wallet gespeicherten Bitcoin unwiederbringlich verloren gehen.

Das Konzept basiert auf Public-Key-Kryptographie, einem Verschlüsselungsverfahren, das es ermöglicht, Informationen sicher zu übertragen, ohne dass die Sicherheit beeinträchtigt wird. Der öffentliche Schlüssel wird aus dem privaten Schlüssel abgeleitet, wobei eine mathematische Beziehung zwischen den beiden Schlüsseln besteht, die es ermöglicht, Transaktionen zu verifizieren und zu autorisieren. Wenn eine Person Bitcoin an eine Wallet senden möchte, verwendet sie den öffentlichen Schlüssel der Wallet, um die Transaktion zu verschlüsseln und zu signieren. Die Transaktion wird dann von der Bitcoin-Blockchain verifiziert und in die öffentliche Transaktionsgeschichte aufgenommen. Um Bitcoin von der Wallet zu senden, muss der Besitzer den privaten Schlüssel verwenden, um die Transaktion zu signieren und zu autorisieren. Dies stellt sicher, dass nur der rechtmäßige Besitzer der Wallet Transaktionen durchführen kann.
Die Sicherheit von Public und Private Keys ist von größter Bedeutung, da der Verlust des privaten Schlüssels dazu führen kann, dass die in der Wallet gespeicherten Bitcoin unwiederbringlich verloren gehen. Daher ist es unerlässlich, den privaten Schlüssel sicher und vertraulich aufzubewahren, beispielsweise durch die Verwendung von Hardware-Wallets oder Papier-Wallets, die vor Online-Bedrohungen schützen können.
Insgesamt sind Public und Private Keys ein wesentlicher Bestandteil des Bitcoin-Ökosystems und stellen sicher, dass Transaktionen sicher und vertraulich durchgeführt werden können. Durch die Verwendung von Public-Key-Kryptographie wird die Integrität und Sicherheit des Bitcoin-Netzwerks gewährleistet, und die richtige Verwaltung und Aufbewahrung der privaten Schlüssel ist entscheidend für den Schutz der in einer Wallet gespeicherten Bitcoin.

KYC - KYC steht für "Know Your Customer" und ist ein wichtiger Bestandteil der Geldwäscheprävention. Es bezeichnet die Verpflichtung von Finanzinstituten und anderen Unternehmen, ihre Kunden eindeutig zu identifizieren und zu überprüfen.
Der KYC-Prozess hat folgende Hauptziele:

- Identifizierung des Kunden: Unternehmen müssen die Identität ihrer Kunden zweifelsfrei feststellen. Dafür werden üblicherweise amtliche Ausweisdokumente wie Personalausweis oder Reisepass verlangt.
- Überprüfung der Identität: Die angegebenen Identitätsinformationen werden überprüft, um sicherzustellen, dass es sich um echte Personen handelt und keine Scheinfirmen oder anonymen Konstrukte.
- Ermittlung des wirtschaftlich Berechtigten: Hinter einer Transaktion oder Geschäftsbeziehung kann eine andere Person als der direkte Vertragspartner stehen, die die tatsächliche Kontrolle ausübt. Auch diese "wirtschaftlich Berechtigten" müssen identifiziert werden.
- Feststellung des Geschäftszwecks: Unternehmen müssen den Zweck und die angestrebte Art der Geschäftsbeziehung ermitteln, um Risiken einschätzen zu können.
- Laufende Überwachung: Auch nach Vertragsabschluss müssen Unternehmen die Aktivitäten und Transaktionen ihrer Kunden überwachen, um Auffälligkeiten frühzeitig zu erkennen.

Der KYC-Prozess ist gesetzlich vorgeschrieben und soll verhindern, dass Kriminelle das Finanzsystem für illegale Zwecke missbrauchen. Durch die genaue Prüfung der Kunden und ihrer Aktivitäten sollen Geldwäsche, Terrorismusfinanzierung und andere schwere Straftaten erschwert

werden. Regelmäßige Aktualisierungen der Kundendaten und eine risikobasierte Herangehensweise sind wichtige Aspekte, um den KYC-Prozess effektiv umzusetzen.

Laser Eyes - Der Begriff "Laser Eyes" in Verbindung mit Bitcoin bezieht sich auf ein visuelles Meme, das von Bitcoin-Befürwortern und -Enthusiasten verwendet wird, um ihre Unterstützung und ihren Optimismus für die Zukunft von Bitcoin zum Ausdruck zu bringen. Das Laser-Eyes-Meme zeigt üblicherweise ein Profilbild oder Avatar, bei dem den dargestellten Personen oder Charakteren rote, laserförmige Augen hinzugefügt werden. Dieses auffällige visuelle Element soll die Entschlossenheit und Leidenschaft der Bitcoin-Anhänger symbolisieren, die fest an einen massiven Kursanstieg von Bitcoin glauben. Die Verwendung von Laser Eyes ist in der Bitcoin-Community weit verbreitet und wird oft in sozialen Medien oder Online-Foren eingesetzt. Es dient dazu, die Zuversicht und den Enthusiasmus der Bitcoin-Gemeinschaft zu demonstrieren und ihre Überzeugung zum Ausdruck zu bringen, dass der Bitcoin-Preis in absehbarer Zeit exponentiell steigen wird. Allerdings wird das Laser-Eyes-Meme auch von Kritikern als Ausdruck einer übertriebenen, irrationalen Euphorie gegenüber Bitcoin gesehen. Sie argumentieren, dass es die Realitäten und Risiken des Kryptowährungsmarktes ausblendet und eine unrealistische Erwartungshaltung fördert. Insgesamt stellen die Laser Eyes ein prägnantes visuelles Symbol dar, das die Leidenschaft und Zuversicht der Bitcoin-Anhänger zum Ausdruck bringt, aber auch als Warnung vor einer überzogenen Euphorie interpretiert werden kann.

Ledger - Ein zentraler Begriff in Bezug auf Bitcoin ist der „Ledger“. Darunter versteht man das öffentliche Hauptbuch oder Transaktionsprotokoll, in dem alle Bitcoin-Transaktionen chronologisch aufgezeichnet werden. Der Ledger fungiert als eine Art digitale Buchhaltung für das Bitcoin-Netzwerk. Jede Überweisung von Bitcoin-Einheiten wird darin erfasst und für alle Teilnehmer transparent dokumentiert. Auf diese Weise wird sichergestellt, dass jede Bitcoin-Transaktion eindeutig nachvollziehbar ist und niemand Bitcoins doppelt ausgibt oder fälschlicherweise Besitzansprüche erhebt. Der Bitcoin-Ledger wird dezentral von allen Knoten im Bitcoin-Netzwerk verwaltet und ständig aktualisiert. Jeder Teilnehmer, der einen Bitcoin-Knoten betreibt, verfügt über eine vollständige Kopie des Ledgers. Dadurch entsteht ein robustes, manipulationsresistentes System, das ohne zentrale Kontrollinstanz auskommt. Die Integrität und Unveränderbarkeit des Bitcoin-Ledgers ist ein Schlüsselprinzip, das das Vertrauen in das dezentrale Finanzsystem von Bitcoin begründet. Jede Transaktion wird kryptografisch signiert und kann nicht rückgängig gemacht oder gefälscht werden, solange die Mehrheit der Netzwerkteilnehmer ehrlich bleibt. Insgesamt stellt der Ledger das zentrale Aufzeichnungssystem dar, das die Funktionsweise und Sicherheit des Bitcoin-Netzwerks gewährleistet, indem alle Überweisungen von Bitcoin transparent und manipulationssicher dokumentiert werden.

Lightning - Lightning ist eine sogenannte "Second Layer"-Lösung für das Bitcoin-Netzwerk, die entwickelt wurde, um einige der Herausforderungen von Bitcoin zu bewältigen, wie z.B. Skalierbarkeit und Transaktionsgeschwindigkeit. Mit Lightning können Benutzer "Mikrotransaktionen" off-chain durchführen, was bedeutet, dass Transaktionen nicht unmittelbar in der Blockchain verzeichnet werden müssen. Stattdessen können mehrere Transaktionen außerhalb der Blockchain durchgeführt werden, bevor die endgültigen Ergebnisse in die Blockchain geschrieben werden. Dies ermöglicht schnellere Transaktionen und reduzierte Transaktionskosten. Lightning nutzt ein Netzwerk von bidirektionalen Zahlungskanälen, die es den Benutzern ermöglichen, direkt miteinander zu interagieren, ohne jede Transaktion auf der Haupt-Blockchain festhalten zu müssen. Dies führt zu mehr Skalierbarkeit und niedrigeren Kosten im Vergleich zu Transaktionen, die ausschließlich auf der Haupt-Blockchain durchgeführt werden.

Light-Node – Siehe Node.

Margening - Das Margening, auch als Margining bezeichnet, ist ein wichtiger Aspekt des Clearing-Prozesses in der Finanzwelt. Es beschreibt die Anforderung an Marktteilnehmer, eine bestimmte Summe an Sicherheiten oder Bareinlagen zu hinterlegen, um ihre Transaktionen und Positionen abzusichern. Der Zweck des Marginings ist es, das Ausfallrisiko für die Clearingstelle und andere Marktteilnehmer zu minimieren. Wenn eine Partei ihre Verpflichtungen nicht erfüllen kann, können die hinterlegten Sicherheiten verwendet werden, um die entstandenen Verluste auszugleichen.
Der Prozess des Marginings funktioniert wie folgt: Zu Beginn einer Transaktion oder beim Eingehen einer Position muss der Marktteilnehmer eine anfängliche Margin, also eine Mindesteinlage, hinterlegen. Diese Margin dient als Sicherheit. Während der Laufzeit der Transaktion oder Position wird der Wert der Sicherheiten laufend überprüft und angepasst. Sinkt der Wert unter ein bestimmtes Niveau, muss der Teilnehmer zusätzliche Sicherheiten nachschießen (Nachschusspflicht). Umgekehrt kann überschüssige Margin auch wieder an den Teilnehmer zurückgegeben werden, wenn der Wert der Positionen steigt.
Das Margening ist ein zentrales Risikomanagement-Instrument, das dazu beiträgt, die Stabilität und Funktionsfähigkeit der Finanzmärkte zu gewährleisten. Es erhöht die Sicherheit für alle Beteiligten und reduziert die Gefahr von Ausfällen und Dominoeffekten. Durch die laufende Anpassung der hinterlegten Sicherheiten wird sichergestellt, dass die Marktteilnehmer jederzeit in der Lage sind, ihre Verpflichtungen zu erfüllen, und so zum reibungslosen Ablauf des Finanzsystems beitragen.

Mempool - Der Mempool bei Bitcoin ist ein wichtiger Teil des Bitcoin-Netzwerks. Er ist eine Art Warteschlange, in der alle Transaktionen zwischengespeichert werden, die noch nicht in einem Bitcoin-Block aufgenommen wurden. Wenn ein Bitcoin-Nutzer eine Transaktion initiiert, wird diese zunächst in den Mempool aufgenommen. Von dort aus werden die Transaktionen dann von den Minern ausgewählt und in einen neuen Bitcoin-Block aufgenommen. Die im Mempool befindlichen Transaktionen warten also darauf, von den Minern in einen Block geschrieben zu werden. Dabei konkurrieren die Transaktionen untereinander, da die Miner normalerweise zuerst diejenigen Transaktionen in einen Block aufnehmen, die die höchsten Transaktionsgebühren bieten. Je mehr Transaktionen im Mempool warten, desto größer wird der Stau. Das kann dazu führen, dass es länger dauert, bis eine Transaktion bestätigt wird. Nutzer können dann die Transaktionsgebühr erhöhen, um ihre Transaktion bevorzugt in einen Block aufnehmen zu lassen. Der Mempool ist also eine wichtige Brücke zwischen den Bitcoin-Nutzern, die Transaktionen initiieren, und den Minern, die diese Transaktionen in neue Blöcke aufnehmen. Er ermöglicht es dem Bitcoin-Netzwerk, Transaktionen effizient zu verarbeiten.

MiCA - Die MiCA-Verordnung (Crypto-Assets Market Regulation / Märkte für Krypto-Vermögenswerte) der Europäischen Union wurde ins Leben gerufen um eine einheitliche Gesetzgebung für Kryptowährungen in der gesamten EU zu schaffen.

Hauptziele der MiCA-Verordnung:

- Einheitliche Regulierung für Krypto-Vermögenswerte in der gesamten EU schaffen
- Rechtssicherheit und Verbraucherschutz für Investoren in Krypto-Assets erhöhen
- Innovationen im Krypto-Sektor fördern und gleichzeitig Risiken minimieren

Die wichtigsten Eckpunkte der MiCA-Verordnung sind wie folgt:

- Klassifizierung von Krypto-Vermögenswerten in verschiedene Kategorien wie Utility-

Token, Anlage-Token, E-Geld-Token und Stablecoins
- Lizenzpflicht und aufsichtsrechtliche Anforderungen für Krypto-Dienstleistungsanbieter
- Offenlegungspflichten und Transparenzregeln für Emittenten von Krypto-Assets
- Besondere Regeln für Stablecoins, um Risiken für die Finanzstabilität zu begrenzen
- Umwelt- und Nachhaltigkeitsanforderungen für Krypto-Projekte
- EU-weite Passporting-Regelung für zugelassene Krypto-Anbieter

Mit MiCA will die EU einen harmonisierten Rechtsrahmen für den Krypto-Markt schaffen, um Innovation zu ermöglichen und gleichzeitig Verbraucherschutz sowie Finanzstabilität zu gewährleisten.

Miner - Miner sind Personen oder Organisationen, die am Bitcoin-Netzwerk teilnehmen, um neue Bitcoin-Transaktionen zu verifizieren und in den Blockchain-Datensatz aufzunehmen. Sie spielen eine wichtige Rolle im Bitcoin-System, da sie für die Aufrechterhaltung und Sicherheit des Netzwerks verantwortlich sind. Ihre Hauptaufgaben sind die Überprüfung von Transaktionen, indem sie die Signatur und den Besitznachweis der beteiligten Adressen überprüfen, sowie die Erstellung von Blöcken, in denen sie die überprüften Transaktionen bündeln und versuchen, den Proof-of-Work-Algorithmus zu lösen, um den nächsten Block in der Blockchain zu generieren. Durch diesen Proof-of-Work-Prozess tragen Miner zur Sicherheit und Integrität des Bitcoin-Netzwerks bei, da es sehr aufwendig ist, das Netzwerk zu manipulieren oder anzugreifen. Als Belohnung für ihre Arbeit erhalten Miner neue Bitcoin-Einheiten sowie Transaktionsgebühren, was ein Anreiz ist, am Netzwerk teilzunehmen und die Verarbeitung von Transaktionen zu unterstützen. Zusammenfassend sind Miner das Rückgrat des Bitcoin-Netzwerks, da sie die Transaktionen verifizieren, neue Blöcke erstellen und so die Sicherheit und Integrität des Systems gewährleisten.

Mining - Beim Bitcoin-Mining, zu deutsch schürfen, handelt es sich um den Prozess, durch den neue Bitcoins erzeugt werden und gleichzeitig die Transaktionen innerhalb des Bitcoin-Netzwerks verarbeitet und gesichert werden. Dies geschieht durch das Lösen komplexer mathematischer Probleme mithilfe leistungsstarker Computer.
Grundsätzlich basiert das Bitcoin-Mining auf dem Proof of Work-Prinzip, bei dem Miner (so werden die Personen oder Unternehmen genannt, die am Mining beteiligt sind) mathematische Rätsel lösen müssen, um neue Blöcke in die Blockchain einzufügen. Die Blockchain ist im Wesentlichen eine öffentliche, dezentralisierte Datenbank, die alle Transaktionen enthält, die jemals in der Geschichte von Bitcoin stattgefunden haben. Die Miner konkurrieren miteinander, um diese mathematischen Rätsel zu lösen, und derjenige, der dies als Erster schafft, erhält die Belohnung in Form von neuen Bitcoins sowie Transaktionsgebühren.
Um an diesem Wettbewerb teilzunehmen, benötigen die Miner spezielle Hardware, wie beispielsweise leistungsstarke Computer mit speziellen Grafikprozessoren (GPUs) oder noch leistungsfähigere spezialisierte Maschinen, die als ASICs (Application-Specific Integrated Circuits) bezeichnet werden. Diese Hardware ist darauf ausgelegt, die komplexen mathematischen Berechnungen so schnell wie möglich durchzuführen, um die Chance zu erhöhen, als Erster das Rätsel zu lösen. Es ist wichtig anzumerken, dass das Bitcoin-Mining nicht nur dazu dient, neue Bitcoins zu erzeugen, sondern auch dazu, die Integrität des Netzwerks zu gewährleisten, indem die Transaktionen bestätigt und in Blöcken gesichert werden. Dieser Prozess sorgt dafür, dass das Bitcoin-Netzwerk sicher und transparent bleibt.
In den letzten Jahren hat sich das Bitcoin-Mining aufgrund des steigenden Schwierigkeitsgrades und des Energieverbrauchs, der mit dem Betrieb leistungsstarker Mining-Hardware verbunden ist, stark weiterentwickelt. Es hat auch zu Diskussionen über Umweltauswirkungen geführt, da einige Mining-Betriebe große Mengen an Energie verbrauchen, insbesondere wenn sie mit nicht

erneuerbaren Energiequellen betrieben werden.
Zusammenfassend lässt sich sagen, dass das Bitcoin-Mining ein wesentlicher Bestandteil des Bitcoin-Netzwerks ist, da es die Erzeugung neuer Bitcoins ermöglicht und gleichzeitig die Sicherheit und Integrität des Netzwerks gewährleistet.

Mining-Node – Siehe Node.

Mining-Pool - Ein Mining-Pool ist ein Zusammenschluss von mehreren individuellen Minern, die ihre Rechenleistung kombinieren, um die Chancen zu erhöhen, Belohnungen aus dem Mining von Kryptowährungen zu erhalten. Diese Pools sind besonders in der Welt des Kryptowährungs-Minings verbreitet, da sie es den Teilnehmern ermöglichen, ihre Ressourcen zu bündeln und die Wahrscheinlichkeit zu erhöhen, dass sie Belohnungen für das Hinzufügen von Transaktionen zur Blockchain erhalten.
Die Funktionsweise eines Mining-Pools ist relativ einfach: Anstatt alleine zu minen, schließen sich mehrere Miner zusammen und kombinieren ihre Rechenleistung. Wenn einer der Miner im Pool erfolgreich einen Block löst und die Transaktionen bestätigt, werden die Belohnungen entsprechend der geleisteten Rechenleistung auf die Teilnehmer des Pools aufgeteilt.
Ein Mining-Pool wird in der Regel von einem Pool-Administrator verwaltet, der die technische Infrastruktur bereitstellt und die Auszahlungen an die Teilnehmer koordiniert. Die Teilnehmer des Pools tragen zur Rechenleistung bei und erhalten im Gegenzug eine Belohnung entsprechend ihres Beitrags.
Die Vorteile eines Mining-Pools liegen in der erhöhten Stabilität und Regelmäßigkeit der Einkünfte im Vergleich zum Solo-Mining. Durch die Kombination der Rechenleistung vieler Miner erhöht sich die Wahrscheinlichkeit, dass der Pool regelmäßig Blöcke löst und Belohnungen erhält. Dies reduziert die Varianz der Einkünfte, da die Belohnungen gleichmäßiger auf die Teilnehmer des Pools verteilt werden.
Darüber hinaus ermöglicht ein Mining-Pool auch kleineren Minern, an der Belohnung des Kryptowährungs-Minings teilzuhaben, ohne über die erforderliche Rechenleistung zu verfügen, um alleine erfolgreich zu sein. Dies trägt zur Dezentralisierung des Mining-Ökosystems bei, da auch kleinere Teilnehmer eine Chance haben, Belohnungen zu erhalten.
Insgesamt ist ein Mining-Pool eine gemeinschaftliche Anstrengung von Minern, um die Chancen auf Belohnungen aus dem Kryptowährungs-Mining zu erhöhen und die Einkünfte zu stabilisieren. Durch die Bündelung von Ressourcen können die Teilnehmer des Pools regelmäßigere Einkünfte erzielen und auch kleinere Miner haben die Möglichkeit, an den Belohnungen des Minings teilzuhaben.

Modern Money Theory - Die Moderne Geldtheorie (MMT) ist ein relativ neues ökonomisches Konzept, das in den letzten Jahren verstärkt diskutiert wird. Befürworter der MMT argumentieren, dass Staaten, die ihre Währung selbst ausgeben können, nicht den üblichen Haushaltsregeln folgen müssen, da sie ihre Finanzen nicht wie Haushalte managen müssen. Stattdessen könnten sie die Wirtschaft durch staatliche Ausgaben ankurbeln, ohne sich um Defizite oder steigende Staatsverschuldung sorgen zu müssen.

Allerdings gibt es viele Kritikpunkte, die an der MMT geäußert werden und die ihre Praxistauglichkeit infrage stellen:

- Inflationsgefahr: Laut MMT-Theorie könnten Staaten unbegrenzt Geld schaffen, um ihre Ausgaben zu finanzieren. Jedoch birgt dies die große Gefahr, dass die Inflation außer Kontrolle geraten könnte. Übermäßige staatliche Ausgaben können zu einer Übererhitzung

der Wirtschaft führen und die Preise in die Höhe treiben.
Inflation=f(Geldmenge,Wirtschaftsleistung)

- Verlust der Unabhängigkeit: Wenn Staaten die Kontrolle über ihre Fiskalpolitik verlieren und sich nur noch auf die Geldpolitik der Zentralbank verlassen, könnten sie ihre wirtschaftspolitische Souveränität einbüßen. Dies könnte zu Interessenkonflikten zwischen Staat und Zentralbank führen.
- Internationale Wettbewerbsfähigkeit: Durch eine expansive Fiskalpolitik und steigende Inflation könnte die internationale Wettbewerbsfähigkeit eines Landes leiden. Dies könnte negative Auswirkungen auf den Außenhandel und die Zahlungsbilanz haben.
- Ethische Bedenken: Die MMT könnte als Rechtfertigung für eine unkontrollierte Staatsverschuldung und Geldentwertung dienen. Dies könnte vor allem zukünftige Generationen belasten und wäre aus ethischer Sicht fragwürdig.

Zusammenfassend lässt sich sagen, dass die Moderne Geldtheorie zwar einige interessante Ansätze liefert, jedoch erhebliche Risiken birgt. Eine unkritische Umsetzung der MMT-Konzepte könnte zu schwerwiegenden wirtschaftlichen und gesellschaftlichen Problemen führen. Stattdessen bedarf es einer umsichtigen und ausgewogenen Wirtschaftspolitik, die die Stabilität des Finanzsystems und die Interessen aller Bürger im Blick hat.

Moscow Time - Im März 2021 hatte der Twitter-Milliardär Jack Dorsey ein Videotelefonat, bei dem er sich mit dem Thema Falschinformationen im Ausschuss des Repräsentantenhauses auseinandersetzte. In seinem Videobild war eine Blockuhr zu sehen. Auf dieser Uhr stand die Zahl 1952, was den Betrag an Satoshis angab, die man zu diesem Zeitpunkt für 1 US-Dollar kaufen konnte. Als ein Nocoiner, ein Bitcoin Unbedarfter, den Stream verfolgte, dachte der Cybersicherheitsforscher Chris Vickery, er hätte ein Geheimnis um die seltsame Uhr in Dorseys Raum gelüftet. Vickery vermutete, dass Dorsey die Uhr nach russischer Zeit eingestellt hatte. Das war jedoch auch seltsam, da die Sonne in Moskau zu diesem Zeitpunkt bereits untergegangen war. Natürlich begannen die Bitcoin-Anhänger auf Twitter, diesen verifizierten Account zu verspotten, und sie hatten ihren Spaß dabei. „Wenn du beginnst, dein Leben in Satoshis zu messen, dann denke daran, dass du jetzt nach Moskauer Zeit lebst.“

Need-to-Know-Prinzip - Das Need-to-know-Prinzip, was übersetzt so viel bedeutet, dass jeder nur so viel Informationen bekommt um seine Tätigkeit zu verrichten zu können, ist ein Machtinstrument, um Informationen und Wissen zu kontrollieren und zu beschränken. Wer darüber entscheidet, wer welche Informationen benötigt, hat die Kontrolle über den Informationsfluss und kann so die Macht- und Wissensverteilung innerhalb einer Organisation steuern. In hierarchischen Strukturen kann das Prinzip dazu verwendet werden, Führungskräfte von Mitarbeitern abzuschotten und deren Einsicht in strategische Entscheidungen zu beschränken. Dadurch entsteht eine Informationsasymmetrie, die es Vorgesetzten ermöglicht, ihre Position zu festigen und Kontrolle auszuüben. Außerdem kann das selektive Zurückhalten von Informationen dazu dienen, bestimmte Personengruppen von Entscheidungsprozessen auszuschließen und ihre Handlungsspielräume einzuschränken. Dies kann zu Intransparenz, Entmündigung und der Konzentration von Macht in den Händen weniger führen. In einer extrem rigiden Auslegung des Prinzips besteht die Gefahr, dass ein regelrechtes "Need-to-know-Denken" entsteht, bei dem der Informationsaustausch generell als Bedrohung angesehen und unnötig erschwert wird. Dies kann die Zusammenarbeit, Kreativität und Innovation in Organisationen erheblich behindern. Daher ist es wichtig, das Need-to-know-Prinzip stets kritisch zu hinterfragen und mit anderen Prinzipien wie Transparenz, Rechenschaftspflicht und Partizipation in Einklang zu bringen. Nur so kann sein Missbrauch als Herrschaftsinstrument vermieden und ein ausgewogener Interessenausgleich gefunden werden.

NFT - NFT steht für "Non-Fungible Token" und bezieht sich auf eine Art von digitalen Vermögenswerten, die auf einer Blockchain-Plattform, in der Regel der Ethereum-Blockchain, erstellt und gehandelt werden. Im Gegensatz zu Kryptowährungen wie Bitcoin oder Ethereum, die fungible Einheiten darstellen, was bedeutet, dass sie untereinander austauschbar sind, sind NFTs einzigartig und nicht austauschbar.
Die Einzigartigkeit von NFTs liegt in ihrer Fähigkeit, digitale Inhalte wie Kunstwerke, Musik, Videos, Sammlerstücke, virtuelle Grundstücke und andere digitale Vermögenswerte zu repräsentieren. Jedes NFT enthält Metadaten, die seine Einzigartigkeit und Eigentumsrechte definieren. Diese Metadaten werden in einem Smart Contract auf der Blockchain gespeichert, was die Authentizität und Unveränderlichkeit des NFT gewährleistet.
Die Funktionsweise von NFTs, aus dem Englischen Non-Fungible Token, oder zu deutsch nicht austauschbare Wertmarke, basiert auf der Ethereum-Blockchain und ihrem Standard namens ERC-721, der speziell für die Erstellung von NFTs entwickelt wurde. Künstler oder Schöpfer können NFTs erstellen, indem sie ihre digitalen Werke tokenisieren und auf einer NFT-Marktplatzplattform veröffentlichen. Käufer können dann diese NFTs erwerben und besitzen, wodurch sie das digitale Werk und die damit verbundenen Eigentumsrechte erhalten.
Die Popularität von NFTs hat in den letzten Jahren stark zugenommen, da sie Künstlern und Schöpfern die Möglichkeit bieten, ihre digitalen Werke zu monetarisieren und direkten Zugang zu einem globalen Markt von Sammlern und Liebhabern zu erhalten. Darüber hinaus ermöglichen NFTs die Schaffung neuer Formen von digitalen Vermögenswerten und die Demokratisierung des Kunst- und Sammlermarktes.
Es gibt jedoch auch einige kontroverse Aspekte und Risiken im Zusammenhang mit NFTs. Dazu gehören Fragen der Urheberrechte und des geistigen Eigentums, da die digitale Natur von NFTs es schwierig machen kann, die Authentizität und Rechtmäßigkeit der zugrunde liegenden Werke zu überprüfen. Darüber hinaus gibt es Bedenken hinsichtlich des Umweltfußabdrucks von NFTs, da die Transaktionen auf der Ethereum-Blockchain Energie verbrauchen, insbesondere im Zusammenhang mit dem Proof-of-Work-Konsensmechanismus.
Insgesamt haben NFTs eine bedeutende Auswirkung auf die digitale Kunst- und Sammlerindustrie, da sie neue Möglichkeiten für Künstler, Schöpfer und Sammler schaffen. Die Technologie hinter NFTs ermöglicht es, digitale Vermögenswerte eindeutig zu identifizieren, zu besitzen und zu handeln, was zu einer neuen Ära der digitalen Wirtschaft und des Eigentums führt.

Nocoiner - Ein Nocoiner ist eine Person, die keine Bitcoins oder andere Kryptowährungen besitzt. Der Begriff leitet sich von "no coins" (keine Münzen) ab und bezeichnet Personen, die nicht in den Krypto-Markt investiert sind. Nocoiners sind oft skeptisch oder sogar ablehnend gegenüber Kryptowährungen eingestellt. Sie sehen in Bitcoin und Co. entweder eine Blase, ein Betrugssystem oder zumindest eine riskante Investition, an der sie nicht interessiert sind. Viele Nocoiners sind traditionelle Investoren, die lieber in etablierte Anlageklassen wie Aktien, Immobilien oder Gold investieren. Sie verstehen die Technologie und das Konzept von Kryptowährungen oftmals nicht oder halten es für zu kompliziert. Im Gegensatz dazu stehen die sogenannten "Bitcoiner" oder "Krypto-Enthusiasten", die fest an das Potenzial von Bitcoin und anderen Digitalwährungen glauben und selbst investiert sind. Zwischen diesen beiden Lagern kommt es nicht selten zu Kontroversen und Debatten über den Wert und die Zukunft von Kryptowährungen. Der Begriff "Nocoiner" wird von Krypto-Befürwortern manchmal etwas abwertend verwendet, um die Skepsis und Ablehnung gegenüber dem Krypto-Bereich zu betonen. Allerdings ist es natürlich jedem selbst überlassen, ob er in Kryptowährungen investieren möchte oder nicht.

Node - Ein Node in einer Blockchain ist im Grunde genommen ein Computer oder ein Gerät, das

an das Blockchain-Netzwerk angeschlossen ist und eine Kopie der gesamten Blockchain-Datenbank enthält. Jeder Node spielt eine wichtige Rolle bei der Verwaltung und Aufrechterhaltung des dezentralen Netzwerks, indem er Transaktionen validiert, neue Blöcke erstellt und die Integrität der gespeicherten Daten gewährleistet.
Es gibt verschiedene Arten von Nodes in einer Blockchain, darunter Full Nodes, Light Nodes und Mining Nodes. Ein Full Node ist ein Computer, der eine vollständige Kopie der Blockchain enthält und aktiv am Prozess der Transaktionsvalidierung und Blockverbreitung teilnimmt. Diese Nodes sind entscheidend für die Sicherheit und Robustheit des Netzwerks, da sie sicherstellen, dass alle Transaktionen den Konsensregeln entsprechen und die Integrität der Blockchain erhalten bleibt.
Ein Light Node, auch bekannt als SPV (Simplified Payment Verification) Node, enthält nur eine Teilmenge der Blockchain-Datenbank und verlässt sich auf Full Nodes, um Transaktionen zu validieren und zu überprüfen. Diese Art von Node wird häufig in Wallet-Applikationen verwendet, da sie weniger Ressourcen benötigt und dennoch in der Lage ist, Transaktionen zu verifizieren, ohne die gesamte Blockchain herunterladen zu müssen.
Mining Nodes sind spezielle Nodes, die an dem Prozess des "Mining" beteiligt sind, bei dem neue Blöcke erstellt und der Blockchain hinzugefügt werden. Diese Nodes führen komplexe Berechnungen durch, um den Proof-of-Work-Konsensmechanismus zu erfüllen und neue Transaktionen zu bestätigen. Durch diesen Prozess werden neue Bitcoins geschaffen, und die Sicherheit des Netzwerks wird gewährleistet.
Die Rolle eines Nodes in einer Blockchain umfasst auch die Verbreitung von Transaktionen und Blöcken im Netzwerk, um sicherzustellen, dass alle Teilnehmer über die neuesten Informationen verfügen. Darüber hinaus können Nodes auch an der Verifikation von Transaktionen, der Durchführung von Smart Contracts und der Bereitstellung von Diensten wie Wallets oder Schnittstellen für Benutzer beteiligt sein.
Insgesamt sind Nodes das Rückgrat einer jeden Blockchain, da sie die Integrität, Sicherheit und Funktionsweise des dezentralen Netzwerks gewährleisten. Durch die Zusammenarbeit und Interaktion der Nodes wird die Dezentralisierung und Widerstandsfähigkeit gegenüber Angriffen oder Ausfällen sichergestellt, was die Grundlage für das Vertrauen und die Zuverlässigkeit einer jeden Blockchain bildet.

Noob / Newbie - Ein Bitcoin-Neuling, Newb oder Newbie bezeichnet eine Person, die neu bei Bitcoin ist und gerade erst beginnt zu lernen, wie es funktioniert, wie man Bitcoin erwirbt und sich möglicherweise in die breitere Bitcoin-Online-Community einzubringen beginnt. Sie werden oft an den grundlegenden Fragen erkannt, die sie stellen, ihrem Mangel an Verständnis oder ihren schlechten Bitcoin-Sicherheits- und Datenschutzpraktiken. Sie können auch leicht beeinflusst werden, da sie kein gefestigtes Verständnis von Bitcoin haben und oft als diejenigen Investoren bezeichnet werden, die bei Korrekturen des Kurses verkaufen, da sie die Volatilität des Assets nicht gewohnt sind. Newbies können auch an ihren grundlegenden Fehlern erkannt werden, wie dem Hereinfallen auf verschiedene Altcoin-Angebote oder Betrügereien, die darauf ausgelegt sind, unerfahrene Bitcoin-Käufer um ihr Bitcoin zu bringen. Newbies befinden sich am Anfang ihrer Bitcoin-Reise und benötigen Anleitung zu allen Aspekten von Bitcoin, vom Funktionsprinzip bis hin zum Erwerb von BTC, zur sicheren Aufbewahrung und vielem mehr.

Nonce - Bei Bitcoin und anderen Kryptowährungen, die auf der Blockchain-Technologie basieren, bezeichnet der Begriff "Nonce", aus dem engl. Number used once (einmalig verwendete Zahl), eine Zeichenfolge, die zusammen mit anderen Transaktionsdaten verwendet wird, um einen gültigen Proof-of-Work zu erzeugen. Beim Mining von Bitcoin-Blöcken müssen Miner einen Hashwert finden, der unter einem bestimmten Zielwert liegt. Dieser Zielwert wird durch die Schwierigkeit des Netzwerks bestimmt. Um einen gültigen Hashwert zu finden, fügen die Miner dem Block-Header, der die Transaktionsdaten enthält, eine Nonce hinzu und berechnen den SHA-

256-Hash. Die Nonce ist eine Zahl, die von den Minern bei jedem Berechnungsversuch erhöht wird, bis ein gültiger Hashwert gefunden wird. Sobald ein Miner einen gültigen Proof-of-Work erbracht hat, wird der Block in die Blockchain aufgenommen und der Miner erhält eine Belohnung.
Die Nonce ist also ein wichtiger Bestandteil des Proof-of-Work-Konzepts von Bitcoin, da sie es den Minern ermöglicht, den Hash-Wert des Blocks so lange zu variieren, bis ein gültiger Wert gefunden wird.

Normie - Der Begriff „Normie“ bezieht sich auf jemanden, dessen Geschmack, Lebensstil, Gewohnheiten, Einstellung und Informationsquellen dem Mainstream-Narrativ entsprechen und weit von der Spitzenposition oder dem Originellen entfernt sind. Ein Normie neigt zur wahrgenommenen Sicherheit sozialer Standards, akzeptierter Praktiken und Trends seiner Zeit und geografischen Gruppe, ohne dabei breitere kulturelle Perspektiven zu berücksichtigen. Normies zeigen ein fehlendes Interesse an Ideen, die nicht leicht zugänglich sind oder außerhalb ihrer/der gesellschaftlichen Akzeptanz liegen. Sie sind Konformisten, Mitläufer. Normies haben oft ein Gefühl der kulturellen Überlegenheit gegenüber der widerspenstigen Bitcoin-Gegenkultur-Bewegung. Sie versuchen häufig, Bitcoiner oder Bitcoin-Narrative zu diskreditieren, da diese immer noch außerhalb ihres mehrheitlichen Denkens liegen, und behaupten, Bitcoiner seien von der Realität entfremdet. Die meisten Normies übernehmen in jungen Jahren die Einstellung, dass Popularität das einzige Maß für gut oder schlecht ist, und können leicht an jedes gewünschte Wertesystem angepasst werden. Normies tendieren dazu, Fiat-Maximalisten zu sein, die Mainstream-FUD-Argumente wiederholen, um Bitcoin abzulehnen, ohne sich die Mühe zu machen, es zu lernen und zu verstehen.

Normopathie - Der Begriff "Normopathie" beschreibt ein Phänomen, das in der Psychologie und Soziologie zunehmend Beachtung findet. Dabei handelt es sich um eine Verhaltensweise, bei der Individuen oder Gruppen dazu neigen, sich in geradezu zwanghafter Weise an gesellschaftliche Normen und Erwartungen anzupassen - selbst dann, wenn diese Normen als dysfunktional oder gar schädlich eingestuft werden können. Das Hauptmerkmal der Normopathie ist der starke Anpassungsdruck, den die Betroffenen verspüren. Sie empfinden einen übermäßigen Drang, sich den geltenden Regeln und Erwartungen der Gesellschaft zu unterwerfen, auch wenn diese im Widerspruch zu ihren persönlichen Bedürfnissen, Überzeugungen oder Impulsen stehen. Um zur Norm zu passen, zeigen Normopathische ein hohes Maß an Konformität und sind nur allzu bereit, ihre eigene Persönlichkeit und Identität zu unterdrücken. Darüber hinaus zeichnen sich Normopathische durch eine auffallende Kritiklosigkeit gegenüber gesellschaftlichen Normen aus. Sie hinterfragen diese nur selten und akzeptieren sie stattdessen meist unhinterfragt. Abweichende Meinungen oder Verhaltensweisen werden oft nur schwer toleriert. Stattdessen dient die Normopathie der Aufrechterhaltung des sozialen Systems, indem Konformität durch soziale Kontrolle erzwungen wird. Kritiker sehen in dieser übertriebenen Anpassungsbereitschaft ein Hemmnis für individuelle Entfaltung und gesellschaftlichen Wandel. Sie argumentieren, dass die Unterdrückung der eigenen Persönlichkeit zulasten der psychischen Gesundheit gehen und kreative, nonkonforme Ideen ersticken kann.

Peer-to-Peer-Netzwerk - Ein Peer-to-Peer-Netzwerk (P2P-Netzwerk) ist ein Netzwerk, in dem die teilnehmenden Computer oder Geräte, auch als "Peers" bezeichnet, direkt miteinander verbunden sind, um Ressourcen wie Dateien, Bandbreite oder Dienste gemeinsam zu nutzen, ohne dass ein zentraler Server erforderlich ist. Im Gegensatz zu herkömmlichen Client-Server-Netzwerken, bei denen ein zentraler Server die Ressourcen bereitstellt und die Kommunikation koordiniert, ermöglicht ein P2P-Netzwerk den direkten Austausch von Informationen zwischen den Teilnehmern.

In einem P2P-Netzwerk können die Teilnehmer sowohl Ressourcen anfordern als auch bereitstellen. Dies bedeutet, dass ein Computer in einem P2P-Netzwerk gleichzeitig als Client und als Server fungieren kann. Die Teilnehmer können Dateien direkt miteinander teilen, ohne dass ein zentraler Speicherort erforderlich ist. Dies hat zur Entstehung von P2P-Dateitauschprotokollen wie BitTorrent, eDonkey und Gnutella geführt, die es Benutzern ermöglichen, Dateien direkt voneinander herunterzuladen, anstatt von einem zentralen Server.
P2P-Netzwerke sind oft dezentralisiert, was bedeutet, dass sie robust gegen Ausfälle sind, da das Fehlen eines zentralen Punktes bedeutet, dass das Netzwerk nicht zusammenbricht, wenn ein einzelner Knoten ausfällt. Sie können auch effizient sein, da die Ressourcen des Netzwerks von den Teilnehmern gemeinsam genutzt werden, was zu einer optimalen Auslastung führt.
P2P-Netzwerke werden in verschiedenen Anwendungen eingesetzt, darunter der Dateiaustausch, die verteilte Berechnung, die Kryptowährungen und die Peer-to-Peer-Kommunikation. Obwohl P2P-Netzwerke viele Vorteile bieten, einschließlich Skalierbarkeit, Widerstandsfähigkeit und Effizienz, gibt es auch Herausforderungen im Zusammenhang mit Sicherheit, Datenschutz und Urheberrechtsverletzungen, die bei der Nutzung von P2P-Netzwerken berücksichtigt werden müssen.

Pizza Day - Der Bitcoin Pizza Day ist ein jährlich begangener Gedenktag in der Bitcoin-Community, der an ein historisches Ereignis erinnert. Am 22. Mai 2010 kaufte ein Mann namens Laszlo Hanyecz zwei Pizzen für 10.000 Bitcoin. Dies war einer der ersten bekannten kommerziellen Transaktionen, bei denen Bitcoin als Zahlungsmittel verwendet wurde. Zu dieser Zeit hatten die 10.000 Bitcoin einen Wert von etwa 25 US-Dollar. Heute wären diese 10.000 Bitcoin rund 300 Millionen US-Dollar wert. Dieser Kauf hat die Bitcoin-Akzeptanz stark vorangetrieben und wird daher jedes Jahr am 22. Mai als "Bitcoin Pizza Day" gefeiert. Es ist ein Gedenktag, an dem die Bitcoin-Community an die frühen Tage und die Bedeutung von Bitcoin als Zahlungsmittel erinnert. Viele Bitcoiner nutzen den Tag, um Pizzen zu essen und an dieses historische Ereignis zu erinnern.

Plebs - Plebs, vom lat. plebs - das gemeine Volk, ist ein Begriff, der von einigen Bitcoinern verwendet wird, um sich auf Personen zu beziehen, die nicht so tief in die Kryptowährungsbranche eingebunden sind oder weniger technisches Verständnis haben. Der Begriff hat einen leicht herablassenden Beigeschmack und wird oft verwendet, um eine Hierarchie zwischen "erfahrenen" Bitcoinern und "unerfahrenen" Nutzern darzustellen. Bitcoiner, die sich selbst als Plebs bezeichnen, sehen sich oft als Teil einer elitären Gruppe, die die wahren Vorzüge und das Potenzial von Bitcoin versteht. Sie grenzen sich damit von Personen ab, die sie als unwissend oder uninteressiert an der tieferen Funktionsweise von Kryptowährungen ansehen. Der Begriff Plebs spiegelt manchmal auch eine gewisse Skepsis gegenüber Mainstream-Akzeptanz und -Adoption von Bitcoin wider. Einige Bitcoiner sehen die zunehmende Popularität von Bitcoin als Bedrohung für die ursprünglichen Ideale und Prinzipien der Kryptowährung an und distanzieren sich daher von der breiten Masse der Nutzer. Insgesamt ist der Begriff Plebs innerhalb der Bitcoin-Community umstritten, da er eine elitäre Haltung und einen teilweise ausgrenzenden Ton gegenüber weniger erfahrenen Bitcoinern vermittelt. Einige Nutzer lehnen die Verwendung des Begriffs ab und plädieren für einen inklusiveren und offeneren Umgang innerhalb der Kryptowährungsszene.

Proof-of-Stake - Proof-of-Stake (PoS) ist ein Konsensmechanismus in Kryptowährungsnetzwerken, der als Alternative zum traditionellen Proof of Work (PoW) verwendet wird. Beim PoS-Ansatz wird die Validierung von Transaktionen und das Hinzufügen neuer Blöcke zur Blockchain nicht über rechenintensive Miningleistung, sondern über das Besitzen von Kryptowährungseinheiten ermöglicht. Der Grundgedanke ist, dass Nutzer, die einen größeren Anteil

am Gesamtnetzwerk halten, ein höheres Interesse daran haben, das Netzwerk stabil und sicher zu halten. Daher werden diese Nutzer als "Staker" ausgewählt, um neue Blöcke zu validieren und dem Netzwerk hinzuzufügen. Der Prozess funktioniert so, dass Staker eine bestimmte Menge ihrer Kryptowährungseinheiten als Einsatz "sperren" und basierend auf der Höhe des Einsatzes und anderen Faktoren zufällig ausgewählt werden, um neue Blöcke zu validieren. Validierte Blöcke werden der Blockchain hinzugefügt und die Staker erhalten dafür eine Belohnung in Form neuer Kryptowährungseinheiten. Sollte ein Staker versuchen, das Netzwerk anzugreifen, riskiert er den Verlust seines Einsatzes als Strafe. Auch wenn Proof-of-Stake im Vergleich zu Proof-of-Work Vorteile in Bezug auf Energieeffizienz und Nachhaltigkeit bietet, ist es wichtig, die Vorzüge und Herausforderungen beider Systeme sorgfältig gegeneinander abzuwägen.
Bitcoin, das auf dem Proof-of-Work-Prinzip basiert, hat sich seit Jahren als äußerst robustes und sicheres Krypto-Netzwerk bewiesen. Die hohe Energie, die für das Mining aufgewendet wird, dient dazu, die Integrität und Dezentralisierung des Netzwerks zu gewährleisten - ein Aspekt, der bei PoS-Konzepten noch stärker diskutiert werden muss.

Proof-of-Work - Das Prinzip des Proof of Work (PoW) ist ein grundlegendes Konzept, das bei der Sicherung und Validierung von Transaktionen in Blockchain-Netzwerken wie Bitcoin verwendet wird. Es dient dazu, die Integrität des Netzwerks zu gewährleisten, indem die Teilnehmer (Miner) mathematische Rätsel lösen, um neue Blöcke zur Blockchain hinzuzufügen. Im Vergleich dazu steht das Proof-of-Stake (PoS), ein alternatives Konsensmechanismus, der ebenfalls zur Validierung von Transaktionen und zur Sicherung der Blockchain verwendet wird, jedoch auf einem anderen Prinzip basiert.
Beim Proof of Work müssen die Miner mathematische Rätsel lösen, die als "Hash-Funktionen" bezeichnet werden. Diese Rätsel erfordern eine enorme Rechenleistung, um gelöst zu werden, und dienen dazu, die Sicherheit des Netzwerks zu gewährleisten, indem sie den Prozess der Blockerstellung und Transaktionsvalidierung aufwändig und zeitaufwendig machen. Der erste Miner, der das Rätsel löst, hat das Recht, einen neuen Block zur Blockchain hinzuzufügen, und erhält dafür eine Belohnung in Form von neuen Bitcoins sowie Transaktionsgebühren. Dieser Prozess wird als "Mining" bezeichnet und erfordert spezielle Hardware sowie einen erheblichen Energieaufwand.
Ein wesentlicher Unterschied zwischen PoW und PoS liegt in der Art und Weise, wie die Sicherheit des Netzwerks gewährleistet wird. Bei PoW basiert die Sicherheit auf der Rechenleistung, die für das Lösen der mathematischen Rätsel erforderlich ist, während bei PoS die Sicherheit auf dem wirtschaftlichen Anreiz basiert, den die Teilnehmer haben, um das Netzwerk intakt zu halten. PoW erfordert eine hohe Rechenleistung und Energieverbrauch, während PoS weniger energieintensiv ist, da es keinen Wettbewerb um das Lösen von Rätseln gibt.

Ein weiterer Unterschied betrifft die Dezentralisierung. PoW-Netzwerke sind oft als dezentralisiert angesehen, da viele Miner aus verschiedenen Teilen der Welt am Mining beteiligt sind. Bei PoS hingegen könnten Netzwerke mit einer starken Konzentration von Kryptowährungseinheiten bei wenigen Teilnehmern als weniger dezentralisiert angesehen werden.

Zusammenfassend lässt sich sagen, dass PoW und PoS unterschiedliche Ansätze zur Sicherung und Validierung von Transaktionen in Blockchain-Netzwerken darstellen. Während PoW auf Rechenleistung und Energieverbrauch basiert, setzt PoS auf wirtschaftliche Anreize und den Einsatz von Kryptowährungseinheiten zur Sicherung des Netzwerks.

Bitcoin ist die einzige große Kryptowährung, die noch den Proof of Work Ansatz verfolgt und damit auch von der SEC (United States Securities and Exchange Commission - Amerikanische Börsenaufsichtsbehörde) als Rohstoff, dem Status von Gold gleich, angesehen wird, während alle anderen Kryptoprojekte wie Aktien behandelt werden.

Public- & Private Key – Siehe Key.

Red Candle – Siehe Green Candle

Rekt - "Rekt" ist ein liebevoller Slangausdruck für "zerstört", was die Emotion ist, die man aufgrund einer schlechten Investitionsentscheidung empfindet, wie z.B. den Verlust des gesamten Geldes durch ein FOMO-Investitionen in einen Shitcoin oder den Verlust von Bitcoin durch Zwangsverkäufe an Börsen aufgrund von zu hoher Hebelwirkung. Mit anderen Worten, du bist "gerekt" geworden. Es ist dieses sinkende Gefühl, das du bekommst, fast wie Schrecken, wenn du erkennst, den Fehler gemacht zu haben, aber jetzt nichts mehr daran ändern kannst, außer das Gefühl des "rekt"-Seins zu empfinden.

Rug Pull Technology - Rug Pull Technologie ist die Technik, die von Betrügern verwendet wird, die das Geld von allen stehlen wollen, die töricht genug sind, auf einen Hype um nutzlose Shitcoins hereinzufallen. Betrüger erstellen schnell einen Token auf der Grundlage eines bestimmten Hypes, lassen den Preis in die Höhe schnellen, so dass andere anfangen, FOMO zu bekommen, und verschwinden dann mit dem Geld, indem sie alles abstürzen lassen, und man sieht sie nie wieder. Ähnlich wie das Wegziehen eines Teppichs unter Ihren Füßen. Stellen Sie sich die Szene vor.

Satoshi - Jede Währung muss teilbar sein, damit sie als Tauschmittel verwendet werden kann. Fiatgeld wie der US-Dollar, oder Euro, wird bei Bedarf in 100 Cent unterteilt. Da Bitcoin dem Fiatgeld überlegen ist, ist seine Teilbarkeit deutlich größer. Während 1 Dollar in 100 Cent aufgeteilt werden kann, lässt sich 1 Bitcoin in 100 Millionen Teile unterteilen.

Ein Bitcoin wird in eine Unterwährungseinheit namens Satoshis unterteilt. Jeder Bitcoin ist bis zu acht Dezimalstellen teilbar.

Der Satoshi ist nach Bitcoins anonymem "Gründer", Satoshi Nakamoto, benannt. Satoshis werden in Alltagsgesprächen über Kryptowährungen auch als "Sats" bezeichnet, da es eine einfachere Art ist, Waren und Dienstleistungen, insbesondere auf Layer-2-Lösungen wie dem Lightning-Netzwerk, zu bepreisen.

SEC - Die SEC (Securities and Exchange Commission) ist die wichtigste Wertpapieraufsichtsbehörde in den Vereinigten Staaten. Ihre zentralen Aufgaben und Zuständigkeiten umfassen die Regulierung und Überwachung des Wertpapiermarktes, den Schutz von Anlegern, die Zulassung und Registrierung sowie die Durchsetzung von Gesetzen und Regulierungen. So erlässt die SEC Vorschriften und Regeln für Unternehmen, die öffentlich gehandelte Wertpapiere ausgeben oder handeln, und überwacht die Einhaltung dieser Regeln durch die Marktteilnehmer. Darüber hinaus stellt sie die Transparenz und Offenlegung relevanter Informationen durch Unternehmen sicher, um das Vertrauen der Anleger zu stärken. Zudem ist die SEC für die Zulassung von Wertpapieren für den öffentlichen Handel sowie die Registrierung von Wertpapiermak-lern, Investmentberatern und Investmentfonds zuständig. Nicht zuletzt spielt die Behörde eine zentrale Rolle bei der Untersuchung von Rechtsverstößen und der Verhängung von Strafen und Sanktionen bei Regelverstößen. Insgesamt hat die SEC einen großen Einfluss auf Unternehmen und Anleger in den Vereinigten Staaten und trägt maßgeblich zur Regulierung und Überwachung des US-amerikanischen Finanzsystems bei.

SegWit - Segwit (Segregated Witness, zu deutsch abgetrennter Zeuge/Beobachter) ist eine technische Verbesserung des Bitcoin-Netzwerks, die 2017 eingeführt wurde.
Ursprünglich war der Platz in den Bitcoin-Blöcken auf ein Megabyte begrenzt, was zu hohen Transaktionsgebühren führte. Segwit wurde entwickelt, um diesen Skalierungsengpass zu lösen und die Effizienz des Netzwerks zu erhöhen. Segwit trennt die Transaktionssignatur (Witness-Daten) vom eigentlichen Transaktionsinhalt. Dadurch können mehr Transaktionen in einem Block untergebracht werden, ohne die Blockgrenze von 1 MB zu erhöhen.
Die Witness-Daten werden separat übertragen und zählen weniger stark für die Blockgrenze.
Die Vorteile dieser Neuerung sind...

- Erhöhung der Transaktionskapazität des Bitcoin-Netzwerks
- Reduktion der Transaktionsgebühren
- Verbesserung der Skalierbarkeit
- Vorbereitung für weitere Upgrades wie Lightning Network

Segwit-Adressen beginnen mit "bc1" und nutzen eine effizientere Adressstruktur. Die Ableitung dieser Adressen unterscheidet sich etwas vom klassischen Prozess. Insgesamt war Segwit ein wichtiger technischer Meilenstein, um die Skalierbarkeit von Bitcoin zu verbessern und das Netzwerk für zukünftige Entwicklungen zu rüsten.

Shill - Ein "Shill" ist ein Scharlatan, der versucht, Sie dazu zu bringen, seine "Shitcoin" zu kaufen, indem er unermüdlich ihre "potenziell massiven Gewinne" anpreist. Es gibt natürlich keine Chance, dass dies passiert, und alles, was Sie tun, wenn Sie das Token kaufen, mit dem Sie betrogen werden, ist, den Shill reicher zu machen, und dann bleiben Sie auf der Strecke.

Dies führt zu einem nie endenden Teufelskreis, da Sie dann selbst zum "Shill" werden, wenn Sie versuchen, Ihre Scheiß-Münze an jemand anderen loszuwerden, während der ursprüngliche Täter längst in der Nacht verschwunden ist. Wenn Sie sich nur auf Bitcoin konzentrieren und nicht auf "Krypto", werden Sie einen Shill von Weitem erkennen und nicht in seine Falle tappen.

Shitcoin - Ein Shitcoin ist eine Kryptowährung, die überhaupt keinen Wert bietet. Wert ist natürlich subjektiv, aber man kann oft erkennen, dass ein Coin nur um seiner selbst Willen geschaffen wurde.
Üblicherweise sind dies Projekte, die ohne wirkliches Nachdenken darüber, wie Nachfrage für die Coins geschaffen werden soll oder welche Probleme sie lösen, aufgesetzt wurden. Manche sind absichtlich als Witze konzipiert, andere machen sich die "Rug-Pull"-Technologie zunutze und locken ahnungslose Neulinge an, die am Ende verprellt werden. Natürlich betrachtet ein Bitcoin-Anhänger jede andere Kryptowährung als Shitcoin, was die Sache viel einfacher macht zu verstehen!

Single-Point-of-Failure - Ein Single Point of Failure (SPOF) ist eine Komponente in einem System oder Netzwerk, deren Ausfall dazu führt, dass das gesamte System oder Netzwerk nicht mehr funktioniert. Anders ausgedrückt gibt es keinen redundanten Backup oder Ausweichplan, falls diese kritische Komponente ausfällt. In einem Netzwerk können verschiedene Elemente potenzielle Single Points of Failure sein, wie etwa Router oder Switches, die als einzige das gesamte Netzwerk verbinden, physische Leitungen, über die alle Daten übertragen werden, eine zentrale Stromversorgung oder ein zentraler Server, von dem alle Dienste und Anwendungen abhängen. Um Single Points of Failure zu vermeiden, ist es wichtig, Redundanz in das

Netzwerkdesign einzubauen. Dies bedeutet, dass es alternative Wege oder Komponenten gibt, falls ein Element ausfällt. Beispiele hierfür sind redundante Router, Switches und Netzwerkleitungen, redundante Stromversorgung, mehrere redundante Server oder Lastverteilung auf mehrere Server sowie automatische Failover-Mechanismen. Durch diese Redundanz kann ein Ausfall einzelner Komponenten abgefedert und die Ausfallsicherheit des gesamten Netzwerks erhöht werden. Eine gewaltige Stärke von Bitcoin ist, dass es als Peer-to-Peer-Netzwerk keine solchen Single-Point-of-Failure gibt.

Smart Contract - Smart Contracts sind computerprotokollbasierte Verträge, die automatisch, transparent und ohne die Notwendigkeit einer Zwischeninstanz ausgeführt werden. Sie basieren auf Blockchain-Technologie, die es ermöglicht, Transaktionen und Verträge sicher und unveränderlich zu speichern. Smart Contracts werden in der Regel in einer speziellen Programmiersprache geschrieben und auf einer Blockchain-Plattform wie Ethereum ausgeführt.
Die Funktionsweise von Smart Contracts beruht auf einem "Wenn-Dann"-Prinzip. Das bedeutet, dass der Vertrag automatisch bestimmte Aktionen ausführt, sobald vordefinierte Bedingungen erfüllt sind. Zum Beispiel könnte ein Smart Contract für den Kauf eines digitalen Gutes so programmiert sein, dass das Gut automatisch an den Käufer übertragen wird, sobald die Zahlung eingegangen ist. Da Smart Contracts auf der Blockchain ausgeführt werden, sind sie transparent, unveränderlich und sicher vor Manipulation.
In der heutigen Geschäftswelt haben Smart Contracts einen bedeutenden Stellenwert, da sie die Möglichkeit bieten, Verträge und Transaktionen effizienter, sicherer und kostengünstiger abzuwickeln. Sie können in verschiedenen Branchen wie Finanzdienstleistungen, Versicherungen, Lieferkettenmanagement und Immobilien eingesetzt werden, um Prozesse zu automatisieren und Vertrauen zwischen den Parteien zu schaffen. Dies kann dazu beitragen, menschliche Fehler zu reduzieren und die Abwicklung von Geschäften zu beschleunigen.
In Bezug auf Bitcoin haben Smart Contracts eine indirekte Verbindung, da Bitcoin selbst keine native Unterstützung für Smart Contracts bietet. Bitcoin ist hauptsächlich als digitale Währung konzipiert und konzentriert sich auf die Bereitstellung einer dezentralen, sicheren und vertrauenswürdigen Methode für den Transfer von Werten. Allerdings gibt es Bemühungen, Smart Contract-Funktionalitäten auf der Bitcoin-Blockchain zu implementieren, wie zum Beispiel das sogenannte "Rootstock" (RSK) Projekt, das eine Sidechain-Lösung für Smart Contracts auf der Bitcoin-Blockchain anbietet.
Insgesamt haben Smart Contracts das Potenzial, die Art und Weise, wie Geschäfte abgewickelt werden, zu revolutionieren, und sie spielen eine wichtige Rolle bei der Weiterentwicklung der Blockchain-Technologie und ihrer Anwendungen in der Geschäftswelt.

Soft Fork - Ein Soft Fork, englisch für weiche Gabelung, ist eine rückwärtskompatible Änderung des Bitcoinnetzwerks. Das bedeutet, dass nach der Einführung eines Soft Forks ältere Bitcoin-Knoten (Nodes) die neuen Regeln weiterhin akzeptieren können, ohne dass sie ein Upgrade durchführen müssen. Normalerweise funktioniert ein Soft Fork folgendermaßen:

1. Entwicklung der neuen Regeln: Die Bitcoin-Entwickler entwerfen neue Regeln oder Funktionen für das Bitcoinnetzwerk. Diese Änderungen müssen so konzipiert sein, dass sie rückwärtskompatibel sind. Das heißt, ältere Nodes müssen sie weiterhin akzeptieren können.
2. Signalisierung und Abstimmung: Die Bitcoin-Knoten signalisieren ihre Unterstützung für den Soft Fork, indem sie spezielle Nachrichten in ihren Blocks übermitteln. Sobald eine bestimmte Mehrheit der Miners (z.B. 95%) den Soft Fork unterstützt, wird er aktiviert.
3. Aktivierung des Soft Forks: Nach Erreichen der Mehrheit treten die neuen Regeln in Kraft. Ab diesem Zeitpunkt müssen alle neuen Blöcke die neuen Regeln erfüllen, um vom Netzwerk akzeptiert zu werden. Ältere Nodes, die den Soft Fork nicht unterstützen,

erkennen diese neuen Blöcke weiterhin an, da die Änderungen rückwärtskompatibel sind.
4. Schrittweise Adoption: Über einen gewissen Zeitraum hinweg werden immer mehr Nodes auf die neuen Regeln umstellen. Irgendwann wird der Soft Fork von der überwiegenden Mehrheit des Netzwerks unterstützt.

Durch die Rückwärtskompatibilität eines Soft Forks können also ältere Kontenpunkte weiterhin am Netzwerk teilnehmen, ohne ein Upgrade durchführen zu müssen. Dies erhöht die Stabilität und Akzeptanz von Änderungen im Bitcoinnetzwerk. Mit diesem Verfahren wurde zum Beispiel 2012 das Pay-to-Script-Hash eingeführt, was komplexere Transaktionen ermöglicht.

Software-Wallet – Siehe Wallet.

Speedy Trial - Das Speedy Trial, zu deutsch beschleunigtes Verfahren, ist ein Mechanismus, der es ermöglicht, Änderungen am Netzwerk schnell und effektiv einzuführen. Dieser Prozess ist darauf ausgelegt, die Meinungen und Zustimmung der Bitcoin-Community in einem relativ kurzen Zeitrahmen einzuholen, bevor eine Änderung final umgesetzt wird. Dies geschieht in mehreren Phasen.

1. Zunächst wird der Vorschlag für eine Änderung von den Bitcoin-Entwicklern eingereicht und öffentlich diskutiert. Dabei werden mögliche Auswirkungen, Vor- und Nachteile sorgfältig geprüft.
2. Anschließend stimmen die Miner - also jene Nutzer, die neue Blöcke zum Blockchain-Netzwerk beisteuern - über den Änderungsvorschlag ab. Hierfür gibt es einen definierten Zeitrahmen von etwa 3 Monaten, in denen 90% der Miner für die Änderung votieren müssen.
3. Wenn diese Zustimmungsschwelle erreicht wird, tritt die Änderung dann nach einer weiteren kurzen Übergangsphase in Kraft. So können wichtige Verbesserungen oder Anpassungen am Bitcoin-Protokoll relativ zeitnah und mit breiter Unterstützung der Gemeinschaft umgesetzt werden.

Das Speedy Trial-Verfahren ist also ein flexibler und reaktionsschneller Mechanismus, um das Bitcoin-Netzwerk nahezu ad hoc weiterzuentwickeln und an neue Anforderungen anzupassen, ohne die grundsätzliche Stabilität und Vertrauenswürdigkeit der Kryptowährung zu gefährden.

Spook - Wie Geister im Geist ist ein "Spuk" etwas, von dem eine Gruppe von Menschen, die Gesellschaft, die Mainstream-Medien oder Influencer Sie glauben lassen, obwohl es das nicht ist – im Grunde also eine Illusion. Zum Beispiel sehen Sie in den sozialen Medien oft ein Konzept, das so oft in Ihrem Newsfeed wiederholt wird, dass Sie anfangen könnten, daran zu glauben, obwohl die Realität ist, dass es nicht real ist. Influencer, Moonboys und sogar einige FUD-Stücke können Spuk sein oder erzeugen, da sie dazu da sind, durch Spaltung der Meinungen online zwischen Dingen, die real sind oder nicht, Aufmerksamkeit und Engagement zu erregen.

Der Ausdruck stammt von Max Stirner, einem deutschen Philosophen des 19. Jahrhunderts, wurde aber im 21. Jahrhundert angemessen "meme-ifiziert".

Staker - Ein Staker ist eine Person oder Einheit, die Kryptowährungen oder andere digitale Assets in einem Proof-of-Stake-Netzwerk hält, um den Konsensbildungsprozess zu unterstützen und zu sichern. In einem Proof-of-Stake-System werden Blöcke nicht durch aufwendiges Mining erzeugt, sondern durch "Staking" bestätigt. Staker "setzten" einen Teil ihrer Kryptowährungen ein, um am Netzwerk teilzunehmen und neue Blöcke zu validieren. Je mehr Kryptowährungen ein

Staker einsetzt, desto höher ist die Wahrscheinlichkeit, dass er zum Validator eines neuen Blocks ernannt wird. Als Belohnung für ihre Teilnahme am Netzwerk erhalten Staker neue Kryptowährungseinheiten oder Transaktionsgebühren. Staker tragen also dazu bei, die Sicherheit und Dezentralisierung des Blockchain-Netzwerks aufrechtzuerhalten, indem sie ihre Vermögenswerte als Pfand einsetzen. Im Gegenzug werden sie für ihren Beitrag zur Netzwerkstabilität belohnt. Das Staking ist ein wichtiges Element von Proof-of-Stake-Systemen und unterscheidet sich grundlegend vom energie-intensiven Proof-of-Work-Konsens, bei dem Rechenleistung eingesetzt wird.

SWIFT - SWIFT steht für "Society for Worldwide Interbank Financial Telecommunication". Es handelt sich um eine kooperative Organisation, die ein Netzwerk für Finanzinstitute betreibt, um den sicheren und standardisierten Austausch von finanziellen Transaktionen zu ermöglichen. SWIFT bietet eine Plattform, über die Banken und andere Finanzinstitute Nachrichten senden und empfangen können, um Zahlungen, Wertpapiertransaktionen und andere Finanzgeschäfte abzuwickeln. Das SWIFT-Netzwerk spielt eine wichtige Rolle im internationalen Zahlungsverkehr und erleichtert die Kommunikation und Abwicklung zwischen verschiedenen Finanzinstituten weltweit.

Token - Ein Token, aus dem Englischen Zeichen, Abzeichen, Merkmal, ist eine digitale Einheit, die in der Regel auf einer Blockchain-Plattform erstellt wird und verschiedene Funktionen haben kann. Tokens können als digitale Vermögenswerte fungieren, die Besitzrechte, Stimmrechte oder Zugriffsrechte repräsentieren. Sie dienen auch als Mittel für den Austausch von Werten innerhalb eines bestimmten Ökosystems. Es gibt verschiedene Arten von Tokens, darunter Utility-Token, Security-Token und Payment-Token.
In Bezug auf Bitcoin gibt es verschiedene Arten von Tokens, die in Verbindung mit der Bitcoin-Blockchain verwendet werden. Einer der bekanntesten Token ist der sogenannte "Bitcoin-Token", der auf anderen Blockchain-Plattformen erstellt werden kann, um den Wert von Bitcoin zu repräsentieren, während er in einem anderen Ökosystem verwendet wird. Diese Tokens werden oft als Wrapped Bitcoin (WBTC) bezeichnet, und sie ermöglichen es Benutzern, Bitcoin auf der Ethereum-Blockchain oder anderen Plattformen zu verwenden, um verschiedene DeFi-Anwendungen zu nutzen, ohne ihre Bitcoin verkaufen zu müssen.
Darüber hinaus gibt es auch sogenannte "Layer-2"-Tokens, die auf der Bitcoin-Blockchain erstellt werden können, um die Skalierbarkeit und die Funktionalität zu verbessern. Diese Tokens, wie das Lightning Network-Token, werden verwendet, um schnellere und kostengünstigere Transaktionen zu ermöglichen, indem sie Transaktionen außerhalb der Haupt-Blockchain ausführen und dann die Ergebnisse auf die Haupt-Blockchain übertragen.
Zusammenfassend lässt sich sagen, dass ein Token eine digitale Einheit ist, die verschiedene Funktionen haben kann, darunter die Repräsentation von Vermögenswerten, die Teilnahme an Governance-Prozessen und die Erleichterung von Transaktionen innerhalb eines bestimmten Ökosystems. Im Zusammenhang mit Bitcoin werden Tokens verwendet, um den Wert von Bitcoin auf anderen Plattformen zu repräsentieren und um die Skalierbarkeit und Funktionalität der Bitcoin-Blockchain zu verbessern.

Tumbler - Ein Bitcoin-Mixer, auch als Tumbler bezeichnet, ist ein Service, der dazu dient, die Rückverfolgbarkeit von Bitcoin-Transaktionen zu erschweren. Der Vorgang funktioniert folgendermaßen: Der Nutzer überweist zunächst seine Bitcoin-Guthaben an die Adresse des Bitcoin-Mixers. Die Bitcoins werden dann mit den Bitcoins anderer Nutzer vermischt, indem komplexe Transaktionspfade und -zeitpunkte erstellt werden. Dadurch wird es schwieriger, die ursprüngliche Herkunft der Bitcoins zurückzuverfolgen. Nach der Vermischung können die Bitcoins schließlich an eine neue, vom Nutzer gewählte Adresse ausgezahlt werden, die nicht mit der

ursprünglichen Adresse des Nutzers verknüpft ist. Der Zweck eines Bitcoin-Mixers ist es, die Anonymität und den Datenschutz des Nutzers zu erhöhen, indem die Verbindung zwischen der eingegebenen und der ausgezahlten Bitcoin-Adresse verschleiert wird. Allerdings ist der Einsatz eines Bitcoin-Mixers umstritten, da er auch für illegale Zwecke missbraucht werden kann.

UTXO - Unspent Transaction Output, zu deutsch nicht verwendeter Transaktionsoutput, (UTXO) ist die Technik, die das Bitcoin-Protokoll verwendet, um Salden zu verfolgen, wenn sie sich zwischen Krypto-Wallets bewegen. Wenn es um die Verfolgung und Verwaltung individueller Krypto-Salden geht, verwenden Blockchain-basierte Protokolle in der Regel eines von zwei verschiedenen Buchhaltungsmodellen. Das eine wird Konto-/Saldo-Modell genannt. Projekte wie Ethereum, Tezos und EOS verwenden dieses Modell, um die Salden zu verfolgen, wenn Blockchain-Nutzer Transaktionen ausführen. Das andere wird Unspent Transaction Output (UTXO)-Modell genannt und von Bitcoin und viele andere Kryptowährungen wie Litecoin, Cardano und Dogecoin verwendet.

Adam Back und der verstorbene Hal Finney waren zwei Mitglieder der Cypherpunk-Kryptografiegruppe, die der Autor des Bitcoin-Whitepaper, Satoshi Nakamoto, häufig besuchte. Die beiden werden dafür gelobt, dass sie das UTXO-Modell unabhängig voneinander zwischen 1997 und 2004 entwickelt haben. Als der Schöpfer von Bitcoin, Satoshi Nakamoto, das Protokoll 2009 startete, wurde es zum ersten operativen Digitalgeld-System, das das UTXO-Modell implementiert. Sowohl Hal Finney als auch Adam Back werden schon lange verdächtigt, Satoshi Nakamoto zu sein, auch wenn es nie bewiesen wurde.

Wenn Sie Bitcoin an jemanden senden, finden einige programmgesteuerte Schritte statt. Einer der ersten Schritte im Transaktionsprozess ist, dass Ihre Krypto-Wallet die Blockchain nach dem Betrag an Mitteln durchsucht, die Sie haben. Diese Mittel werden als nicht verwendete Transaktionsausgaben (UTXOs) bezeichnet. Sie können UTXOs als Wechselgeld ansehen, das von früheren Bitcoin-Transaktionen übrig geblieben ist. Die Mittel gelten als "nicht verwendet", da sie frei verfügbar sind, um sie an jemanden zu senden oder in eine andere Wallet zu verschieben. Sie werden "Transaktionsausgaben" genannt, weil sie aus vorherigen Transaktionen entstanden sind.
Dazu ein Beispiel:
Wenn Sie mit einem 20 € Schein 12 € für ein Mittagessen ausgeben, hätten Sie 8 € Bargeld übrig. In diesem Beispiel wäre das übrige 8 € eine nicht verwendete Transaktionsausgabe. Es würde in Ihre Wallet zurückfließen, um für etwas anderes verwendet zu werden. Genau so funktionieren Bitcoin-UTXOs. Wenn Sie eine Transaktion tätigen, werden Ausgaben aus vorherigen Bitcoin-Transaktionen, also Ihr Bitcoin-Wechselgeld, als Eingaben für neue Transaktionen verwendet. Ein weiterer wichtiger Vergleich zwischen physischen Bargeldtransaktionen und UTXOs ist, dass beide vollständig ausgegeben werden müssen und nicht unterteilt werden können. Wenn Sie einen 5 Bitcoin UTXO haben und jemandem 1 BTC senden möchten, müssen Sie den gesamten UTXO im Wert von 5 Bitcoin senden und erhalten einen neuen UTXO im Wert von 4 BTC abzüglich etwaiger Gebühren zurück.
Genau wie im oben genannten Beispiel, wo Sie einen ganzen 20 € Schein bezahlen, um ein 8 € Mittagessen zu kaufen.
Wenn ein UTXO ausgegeben wird, gilt er als "verbraucht" und wird technisch aus dem Umlauf genommen. Jegliches Wechselgeld wird als ein komplett neuer UTXO generiert. Dieser Teil des UTXO-Systems ist, wie Bitcoin das Doppelausgabenproblem (Double Spending) löst.
Genau wie Sie einem Händler keinen 5 € Schein geben und dann denselben 5 € Schein an jemand anderen weitergeben können, kann ein Bitcoin-Nutzer denselben nicht verwendeten Transaktionsoutput nicht in zwei separaten digitalen Transaktionen verwenden. Wenn eine Person versucht, denselben UTXO zweimal auszugeben, landen die beiden Transaktionen in einem

Mempool- einer Art Warteraum für anstehende Transaktionen. Sie bleiben dort, bis erfolgreiche Miner, die den Proof of Work-Wettbewerb gewonnen haben, sie in neue Blöcke aufnehmen. Selbst wenn beide Transaktionen in zwei separate Blöcke aufgenommen und gleichzeitig verarbeitet werden, würde aufgrund der Zeitstempelung eine der Transaktionen vor der anderen verifiziert werden. Nach einer Anzahl von Bestätigungen (neuen Blöcken, die zur Blockchain hinzugefügt werden) würden andere Knoten die zweite ungültige Transaktion markieren und ablehnen.
Man kann sich die UTXO also vorstellen wie Geldpakete, die mit jeder Ausgabe/jedem Kauf immer kleiner werden, analog wie Geldscheine, nur das die Pakete nicht auf feste Nennwerte beschränkt sind.

Wallet - Eine Bitcoin-Wallet, aus dem Englischen für Brieftasche, ist im Grunde genommen eine Softwareanwendung, die es einem ermöglicht, Bitcoin zu senden, zu empfangen und zu speichern. Sie fungiert als eine Art digitale Geldbörse, in der die privaten Schlüssel gespeichert werden, die zur Autorisierung von Bitcoin-Transaktionen erforderlich sind. Die Wallet verwaltet auch die öffentlichen Schlüssel, die es anderen ermöglichen, Bitcoin an die Wallet zu senden.
Es gibt verschiedene Arten von Bitcoin-Wallets, darunter Hardware-Wallets, Software-Wallets, Papier-Wallets und Online-Wallets. Jede Art hat ihre eigenen Vor- und Nachteile in Bezug auf Sicherheit und Benutzerfreundlichkeit.
Eine Hardware-Wallet ist eine physische elektronische Vorrichtung, die speziell für die sichere Aufbewahrung von Bitcoin entwickelt wurde. Sie ist in der Regel nicht mit dem Internet verbunden, was sie vor Online-Bedrohungen schützt. Software-Wallets sind Programme, die auf einem Computer oder Smartphone installiert werden und eine bequeme Möglichkeit bieten, auf Bitcoin zuzugreifen. Allerdings sind sie anfälliger für Malware-Angriffe. Papier-Wallets sind physische Dokumente, auf denen die Bitcoin-Adresse und der private Schlüssel gedruckt sind. Sie bieten eine hohe Sicherheit, erfordern jedoch besondere Vorsicht im Umgang, um Verlust oder Beschädigung zu vermeiden. Online-Wallets sind Wallets, die über das Internet zugänglich sind, entweder über eine Börse oder eine Wallet-Dienstleistung. Sie sind bequem, bergen aber das Risiko von Hacking-Angriffen.
Die Sicherheit einer Bitcoin-Wallet ist von größter Bedeutung, da der Verlust des privaten Schlüssels dazu führen kann, dass die in der Wallet gespeicherten Bitcoin unwiederbringlich verloren gehen. Daher ist es wichtig, Sicherheitsvorkehrungen zu treffen, wie beispielsweise die Verwendung von Zwei-Faktor-Authentifizierung, regelmäßige Sicherung der Wallet und die Vermeidung von verdächtigen oder unsicheren Websites und Anwendungen.
Zusammenfassend ist eine Bitcoin-Wallet eine digitale Geldbörse, die es Benutzern ermöglicht, Bitcoin sicher zu speichern, zu senden und zu empfangen. Es gibt verschiedene Arten von Wallets, von Hardware- und Software-Wallets bis hin zu Papier- und Online-Wallets, und die Sicherheit ist ein entscheidender Faktor bei der Auswahl und Verwendung einer Wallet.

Nützliche Internetseiten zum Thema Bitcoin

- https://leon-verde.com – Meine Wissensseite, auf der noch mehr Informationen rund um Bitcoin zusammengetragen sind.
- https://www.blocktrainer.de – Eine super Quelle ist der Blocktrainer. Auf dieser Seite findet man aktuelle Informationen, historisches und auch Meinungsartikel. Sehr gut sind die Vlogs, die Roman Reher über YouTube anbietet.
- https://bitcoin.org – Multilinguale Wissenseite
- https://mempool.space/de/ - Mempool.space zeigt die einzelnen Blöcke in einem tollen Dashbord an.
- https://timechaincalendar.com/de – Die Bitcoin Uhr
- https://coinmarketcap.com – CoinMarketCap sehr übersichtliche Seite zu Kursen und anderen Kennzahlen.
- https://coinatmradar.com – Übersichtsseite mit Karten zu Bitcoinautomaten und weiteren wertvollen Informationen.
- https://www.bitcoinqrcodemaker.com – Ein Onlinetool um QR-Codes aus Bitcoinadessen zu generieren.

Stichwortverzeichnis

Abbildungsverzeichnis