



Bitcoin-Diplom

Finanzielle Bildung für das Bitcoin-Zeitalter

Arbeitsbuch für Lernwillige

Deutsche Version | September 2023

Mi Primer Bitcoin hat dieses Werk erstellt und unter Creative Commons frei verfügbar gemacht.

Dieses Werk ist lizenziert unter einer
Creative Commons Lizenz
Namensnennung-Weitergabe unter gleichen Bedingungen
4.0 International (CC BY-SA 4.0)





Bitcoin-Diplom

Finanzielle Bildung für das Bitcoin-Zeitalter

Arbeitsbuch für Lernwillige

Deutsche Version | September 2023



JETZT SPENDEN:



EL SALVADOR

bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf

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

- Stefan Gerber (Übersetzung)
Twitter: @w4ttSoLdAt,
Spende: w4tt5old4t@getalby.com;
- Thomas Geier (Lektorat)
Twitter: @DerGeier21,
Spende: dergeier@getalby.com;
- Bitboxer (Layout)
Twitter: @GhostofBitboxer,
Spende: BitBoxer75@getalby.com.



slightsock95@walletofsatoshi.com

A P R Y C Ö T

Danksagung

Das Bitcoin-Diplom war ein Riesenerfolg und ist schneller gewachsen, als alle erwartet haben. Wir möchten all den wunderbaren Menschen, die uns hierher gebracht haben, Anerkennung zollen.

Dalia Platt ist die Leiterin der Lehrplanentwicklung und von Anfang an die treibende Kraft hinter unseren Inhalten. Sie ist ein Rockstar. Für diese Ausgabe hatte sie großartige Hilfe von einigen erstaunlichen Mitwirkenden, darunter Madelyn Hereford, Greg Foss, Ronny Avendano, Alejandro Galán, Evelyn Lemus, Gerardo Linares, Marc Platt, Jim Platt, Napoleón Osorio, Victor Yasbek, Robert Malka und Arel Edelkamp. Gloriana Solano, Raul Guirola, Giacomo Zucco, Gerson Martinez, Vriti Saraf und andere unterstützten frühere Ausgaben. Gerardo Apostolo und Enrique Jubis von ACTIVA haben ebenfalls einen unglaublichen Beitrag geleistet.

Die Geschichte des Bitcoin-Diploms begann im Februar 2022 bei einem Treffen in *La Pacheco*, einer öffentlichen Schule in San Marcos in El Salvador. Unter den Anwesenden waren der innovative Direktor der Schule, Asael Rodriguez, der Befürworter der Bitcoin-Bildung und Kongressabgeordnete Rodrigo Ayala und der Community-Builder für Ibex Mercado, Carlos Toriello, der andere Bitcoiner, mich eingeschlossen, zu einer Besichtigung der Schule und einer Diskussion über Bildung einlud.

Die ersten Bitcoin-Diplomstudenten begannen im April mit der frühen Unterstützung von Ibex und Hunderten von Einzelspendern. Im Juni machte die erste Gruppe von 38 Studenten ihren Abschluss in *La Pacheco* und wir begannen zu expandieren. Dank der enormen Unterstützung durch neue Spender und Sponsoren, darunter einige örtliche Bürgermeister, Bitfinex und Bitcoin Beach, hat sich die Zahl der Studenten alle zehn Wochen mehr als verdoppelt – ein Trend, der es uns ermöglichen wird, dieses Jahr Tausende von Studenten im ganzen Land zu erreichen. Im Februar 2023 begann die Auslieferung des Lehrplans in Guatemala, und es ist geplant, ihn noch vor Jahresende in viele weitere Länder zu bringen, darunter Kolumbien, Honduras, Südafrika, Ecuador und die Vereinigten Staaten. Die Spenden aus diesen Programmen werden noch mehr Studenten in El Salvador zugute kommen.

Das Arbeitsbuch zum Bitcoin-Diplom wurde als Open Source veröffentlicht. Es ist frei verfügbar und wurde übersetzt, ausgedruckt und unabhängig in Gemeinschaften auf der ganzen Welt für den Unterricht verwendet, von Südkorea bis Uruguay.

Mi Primer Bitcoin ist eine Non-Profit-Organisation mit einer einzigartigen Mission – qualitativ hochwertige, unabhängige und unparteiische, gemeinschaftsbasierte Bitcoin-Bildung für jeden in El Salvador so schnell wie möglich bereitzustellen. Als die erste Nation, die Bitcoin einführt, wird El Salvador ein Beispiel für die Welt sein; wir können entscheiden, welche Art von Beispiel das sein wird. Unser Ziel ist es, eine Nation zu lehren und die Welt zu verändern. Ich weiß, dass sich das verrückt anhört, aber ich denke, wir sind auf einem guten Weg, und das Bitcoin-Diplom ist ein wichtiger Teil davon.

For a better world,

John Dennehy
Gründer
Mi Primer Bitcoin
März 2023

Danksagung der Übersetzer

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

Die beteiligten Content Plebs haben im März 2023 begonnen, ehrenamtlich eine deutsche Version zu erstellen. Dazu wurde das Arbeitsbuch gründlich übersetzt, lektoriert und teilweise überarbeitet, indem einige Fehler sowie die umfangreiche Farbcodierung beseitigt wurden. Dabei wurde stets auf das passende Format und Design geachtet. Es war uns eine Ehre!

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

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

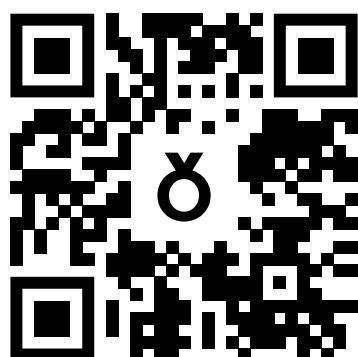
Einundzwanzig Millionen Mal Danke!

Für eine bessere Welt,

Stefan Gerber, Thomas Geier und BitBoxer

Aprycot Media Content Plebs

www.Aprycot.Media



[https://miprimerbitcoin.io/
en/my-first-bitcoin/](https://miprimerbitcoin.io/en/my-first-bitcoin/)



[https://github.com/
MiPrimerBitcoin](https://github.com/MiPrimerBitcoin)



Inhaltsverzeichnis

Kapitel 1 – Die Macht des Geldes	11
1.0 Seid ihr bereit?	12
1.1 Gruppendiskussion: Was ist Geld?	12
1.2 Die begrenzte Welt: Umgang mit Knappheit in einer wachsenden Wirtschaft	13
1.3 Definition von Geld	15
1.3.1 Wir können es benutzen, aber auch definieren?	15
1.3.2 Funktionen von Geld	17
1.3.3 Eigenschaften von Geld	18
1.3.4 Arten von Geld	21
Kapitel 2 – Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit	27
2.0 Einleitung	28
2.0.1 Gemeinschaftsübung: Tauschhandelsspiel	28
2.1 Frühe Formen von Geld	30
2.2 Von Waren zu Schuldscheinen	31
2.3 Übergang von solidem zu unsolidem Geld	32
2.4 Wo stehen wir heute?	35
2.5 Der Preis der Kontrolle: Ein Blick auf Überwachung, Zensur und Regulierung	35
2.5.1 Der Aufstieg einer bargeldlosen Gesellschaft	35
2.5.2 Überwachung	40
2.5.3 Finanzielle Regulierungen und Zensur	40
Kapitel 3 – Die dunkle Seite von Fiat	45
3.0 Gemeinschaftsübung: Die Auswirkungen der Inflation: Eine Auktionsübung	46
3.1 Die größten Bedrohungen für dein Geld:	
Inflation, Entwertung und Kaufkraftverlust	48
3.2 Schulden: Der schmale Grat zwischen Hilfe und Schaden	52
3.3 Die Fed und ihre Partner:	
Wie Regierung und Banken die Geldmenge kontrollieren	53
3.4 Die Magie der Geldschöpfung	
3.4.1 Der Zeitwert des Geldes und seine Rolle für das Wirtschaftswachstum	55
3.4.2 Geld sparen in schwierigen Zeiten	56
3.4.3 Mindestreserve-System (Fractional Reserve)	57
3.4.4 Gemeinschaftsübung: Mindestreserve-Bankwesen	58

Kapitel 4 – Die Zukunft ist dezentral:

Die Ermächtigung von Gemeinschaften und Individuen	63
4.0 Von der Krise zur Innovation:	
Die Cypherpunks und die Schaffung einer dezentralen digitalen Währung	64
4.1 Missbrauch der Zentralisierung	64
4.1.1 Zentralisierte Systeme	64
4.1.2 Die Intermediäre:	
Ein Überblick über die Akteure bei einer Kreditkartentransaktion	66
4.2 Ein leistungsfähiges Instrument zur Überwindung der Grenzen der Zentralisierung	68
4.2.1 Gemeinschaftsübung: Dezentrales Konsensspiel mit böswilligen Akteuren	69
4.3 Transaktionen sind nur Handelsvereinbarungen	70
4.3.1 Vertrauen oder nicht vertrauen	70
4.3.2 Lasst uns Vertrauen gegen Regeln tauschen	71
4.4 Die Entfesselung der Macht der Blockchain: Eine Technologie revolutioniert die Zukunft	72

Kapitel 5 – Die Zukunft des Geldes: Eine Einführung in Bitcoin **75**

5.0 Der geheimnisvolle Schöpfer von Bitcoin:	
Die Identität von Satoshi Nakamoto und sein Whitepaper	76
5.1 Erläuterung von Bitcoin und Bitcoin in diesem Buch	78
5.1.1 Was ist Bitcoin? Was ist Bitcoin?	78
5.1.2 Was ist der Unterschied zwischen Bitcoin und Bitcoin?	79
5.1.3 Warum mit Bitcoin beschäftigen, wenn man es sich nicht leisten kann?	79
5.1.4 Woraus besteht Bitcoin?	79
5.1.5 Warum ist Bitcoin gutes Geld?	80
5.1.6 Was geht mich das an?	80
5.1.7 Wie BENUTZT man Bitcoin?	81
5.1.8 Wie kann man Bitcoin VERSENDEN oder AUSGEBEN?	81
5.1.9 Wie ERHÄLT man Bitcoin?	81
5.1.10 Kann Bitcoin abgeschaltet werden?	81
5.1.11 Wie behält die Blockchain den Überblick darüber, wer welche Bitcoin ausgibt?	82
5.1.12 Wie gelangen neue Bitcoin in das Netzwerk?	82
5.1.13 Was ist eine Bitcoin-Transaktion?	82
5.1.14 Sind Bitcoin-Transaktionen sicher?	84
5.2 Wer ist wer und was ist was in der Bitcoin-Welt?	87
5.3 Ablauf einer Bitcoin-Transaktion	89
5.3.1 Gemeinschaftsübung: Bitcoin-Transaktionen in Aktion	93
5.4 Wodurch erhält Bitcoin seinen Wert?	95



Kapitel 6 – Bitcoin Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen	99
6.0 Vom Neuling zum Profi: Ein Leitfaden für die Bitcoin-Wallet	100
6.1 Der Vorgang des Onboardings und der Sicherung deiner Bitcoin	103
6.1.1 Gemeinschaftsübung: Selbstverwahrung und selbstbewusster Umgang mit der Wallet	104
6.1.2 Gemeinschaftsübung: Wie erhalte ich Bitcoin (im Detail)?	105
6.1.3 Gemeinschaftsübung: Wie sende ich Bitcoin und bezahle für Waren und Dienstleistungen (im Detail)?	105
6.2 On-Chain vs. Off-Chain	106
6.3 Das Lightning-Netzwerk	107
6.3.1 Eine Lightning-Transaktion	109
6.3.2 Gemeinschaftsübung: Lightning-Wallet-Staffellauf	112
6.3.3 Gemeinschaftsübung: Interaktive Lightning-Online-Demo	112
Kapitel 7 – Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs	115
7.0 Die Beseitigung des Problems der doppelten Ausgaben: Bitcoins Lösung	117
7.1 Die Nachverfolgung deiner Geldeinheiten	119
7.2 Sicherheit und Geheimhaltung	122
7.3 Der „Mempool“ oder Memorypool: Der Auffangbehälter für Bitcoin-Transaktionen	127
7.3.1 Gemeinschaftsübung: In der Warteschleife: Die unbestätigten Transaktionen des Bitcoin-Netzwerks	128
7.4 Hinter den Kulissen der Blöcke: Das Geheimnis vom Bitcoin-Scripting	129
7.4.1 Ein technischer Einblick in Bitcoin-Transaktionen	131
Kapitel 8 – Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain	135
8.0 Die Juwelen der Blockchain: Die Miner und der Mining-Prozess	136
8.1 Das dynamische Belohnungssystem des Bitcoin-Minings: Blocksubventionen, Transaktionsgebühren und Halvings	137
8.2 Die entscheidende Aufgabe des Bitcoin-Minings: Die Sicherung der Blockchain	139
8.3 Analyse eines Blocks	142

8.4 Hashes erneut hashen	146
8.5 Das Mining eines Blocks Schritt für Schritt erklärt	148
8.5.1 Gemeinschaftsübung: Interaktive Mining-Übung	150
8.5.2 Überblick über den gesamten Transaktionsvorgang	151
8.5.3 Vertrauen ist gut, Kontrolle ist besser (Don't Trust, Verify)	152
8.6 Gemeinschaftsübung: Transaktion mit UTXOs	153
 Kapitel 9 – Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft	157
9.0 Warum Bitcoin?	158
9.1 Die Zukunft von Bitcoin	158
9.1.1 Der Lindy-Effekt	159
9.2 Bitcoin ist mehr als nur digitales Geld	160
9.3 Die Probleme und Herausforderungen	161
9.3.1 Das regulatorische Umfeld für Bitcoin	161
9.3.2 Der Energieverbrauch beim Bitcoin-Mining	162
9.4 Die Risiken	163
9.5 Trading mit und Investieren in Bitcoin	164
 Kapitel 10 – Von Bits zu Bitcoin: Das Zusammensetzen des Puzzles	171
10.0 Nur ein paar Fakten, ein paar Witze ... und der Fachjargon	172
10.1 Richtlinien für die Einreichung und Bewertung der Abschlussarbeit von Mi Primer Bitcoin	174
 Weiterführende Quellen	177
 Glossar	181



Warum Bitcoin?

Kritisches Denken: Warum ist *Bitcoin* wichtig für dich und wie wird es deiner Meinung nach die Menschheit verändern?

Bitcoin-Diplom

*Eine zehnwöchige Transformationsreise
durch unabhängige, unparteiische,
hochwertige und kostenlose Bildung*

Was auch immer Bitcoin sein mag; die meisten Menschen verstehen noch nicht, worum es bei dieser kontroversen und einflussreichen Innovation geht und wie sie funktioniert.
Dies ist ein preisgekrönter Dokumentarfilm, der dir hilft, diese Fragen zu beantworten.



<https://www.youtube.com/watch?v=0wwzyi8E2zQ>

Bevor man sich mit **Bitcoin** beschäftigt, ist es wichtig, die Grundlagen des Geldes, seine Geschichte und das aktuelle Finanzsystem zu kennen. Das Verständnis dieser Konzepte bietet eine solide Grundlage, um die einzigartige und disruptive Natur von **Bitcoin** zu verstehen. Indem du etwas über die Entwicklung des Geldes lernst, wirst du in der Lage sein, das Potenzial und die Grenzen des aktuellen Finanzsystems besser zu verstehen und wie **Bitcoin** darauf abzielt, diese zu überwinden. Ohne diese Grundlage kann es schwierig sein, die Bedeutung und den potenziellen Einfluss von vollständig zu erfassen. Vertraue dem Lernprozess und bleibe fokussiert, denn die Belohnung in Form eines tieferen **Bitcoin** Verständnisses und einer größeren Wertschätzung dieses hochmodernen Bereichs wird es wert sein.

Eine Botschaft von unserem Gründer



<https://miprimerbitcoin.io/educacion-bitcoin/>



Kapitel 1

Die Macht des Geldes

1.0 Seid ihr bereit?

1.1 Gruppendiskussion: Was ist Geld?

**1.2 Die begrenzte Welt: Umgang mit Knappheit
in einer wachsenden Wirtschaft**

1.3 Definition von Geld

1.3.1 Wir können es benutzen, aber auch definieren?

1.3.2 Funktionen von Geld

1.3.3 Eigenschaften von Geld

1.3.4 Arten von Geld



1.0 Seid ihr bereit?

Bitcoin wurde schon oft als Modeerscheinung, Betrug oder „magisches Internet-Geld“ bezeichnet. Doch hinter dem Hype verbirgt sich eine mächtige Technologie, die das Potenzial hat, die Art und Weise, wie wir über Geld denken und es verwenden, zu verändern. Das Potenzial, die Welt so zu verändern, dass „normale Menschen“ wie du und ich die Möglichkeit haben, Vermögen aufzubauen, wirklich frei zu werden und das Leben zu leben, das wir leben wollen. In diesem Kurs werden wir die Schwächen und Grenzen unseres derzeitigen Finanzsystems untersuchen und wie *Bitcoin* dafür eine mögliche Lösung bietet. Wenn ihr also bereit seid, die Schlagzeilen hinter euch zu lassen und mehr über die realen Möglichkeiten von *Bitcoin* erfahren, dann lasst uns in den Kaninchenbau eintauchen.

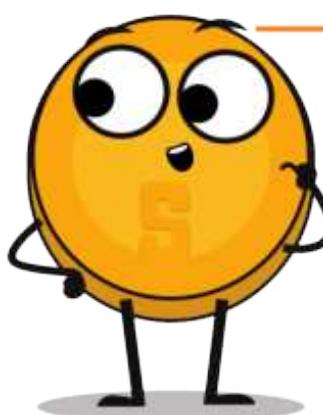
1.1 Gruppendiskussion: Was ist Geld?

- Bitte iss jetzt noch nicht das Bonbon, das auf deinem Schreibtisch liegt!
- Wer wäre bereit, sein Bonbon gegen einen 1-Dollar-Schein einzutauschen?
- Nun hebt die Hand, wenn ihr immer noch bereit wärt, euer Bonbon gegen einen 1-Monopoly-Dollar-Schein einzutauschen – anstatt gegen den 1-Dollar-Schein!
 - Warum bzw. warum nicht?



- Was macht den einen Schein so begehrswert und den anderen so gut wie wertlos?
- Wodurch erhält Geld seinen „Wert“?
- Woher kommt das Geld und wer entscheidet, wie viel davon gedruckt werden soll?
- Warum nicht mehr Geld drucken und gleichmäßig an alle verteilen?
- Ist Geld durch Gold gedeckt? Oder durch irgendeinen anderen Rohstoff?
- Wie viele Menschen verwenden überhaupt noch Bargeld?

Hallo, ich bin Satoshi, ein interaktiver Assistent, der dich durch das *Bitcoin Diplom* begleiten wird. Ich werde dir während des Kurses Informationen und Empfehlungen geben.



Der einzige Unterschied zwischen diesen beiden Scheinen ist *dein Glaube, dass der eine wertvoller ist als der andere.*



1.2 Die begrenzte Welt: Umgang mit Knappheit in einer wachsenden Wirtschaft

Stell dir vor, du bist in einer Wüste gestrandet und hast nur noch eine Flasche Wasser. Du bist durstig und brauchst dringend etwas zu trinken, aber du weißt auch, dass du das Wasser zum Überleben brauchst, bis du mehr findest. Dies ist ein klassisches Beispiel für Knappheit – du hast nur eine begrenzte Menge einer Ressource (Wasser) und musst dich entscheiden, wie du sie nutzen willst.

In dieser Situation kannst du beschließen, das Wasser zu rationieren und über einen längeren Zeitraum hinweg kleine Schlucke zu nehmen, damit es möglichst lange reicht. Oder du entscheidest dich dafür, so viel wie möglich auf einmal zu trinken, in der Hoffnung, dass der Flüssigkeitsschub dir die nötige Energie gibt, um mehr Wasser zu finden. Unabhängig davon, welche Wahl du triffst, stehst du vor einer schwierigen Entscheidung.



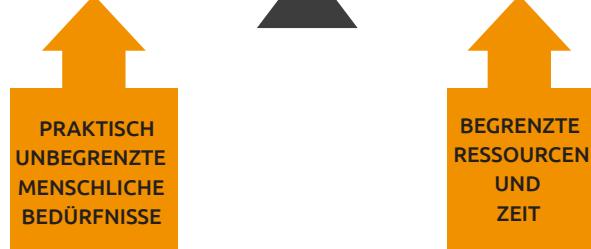
Knappheit zwingt uns dazu, die Vor- und Nachteile der Nutzung unserer Ressourcen abzuwägen und Kompromisse zu schließen.

In diesem Fall musst du dich entscheiden, ob du deinen *unmittelbaren* Durst stillen oder das Wasser für *später* aufbewahren willst.

Dieses Konzept der *Knappheit* gilt für alle Arten von Ressourcen, nicht nur für Wasser. Ob es sich um Geld, Zeit oder sogar Liebe und Aufmerksamkeit handelt, wir stehen ständig vor der Entscheidung, wie wir unsere begrenzten Ressourcen einsetzen sollen.

Wir wollen Nahrung,
Reisen, Unterhaltung,
Unterkunft, Autos,
Medikamente,
Schmuck, etc.
 ∞

Land, Arbeit,
Kapital, Unternehmen



- Es gibt zwei Arten von Knappheit: **vom Menschen verursachte Knappheit** und **natürliche Knappheit**.

- **Die künstliche Verknappung**, auch als *zentralisierte Verknappung* bekannt, umfasst Dinge wie limitierte Ausgaben von Designertaschen, seltene Sammelkarten und nummerierte Kunstwerke. Diese können leicht reproduziert oder gefälscht werden.
- **Natürliche Knappheit**, auch bekannt als *dezentrale Knappheit*, umfasst Dinge wie Salz, Muscheln und Edelmetalle wie Gold. Diese sind schwieriger zu reproduzieren oder zu fälschen.

- Der Hauptunterschied zwischen den beiden ist die Kontrolle. Zentralisierte Knappheit wird von einer einzigen Instanz kontrolliert, z. B. einem Unternehmen oder einer Regierung, während dezentralisierte Knappheit von niemandem kontrolliert wird.

Knappheit beeinflusst unsere Entscheidungen, und wenn wir sie verstehen, können wir unsere Entscheidungsfindung verbessern. Wir müssen oft zwischen unmittelbaren Gewinnen und langfristigen Vorteilen wählen, und diese Abwägungen bestimmen unseren Weg zum Erreichen unserer Ziele.

Die Macht des Geldes

- Im Kontext des Beispiels in der Wüste bedeutet dies, dass du eher das sofortige Trinken des gesamten Wasser vorziehen könntest, auch wenn dies bedeutet, dass du später kein Wasser mehr übrig haben wirst. Das liegt daran, dass der unmittelbare Durst dringender ist, als der Durst, den du später verspüren kannst.
- Wenn du hingegen das Wasser rationierst und es langsam trinkst, hast du eine niedrige Zeitpräferenz. Das bedeutet, dass du bereit bist, mit dem Stillen deines Durstes zu warten, um langfristig eine größere Überlebenschance zu haben.



Die Zeitpräferenz bezieht sich auf die Idee, dass Menschen im Allgemeinen lieber JETZT etwas haben wollen als später.

NIEDRIG



HOCH



- Nehmen wir zum Beispiel an, man hat die Möglichkeit, 100 Euro heute oder 110 Euro in einem Jahr zu erhalten. Wenn man eine hohe Zeitpräferenz hat, würde man sich vielleicht dafür entscheiden, die 100 Euro heute zu erhalten, weil man die unmittelbare Befriedigung, das Geld jetzt zu haben, mehr schätzt als den potenziellen Nutzen, auf die zusätzlichen 10 Euro in einem Jahr zu warten. Wenn man hingegen eine niedrige Zeitpräferenz hat, ist man vielleicht bereit, auf die größere Belohnung in der Zukunft zu warten, weil man weniger auf unmittelbare Befriedigung und mehr auf langfristige Planung bedacht ist.

Das Konzept der **Opportunitätskosten** ist eng mit dem Konzept der **Knappheit** und der **Zeitpräferenz** verbunden.



Unter **Opportunitätskosten** versteht man den Wert der nächstbesten Alternative, auf die man bei einer Entscheidung verzichtet.

Jede Entscheidung ist mit Abwägungen verbunden.

- Im Beispiel der Wüste sind die Opportunitätskosten für das sofortige Trinken des gesamten Wassers die Überlebensvorteile, die man durch die Rationierung des Wassers und seine Verwendung über einen längeren Zeitraum hinweg erzielt hätte.

Die heutige Entscheidung:



Kauf eines 7-Euro-Erdbeer-Smoothies.

JETZT



7 € auf andere Weise ausgeben.

SPÄTER



Von den regelmäßig gesparten 7 € profitieren.





- Nehmen wir an, du beschließt, das Wasser zu rationieren und über einen längeren Zeitraum kleine Schlucke zu nehmen. So hast du die Energie und die Flüssigkeitszufuhr, die du brauchst, um nach mehr Wasser zu suchen.
- Bei deiner Suche stößt du jedoch auf einen Kaktus, in dem sich eine kleine Menge Wasser befindet. Es ist nicht viel, aber es reicht, um deinen Durst für den Moment zu stillen. Hättest du beschlossen, dein gesamtes Wasser auf einmal zu trinken, hättest du vielleicht nicht die Energie gehabt, nach mehr Wasser zu suchen und auf den Kaktus zu stoßen. In diesem Fall wären die Opportunitätskosten für das Trinken des gesamten Wassers auf einmal die Chance gewesen, den Kaktus zu finden und mehr Flüssigkeit zu dir zu nehmen.

Dieses Beispiel veranschaulicht, dass die Opportunitätskosten nicht nur die unmittelbare Abwägung zwischen zwei Optionen betreffen, sondern auch die potenziellen zukünftigen Chancen, die wir durch unsere Entscheidungen erhalten oder verlieren können. Unsere Bereitschaft, auf eine größere Belohnung in der Zukunft im Austausch für eine geringere Belohnung in der Gegenwart zu verzichten, wird von unserer **Zeitpräferenz** beeinflusst, d. h. davon, wie sehr wir sofortige Befriedigung gegenüber langfristiger Planung schätzen.

Auch Unternehmen, Regierungen und Gesellschaften müssen Entscheidungen treffen.

UNTERNEHMEN	REGIERUNGEN/GESELLSCHAFTEN
Entlassung von 200 Mitarbeitern oder Einfrieren der Löhne	Bau einer neuen Autobahn oder Erhöhung der Lehrergehälter
Kreditaufnahme oder Gewinnung weiterer Anteilseigner	Finanzierung der Forschung zur Krebsbehandlung oder saubere Energie

1.3 Definition von Geld

1.3.1 Wir können es benutzen, aber auch definieren?

Hast du jemals darüber nachgedacht, was Geld wirklich ist? Hast du dich jemals gefragt, was Geld, nun ja, zu Geld macht? Die meisten von uns wissen, wie man damit umgeht, aber nur wenige von uns verstehen, woher es kommt oder wie es funktioniert.

Geld ist im Wesentlichen ein Mittel zum Austausch von Waren und Dienstleistungen. Es repräsentiert den Wert dieser Güter in einer Form, die leicht gehandelt werden kann.



Die Macht des Geldes

Es kann viele verschiedene Formen annehmen, z. B. Papierscheine, Metallmünzen und elektronische Zahlungen. In der Regel wird Geld von Regierungen oder anderen Behörden ausgegeben und kontrolliert.

Aber Geld ist so viel mehr als nur ein physisches oder digitales Tauschmittel. Es ist wie eine universelle Sprache, die es uns ermöglicht, mit Menschen auf der ganzen Welt zu handeln, auch wenn wir nicht dieselbe Sprache sprechen oder dieselbe Kultur haben. Man kann zum Beispiel am anderen Ende der Welt sein und trotzdem Geld „sprechen“, indem man ein Produkt auf den Ladentisch legt und es in die Landeswährung umtauscht oder eine Kreditkarte benutzt. Geld ist wie ein sozialer Vertrag, der es uns ermöglicht, Tauschgeschäfte zu tätigen, ohne dass wir auf Tauschhandel angewiesen sind oder jemanden finden müssen, der das, was wir anbieten, unbedingt haben will. Wenn eine Gruppe von Menschen anfangen würde, Schokolade als Zahlungsmittel für die meisten Waren und Dienstleistungen zu akzeptieren, würde Schokolade zu Geld werden. (Obwohl wir sie eher als schlechtes Geld betrachten könnten, da sie in einigen Teilen der Welt schmelzen würde.)

Wie der französische Wirtschaftswissenschaftler Jean Baptiste Say feststellte, „erfüllt das Geld bei einem Tausch nur eine momentane Funktion; und wenn die **Transaktion** schließlich abgeschlossen ist, wird man immer feststellen, dass eine Art von Ware gegen eine andere getauscht wurde.“

Mit anderen Worten: Geld selbst hat nicht die Macht, die menschlichen Bedürfnisse zu befriedigen. Es ist nur ein Werkzeug, mit dem wir eine Ware gegen eine andere tauschen können.



Wie einfach oder durchführbar wäre dieser Handel ohne Geld?

Würdest du eine Kuh gegen 1.000.000 Erdbeeren tauschen?
Oder 600.000 Erdbeeren?
Wie wäre es mit 50.000?



Eine Transaktion ist ein Austausch oder ein Transfer von Waren und Dienstleistungen. Es ist eine Form des Wertaus tauschs zwischen zwei oder mehreren Parteien.

Es gibt viele verschiedene Arten von Transaktionen, die von einfachen Tauschgeschäften (z. B. dem Kauf eines Sandwiches in einem Feinkostladen) bis hin zu komplexeren Finanztransaktionen (z. B. dem Kauf eines Hauses oder der Investition in Aktien oder Anleihen) reichen. Transaktionen können persönlich, telefonisch, online oder auf andere Weise abgewickelt werden, und es kann eine Vielzahl von Parteien beteiligt sein, darunter Privatpersonen, Unternehmen und Finanzinstitute.

Geld IST der Wert, MIT dem Waren getauscht werden.

Geld IST NICHT der Wert, FÜR den Waren getauscht werden.



Schau dir dieses kurze Video an!



<https://youtu.be/lnwVM6s7WoY>



Zusammenfassend kann man sagen, dass Geld:

- den Handel erleichtert, weil es von allen als endgültige Zahlung akzeptiert wird.
- es uns ermöglicht, den Wert zu messen und Vergleiche zwischen verschiedenen Waren und Dienstleistungen anzustellen.
- unsere Zeitpräferenz senkt, da es uns ermöglicht, zu sparen und es in der Zukunft auszugeben.

1.3.2 Funktionen von Geld

Wenn es um den Kauf und Verkauf von Waren und Dienstleistungen geht, ist Geld der wichtigste Akteur. Es hat mehrere wichtige Aufgaben, wie zum Beispiel:

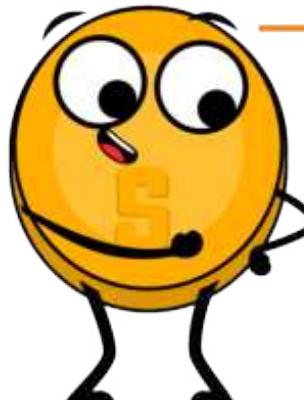
● **Tauschgeschäfte vereinfachen:** Mit Geld muss man nicht erst jemanden finden, der genau das haben will, was man tauschen will. Stattdessen kann man mit Geld alles kaufen und verkaufen, was man will, was den Handel und die Geschäfte viel bequemer und effizienter macht.

Tauschmittel



● **eine Recheneinheit zu sein:** Geld bietet einen universellen Wertmaßstab, der es den Menschen ermöglicht, den Preis verschiedener Waren und Dienstleistungen auszudrücken und zu vergleichen. Dies ermöglicht einen effizienteren und transparenteren Markt, auf dem die Menschen fundierte Entscheidungen über Kauf und Verkauf treffen können.

○ Stell dir Folgendes vor: Wenn du ein neues Auto kaufen willst, könntest du die Preise verschiedener Autohäuser vergleichen und auf der Grundlage des Europapreises eine fundierte Entscheidung über den Kauf treffen. Ohne eine Recheneinheit müsstest du versuchen, den Wert eines Autos mit dem eines anderen zu vergleichen, indem du etwas anderes heranziehst, z. B. die Anzahl der Kühe, die es wert war, oder die Zeit, die es dauerte, das Auto herzustellen.



Recheneinheit

Die Verbraucher kennen den Wert einer Sache, wenn man ihr einen Preis (Geldwert) zuweist.

MP3-Player
29,00 €



MP3-Player
129,00 €



Die Macht des Geldes

- ein Wertaufbewahrungsmittel zu sein: Geld sollte seinen Wert im Laufe der Zeit beibehalten, so dass es als Mittel zum Sparen und Investieren des Wertes der menschlichen Arbeit genutzt werden kann. Dies ermöglicht es den Menschen, mit Geld problemlos für die Zukunft zu planen und sich gegenseitig Geld zu leihen und zu verleihen.

Was ist dein Wertspeicher?	BTC (USD)	Gold (USD)	USD (EUR)	ETH (USD)
14. März 2019	\$3.846	\$1.293	€0,8817	\$136,86
14. März 2020	\$5.258	\$1.529	€0,90056	\$127,76
Gewinn/Verlust	+36,71%	+18,25%	+2,14%	-6,65%

Wenn du also das nächste Mal für etwas Besonderes sparst, denk daran, dass Geld mehr ist als nur ein Mittel um Dinge zu bezahlen – es ist ein Instrument, das dir hilft, deine Zukunft zu planen und in sie zu investieren.

Diese drei Funktionen sind es, die es den Volkswirtschaften ermöglichen, komplex und dynamisch zu werden. Ohne Geld wäre es viel schwieriger, Waren und Dienstleistungen zu kaufen und zu verkaufen, und unsere Wirtschaft wäre viel weniger entwickelt.

Gemeinschaftsübung: Welche Funktion des Geldes passt zu folgenden Beispielen?

- Paul beschloss, einen Teil seines wöchentlichen Gehalts zu sparen, um einen Welpen zu kaufen.
- Tom kauft bei einem Imbiss zwei Pizzastücke für 8,30 €.
- Mark kann sich nicht entscheiden, ob er Konzertkarten für 75 € oder einen Skipass für 95 € kaufen soll.

1.3.3 Eigenschaften von Geld

Im Laufe der Zeit haben die Menschen schließlich erkannt, dass Geld bestimmte Eigenschaften besitzt, um als Tauschmittel wirksam zu sein. Zu diesen Eigenschaften gehören Langlebigkeit, Tragbarkeit, Teilbarkeit, Fungibilität, Knaptheit und Akzeptanz.

- Langlebigkeit** bezieht sich auf die Fähigkeit des Geldes, dem physischen Verfall zu widerstehen und über die Zeit hinweg haltbar zu sein. Dadurch wird sichergestellt, dass Geld in einem akzeptablen und erkennbaren Zustand in der Wirtschaft zirkulieren kann.

Gold ist ein beständiges Material, das Verschleißerscheinungen standhält und somit die Langlebigkeit von Geld gut repräsentiert.





Kapitel 1

- **Tragbarkeit** bezieht sich auf die Leichtigkeit, mit der Geld transportiert und herumgetragen werden kann. Dies ermöglicht es den Menschen, mit Geld problemlos Waren und Dienstleistungen zu kaufen und zu verkaufen.

Kreditkarten sind tragbar, da sie leicht in einer Brieftasche oder einem Portemonnaie mitgeführt werden können, was sie zu einem guten Beispiel für die Tragbarkeit des Geldes macht.



- **Akzeptanz** bezieht sich auf die weit verbreitete Akzeptanz von Geld als Zahlungsmittel, sodass die Menschen es ohne Bedenken für den Kauf und Verkauf von Waren und Dienstleistungen verwenden können.

Der US-Dollar ist ein allgemein anerkanntes Zahlungsmittel und damit ein gutes Beispiel für die Akzeptanz des Geldes.



- **Knappheit** bezieht sich auf das begrenzte Angebot an Geld, das dazu beiträgt, seinen Wert zu erhalten und zu verhindern, dass wir mehr Geld ausgeben müssen, um die gleiche Menge an Waren zu kaufen.

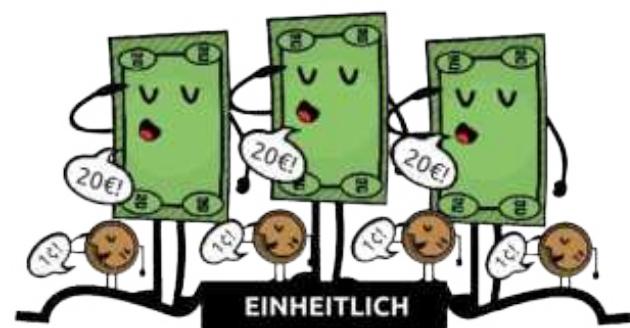
Sammlermarken, insbesondere seltene und wertvolle, können eine gute Form des Geldes sein, da sie selten sind und im Laufe der Zeit an Wert gewinnen können. Briefmarkensammler nutzen ihre Briefmarken oft als eine Möglichkeit, ihr Vermögen zu investieren und ihr Portfolio zu diversifizieren.



- **Fungibilität** bezieht sich auf die Austauschbarkeit des Geldes, sodass eine Geldeinheit einer anderen Einheit desselben Wertes gleichwertig ist.

Geld sollte **einheitlich** sein.

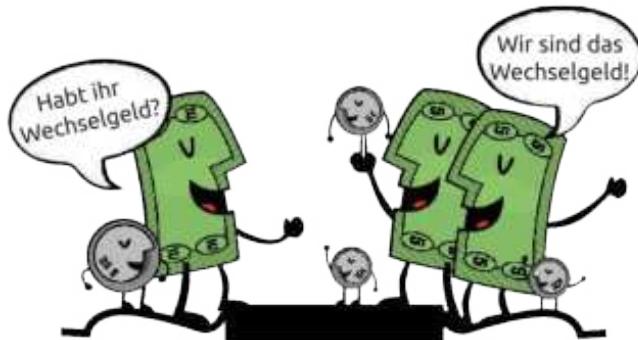
Kupfermünzen haben eine einheitliche Größe und ein einheitliches Gewicht und sind damit ein gutes Beispiel für die Einheitlichkeit des Geldes.



Die Macht des Geldes

- **Teilbarkeit** bezieht sich auf die Fähigkeit des Geldes, in kleinere Einheiten unterteilt zu werden, sodass die Menschen es für Käufe in unterschiedlicher Höhe verwenden können.

Papiergegscheine können leicht in kleinere Einheiten unterteilt werden, was sie zu einem guten Beispiel für die Teilbarkeit von Geld macht.



Insgesamt machen diese Eigenschaften Geld zu einem nützlichen und wirksamen Instrument zur Erleichterung von Handel und Gewerbe, und sie sind für die Entwicklung und Stabilität von Volkswirtschaften unerlässlich.

Gemeinschaftsübung: Verschiedene Vermögenswerte haben unterschiedliche Eigenschaften und erfüllen die Funktionen von Geld in unterschiedlichem Maße. Die Gesellschaft bestimmt letztendlich, welcher Vermögenswert als Geld verwendet wird, basierend auf Faktoren wie Stabilität, Knappheit, Teilbarkeit, Übertragbarkeit und Akzeptanz als Tauschmittel.

Um zu bestimmen, wie gut verschiedene Gegenstände die spezifischen Merkmale von Geld erfüllen, könnt ihr jeden Gegenstand auf einer Skala von 1 bis 5 für jedes Merkmal bewerten. Wenn ihr die Punkte für jeden Gegenstand zusammenzählt, könnt ihr feststellen, welcher Gegenstand am besten als Geldform geeignet ist.

[0 = schlecht; 3 = gut; 5 = ausgezeichnet]

* Bitte füllt die Spalte für **Bitcoin** nicht aus; wir werden später im Kurs darauf zurückkommen.

 Stell dir die folgenden Fragen, um festzustellen, inwieweit die verschiedenen Gegenstände in der Tabelle die Merkmale von Geld erfüllen!

- **Langlebigkeit:** Kann das Geld im Laufe der Zeit Verschleiß und Abnutzung standhalten?
- **Tragbarkeit:** Kann das Geld leicht transportiert und an verschiedenen Orten verwendet werden?
- **Fungibilität:** Ist das Geld mit anderen Formen von Geld austauschbar?
- **Akzeptanz:** Ist das Geld als Zahlungsmittel weitgehend akzeptiert?
- **Knappheit:** Ist das Geld knapp und nicht zu reichlich vorhanden?
- **Teilbarkeit:** Kann das Geld für Transaktionen in kleinere Einheiten geteilt werden?





Eigenschaften von gutem Geld	Kühne	Zigaretten	Diamanten	Euro	Bitcoin
LANGLEBIGKEIT					
TRAGBARKEIT					
EINHEITLICHKEIT					
AKZEPTANZ					
KNAPPHEIT					
TEILBARKEIT					
GESAMT					

1.3.4 Arten von Geld

Wenn es um Geld geht, gibt es zwei Hauptkategorien: **physisch** und **digital**.

Für **physisches Geld** gibt es drei Optionen:

- **Fiat-Geld** ist das, was wir jeden Tag benutzen, wie z. B. Papierscheine und Münzen. Es wird von der Regierung emittiert und als Zahlungsmittel akzeptiert, auch wenn es nicht durch ein physisches Gut gedeckt ist.
- **Repräsentatives Geld** stellt einen Anspruch auf ein physisches Gut dar. Wie Fiat-Geld kann es auch ein Papierschein sein (z. B. ein Gold- oder Silberzertifikat), aber im Gegensatz zu Fiat-Geld ist es durch ein physisches Gut gedeckt, das die Gesellschaft als wertvoll erachtet. Das bedeutet zum Beispiel, dass ein Goldzertifikat im Wert von einem US-Dollar bei einer Bank gegen Gold im Wert von einem US-Dollar getauscht werden kann, was früher in vielen Ländern der Fall war.
- **Waren geld** ist ein physischer Gegenstand, der einen inneren Wert hat und als Tauschmittel allgemein akzeptiert wird. Gold und Silber gehören zu dieser Kategorie.

Die Macht des Geldes



Geld ist
nicht gleich
Geld!



Waren geld



Gegenstände wie dieses Schießpulver dienten einst als Waren geld.

Repräsentatives Geld



Repräsentatives Geld wie dieses Silberzertifikat konnte in Silber umgetauscht werden.

Fiat-Geld



Heute sind die Banknoten der Federal Reserve Fiat-Geld, das von der Regierung als akzeptiertes Mittel zur Begleichung von Schulden verordnet wurde.



Waren (oder Waren geld) werden oft als „fungibel“ und von gleichbleibender Qualität angesehen. So wird beispielsweise ein Barrel Öl im Allgemeinen als dasselbe angesehen wie jedes andere Barrel Öl, unabhängig davon, woher es kommt oder wer es produziert hat.



Zahlungsnetzwerke sind wie digitale Autobahnen, über die elektronische Währungen online von einem Ort zum anderen gelangen können. Sie machen es einfacher, schneller und sicherer, Dinge online zu bezahlen, egal ob man eine Kryptowährung wie **Bitcoin** oder eine traditionelle Zahlungsmethode wie eine Kreditkarte verwendet.

Elektronische Währungen sind eine Art von Geld, das für Online-Transaktionen verwendet werden kann. Sie sind wie digitale Versionen von regulärem Geld, wie Dollar oder Euro, und können verwendet werden, um Dinge online über Zahlungsnetzwerke zu kaufen und zu verkaufen.



Digitale Zentralbank-Währungen (CBDCs):

Dabei handelt es sich um digitale Versionen der Fiat-Währung eines Landes, die von der Zentralbank emittiert und abgesichert und daher von der Regierung vermittelt werden. Das heißt, die Regierung ist der Mittelsmann beim Umtausch.





Kapitel 1

Digitale Zahlungsnetzwerke im traditionellen Finanzsystem bestehen aus der Technologie und den Systemen, die die Durchführung und Verarbeitung elektronischer Zahlungen ermöglichen, z. B. Bankserver, Datenbanken und sichere Netze. Es gibt jedoch immer einen Mittelsmann, z. B. eine Bank oder ein Finanzinstitut, der eine Gebühr erhebt und die Befugnis hat, Transaktionen zu akzeptieren, zu stornieren, zurückzuweisen oder zu verzögern.

Die wichtigsten Arten von digitalen Zahlungsnetzwerken im zwischengeschalteten Finanzsystem sind:

- **Kartennetzwerke:** Dies sind Netzwerke, die den Geldtransfer zwischen Finanzinstituten und Händlern erleichtern, wenn ein Kunde einen Kauf mit einer Debit- oder Kreditkarte tätigt. Beispiele sind Visa, Mastercard und American Express.
- **Digitale Geldbörsen (Wallets):** Eine digitale Brieftasche ist ein Online-Konto, in dem die Nutzer ihre elektronischen Währungen (d. h. digitale Vermögenswerte wie digitales Fiat-Geld, Kryptowährungen oder Treuepunkte) speichern und verwalten können. Nutzer können mit ihrer elektronischen Geld-börse Zahlungen vornehmen, indem sie Geld von ihrem Konto auf das Konto des Empfängers überweisen.
- **Kryptowährungen:** Digitale Währungen, die digitale Zahlungsnetzwerke nutzen, um sich online von einem Ort zum anderen zu bewegen. Man kann sie sich als Autos auf digitalen Autobahnen vorstellen, die direkt von einem Punkt zum anderen fahren können, ohne an Zwischenstationen wie Mautstellen anzuhalten. Das bedeutet, dass Kryptowährungen direkt übertragen und umgetauscht werden können, ohne dass ein Mittelsmann wie eine Bank erforderlich ist.

Der Zahlungsvorgang mit der Kreditkarte



Der Zahlungsvorgang mit Kreditkarte ist ein Beispiel für ein Zahlungsnetzwerk.



Stablecoins sind Kryptowährungen, die so konzipiert sind, dass sie einen stabilen Wert im Verhältnis zu einem Vermögenswert, wie dem US-Dollar, behalten. Einige sind durch physische Vermögenswerte gedeckt, und alle werden als Wertaufbewahrungsmittel oder zur Durchführung von Transaktionen ohne die Volatilität verwendet, die mit anderen Kryptowährungen verbunden sein kann.

Die Macht des Geldes

Eine Währung, die ohne Mittelsmänner funktioniert, ist effizienter und für die Gesellschaft vorteilhafter. Sie verhindert, dass einige wenige Personen ihre Macht bündeln und die Geldmenge kontrollieren.

Eine Technologie zu finden, die sichere Transaktionen ermöglicht, ohne auf das Vertrauen zwischen den Parteien angewiesen zu sein, war jedoch schon immer eine Herausforderung. Um dies zu erreichen, muss eine Währung geschaffen werden, die wie das Internet funktioniert, wo die Kontrolle auf alle und niemanden gleichzeitig verteilt ist. Dies erfordert die Zustimmung aller Parteien – auch von denjenigen, die die Macht sind –, die Kontrolle zum Wohle der Allgemeinheit abzugeben.



Doch wie würde eine solche Währung aussehen?



Kapitel 1





Kapitel 2

Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

2.0 Einleitung

2.0.1 Gemeinschaftsübung: Tauschhandelsspiel

2.1 Frühe Formen von Geld

2.2 Von Waren zu Schuldscheinen

2.3 Übergang von solidem zu unsolidem Geld

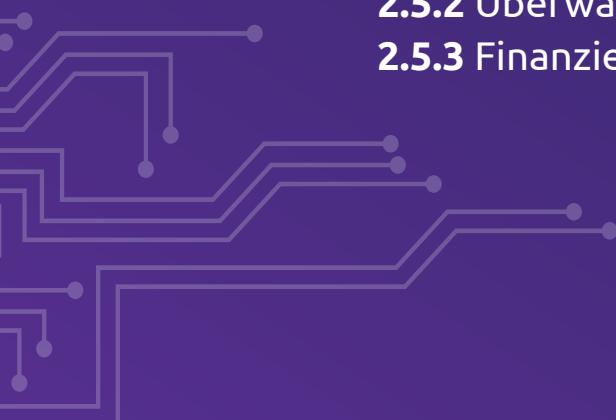
2.4 Wo stehen wir heute?

2.5 Der Preis der Kontrolle: Ein Blick auf Überwachung, Zensur und Regulierung

2.5.1 Der Aufstieg einer bargeldlosen Gesellschaft

2.5.2 Überwachung

2.5.3 Finanzielle Regulierungen und Zensur

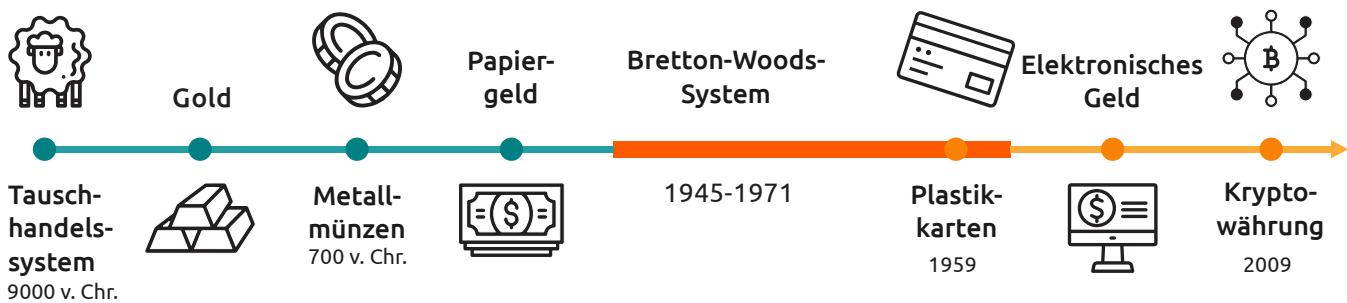


Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

2.0 Einleitung

Das Konzept des Geldes hat sich im Laufe der Zeit weiterentwickelt. In seinen frühen Formen diente Geld dazu, den Handel und den Austausch von Waren und Dienstleistungen zu erleichtern.

- In den alten Zivilisationen verließen sich die Menschen auf den Tauschhandel, ein System des direkten Austauschs von Waren und Dienstleistungen ohne Verwendung eines Zahlungsmittels.
- Später wurden Metallmünzen und Papiergegeld als bequemere Formen des Geldes eingeführt und ebneten den Weg für die hoch entwickelten Finanzsysteme, die wir heute haben.



In diesem Kapitel begeben wir uns auf eine Reise durch die Zeit und erleben die Entwicklung des Geldes aus erster Hand. Wir werden seine Ursprünge zurückverfolgen und beobachten, wie es sich im Laufe der Geschichte verändert und angepasst hat.

2.0.1 Gemeinschaftsübung: Tauschhandelsspiel

● Runde 1 – Tauschhandel

Wir schreiben das Jahr 6000 vor Christus. Natürlich wurde das Geld, wie wir es kennen, noch nicht erfunden. Ihr befindet euch in Mesopotamien und tauscht Waren und Dienstleistungen direkt miteinander aus, indem ihr **Tauschhandel** betreibt.



Nebenbei bemerkt, akzeptieren viele Unternehmen nach wie vor nicht-monetäre Zahlungen für ihre Dienstleistungen, und die Regierungen behandeln diese Tauschgeschäfte bei der Steuererklärung genauso wie Währungstransaktionen.

- Schneidet euer Blatt Papier an der gestrichelten Linie ab. Euer Ziel ist es, euer „Habgut“ so oft wie nötig zu tauschen, um euer ursprüngliches „Bedürfnis“ zu bekommen. Ihr könnt euer ursprüngliches „Bedürfnis“ nicht ändern. Ihr habt fünf Minuten Zeit, um das Ziel dieser Übung zu erreichen.
- Wenn euer neues „Habgut“ mit eurem ursprünglichen „Bedürfnis“ übereinstimmt, kehrt zu eurem Platz zurück. Wenn ihr nach Ablauf der Zeit keinen Handelspartner gefunden habt, kehrt trotzdem zu eurem Platz zurück.



Kapitel 2

 Wer es geschafft hat, sein Bedürfnis nach einem Tauschvorgang zu bekommen, hebt bitte die Hand! Wer hat es nach zwei Tauschvorgängen geschafft? Wer nach drei?

Fragen: Beantwortet folgende Fragen kurz, aber aussagekräftig!

1. Warum konnten einige von euch jemanden zum Tauschen finden und andere nicht?

2. Was sind die Vorteile des Tauschhandels?

3. Was sind nach eurer Erfahrung mit dieser Übung die Nachteile des Tauschhandels?

● Runde 2 – Warengeld

Wir machen einen zeitlichen Sprung und reisen an die Westküste Afrikas des 14. Jahrhunderts vor Christus. Der Tauschhandel ist mühsam und ineffizient geworden. Wir haben uns als Zivilisation weiterentwickelt und verwenden jetzt **Warengeld**.

Von Kaurimuscheln zu Münzen



1300 v. Chr.



1000 v. Chr.



687 v. Chr.

Trivia

Kaurimuscheln wurden in einigen Teilen Afrikas bis ins 20. Jahrhundert als gesetzliches Zahlungsmittel akzeptiert.

Diese Proto-Münzen hatten eine ovale Form, bestanden aus „Elektrum“ (einer Gold-Silber-Legierung) und hatten nur auf einer Seite ein Motiv.

1300 v. Chr.

Kaurimuscheln sind in den meisten Teilen Asiens, Afrikas, Ozeaniens und in einigen Teilen Europas die vorherrschende Form der Bezahlung.

1000 v. Chr.

Die westliche Zhou-Dynastie in China beginnt mit der Verwendung von Metallmünzen.

687 v. Chr.

König Alyattes von Lydien (der heutigen Türkei) lässt die ersten Metallmünzen in der westlichen Welt prägen.

Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

Die Lehrkraft hat dir (der Einfachheit halber) eine Makkaroni gegeben. Nehmen wir an, dass der Preis jedes Gutes vereinbarungsgemäß eine Makkaroni wert ist. Dein Ziel ist es wieder, das zu bekommen, was du „willst“. Nun ist unsere Spezies aber etwas schlauer geworden und hat einen Weg gefunden, bestimmte Probleme zu lösen.

- Warum betrachten wir Makkaroni als Waren Geld?
- Wie bekommen wir jetzt die Dinge, die wir wollen?
- War die Makkaroni-Runde einfacher?
- Warum, glaubst du, hat Geld die Waren ersetzt?
- Inwiefern ist die Verwendung von Waren Geld effizienter als der Tauschhandel?
- Was sind die Nachteile der Verwendung von Makkaroni als Geld?

Was glaubst du, was geschah, als Spanien begann, Schiffsladungen von Makkaroni in deine Gemeinschaft zurückzubringen (Gold und Silber aus Amerika zurück nach Spanien)?

2.1 Frühe Formen von Geld



Schau dir dieses kurze Video an, um mehr über die Ursprünge des Tauschs zu erfahren, in der Reihe „Die Geschichte des Papiergegeldes“.

<https://youtu.be/-nZkP2b-4vo>

In **Tauschwirtschaften** tauschen die Menschen untereinander auf der Grundlage des relativen Werts der von ihnen angebotenen Waren und Dienstleistungen. **Tauschwirtschaften** sind *ineffizient* und können schwierig zu handhaben sein, insbesondere in komplexen Gesellschaften



Eine Situation, die als **Zusammentreffen von Bedürfnissen** bekannt ist, ist in jedem Tauschsystem notwendig, da die Menschen immer jemanden finden müssen, der das hat, was sie wollen, aber auch das will, was sie anzubieten haben.



Ich gebe dir Schuhe für deinen Weizen.

Ich brauche keine Schuhe. Ich brauche Kleidung.

Ich will Schuhe, aber ich habe keinen Weizen.



Nehmen wir an:

- Joseph will seine Banane gegen Marias Kokosnuss tauschen.
- Aber Maria will ihre Kokosnuss nur gegen Pauls Mango tauschen.
- Und Paul will seine Mango nur gegen Josephs Banane tauschen.
- Sie befinden sich in einem nicht enden wollenden Kreislauf des Fruchthandels, ohne dass es zu einer doppelten Übereinstimmung der Bedürfnisse kommt.
- Joseph schlägt vor, die Früchte gegen eine kalte Limonade einzutauschen, aber sie stellen fest, dass sie sich auf einer abgelegenen Insel befinden und es keine Limonade gibt.
- Sie beschließen, sich einfach an den Strand zu setzen und ihre Früchte in Ruhe zu genießen.

Die Verwendung einer **gemeinsamen Recheneinheit**, wie z. B. einer „Limonade“, macht Handel und Gewerbe viel effizienter. In der Antike begannen die Menschen damit, Perlen, Muscheln und andere Gegenstände, die in ihrer Gesellschaft einen Wert hatten, als **Zahlungsmittel** zu verwenden.

2.2 Von Waren zu Schulscheinen

Da ihr und eure Gemeinschaft immer mehr in Handel und Gewerbe involviert seid, erkennt ihr die Grenzen des Tauschhandels und anderer Formen des nicht-monetären Austauschs. Ihr beschließt, die Verwendung von **Metallmünzen** als **Geldform** einzuführen.



Diese Metallmünzen werden aus wertvollen Materialien wie Gold und Silber hergestellt und dienen als Zahlungsmittel und Recheneinheit, um Handel und Gewerbe zu erleichtern: **Warengeld**.

Warum Geld erfunden wurde



Das ist die zweite Episode von „Die Geschichte des Papiergegeldes“ mit dem Titel *Nicht nur Nudeln*.



<https://youtu.be/-nZkP2b-4vo>

Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

Je häufiger ihr jedoch Metallmünzen verwendet, desto mehr stoßt ihr auf einige Nachteile. Sie können schwer und unbequem sein, wenn man sie bei großen Transaktionen mit sich führt, und ihr stellt fest, dass einige Leute das System ausnutzen, indem sie die Münzen einschmelzen und neue Münzen herstellen, wobei sie sie mit billigeren Metallen mischen, was die Preise steigen lässt und das Vertrauen in das System untergräbt.

Um diese Probleme zu lösen, beginnt ihr und eure Gemeinschaft, Papierbelege als Geld zu verwenden. Diese Papierscheine, die ihren Ursprung im alten China haben, sind eine bequeme und leicht austauschbare Form der Währung. Sie sind durch Gold und andere wertvolle Metalle gedeckt und können vom 17. bis 19. Jahrhundert in diese Metalle umgetauscht werden. Dies ermöglicht es euch, eine tragbarere und leichter übertragbare Form von Geld zu haben, während der Wert und die Sicherheit von Edelmetallen erhalten bleiben.



2.3 Übergang von solidem zu unsolidem Geld

Was passiert, wenn man versucht, die Papiergegeld-Doktrin in die Praxis umzusetzen? Finde es heraus in der vierten Folge von „Die Geschichte des Papiergegeldes“.



<https://youtu.be/lzH1p3t2oRE>

Nun springen wir ins 17. Jahrhundert in Schweden. Jetzt seid ihr bei der Aufbewahrung eures wertvollen Vermögens vollständig von Banken abhängig. Ihr bemerkst jedoch, dass mit diesen Bankern etwas faul ist. Es scheint, dass sie mehr Papierbelege ausstellen, als sie Gold lagern, sodass sie mehr Geld erschaffen können, als sie an Vermögenswerten haben, um es zu decken. Diese hinterhältige Praxis ermöglicht es den Bankern, von der Differenz zwischen dem Wert der Papierbelege und dem Wert des Goldes, das sie für ihre Kunden aufbewahren, zu profitieren.



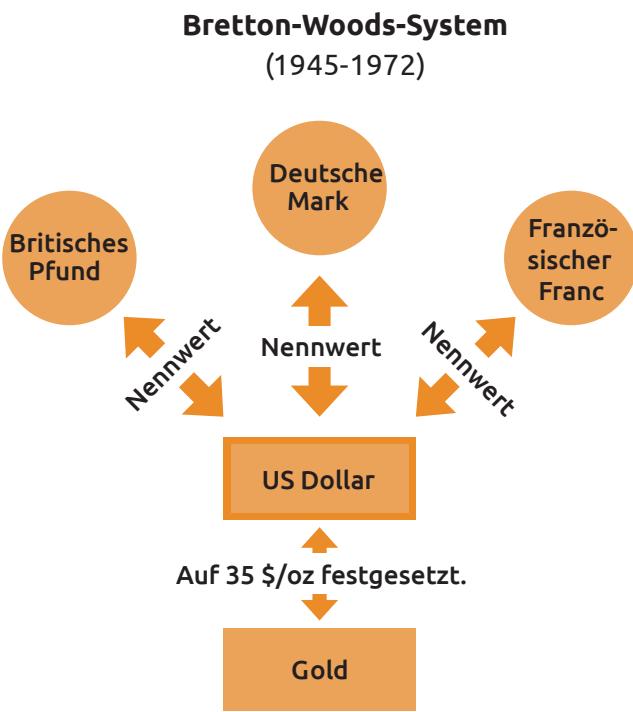


Euch ist klar, dass dies eine große Veränderung in der Funktionsweise des Geldes bedeutet. Ihr bewegt euch von einem System soliden Geldes (d. h. Geld, das durch Edelmetalle gedeckt ist) zu einem System unsoliden Geldes (d. h. Fiat-Währung, die nicht durch einen physischen Rohstoff gedeckt ist). Dieser Übergang geschah nicht über Nacht, sondern war ein allmählicher Prozess, der von mehreren Faktoren beeinflusst wurde. Die industrielle Revolution mit ihrer Massenproduktion und Verstädterung spielte eine Rolle, ebenso wie das Wachstum fortschrittlicher Finanzsysteme wie Banken und Aktienmärkte. Die Entstehung von Zentralbanken und anderen Währungsbehörden trug zur Zentralisierung oder Kontrolle des Geldes bei und führte zur Emission von Fiat-Währungen zur Unterstützung des Wirtschaftswachstums.



Ihr seht aber auch die **Schattenseiten dieser Zentralisierung**: unverantwortlicher Konsum, steigende Schulden und Manipulation der Bürger durch wirtschaftliche Anreize.

Bis zum Ersten Weltkrieg konnte man sein Papiergelede in eine festgelegte Menge Gold umtauschen. Doch die beiden Weltkriege und die Wirtschaftskrise von 1929 setzten dem ein Ende. 1944 wird das Bretton-Woods-Abkommen unterzeichnet, das den US-Dollar als Weltreservewährung festlegt und den Wert des US-Dollars an den Goldpreis von 35 Dollar pro Unze bindet. Die Währungen der anderen Länder werden an den Dollar gekoppelt, was zur Stabilisierung der internationalen Finanzmärkte beiträgt.



Leider beginnt das System Ende der 1960er Jahre zusammenzubrechen, was 1971 zum Nixon-Schock führt, als die US-Regierung die Konvertierbarkeit des Dollars in Gold aufhebt. Dies markiert das Ende des Goldstandards und den Beginn einer Welt, die von der Schaffung und Anhäufung von Schulden bestimmt wird.

Im Laufe des täglichen Lebens werdet ihr feststellen, dass der Wert des Geldes nicht mehr so stabil ist wie früher. So wie ein biegbares Lineal es schwierig macht, die Länge eines Tisches genau zu messen, kann das Leben in einer Fiat-Welt, in der der Wert des Geldes der Unberechenbarkeit der Machthaber unterliegt, es auch schwierig machen, den Wert von Waren und Dienstleistungen genau zu messen. Ihr empfindet Verwirrung und Unbehagen bei der Anpassung an eine Welt, in der der Wert des Geldes nicht mehr an ein physisches Gut wie Gold gebunden ist.

Vom Tauschhandel bis Bitcoin und CBDCs: Eine Reise durch die Zeit

Ihr seht die Auswirkungen dieses Wandels auf die Weltwirtschaft und beginnt, die Stabilität und Zuverlässigkeit von Fiat-Währungen in Frage zu stellen. Ihr erkennt, dass der Dollar in dieser modernen Welt nicht mehr unveränderlich und beständig ist, wie er es war, als er an Gold gebunden war, sondern stattdessen Schwankungen unterworfen ist. Dies erschwert die Verwendung des Dollars als Rechengröße, da sein Wert durch verschiedene Faktoren wie Inflation (steigende Preise), Zinssätze, die Stärke der Wirtschaft eines Landes, politische Ereignisse, Marktspekulationen und die Nachfrage im internationalen Handel beeinflusst wird. Es kann eine verwirrende und unvorhersehbare Zeit sein, in der ihr versucht, euch mit dem ständig wechselnden Wert des Dollars und seinen Auswirkungen auf euer tägliches Leben zurechtzufinden.

Trotz der Bemühungen, die Lebensqualität durch moderne Geldsysteme, höhere Effizienz, besseren Zugang zu Informationen und verbesserte Kommunikation zu verbessern, beginnt der Lebensstandard der meisten Menschen zu sinken:

- ① Missbrauch der Zentralisierung.
- ① steigende Preise.
- ① stagnierende Reallöhne.
- ① schwächelnde Währungen.
- ① die Notwendigkeit, mehr Geld für weniger Dinge auszugeben.

Dies ist eine Herausforderung für Menschen mit geringeren wirtschaftlichen Ressourcen, die möglicherweise nur begrenzten Zugang zu Bildung, Krediten, Ressourcen, sozialen Netzwerken und politischer Vertretung haben, was zu potenziellen Nachteilen bei ihren Erfolgsaussichten führt.

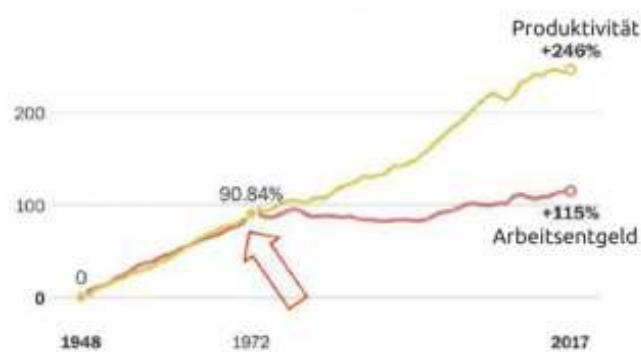
Dadurch scheinen die Reichen immer reicher und die Armen immer ärmer zu werden.



„Ich glaube nicht, dass wir jemals wieder gutes Geld haben werden, solange wir die Sache nicht aus den Händen der Regierung nehmen... alles, was wir tun können, ist, auf irgendeine schlaue, umständliche Weise etwas einzuführen, das sie nicht aufhalten können.“

Friedrich Hayek,
Nobelpreisträger für Wirtschaft

Wachstum von Produktivität und
Stundenlöhnen (1948-2017)



ANMERKUNG: Das Arbeitsentgelt umfasst Löhne und Sozialleistungen für Produktionsarbeiter und andere Arbeitnehmer.

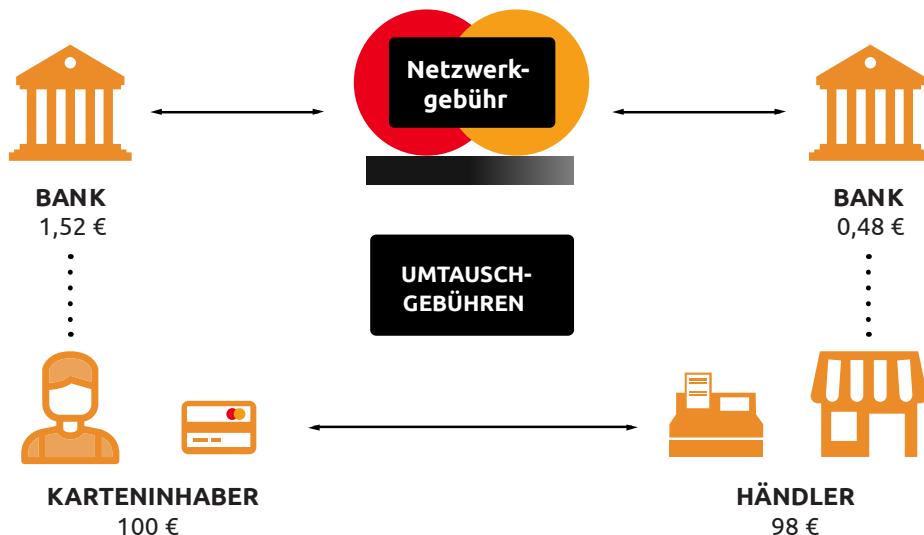




2.4 Wo stehen wir heute?

Seit der Einführung der ersten Kreditkarte in den 1950er Jahren haben wir bis heute einen langen Weg zurückgelegt. Mit den Plastikkarten können wir kaufen, was immer wir wollen, wann immer wir wollen, ohne jede Mühe. Es ist, als würde sich eine Welt mit unendlichen Möglichkeiten eröffnen, und die Vorfreude darauf, zu entdecken, was sie zu bieten hat, ist spürbar ... so dachten wir zumindest. Wir wussten nicht, dass unsere Abhängigkeit von Krediten schmerzhafte Folgen haben würde – wie die Erhöhung der Gesamtkosten von Waren und die Förderung einer bestimmten Wirtschaft, die zum Scheitern verurteilt ist.

Mit dem technologischen Fortschritt schreitet auch die Art und Weise, wie wir mit Geld umgehen, voran. Das Internet wird zu einem wichtigen Akteur in der Finanzwelt. Online-Banking und E-Commerce-Webseiten machen es möglich, Geld vollständig online zu verwalten und auszugeben.



Im Jahr 2009 wird dann die erste dezentrale Kryptowährung, *Bitcoin*, geschaffen. Dessen wachsende Popularität inspiriert die Entwicklung neuer Technologien und unbekannter Grenzen für die Zukunft des Geldes. Und so schließt sich, wie wir lernen werden, der Kreis vom soliden zum unsoliden Geld und wieder zurück, wobei solides Geld zum ersten Mal seit fast hundert Jahren neuen Wind in seine Segel bekommt.

2.5 Der Preis der Kontrolle: Ein Blick auf Überwachung, Zensur und Regulierung

2.5.1 Der Aufstieg einer bargeldlosen Gesellschaft

Als in den 1950er Jahren die erste Kreditkarte eingeführt wurde, freuten sich die Menschen über den Gedanken, nie wieder Bargeld bei sich tragen zu müssen – nie wieder umständliches Suchen nach Kleingeld oder Ausfüllen von Schecks an der Kasse. All die lästigen Mittelsmänner können nun ihren Anteil kassieren, ohne dass man es merkt, genau wie bei einer Maut in einem Netzwerk. Ah, die Bequemlichkeit der modernen Finanzwelt.

Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

Aber mit dem Aufkommen digitaler Währungen wie CBDCs ist es so, als ob wir nicht mehr eine Gebühr für die Nutzung des Netzwerks zahlen, sondern um Erlaubnis bitten müssen. Schlimmer noch, jetzt erwarten wir, dass wir bei jeder Nutzung von der Regierung durchsucht, gescannt und geprüft werden. Kontrolle und Überwachung sind an die Stelle der Bequemlichkeit getreten. Und genau wie die Gebühren für die Nutzung des Netzwerks haben auch diese Eingriffe in unser Finanzleben ihren Preis, sei es in Form von Geld, einer Verletzung der Privatsphäre oder dem Verlust der Autonomie.

Da immer mehr unserer täglichen Transaktionen online abgewickelt werden, nimmt die Verwendung von Bargeld ab. Regierungen und Finanzinstitute auf der ganzen Welt fördern den elektronischen Zahlungsverkehr und gehen gegen die Verwendung von Bargeld vor. Dieser Trend hat eine Debatte über die Zukunft des Bargelds und die möglichen Folgen einer bargeldlosen Gesellschaft ausgelöst.

Der Krieg gegen das Bargeld ist ein Begriff, der sich auf die verschiedenen Bemühungen bezieht, die Verwendung von physischem Geld zu reduzieren, Scheine mit hohem Nennwert abzuschaffen und die Verwendung von elektronischen Zahlungen zu fördern.

Die Befürworter der Bargeldabschaffung argumentieren, dass Transaktionen dadurch schneller, bequemer und sicherer werden. Kritiker befürchten jedoch, dass dies zu einem Verlust der Privatsphäre und der finanziellen Inklusion sowie zu einem erhöhten Risiko von Betrug und Cyberangriffen führen könnte.



Frage: Wie gefährden herkömmliche Bankmethoden die Finanzdaten von Einzelpersonen?

Antwort: Mit Kreditkarten, Debitkarten, Überweisungen und anderen zentral gesteuerten Zahlungsnetzwerken geben Einzelpersonen ihre privaten Finanztransaktionsdaten an Dritte weiter und opfern damit möglicherweise ihr Recht auf Privatsphäre.

In dieser Infografik geben wir einen Überblick über den Krieg gegen das Bargeld und beleuchten alle Seiten der Debatte. Wir beleuchten die Gründe für den Vorstoß in eine bargeldlose Gesellschaft, die damit verbundenen Herausforderungen und Bedenken, sowie die potenziellen Auswirkungen auf Einzelpersonen, Unternehmen und die Gesellschaft als Ganzes.



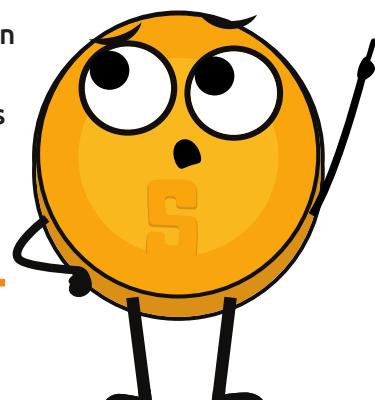
Die Frage ist, ob wir bereit sind, den Preis für die Annehmlichkeiten des modernen Finanzwesens zu zahlen, oder ob wir nach alternativen Möglichkeiten suchen, die unsere Freiheit und Privatsphäre in den Vordergrund stellen.



Der globale Krieg gegen Bargeld

Die Gesetzgeber versuchen weltweit, die Verwendung von Bargeld zu unterbinden. Diese Bewegung wird oft als „*Krieg gegen das Bargeld*“ bezeichnet, und es sind drei Hauptakteure beteiligt:

- Die Initiatoren
- Die Feinde
- Die Opfer des Kreuzfeuers



Desjardins, Jeff. „The Global War on Cash.“ Visual Capitalist, 27. Januar 2017, <https://www.visualcapitalist.com/global-war-cash/>.



WER?

Regierungen, Zentralbanken

WARUM? Die Abschaffung des Bargelds wird es einfacher machen, alle Arten von Transaktionen zu verfolgen, auch die von Kriminellen.

WER?

Kriminelle, Terroristen

WARUM? Banknoten mit großem Nennwert erleichtern die Durchführung illegaler Transaktionen und erhöhen die Anonymität.

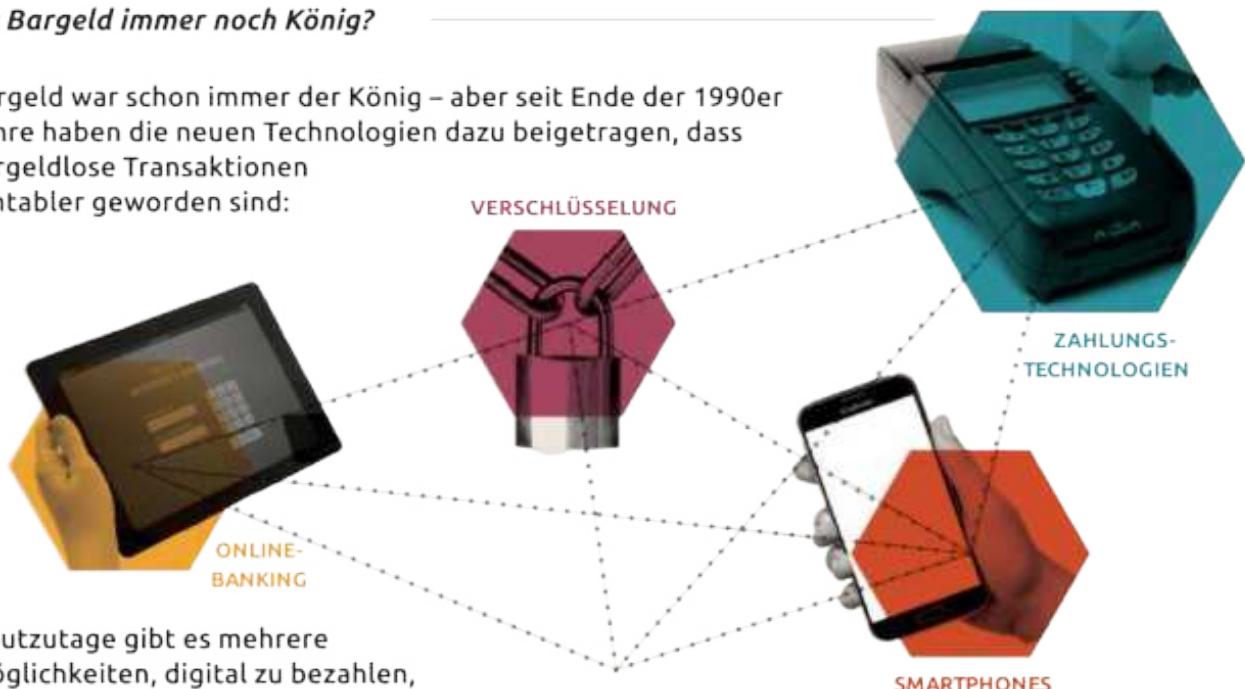
WER?

Die Bürger

WARUM? Die zwangsweise Abschaffung des physischen Bargelds wird sich möglicherweise auf die Wirtschaft und die sozialen Freiheiten auswirken.

Ist Bargeld immer noch König?

Bargeld war schon immer der König – aber seit Ende der 1990er Jahre haben die neuen Technologien dazu beigetragen, dass bargeldlose Transaktionen rentabler geworden sind:



Heutzutage gibt es mehrere Möglichkeiten, digital zu bezahlen, unter anderem:



INTERMEDIÄRE



ONLINE-BANKING

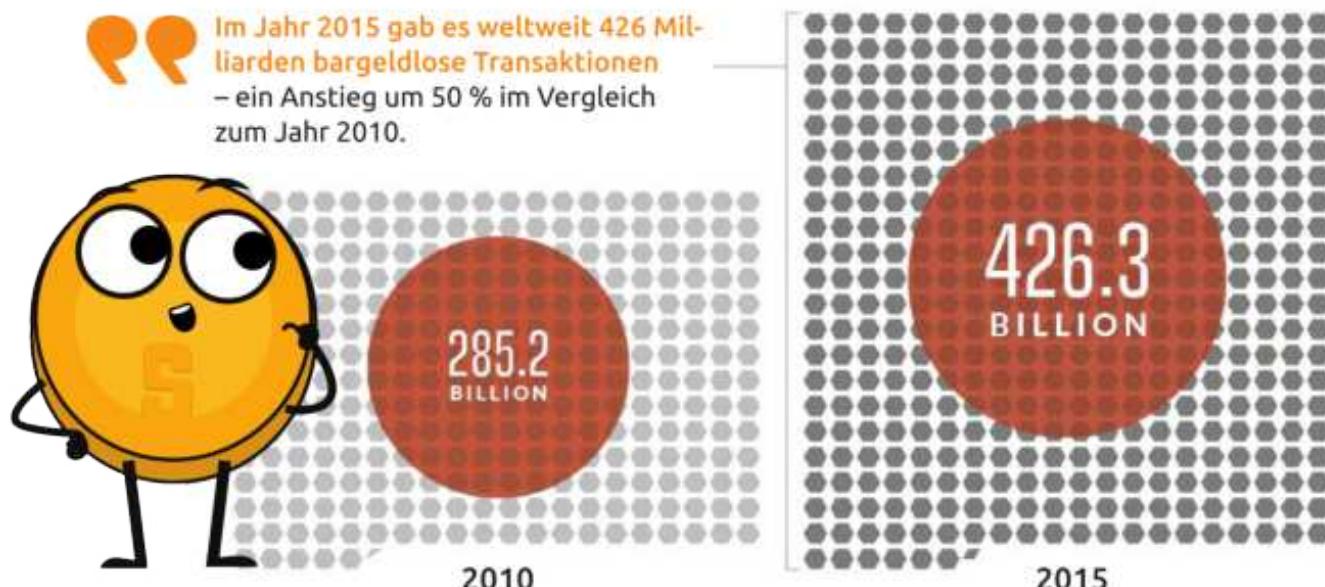


SMARTPHONES



KRYPTOWÄHRUNG

Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit



Die ersten Schüsse sind gefallen

Der Erfolg dieser neuen Technologien hat die Gesetzgeber zu der Forderung veranlasst, dass alle Transaktionen jetzt digital erfolgen sollten. Hier sind ihre Argumente für eine bargeldlose Gesellschaft:

Wenn Banknoten mit hohen Nennwerten aus dem Verkehr gezogen werden, wird es schwieriger für Terroristen, Drogenhändler, Geldwäscher und Steuerhinterzieher.

1 Eine Million US-Dollar in 100-Dollar-Scheinen wiegen nur zehn Kilogramm.

2 Kriminelle bewegen jedes Jahr zwei Billionen US-Dollar auf der ganzen Welt.

3 Der 100-Dollar-Schein der USA ist die beliebteste Banknote der Welt, von der zehn Milliarden Exemplare im Umlauf sind.

Rückverfolgbares Geld bedeutet höhere Steuereinnahmen. Das bedeutet auch, dass bei allen Transaktionen ein Dritter beteiligt ist.

Die Zentralbanken können Zinssätze diktieren, die Ausgaben fördern (oder hemmen), um die Inflation in den Griff zu bekommen. Dies schließt die Null- oder Negativzinspolitik (ZIRP oder NIRP) ein.

2 Dadurch erhalten die Regulierungsbehörden mehr Kontrolle über die Wirtschaft.

Bargeldlose Transaktionen sind schneller und effizienter.

3 Den Banken würden weniger Kosten entstehen, da sie nicht mit Bargeld umgehen müssten.

✓ Auch die Einhaltung von Vorschriften und die Berichterstattung werden dadurch erleichtert.

Einigen Experten zufolge kann die „Last“ des Bargelds bis zu 1,5 % des BIP betragen.



Kapitel 2

Damit dies möglich ist, muss Bargeld, insbesondere große Scheine, abgeschafft werden.



Letzten Endes werden weltweit immer noch etwa 85 % aller Transaktionen mit Bargeld abgewickelt.

Im Kreuzfeuer gefangen

Die Schüsse, die die Regierungen im Kampf gegen das Bargeld abfeuern, können mehrere ungewollte Opfer fordern.



Privatsphäre

- ▶ Bargeldlose Transaktionen würden immer einen Vermittler oder eine dritte Partei einbeziehen.
- ▶ Verstärkter Zugriff der Behörden auf persönliche Transaktionen und Aufzeichnungen.
- ▶ Bestimmte Arten von Transaktionen (Glücksspiele usw.) könnten von den Regierungen verboten oder eingefroren werden.
- ▶ Dezentrale Kryptowährungen könnten eine Alternative für solche Transaktionen sein.

Ersparnisse

Die Sparer hätten nicht mehr die individuelle Freiheit, Vermögen „außerhalb“ des Systems zu lagern.



Die Abschaffung des Bargelds macht negative Zinssätze (NIRP) alle Sparer für Bankenrettungsszenarien „am Haken“ wären.

Eine bargeldlose Gesellschaft würde auch bedeuten, dass alle Sparer für Bankenrettungsszenarien „am Haken“ wären.

Die Sparer hätten nur begrenzte Möglichkeiten, auf extreme monetäre Ereignisse wie Deflation oder Inflation zu reagieren.



Menschenrechte

- ▶ Die rasche Demonetisierung hat das Recht der Menschen auf Leben und Nahrung verletzt.
- ▶ In Indien hat die Abschaffung der 500- und 1000-Rupien-Scheine zu zahlreichen menschlichen Tragödien geführt, darunter die Verweigerung der Behandlung von Patienten und die Unmöglichkeit, sich Lebensmittel zu leisten.
- ▶ Die Demonetisierung schadet auch den Menschen und kleinen Unternehmen, die ihren Lebensunterhalt im informellen Sektor der Wirtschaft verdienen.

Cybersicherheit

Mit der digitalen Speicherung von Vermögenswerten steigen das potenzielle Risiko und die Auswirkungen von Internetkriminalität. Hackerangriffe oder Identitätsdiebstahl könnten die Ersparnisse der Menschen vernichten.



Laut Juniper Research betragen die Kosten von Datenschutzverletzungen im Internet im Jahr 2019 2,1 Billionen US-Dollar.



Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

2.5.2 Überwachung

Überwachung ist eine heikle Angelegenheit. Einerseits hilft sie, Menschen zu erwischen, die schlimme Dinge tun, wie zum Beispiel Geldwäsche. Aber je mehr Betrug geschieht, desto mehr Überwachung ist nötig, was zu Eingriffen in die Privatsphäre durch die Technologie führen kann. Privatunternehmen können deine persönlichen Daten auch zu ihrem eigenen Vorteil sammeln und weitergeben, und die Risiken dieser Überwachung können Betrug, Belästigung, Erpressung, Identitätsdiebstahl und sogar die Nachverfolgung deiner Kartenkäufe umfassen. Mit dem Aufkommen von KI und maschinellem Lernen wird es für Regierungen und Unternehmen sogar noch einfacher, in unsere Privatsphäre einzudringen. Außerdem sind es oft die ohnehin schon benachteiligten oder unterprivilegierten Menschen, die am stärksten betroffen sind.

Die Auswirkungen von KI und Technologie auf den Datenschutz und die Überwachung der Zukunft

Zukünftiger Effekt	Die Reichen	Die Armen
Zugang zu persönlichen Daten.	Sie haben möglicherweise Zugang zu umfangreichen persönlichen Informationen und können diese nutzen, um fundierte Entscheidungen zu treffen.	Möglicherweise fehlen diese Informationen und sie müssen sich auf veraltete oder unzuverlässige Quellen verlassen.
Die Fähigkeit, die Welt in ihrem eigenen Interesse zu gestalten.	Sie können ihren Zugang zu Daten nutzen, um die Welt in ihrem eigenen Interesse zu gestalten.	Sie haben möglicherweise wenig Einfluss auf das Geschehen.
Kontrolle über andere.	Sie können durch ihren Zugang zu Daten Kontrolle über die Armen ausüben, was zu einem Verlust der individuellen Freiheit führt.	Wenig Kontrolle; sie werden oft kontrolliert.
Anfälligkeit für digitalen Betrug, Online-Belästigung, Erpressung und Identitätsdiebstahl.	Mit mehr Informationen und mehr Schutz vor solchen Beträgereien sind sie wahrscheinlich weniger anfällig für diese Probleme.	Sie sind möglicherweise anfälliger für diese Probleme, weil sie keinen Zugang zu Ressourcen und Informationen haben.

2.5.3 Finanzielle Regulierungen und Zensur

Finanzielle Regulierungen, Zensur und Verbote können für die Gesellschaft und ihre Bürger eine emotional und finanziell belastende Realität sein. Es gibt sie in vielen Formen, wie zum Beispiel:

- Kapitalverkehrskontrollen oder Sanktionen:** Wenn die Ausgaben außer Kontrolle geraten, können Regierungen Preiskontrollen einführen, um das Problem zu lösen. Aber manchmal machen diese Kontrollen die Dinge noch schlimmer. Regierungen können auch einschränken, wie viel Geld die Bürger überweisen, umtauschen oder außer Landes bringen können, sowie ein Sozialkreditsystem schaffen, das zur Kontrolle der Bürger verwendet werden kann.



- Wie funktioniert das chinesische System der Sozialkreditpunkte? In China werden Finanztransaktionen und andere Daten aller Bürger zentral erfasst und zur Erstellung eines Sozialkreditsystems verwendet, das zur Kontrolle der Bürger eingesetzt werden kann.

- Denk daran, was 2015 in Griechenland geschah:

Die Bürger konnten auf Anweisung der Regierung nur 60 Euro pro Tag abheben. In ähnlicher Weise können die Chinesen nur begrenzte Mengen an Renminbi aus dem Land schicken.

- In Argentinien hat es mehrere Fälle gegeben, in denen die Regierung strenge Devisenkontrollen eingeführt hat, um den Peso zu stabilisieren. Einer dieser Fälle war 2011, als die Regierung Kapitalkontrollen einführte, um den Abfluss von US-Dollar aus dem Land einzudämmen und eine weitere Abwertung des Pesos zu verhindern. Ein weiterer Fall war 2019.

- **Restriktive Bankrichtlinien:** Hast du schon einmal versucht, an einem Geldautomaten Bargeld abzuheben, um dann festzustellen, dass du dein Tageslimit erreicht hast?

Oder vielleicht hast du schon einmal versucht, einem Freund Geld zu überweisen, und es wurde dir gesagt, dass du nur einen bestimmten Höchstbetrag überweisen kannst. Dies sind nur einige Beispiele für restriktive Bankrichtlinien, die es schwierig machen, über dein eigenes Geld zu verfügen und damit zu tun, was du willst.

Außerdem können Banken für die meisten Transaktionen Gebühren erheben und nur zu bestimmten Zeiten geöffnet sein, was es schwierig macht, an dein Bargeld heranzukommen oder finanzielle Entscheidungen zu treffen. Wer viel Bargeld mit sich herumträgt, erhöht sein Risiko, ausgeraubt zu werden. Hinzu kommt, dass Banken den Wohlhabenden manchmal zinsgünstige Kredite anbieten, während sie die Armen an Kredithäie verfüttern und ihnen höher verzinsten Kredite anbieten. Auf diese Weise profitiert das Finanzsystem häufig von der Kluft zwischen Arm und Reich.



Schau dir den folgenden Artikel an:
„Was man über Geldtransporte nach und aus China wissen muss“.

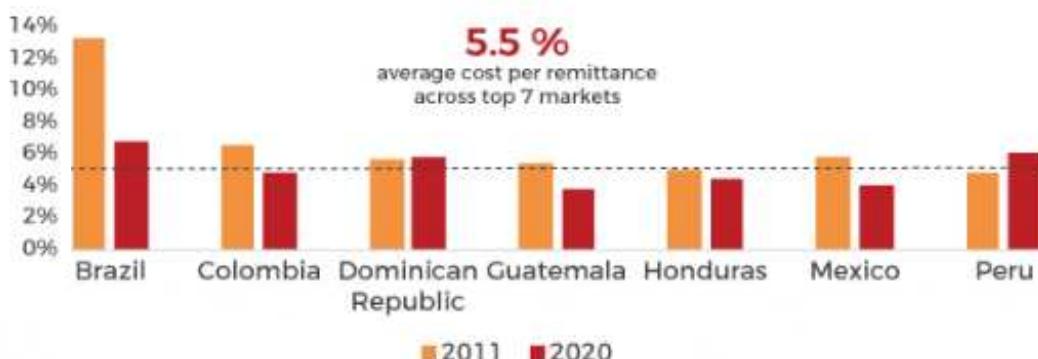
[https://nhglobalpartners.com/
moving-money-in-and-out-china-rules](https://nhglobalpartners.com/moving-money-in-and-out-china-rules)



Vom Tauschhandel zu Bitcoin und CBDCs: Eine Reise durch die Zeit

- **Teure Überweisungen:** Das Senden von Geld in andere Länder kann aufgrund der Gebühren von Banken und anderen Finanzinstituten teuer sein. Viele einkommensschwache Familien in Entwicklungsländern sind auf das Geld von im Ausland lebenden Verwandten angewiesen, um über die Runden zu kommen. Hohe Gebühren für internationale Geldtransfers können jedoch den Betrag, den der Empfänger tatsächlich erhält, schmälern. Dies kann es Familien erschweren, sich die Grundbedürfnisse wie Nahrung, Wohnung und Bildung zu leisten.

Durchschnittliche Überweisungsgebühren in Lateinamerika
(% der Transaktion)



- Stell dir eine Familie in einem ländlichen Dorf in Brasilien vor, die auf das Geld eines Verwandten angewiesen ist, der in den USA arbeitet. Wenn der Verwandte 100 US-Dollar schickt, aber die Bank eine Gebühr von sieben Dollar für die Überweisung erhebt, erhält die Familie nur 93 Dollar. Das mag nicht viel erscheinen, aber für eine Familie, die mit einem knappen Budget lebt, können sieben Dollar einen großen Unterschied ausmachen.

- **Die Banklosen und jene mit mangelhaftem Zugang zu Banken:** Leider haben nicht alle Menschen Zugang zu traditionellen Bankdienstleistungen, sei es, weil sie die Voraussetzungen für die Eröffnung eines Kontos nicht erfüllen oder weil sie in Gebieten leben, in denen Bankdienstleistungen nicht verfügbar sind. Dies kann den Menschen den Zugang zu Finanzdienstleistungen und die Teilnahme an der globalen Wirtschaft erschweren.



45%
der Haushalte, die keine Bankverbindung haben, besitzen Kryptowährungen, verglichen mit

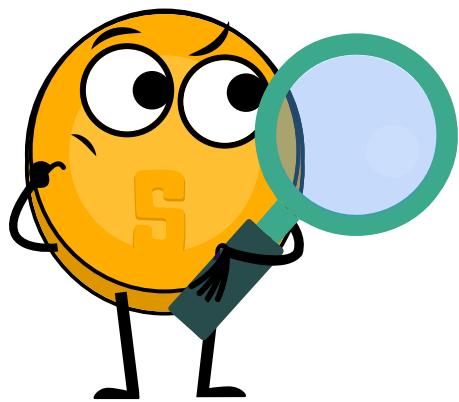


19%
der Allgemeinbevölkerung.

- Aber halt, das ist noch nicht alles! Regierungen können auch den Wechselkurs ihrer Währung kontrollieren, was den Geldumtausch zwischen Ländern erschweren oder zu **ungünstigen Wechselkursen** führen kann. Finanzinstitute können **Spenden** an bestimmte Organisationen oder Personen **sperren** oder dein Bankkonto ganz auflösen. Soziale Medienplattformen und Finanzinstitute können bestimmte Inhalte entfernen, wenn sie der Meinung sind, dass diese Fehlinformationen verbreiten oder gegen ihre Gemeinschaftsstandards oder -richtlinien verstößen. Dies wird manchmal als Zensur bezeichnet und kann eine breite Palette von Maßnahmen umfassen, wie z. B. das Sperren oder Unterdrücken von Inhalten, die Einschränkung des Zugangs oder die vollständige Entfernung von Informationen.



Kapitel 2



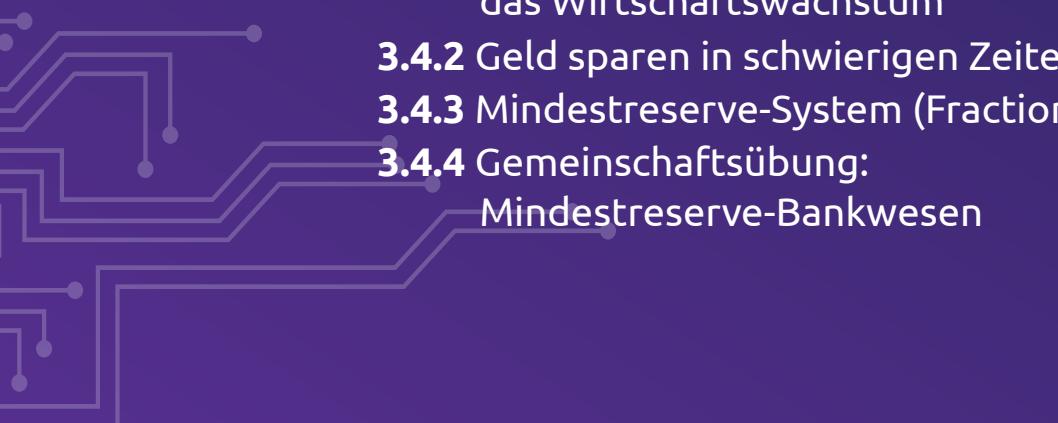
Überwachung, Kontrolle und versteckte Gebühren sind nur die politischen Schattenseiten des derzeitigen Systems, in dem wir leben. Leider gibt es auch eine Reihe von versteckten wirtschaftlichen Kosten, von denen wir oft nichts erfahren.



Kapitel 3

Die dunkle Seite von Fiat

- 3.0 Gemeinschaftsübung: Die Auswirkungen der Inflation:
Eine Auktionsübung**
- 3.1 Die größten Bedrohungen für dein Geld: Inflation,
Entwertung und Kaufkraftverlust**
- 3.2 Schulden: Der schmale Grat zwischen Hilfe und Schaden**
- 3.3 Die Fed und ihre Partner: Wie Regierung und Banken
die Geldmenge kontrollieren**
- 3.4 Die Magie der Geldschöpfung**
 - 3.4.1 Der Zeitwert des Geldes und seine Rolle für
das Wirtschaftswachstum**
 - 3.4.2 Geld sparen in schwierigen Zeiten**
 - 3.4.3 Mindestreserve-System (Fractional Reserve)**
 - 3.4.4 Gemeinschaftsübung:
Mindestreserve-Bankwesen**



Die dunkle Seite von Fiat

3.0 Gemeinschaftsübung: Die Auswirkungen der Inflation: Eine Auktionsübung

Ziel: Das Konzept der **Geldmenge** verstehen und wissen, wie sie die Preise von Waren und Dienstleistungen in einer Volkswirtschaft beeinflusst.

Definitionen:

- Die **Geldmenge** ist der Gesamtbetrag des Geldes, der zu einem bestimmten Zeitpunkt in einer Volkswirtschaft im Umlauf ist. Dies umfasst:
 - Physisches Geld, wie Münzen und Scheine.
 - Elektronisches Geld auf Bankkonten.
 - Die Geldmenge ist ein wichtiges Konzept in den Wirtschaftswissenschaften, da sie den allgemeinen Zustand einer Wirtschaft beeinflussen kann.
- Eine **Auktion** ist ein öffentlicher Verkauf, bei dem Waren oder Eigentum an den Meistbietenden verkauft werden.

Gemeinschaftsübung: Befolgt die folgenden Anweisungen!

1. Ihr erhaltet von der Lehrkraft einen zufälligen Betrag an Monopoly-Geld. Dies stellt die Geldmenge in einer Gesellschaft dar.

2. Tragt die gesamte Geldmenge in die vorgesehene Tabelle ein!

3. Die Lehrkraft versteigert einen Schokoriegel an die Studenten. Um den Schokoriegel zu gewinnen, müsst ihr mit eurem Monopoly-Geld das höchste Gebot abgeben. Notiert das Höchstgebot neben dem Geldvorrat!

4. Die Lehrkraft fügt dann der gesamten Geldmenge einen erheblichen Betrag an Monopoly-Geld hinzu. Dies stellt eine Erhöhung der Geldmenge in einer Volkswirtschaft dar. Später werdet ihr lernen, wie die Geldmenge in einer Volkswirtschaft erhöht oder verringert wird.

5. Die Lehrkraft versteigert einen zweiten Schokoriegel nach demselben Verfahren wie zuvor. Notiert das Gebot, das den Zuschlag erhalten hat, neben dem Geldangebot auf der Tabelle!

6. Die Lehrkraft wird die Auktion ein drittes Mal wiederholen.



Gesellschaften können oft unvorhersehbar und ungerecht sein, wie die Simulation der Lehrkraft zeigt, die nach dem Zufallsprinzip einen beträchtlichen Geldbetrag an einige wenige Studenten verteilt. Dies entspricht Situationen aus dem wirklichen Leben, in denen es zu einer ungleichen Verteilung von Ressourcen und Chancen kommen kann, und verdeutlicht die inhärente Zufälligkeit und Ungerechtigkeit in vielen Situationen.





Kapitel 3

Runde	Geldmenge	Höchstes Gebot

Fragen: Beantwortet die folgenden Fragen auf der Grundlage dessen, was ihr in der Übung gelernt habt!

1. Wie hat sich der Anstieg der Geldmenge auf die Gebote für die Schokoriegel ausgewirkt?

2. Welche Beziehung besteht zwischen der Geldmenge und der Inflation?

3. Welche Bedeutung hat die Geldmenge in der realen Welt?

4. Fallen euch weitere Faktoren ein, die die Preise von Waren und Dienstleistungen beeinflussen können?

Die dunkle Seite von Fiat

3.1 Die größten Bedrohungen für dein Geld: Inflation, Entwertung und Kaufkraftverlust

Das derzeitige globale Wirtschaftsklima ist eine Herausforderung, die das Sparen erschweren kann. Ein Faktor, der dazu beiträgt, ist die Inflation, ein Phänomen, das auftritt, wenn der Wert des Geldes mit der Zeit abnimmt. Selbst wenn man jetzt mehr Geld spart, kann es sein, dass es in der Zukunft nicht mehr die gleiche Kaufkraft hat, was bedeutet, dass man mit mehr Geld weniger kaufen kann. Wenn man die wirtschaftlichen Bedingungen und ihre Auswirkungen auf seine persönlichen Finanzen kennt, kann man fundierte Entscheidungen über Sparen und Ausgaben treffen.



Die Kaufkraft ist die Menge an Waren oder Dienstleistungen, die man mit einem bestimmten Geldbetrag kaufen kann.

Beginnen wir mit einem realistischen Szenario, um jeden Begriff zu erklären.

René ist ein Student, der in einer kleinen Wohnung lebt. Er arbeitet Teilzeit in einem Café, um seinen Lebensunterhalt und seine Studiengebühren zu bestreiten. Seit er unabhängig lebt, ist René ein Profi im Führen seines eigenen **Kassenbuchs**.

Zu Beginn des Jahres hatte er 10.000 Euro für seinen Lebensunterhalt eingeplant, einschließlich Miete, Lebensmittel und andere notwendige Dinge.



1956



2020



2056



Inflation ist ein Anstieg des allgemeinen Preisniveaus für Waren und Dienstleistungen in einer Volkswirtschaft über einen bestimmten Zeitraum hinweg. Wenn das allgemeine Preisniveau steigt, kann man mit jeder Währungseinheit weniger Waren und Dienstleistungen kaufen. Folglich spiegelt die Inflation einen Rückgang der Kaufkraft des Geldes wieder – einen Verlust des realen Wertes des Zahlungsmittels und der Recheneinheit in einer Volkswirtschaft.



Ein Kassenbuch ist eine detaillierte Aufzeichnung all deiner Geldtransaktionen. Egal, ob du Geld verdienst oder ausgibst, ein Kassenbuch hilft dir, den Überblick zu behalten.



Kapitel 3

Dies waren seine Transaktionen im Januar:

Datum	Beschreibung	Betrag	Art	Saldo
01.01.2023	Startguthaben			1600,00 €
01.01.2023	Miete für Januar	800,00 €	Abbuchung	800,00 €
05.01.2023	Lebensmittel	100,00 €	Abbuchung	700,00 €
15.01.2023	Teilzeit-Gehaltsscheck	500,00 €	Gutschrift	1200,00 €
20.01.2023	Benzin für das Auto	50,00 €	Abbuchung	1150,00 €
30.01.2023	Lehrbücher	150,00 €	Abbuchung	1000,00 €

Aus diesem Kassenbuch geht hervor, dass René am 1. Januar ein Guthaben von 1600 € auf seinem Konto hatte, wovon er 800 € für die Miete des Monats ausgab. Dann gab er 100 € für Lebensmittel aus (Abbuchung) und erhielt 500 € (Gutschrift) von seinem Teilzeitjob, was sein Guthaben auf 1200 € erhöhte. Anschließend gab er Geld für Benzin und Lehrbücher aus, sodass sein Guthaben am Ende des Monats auf 1000 € sank.

Zwölf Monate später stellt René bei einem Mittagessen mit seinem Großvater fest, dass sein Budget nicht mehr so lange reicht wie früher. Er stellt fest, dass die Preise für die Waren und Dienstleistungen, die er benötigt, im letzten Jahr erheblich gestiegen sind, und fragt sich, warum. Dann sah er dieses Bild und konnte seinen Augen nicht trauen.

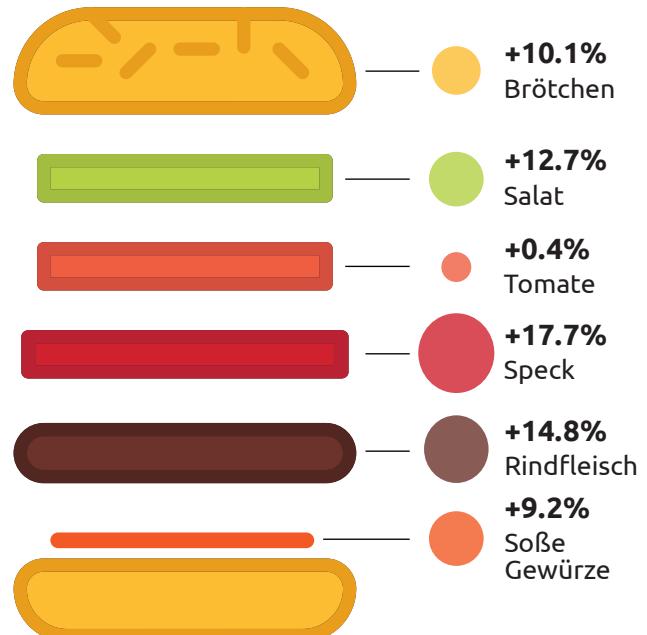
Als er seinen Großvater darauf ansprach, wurde ihm gesagt: „1956 war ich noch ein junger Mann, der in die Welt hinausging. Ich erinnere mich, dass ich als Fabrikarbeiter 100 Euro im Monat verdiente. Das mag nach heutigen Maßstäben nicht viel erscheinen, aber damals war es ein anständiger Lohn. Ich konnte sogar so viel Geld sparen, dass ich mir ein kleines Haus in der Vorstadt kaufen konnte.“

Wie wir sehen können, sind die Kosten für jeden Artikel im **Warenkorb** gestiegen, was zu einem Gesamtrückgang seiner Kaufkraft führt.

Zum Glück kann René mit einem Kassenbuch umgehen, denn es zeigt ihm deutlich, wie seine jährliche Kaufkraft gesunken ist.

Wie die Inflation den Preis eines Hamburgers veränderte

Preisveränderung ausgewählter Zutaten eines Hamburgers gegenüber dem Vorjahr (April 2021 - April 2022)



* Basierend auf Einzelhandelspreisen, städtische Verbraucher.

Die dunkle Seite von Fiat

René: „Was? Das ist doch verrückt. Ich kann mir nicht einmal vorstellen, was meine Miete damals gekostet hätte.“

Großvater: „Nun, lass mich mal sehen. Wenn wir die Inflation mit einbeziehen, hätte ich für 1 Euro etwa 10 Tüten Brezeln gekauft.“

René: „Wow, das ist wirklich interessant, Opa. Aber wie viel wäre das heute wert?“

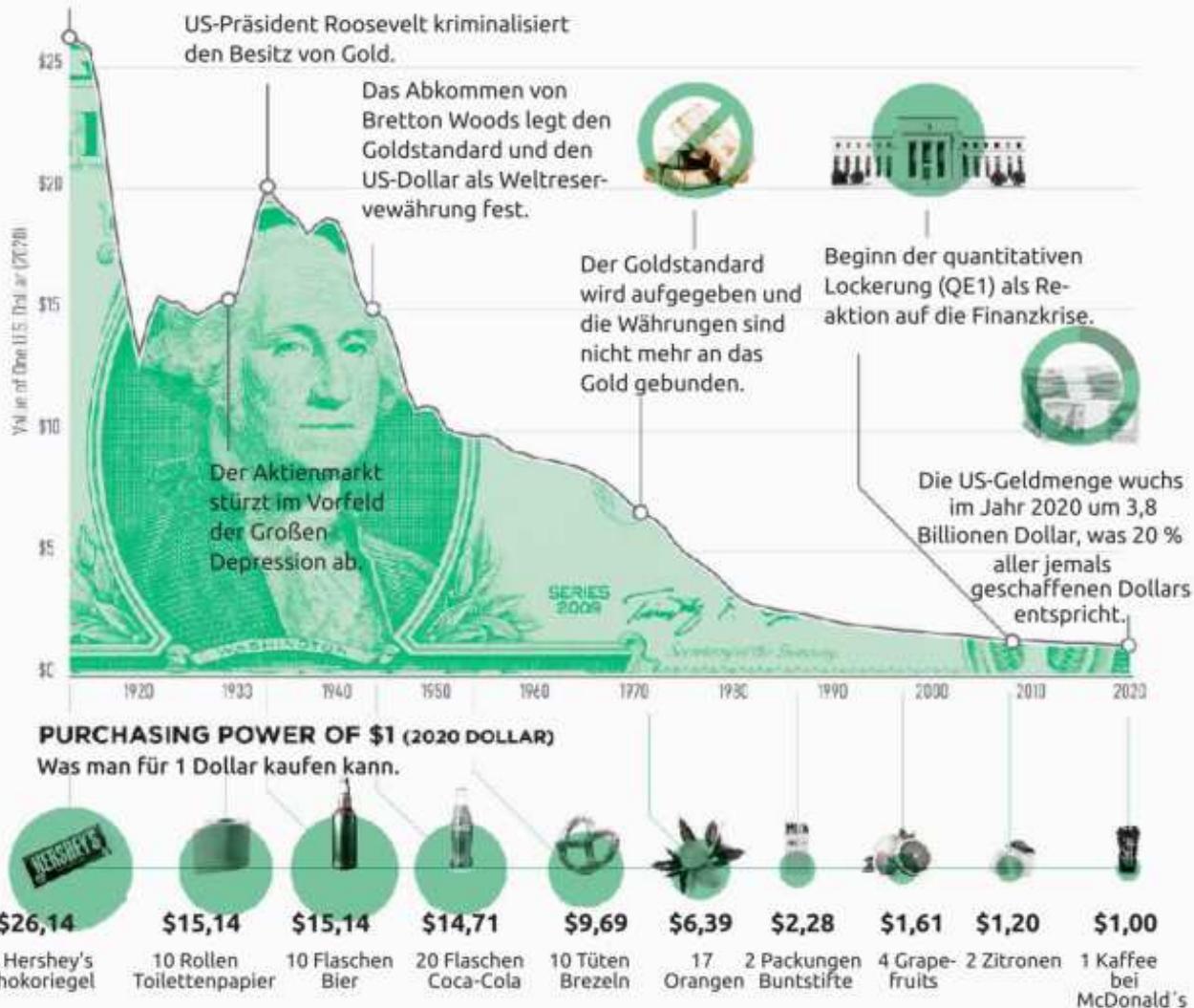
Großvater: „Oh, damals war alles viel billiger! Ein Laib Brot kostete nur ein paar Cent, und ein Liter Benzin konnte man für nicht mal 7 Cent kaufen. Es ist unglaublich, wie sehr die Lebenshaltungskosten gestiegen sind.“

Der Wert eines Dollars

Kaufkraft des US-Dollars

Die Kaufkraft des US-Dollars ist im Laufe des letzten Jahrhunderts aufgrund der steigenden Inflation und Geldmenge stark gesunken.

Mit dem Federal Reserve Act wird eine Zentralbank geschaffen, die in der Lage ist, die Geldmenge des Landes zu verwalten.





Kapitel 3

- René muss für denselben Warenkorb an Waren und Dienstleistungen, den er im Vorjahr gekauft hat, zusätzlich 1000 € einplanen.
 - Das bedeutet, dass sich seine Kaufkraft um 1000 € verringert hat, da er **nun mehr Geld ausgeben muss, um die gleichen Waren und Dienstleistungen zu kaufen.**
- Der Waren- und Dienstleistungskorb umfasst die Miete für seine Wohnung, Lebensmittel und andere notwendige Dinge.
- Die folgende Tabelle zeigt die Kosten für jeden Artikel im **Warenkorb** im ersten und im zweiten Jahr sowie die prozentuale Preissteigerung:

Artikel	Kosten 1. Jahr	Kosten 2. Jahr	Anstieg in %
Miete	4000 €	4500 €	12,5%
Lebensmittel	2000 €	2300 €	15%
andere Notwendigkeiten	4000 €	4200 €	5%
Gesamt	10000 €	11000 €	10%

René verdient in einem Jahr mehr, als sein Großvater je verdient hat, aber das schreckt auch vom Sparen ab. Es ist vorteilhafter, das Geld jetzt auszugeben, da sein Wert sinkt. Dies behindert die Fähigkeit, für die Zukunft zu planen. Wie in einer früheren Grafik (in Abschnitt 2.3) gezeigt, stagniert das jährliche Gehaltswachstum in den Vereinigten Staaten für den Durchschnittsbürger, was bedeutet, dass die meisten Menschen trotz härterer Arbeit keine Gehaltserhöhungen in gleichem Maße erhalten wie der Wert ihres Geldes sinkt.

Für René hätte es schlimmer kommen können. So erlebte Simbabwe in den späten 2000er Jahren eine Hyperinflation, als die Wirtschaft des Landes durch eine Kombination aus politischer Instabilität, wirtschaftlicher Misswirtschaft und externen Faktoren wie Dürre und Sanktionen in Mitleidenschaft gezogen wurde. Infolgedessen stürzte der Wert des simbabwischen Dollars (ZWD) ab und die Regierung war gezwungen, mehr Geld zu drucken.

- Der 100.000-ZWD-Schein wurde 2008 in Simbabwe eingeführt. Aufgrund der Hyperinflation war er damals nur ein paar US-Dollar wert.
- Trotz seines hohen Nennwerts reichte der 100.000-ZWD-Schein nicht aus, um Grundbedürfnisse wie Lebensmittel oder Kraftstoff zu kaufen, und die Menschen mussten große Bargeldbündel mit sich führen, um alltägliche Einkäufe zu tätigen.

Betrachtet man die erheblichen Preissteigerungen seit Mitte der 50er Jahre in den USA und das Beispiel der Hyperinflation in Simbabwe, so wird deutlich, dass die Auswirkungen der Inflation auf die Kaufkraft des Einzelnen je nach Standort und Zeitraum, in dem er gelebt hat, sehr unterschiedlich sein können.

Die Inflation trifft diejenigen, die in armen Ländern leben, in der Regel viel stärker als diejenigen, die in reichen Ländern leben. Dies unterstreicht die Tatsache, dass es oft reines Glück ist, wo und wann ein Mensch geboren wird, und

Was genau ist also Inflation?
Warum ist sie so gefährlich?
Steve Forbes schlüsselt es auf.



<https://youtu.be/syf-1nklmg>



Die dunkle Seite von Fiat

dass die Umstände der Geburt eines Menschen erhebliche Auswirkungen auf seine Lebensqualität und seine wirtschaftlichen Möglichkeiten haben können.

3.2 Schulden: Der schmale Grat zwischen Hilfe und Schaden

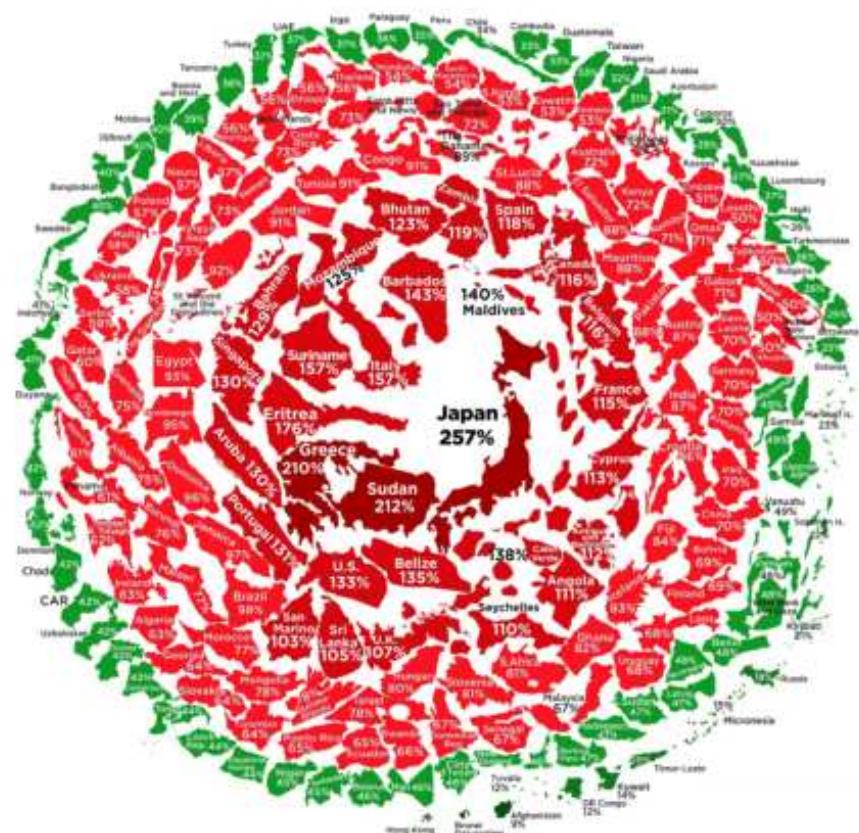
Verschuldung ist ein zweischneidiges Schwert. Es ist richtig, dass die Aufnahme von Krediten einen dringend benötigten finanziellen Impuls geben kann, sei es für Privatpersonen, die eine große Anschaffung tätigen, für Unternehmen, die in ihr Wachstum investieren, oder für Regierungen, die wichtige Dienstleistungen finanzieren. Aber eine zu hohe Kreditaufnahme kann zum finanziellen Ruin führen. Wenn man die Zinsen für seine Schulden nicht mehr bezahlen kann, wird es immer schwieriger, seine Rechnungen zu bezahlen und sich über Wasser zu halten. Dies gilt insbesondere dann, wenn ein Unternehmen weitere Schulden aufnimmt, um bestehende Schulden zu tilgen, und in einen Teufelskreis gerät, der als „Schuldenspirale“ bekannt ist.



Schulden sind Geldbeträge, die eine Person oder Organisation einer anderen schuldet. Wenn man Schulden hat, muss man das Geld, das man schuldet, in der Regel mit Zinsen, bis zu einem bestimmten Datum zurückzahlen.

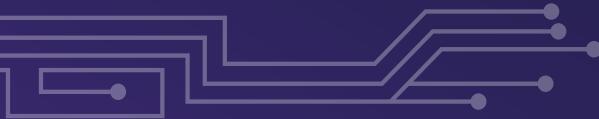
Die Schuldenkrise ist ein weltweites Problem, auch in den Vereinigten Staaten. Derzeit gibt die Regierung mehr Geld aus, als sie einnimmt. Um ihre Rechnungen zu bezahlen, nimmt sie immer mehr Geld auf. Dieser Kreislauf aus Schulden und höheren Kreditkosten kann jedoch bald die Kreditwürdigkeit der Regierung beeinträchtigen. Wenn die Schulden zu hoch werden, könnte die Regierung in finanzielle Schwierigkeiten geraten und möglicherweise bankrott gehen, so wie es viele andere Länder in der Vergangenheit getan haben.

Der Stand der weltweiten Staatsverschuldung



Verschuldung im Verhältnis zum BIP 2021 (%)





- Die von der Regierung aufgenommenen Schulden können langfristige Auswirkungen auf künftige Generationen haben.
- Mehr Geld zu drucken, um Ausgaben zu finanzieren, kann zu einer Abwertung der Währung und einem möglichen Zusammenbruch des Währungssystems führen.

Doch wie lässt sich das Risiko messen, dass ein Land zu viele Schulden aufnimmt? Eine Möglichkeit ist die **Schuldenquote**, die den Anteil der Gesamtverschuldung eines Landes am BIP angibt.

- Die **Schuldenquote** ist ein Indikator dafür, ob ein Land seine Schulden bezahlen kann.
 - Ist die Quote hoch, hat das Land möglicherweise Probleme, seine Schulden in Zukunft zu bezahlen.
 - Ist die Quote niedrig, kann das Land seine Schulden leicht zurückzahlen und ist in guter finanzieller Verfassung.
- Es ist wichtig, sich daran zu erinnern, dass das Verhältnis von Schulden zum BIP nur ein Teil des Verständnisses der finanziellen Situation eines Landes ist.



Das **Bruttoinlandsprodukt** (BIP) ist ein Maß für den Gesamtwert der in einem Land über einen bestimmten Zeitraum, in der Regel ein Jahr, produzierten Waren und Dienstleistungen. Es wird häufig als Maß für die Größe und Gesundheit einer Volkswirtschaft verwendet.

3.3 Die Fed und ihre Partner:

Wie Regierung und Banken die Geldmenge kontrollieren

Hast du schon einmal darüber nachgedacht, woher die Billionen von Dollar an Konjunkturfördermitteln stammen, die während der Pandemie verteilt wurden, und wer darüber entscheidet, wie viel und an wen sie verteilt werden? Die Zuteilung dieser Mittel hat große Auswirkungen auf die Gesellschaft und die Wirtschaft, bleibt aber oft weitgehend ungeprüft.

Es gibt mehrere Instrumente, die Zentralregierungen einsetzen können, um die **Geldmenge** zu einem bestimmten Zeitpunkt zu steuern.

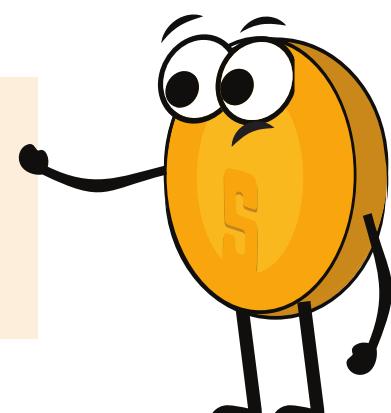
- Zentralbanken und Regierungen können geld- und fiskalpolitische Instrumente einsetzen, um die Geldmenge und die Wirtschaft zu beeinflussen.



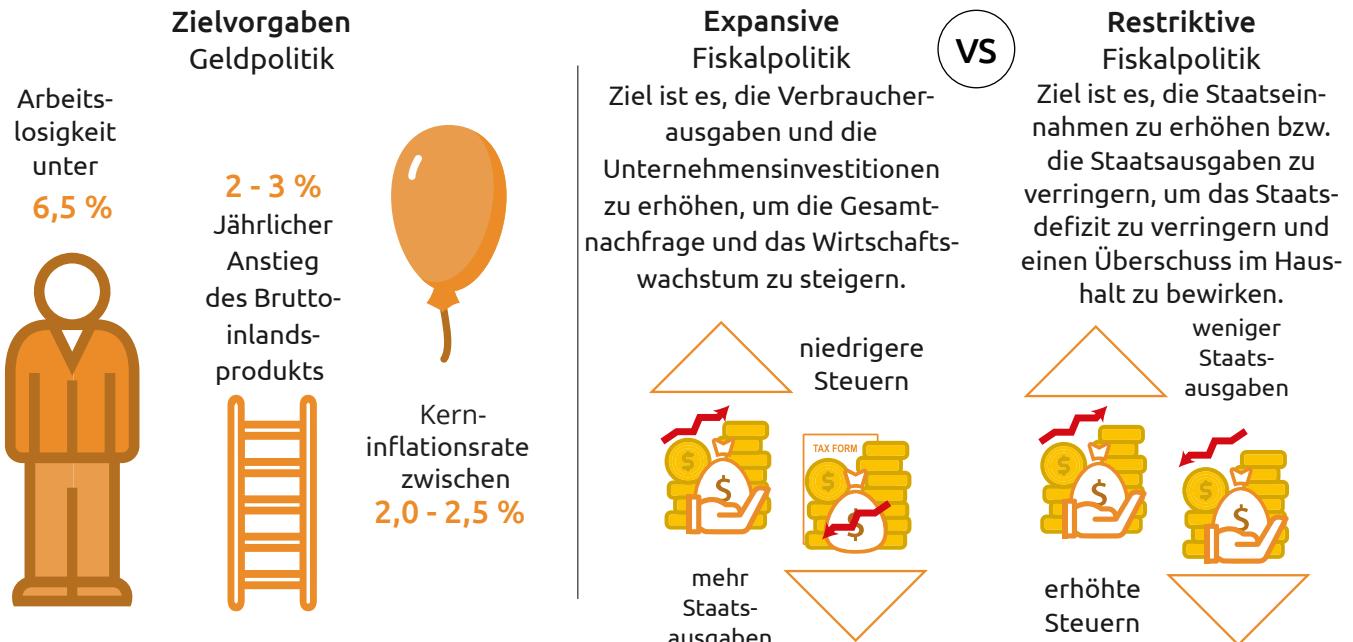
Die Zentralbank der Vereinigten Staaten wird **Federal Reserve** oder Fed genannt.



Die Regierungen können sich Geld leihen, um die Wirtschaft anzukurbeln, aber das kann zu Inflation führen, wenn sie mehr Geld drucken müssen, um die Kredite zurückzuzahlen.



Die dunkle Seite von Fiat



Politik	Beschreibung	Beispiel
Geldpolitik	Bei der Geldpolitik werden die Zins- sätze angepasst, um die Umlaufmenge des Geldes zu steuern.	Die Federal Reserve erhöht die Zins- sätze, um die Inflation zu bremsen, oder sie kann sie senken, um die Beschäftigung zu fördern.
Fiskalpolitik	Bei der Fiskalpolitik geht es darum, die Wirtschaft durch Ausgaben- und Steuerpolitik zu beeinflussen.	Die Regierung erhöht die Ausgaben für Infrastrukturprojekte, um das Wirtschaftswachstum anzukurbeln. Sie kann auch die Steuern senken, damit die Menschen mehr ausgeben.
Wechselkurs- politik	Die Verwendung des Wechselkurses eines Landes (der Wert seiner Währung im Verhältnis zu anderen Währungen), um den Handel und die Wirtschaft zu beeinflussen.	Die chinesische Regierung koppelt den Wert des Yuan an den US-Dollar, um die Wechselkurse zu stabilisieren.
Angebotsschock	Ein plötzliches und unerwartetes Ereignis, das das Angebot an Waren und Dienstleistungen unterbricht und zu Veränderungen der Preise und der Geldmenge führt.	Eine Naturkatastrophe, die einen erheblichen Teil der landwirtschaftlichen Produktion eines Landes zerstört und zu Nahrungsmittelknappheit und Preissteigerungen führt.
Preiskontrolle	Von der Regierung festgelegte Obergrenzen für die Preise von Waren und Dienstleistungen, um die Inflation einzudämmen oder die Preise zu stabilisieren.	Die Regierung legt einen Höchstpreis für Benzin fest, um in einer Krise Preistreiberei zu verhindern.



3.4 Die Magie der Geldschöpfung

3.4.1 Der Zeitwert des Geldes und seine Rolle für das Wirtschaftssystem

Hast du dich jemals gefragt, warum Banken ihren Kunden so viele Dienstleistungen anbieten? Auch wenn es den Anschein hat, dass sie großzügig sind, darf man nicht vergessen, dass Banken Unternehmen sind und ihr Hauptziel darin besteht, Gewinne zu erzielen. Aber wie können sie einen Gewinn erzielen, wenn sie Geld in Form von Krediten verschenken?

Neben der Verzinsung von Einlagen erwirtschaften Banken auch auf andere Weise Einnahmen, unter anderem durch:

1. Erhebung von Zinsen für Kredite, die sie vergeben.
2. Gebühren für Dienstleistungen wie die Nutzung von Geldautomaten und die Kontoführung.
3. Investitionen, wie den Kauf und Verkauf von Wertpapieren oder Investitionen in Immobilien.
4. Einbehaltung eines bestimmten Prozentsatzes der Kredite als Reserve und Investition oder Verleihen des Restes.
5. Zahlung von Zinsen auf Einlagen und Erhebung von Gebühren für Giro- und Sparkonten.



Indem die Banken sich Geld zu niedrigen Zinsen leihen und es zu höheren Zinsen verleihen, können sie Gewinne erzielen. Außerdem erzielen sie Einnahmen durch Gebühren und Anlagetätigkeiten.

Aber warum sollte dies für dich als Einzelperson von Bedeutung sein? Kennst du den Satz „Ein Dollar heute ist mehr wert als ein Dollar morgen“? Dieses Konzept ist als **Zeitwert des Geldes** bekannt, und es geht darum, dass Geld in der Gegenwart mehr wert ist als in der Zukunft. Der Grund dafür ist, dass **Geld angelegt werden kann, um Zinsen zu verdienen, und dass Geld im Laufe der Zeit durch die Inflation an Wert verlieren kann.**

Mit anderen Worten: Wenn man Geld auf einem Sparkonto liegen hat, das einen niedrigen Zinssatz bringt, wird es in Zukunft nicht mehr so viel wert sein wie heute. Wenn man hingegen sein Geld in etwas investiert, das die Möglichkeit einer höheren Rendite bietet, kann man einen Vorteil daraus ziehen.



Banken leihen sich Geld von Einlegern zu einem Zinssatz (sagen wir 5 %).



Die Banken verleihen dieses Geld zu einem höheren Zinssatz an die Kreditnehmer (sagen wir 9 %).



Die Banken zahlen Zinsen aus den Zinseinnahmen der Kreditvergabe (9 % - 5 % = 4 %) und behalten den Rest als ihren Gewinn.



Um sicherzustellen, dass dein Geld im Laufe der Zeit seinen Wert behält, besteht das Ziel einer Investition darin, eine Rendite zu erzielen, die über der Inflationsrate liegt. Auf diese Weise wird dein Geld in der Zukunft mehr wert sein als heute.

Die dunkle Seite von Fiat

3.4.2 Geld sparen in schwierigen Zeiten

Die derzeitige Weltwirtschaftslage, die durch die Pandemie negativ beeinflusst wurde, hat Herausforderungen wie eine hohe Inflation und niedrige Zinsen auf Sparkonten mit sich gebracht. Diese Bedingungen können es schwierig machen, effektiv Geld zu sparen, da die Inflation den Wert der Währung mit der Zeit auffrisst. Selbst wenn man heute spart, könnte man in Zukunft weniger Kaufkraft haben.

Aber keine Sorge! Es gibt immer noch Möglichkeiten, Geld zu sparen und finanziell abgesichert zu sein. Hier sind ein paar Ideen zum Ausprobieren:

- **Erstelle ein Budget:** Ein Haushaltsplan ist ein Plan, wie du dein Geld verwenden wirst. Er kann dir helfen zu erkennen, wo du zu viel Geld ausgibst und wo du sparen kannst. Leg dir jeden Monat etwas Geld zum Sparen beiseite und suche nach Möglichkeiten, deine Ausgaben zu reduzieren.
- **Beginne zu investieren:** Investitionen sind eine Möglichkeit, dein Geld mit der Zeit wachsen zu lassen. Es gibt viele Arten von Anlagen, und du kannst eine finden, die zu deinem Budget und deiner Risikobereitschaft passt.
- **Werde kreativ:** Es gibt viele kreative Möglichkeiten, Geld zu sparen. Du kannst versuchen, dir selbst die Haare zu schneiden oder mit anderen Tauschhandel für Waren und Dienstleistungen zu betreiben. Sei offen dafür, neue Dinge auszuprobieren und nach nicht traditionellen Lösungen für deine finanziellen Probleme zu suchen.

○ Die Aufnahme von Schulden ist im Allgemeinen akzeptabel, solange das Geld dazu verwendet wird, Einkommen zu erzielen und die Kaufkraft in der Zukunft zu erhöhen. Denn die Aufnahme von Krediten kann einer Einzelperson oder einem Unternehmen ermöglichen, Investitionen zu tätigen, die ihre Produktivität und Effizienz steigern und letztlich zu höheren Gewinnen und finanzieller Stabilität führen.

○ Wenn ein Landwirt beispielsweise einen Kredit aufnimmt, um neue Geräte zu kaufen, mit denen er seine Ernte schneller und effizienter einfahren kann, kann er möglicherweise mehr Einkommen erzielen und dadurch seine Kaufkraft erhöhen. Wird das Geld hingegen zur Verschwendug von Ressourcen oder für unproduktive Investitionen verwendet, kann dies zu finanziellen Schwierigkeiten führen und wäre keine kluge Entscheidung.

Wenn man seine Finanzen selbst in die Hand nimmt und flexibel ist, kann man schwierige Wirtschaftslagen besser überstehen und als Sieger hervorgehen.

Der 50/30/20-Ausgabeplan



- 20 % Ziele
- 30 % flexible Ausgaben
- 50 % notwendige Ausgaben



3.4.3 Mindestreserve-System (Fractional Reserve)

Bisher haben wir darüber gesprochen, wie Zentralbanken wie die Federal Reserve die Geldmenge verwalten, wie Banken Geld für sich selbst verdienen und wie man Geld spart, aber wir haben noch nicht darüber gesprochen, wie neues Geld tatsächlich geschaffen und in eine Gesellschaft eingeführt wird. Es mag wie Magie erscheinen, aber es steckt ein interessanter Prozess dahinter.

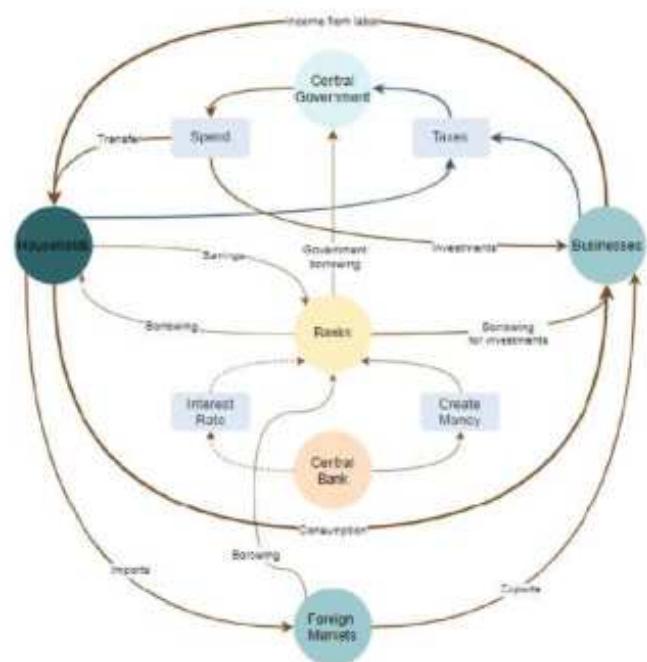
Wie kommt eigentlich **neues** Geld in Umlauf und sorgt für Wirtschaftswachstum? Im Gegensatz zu physischen Ressourcen wie Nahrung oder Wasser, die zur Neige gehen können, hat Geld keine feste Grenze! Wie funktioniert es also?

Die Regierung, die Zentralbank und die privaten Banken spielen alle eine Rolle in diesem Prozess.

Hier ist eine vereinfachte Version, wie die Federal Reserve (Fed) 100 Millionen US-Dollar in Umlauf bringen kann:

1. Die Fed beschließt, dass sie die Geldmenge um 100 Millionen Dollar erhöhen will. Diese Entscheidung wird in der Regel auf der Grundlage der **geldpolitischen Ziele** der Fed getroffen, wie z. B. die Förderung des Wirtschaftswachstums oder die Stabilisierung der Preise.
2. Die Fed weist eine große Geschäftsbank an, auf ihrem Konto bei der Fed eine Einlage in Höhe von 100 Millionen Dollar anzulegen. Diese Einlage wird aus dem Nichts geschaffen und ist nicht durch materielle Vermögenswerte gedeckt.
 - Wenn eine Geschäftsbank eine Einlage bei der Fed macht, leiht sie sich im Grunde Geld von der Fed. Die Fed stellt der Bank die Mittel für die Einlage zur Verfügung, und im Gegenzug muss die Bank Zinsen für das Darlehen zahlen und das Darlehen schließlich zurückzahlen.
3. Die Mitgliedsbank verwendet dann diese neuen 100 Millionen Dollar Einlagen zur Vergabe von Krediten an Unternehmen oder Privatpersonen oder zum Kauf von Wertpapieren wie Staatsanleihen.
4. Die Unternehmen oder Einzelpersonen, die diese Darlehen erhalten, können das Geld verwenden, um Einkäufe zu tätigen, Rechnungen zu bezahlen oder in andere Vermögenswerte zu investieren. Dies erhöht das Gesamtangebot an Geld in der Wirtschaft.
5. Wenn das Geld zirkuliert und ausgegeben wird, landet es schließlich bei anderen Banken, die es dann für ihre eigenen Kredite und Investitionen verwenden können. Dieser Prozess setzt sich fort, bis die 100 Millionen Dollar vollständig in Umlauf sind.

Insgesamt trägt die Fähigkeit der Fed, neues Geld über das Bankensystem in Umlauf zu bringen, dazu bei, das Wirtschaftswachstum zu stimulieren und ihre geldpolitischen Ziele zu erreichen.



Die dunkle Seite von Fiat

Die Banken schaffen tatsächlich jedes Mal **neues** Geld, wenn sie Kredite an Kunden vergeben oder Investitionen tätigen. Was? Ja, du hast richtig gelesen. Wenn eine Bank einen Kredit vergibt, schafft sie Geld, indem sie dem Konto des Kreditnehmers neue Mittel in Höhe des Kreditbetrags zuführt. Der Kreditnehmer kann dieses Geld dann verwenden, um Einkäufe zu tätigen oder Rechnungen zu bezahlen, wodurch sich das Gesamtangebot an Geld in der Wirtschaft effektiv erhöht. Wir werden als nächstes sehen, wie das geschieht.

3.4.4 Gemeinschaftsübung: Mindestreserve-Bankwesen

Bei dem als „**Fractional-Reserve-Banking**“ bekannten Verfahren **halten die Banken nur einen Bruchteil ihrer Einlagen als Reserven und verleihen den Rest**. Solange sie einen bestimmten, von der Zentralbank festgelegten Mindestreservesatz einhalten, können die Banken mehr Geld schaffen, als sie zur Verfügung haben. Diese Fähigkeit, neues Geld zu schaffen, kann jedoch auch das Risiko einer übermäßigen Kreditaufnahme und finanzieller Instabilität mit sich bringen, wenn sie nicht sorgfältig gesteuert wird.

Der **Mindestreservesatz** ist eine Regel, die den Banken vorschreibt, wie viel Geld sie in ihren Tresoren aufbewahren müssen und wie viel sie ausleihen dürfen. Er wird von der **Zentralbank festgelegt**, einer speziellen Gruppe von Personen, die für eine gesunde Wirtschaft zuständig ist.

In dieser Übung werden wir das Konzept des **Mindestreserve-Bankwesens** erforschen und untersuchen, wie es zur **Entwertung** einer Währung, zur Inflation und zu einer Abnahme der **Kaufkraft** führen kann.

- Nehmen wir an, die gesamte Geldmenge in der Wirtschaft beträgt 1000 Euro und der Mindestreservesatz beträgt 50 %. Das bedeutet, dass die Bank für jede 1000 Euro in der Wirtschaft 50 % davon als Reserve halten muss.
- Wenn Hendrik 1000 € bei der Bank einzahlt und Susi später bei der Bank einen Kredit beantragt, kann die Bank bei dem geforderten Verhältnis die Hälfte behalten und die andere Hälfte verleihen, sie würde ihr also 500 € leihen. Infolgedessen würde die Gesamtgeldmenge von 1000 € auf 1500 € steigen.

Fractional-Reserve-Banking
½ wird behalten



Die Formel lautet: *Geldschöpfung = Gesamtgeldmenge in der Wirtschaft ÷ Mindestreservesatz.*



Kapitel 3

Gemeinschaftsübung: Anhand der obigen Formel lässt sich der geschaffene Geldbetrag wie folgt berechnen:

- Geschaffenes Geld = 1000 € / 50 % = 2000 €

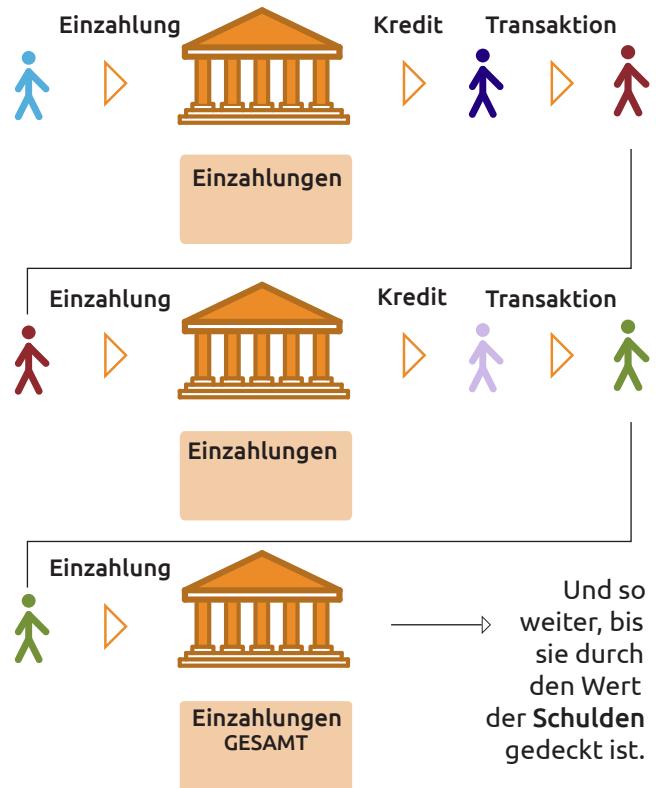
*Bitte beachtet, dass dies stark vereinfacht ist!

Wir werden die Geldschöpfung in einer kleinen Volkswirtschaft modellieren (die aus sechs Teilnehmern bestehen wird; einer davon wird die Rolle einer Bank übernehmen). Der von der Zentralbank festgelegte **Mindestreservesatz** wird als Anteil der Kundeneinlagen berechnet und bestimmt, wie viel die Geschäftsbanken aufbewahren müssen, anstatt es auszuleihen. Nehmen wir für die Zwecke dieser Simulation an, dass ein Mindestreservesatz von 10 % vorgeschrieben ist.

- Wenn eine Bank zum Beispiel 100 € erhält und 10 % davon als Mindestreserve einbehalten muss, kann sie 90 € verleihen. Wenn dieser Kredit bei einer anderen Bank eingezahlt wird, kann diese Bank 81 € ausleihen, und so weiter.
- Dadurch entsteht ein **Multiplikatoreffekt**, der die **Geldmenge** insgesamt erhöht. Dies kann die Wirtschaft ankurbeln, aber auch zu Inflation führen, wenn die Geldmenge zu schnell wächst.
- Um herauszufinden, wie viel Geld mit einem bestimmten prozentualen Verhältnis geschaffen wird, könnt ihr eine Formel verwenden.
- Um die Formel anwenden zu können, müsst ihr zunächst die gesamte Geldmenge in der Wirtschaft kennen. Dies ist das gesamte Geld, das zum Kauf und Verkauf von Waren und Dienstleistungen verwendet wird. Dann müsst ihr den Mindestreservesatz kennen, d. h. den Prozentsatz des Geldes, den eine Bank vorrätig halten muss und nicht verleihen kann.
- Zusammenfassend lässt sich sagen, dass eine Bank, wenn sie Geld verleiht, neues Geld schafft, das vorher nicht existierte, und dass dadurch die Gesamtgeldmenge in der Wirtschaft steigt.
- In der Regel haben Länder mit volatilen Volkswirtschaften oder hohen Inflationsraten hohe Reservesätze, um Risiken zu mindern und das Finanzsystem zu stabilisieren.

Wir brauchen die folgenden Freiwilligen:

- A = Einzahler (Lottogewinner) (Hellblau)
B = Bankangestellter (Bank)
C = 1. Schuldner (Dunkelblau)
D = Grundstückseigentümer/Einzahler (Rot)
E = 2. Schuldner (Hellviolett)
F = Eigentümer einer Kunsthalle/Einzahler (Grün)



Die dunkle Seite von Fiat

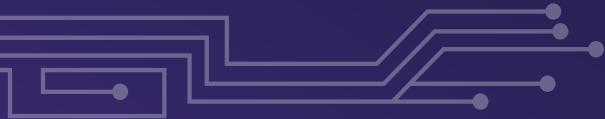
A hat gerade 100.000 € in der Lotterie gewonnen und geht zu einer neu eröffneten Bank, um sie einzuzahlen. Die Bank, B, hat eine Mindestreservesatz von 10 %. Wie viel muss B in seinem Tresor aufbewahren? _____. Am nächsten Morgen betritt C die Bank und bittet um einen Kredit. Wie viel kann die Bank ihm leihen? _____. C lehnt sich den Höchstbetrag, weil er eine Anzahlung für ein Haus leisten möchte. C unterschreibt den Scheck und übergibt ihn an D. D geht dann zur Bank und zahlt den Scheck ein. Wie viel hat D eingezahlt? _____. Wie hoch ist der Gesamtbetrag der Einlagen, die derzeit bei der Bank verzeichnet sind? _____.

E betritt die Bank und bittet um einen großen Kredit. Die Bank sagt, dass sie ihm höchstens _____ leihen kann. E verlässt die Bank mit dem Geld und geht zu F, um ein Kunstwerk zu kaufen. Nach einem Hin und Her wird das Kunstwerk genau zu dem Preis verkauft, den E sich bei der Bank geliehen hat. E bezahlt F. F zahlt das Geld bei der Bank ein. Wie hoch ist der Gesamtbetrag der Einlagen in diesem Moment? _____.

Name	Einzahlung	Kreditbetrag	Reservebetrag
A			
C			
D			
E			
F			

Wie viel Geld wird also mit diesen 100.000 Euro tatsächlich geschaffen, wenn das Geld weiterhin in der Wirtschaft zirkuliert?

Wenn der Mindestreservesatz hoch ist, müssen die Banken mehr Geld in ihren Tresoren aufbewahren und können weniger Geld ausleihen. Dies kann es Menschen und Unternehmen erschweren, sich Geld zu leihen, und kann die Wirtschaft bremsen. Wenn der Mindestreservesatz niedrig ist, müssen die Banken weniger Geld in ihren Tresoren aufbewahren und können mehr Geld ausleihen. Dadurch können sich Menschen und Unternehmen leichter Geld leihen und die Wirtschaft kann schneller wachsen.



Kapitel 3

Können wir also die Antwort für unsere Gemeinschaftsübung herausfinden, bei der die Reserve 10 % beträgt? (Denkt daran, 10 % in die Dezimalform $10\% = 0,1$ umzuwandeln)!

Nur so aus Neugier: Wie viel Geld würde in einer Volkswirtschaft geschaffen werden, wenn der Mindestreservesatz auf 1 % gesenkt würde? (Dazu 100.000 € durch 0,01 geteilt werden). Überrascht?

- Seit 2020 hat die Federal Reserve (die Zentralbank der USA) den **Mindestreservesatz auf null Prozent gesenkt**, um die Wirtschaft anzukurbeln.



Kapitel 4

Die Zukunft ist dezentral: Die Ermächtigung von Gemeinschaften und Individuen

4.0 Von der Krise zur Innovation: Die Cypherpunks und die Schaffung einer dezentralen digitalen Währung

4.1 Missbrauch der Zentralisierung

4.1.1 Zentralisierte Systeme

4.1.2 Die Intermediäre: Ein Überblick über die Akteure bei einer Kreditkartentransaktion

4.2 Ein leistungsfähiges Instrument zur Überwindung der Grenzen der Zentralisierung

4.2.1 Gemeinschaftsübung: Dezentrales Konsensspiel mit böswilligen Akteuren

4.3 Transaktionen sind nur Handelsvereinbarungen

4.3.1 Vertrauen oder nicht vertrauen

4.3.2 Lasst uns Vertrauen gegen Regeln tauschen

4.4 Die Entfesselung der Macht der Blockchain:
Eine Technologie revolutioniert die Zukunft



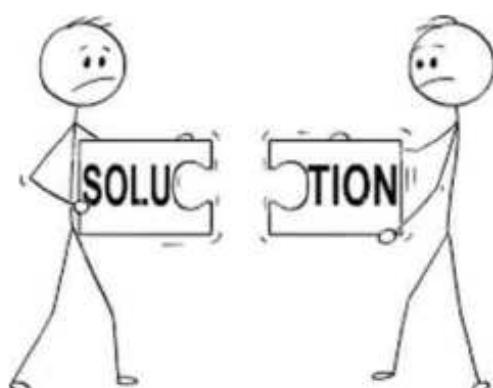
Die Zukunft ist dezentral: Die Ermächtigung von Gemeinschaften und Individuen

4.0 Von der Krise zur Innovation:

Die Cypherpunks und die Schaffung einer dezentralen digitalen Währung

Vor der Erfindung von *Bitcoin* suchten die Menschen nach Möglichkeiten, die Probleme des traditionellen Finanzwesens, wie Betrug, Korruption und mangelndes Vertrauen in Finanzinstitute, zu lösen. Diese Probleme wurden durch die globale Finanzkrise von 2008 noch dringender. Als Reaktion darauf machte sich eine Gruppe technisch versierter und vorausschauender Personen, die sogenannten Cypherpunks, daran, eine **digitale Währung** zu schaffen, die für Online-Transaktionen **ohne die Notwendigkeit von Intermediären** wie Banken verwendet werden konnte.

Die Cypherpunks waren Rebellen und Visionäre, die an die Macht der Technologie glaubten, um positive Veränderungen herbeizuführen und traditionelle Machtstrukturen in Frage zu stellen. Viele von ihnen engagierten sich für Aktivismus und Bürgerrechte, und sie waren durch eine gemeinsame Leidenschaft für Technologie und den Wunsch, diese zur Gestaltung der Zukunft zu nutzen, geeint.



Frage: Wie kann der Einzelne seine finanzielle Souveränität zurückgewinnen?

Antwort: Die Cypherpunk-Bewegung zielt darauf ab, ein neues Finanzsystem zu schaffen, das die Sicherheit, die Privatsphäre und die Freiheit des Einzelnen respektiert, um die finanzielle Souveränität wiederzuerlangen.

Und so machten sie sich daran, *Bitcoin* zu schaffen, eine digitale Währung, die die Art und Weise, wie wir über Geld und finanzielle Transaktionen denken, revolutionieren sollte. Dazu mussten sie einen Weg finden, um Transaktionen aufzuzeichnen, der sicherer und transparenter war als herkömmliche zentralisierte Kassenbuch- bzw. Ledger-Systeme. Warum waren sie dieser Meinung?

4.1 Missbrauch der Zentralisierung

4.1.1 Zentralisierte Systeme

Die Zentralisierung der Macht führt häufig zu Korruption, die wiederum zu einer Misswirtschaft bei den Ressourcen, einschließlich der finanziellen Ressourcen, führen kann. Dies kann diejenigen, die in der Hierarchie niedriger stehen und nicht so viel Einfluss oder Macht haben, unverhältnismäßig stark treffen, sodass sie die Folgen von Korruption und Misswirtschaft am stärksten zu spüren bekommen.

Das moderne Fiat-System zeichnet sich durch eine Zentralisierung der Kontrolle aus, wobei eine kleine Gruppe von Banken und anderen Finanzinstituten ein erhebliches Gewicht in der Wirtschaft hat.



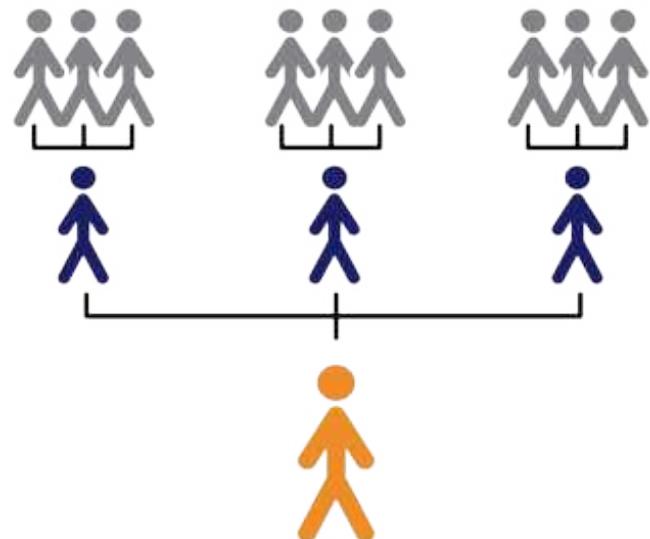
Kapitel 4

Ein zentralisiertes System kann man sich als einen Baum mit einem einzigen Stamm vorstellen. Der Stamm stellt die zentrale Behörde oder Kontrollstelle dar, und die Äste stehen für die verschiedenen Teile des Systems, die von der zentralen Behörde kontrolliert werden. In dieser Analogie ist der Baum verwundbar, wenn der Stamm beschädigt oder erkrankt ist, da der gesamte Baum auf den Stamm angewiesen ist.



Zentralisierte Systeme haben viele **Nachteile**, unter anderem:

- **Schwachstelle:** Ein zentralisiertes System hängt von einem einzigen Punkt ab, und wenn dieser Punkt ausfällt, kann das gesamte System ausfallen.
- **Kontrolle und Macht:** Diejenigen, die zentralisierte Systeme kontrollieren, haben viel Macht und Einfluss darauf, wie sie funktionieren.
- **Ineffizienz und Intermediäre:** Zentralisierte Systeme arbeiten oft mit Intermediären, was sie langsam machen und zusätzliche Kosten verursachen kann.
- **Fehlende Autonomie:** Die Menschen sind möglicherweise nicht in der Lage, ihre eigenen finanziellen Entscheidungen zu treffen.
- **Zensur und Beschränkungen:** Es besteht die Gefahr, dass der Zugang zu bestimmten Finanzmitteln in zentralisierten Systemen blockiert oder eingeschränkt wird.
- **Mögliche Skalierungsprobleme:** Zentralisierte Systeme können nur schwer mit der steigenden Nachfrage nach Finanzdienstleistungen und Ressourcen Schritt halten.
- **Sicherheitsrisiken:** Zentralisierte Systeme können Schwachstellen aufweisen, die Hacker nutzen können, um sich Zugang zu verschaffen oder Schaden anzurichten.
- **Mangel an Transparenz und Vertrauen:** Es kann schwierig sein, die Funktionsweise zentralisierter Systeme zu verstehen und fundierte Entscheidungen über sie zu treffen, da sie möglicherweise *nicht transparent oder vertrauenswürdig* sind.



Die Zukunft ist dezentral: Die Ermächtigung von Gemeinschaften und Individuen

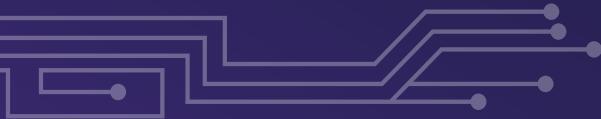
4.1.2 Die Intermediäre:

Ein Überblick über die Akteure bei einer Kreditkartentransaktion

Modernes Bankwesen ist simpel, oder? Zum Beispiel etwas so scheinbar Einfaches wie der Kauf eines Hamburgers mit einer Kreditkarte. Auf den ersten Blick mag es anspruchslos und harmlos erscheinen. Aber wenn wir die einzelnen Schritte aufschlüsseln und uns die beteiligten Mittelsmänner ansehen, wirst du vielleicht überrascht sein, was wir entdecken. Gibt es Unannehmlichkeiten, Ineffizienzen, vielleicht sogar versteckte Gefahren, die im Verborgenen lauern? Lasst es uns herausfinden.

Schritt	Transaktion	Beschreibung (Beispiel)
1	Karteninhaber - Händler	Du bestellst im Fast-Food-Restaurant einen Hamburger und bezahlst mit Citi-Mastercard.
2	Händler - Zahlungsabwickler	Das Restaurant schickte eine Autorisierungsanfrage an seinen Zahlungsabwickler.
3	Zahlungsabwickler - Kreditkartennetzwerk	Der Abwickler erhält die Anfrage und leitet sie an Mastercard weiter.
4	Kreditkartennetzwerk - zuständige Bank	Mastercard leitet die Anfrage weiter an deine Bank, CitiBank.
5	zuständige Bank - Kreditkartennetzwerk	CitiBank Überprüft die Kartendaten sowie die verfügbaren Mittel und sendet ihre Antwort (genehmigt oder abgelehnt) an Mastercard.
6	Kreditkartennetzwerk - Zahlungsabwickler	Mastercard schickt die Autorisierung zurück zum Zahlungsabwickler.
7	Zahlungsabwickler - Händler	Der Abwickler schickt die Autorisierung zurück zum Restaurant.
8	Händler - Karteninhaber	Du bekommst deinen Hamburger.





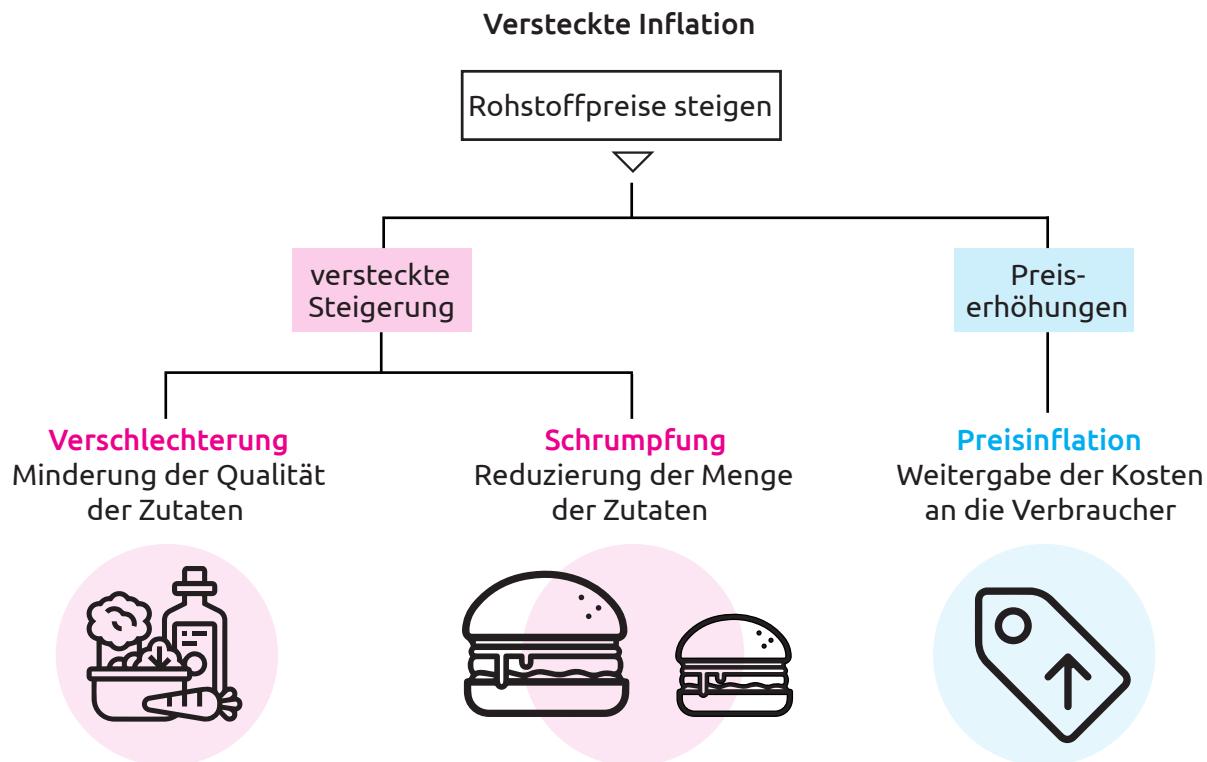
Zu diesem Zeitpunkt haben noch keine Gelder den Besitzer gewechselt, außer vielleicht einer kleinen **Genehmigungsgebühr**. Die Transaktion existiert nur auf dem „Papier“. Das Restaurant muss seine Verkäufe für den Tag abschließen oder ausbuchen. Der Abschlussprozess könnte wie folgt aussehen:

1. Der Restaurantschalter oder das POS-System (Point-of-Sale) sendet die Transaktionen des Tages an den *Zahlungsabwickler*.
2. Der *Abwickler* sendet die Transaktionsdaten an *Mastercard*.
3. *Mastercard* sendet die Transaktionen an *CitiBank*.
4. Die *Citibank* bestätigt die Autorisierungen, **behält ihre Verrechnungsgebühr ein** (in Nordamerika gibt es über 900 mögliche Gebührenordnungen) und überweist die Gelder zurück an *Mastercard*.
5. *Mastercard* **erhebt eine Gebühr** und leitet das Geld an den *Zahlungsabwickler* weiter.
6. Der *Abwickler* **nimmt seine anteilige Gebühr**, wie im Vertrag mit dem Händler festgelegt, und überweist das Geld auf das Bankkonto des Restaurants.

Wer, glaubst du, hat die Gebühren bezahlt? Du natürlich! Aber hat dich jemand darüber informiert? Nein! Die Gebühren waren in den Kosten des Hamburgers versteckt.

Und all dies geschieht, ob du es glaubst oder nicht, weil wir uns auf die Zentralisierung verlassen.

Die moderne Bankenwelt birgt verschiedene Risiken, wie z. B. versehentliches doppeltes Durchziehen der Karte, Kreditkartenbetrug, Fehler von Menschen und Computern sowie mögliche Hacks.



Die Zukunft ist dezentral: Die Ermächtigung von Gemeinschaften und Individuen

4.2 Ein leistungsfähiges Instrument zur Überwindung der Grenzen der Zentralisierung

Dezentrale Systeme hingegen kann man sich wie einen Wald vorstellen. Jeder Baum steht für einen unabhängigen Teilnehmer, und der Wald steht für das Gesamtsystem. In dieser Analogie ist der Wald widerstandsfähiger als ein einzelner Baum, da er nicht von einer einzelnen Schwachstelle abhängig ist. Wenn ein Baum beschädigt wird oder erkrankt, kann der Rest des Waldes weiter gedeihen. Die Bäume des Waldes teilen sich den Boden, die Nährstoffe, die Sonne und den Regen.



Dezentralisierte Systeme wie Gemeinschaften, Netzwerke und Wälder funktionieren am besten, wenn eine vielfältige Gruppe von Personen zusammenarbeitet, anstatt dass eine einzige zentrale Instanz alle Regeln vorgibt.



Ein Netzwerk ist eine Gruppe von Knotenpunkten (Nodes), die auf irgendeine Weise miteinander verbunden sind. Diese Verbindung ermöglicht es den Geräten, Informationen auszutauschen und miteinander zu kommunizieren.

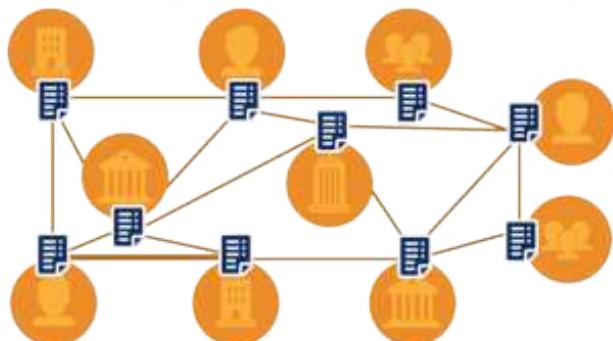


Ein Node ist ein an ein Netzwerk angeschlossener Computer, der Informationen austauschen und/oder empfangen und mit den anderen Nodes kommunizieren kann.

Vorteile eines dezentralen Systems:

- Es ist widerstandsfähiger und zuverlässiger, weil es keine einzelne Schwachstelle gibt. Wenn ein Teil des Systems ausfällt, kann der Rest weiterarbeiten.
- Mit der richtigen Verschlüsselung ist die Dezentralisierung sicherer, da es keinen zentralen Kontrollpunkt gibt, der von Hackern angegriffen werden kann.

Distributed Ledger Technology (Technologie des verteilten Kassenbuchs)





- Es kann einem helfen, souverän zu werden, was bedeutet, dass man mehr Kontrolle und Autonomie über sein eigenes Vermögen und seine Entscheidungen hat, anstatt sich auf eine zentrale Instanz zu verlassen.
- Es kann transparenter sein, weil alle Nodes Zugang zu denselben Informationen haben und sehen können, was im System passiert.
- Es kann genehmigungsfrei sein, d. h. jeder kann dem System beitreten oder daran teilnehmen, ohne die Genehmigung einer zentralen Instanz zu benötigen.
- Es kann unbegrenzt sein, d. h. es gibt keine vorgegebene Grenze für die Anzahl der Nodes, die dem System beitreten können.
- Jeder Node hat die gleichen Möglichkeiten, etwas zum Netzwerk beizutragen und es zu beeinflussen, was es zu einer demokratischeren und integrativeren Struktur macht.
- Die Teilnehmer können auch Pseudonyme oder „Spitznamen“ verwenden, um ihre Privatsphäre und Sicherheit zu schützen, was das System widerstandsfähiger gegen Zensur und Angriffe machen kann.



Dezentralisierte Knappheit wird oft als positiv für Geld angesehen, weil sie Inflation und Manipulation durch eine zentrale Instanz verhindert.

Aber auch dezentrale Systeme haben ihre **Schwierigkeiten** und Grenzen.

- Bei dezentralen Systemen ist es unter Umständen aufwändiger, alle angeschlossenen Geräte (Nodes) dazu zu bringen, sich zu einigen und zusammenzuarbeiten.
- Dezentralisierte Systeme sind auch anfälliger für Probleme, die durch böswillige Akteure oder Geräte (bösnartige Nodes) verursacht werden, die dem Netzwerk schaden könnten.

4.2.1 Gemeinschaftsübung: Dezentrales Konsensspiel mit böswilligen Akteuren

In einem dezentralen Netzwerk bezieht sich der Begriff Konsens auf den Prozess der Einigung zwischen den Mitgliedern des Netzes. Dies kann zu Schwierigkeiten führen, da es keine zentrale Autorität gibt, die Entscheidungen trifft oder Konflikte löst. Stattdessen müssen Entscheidungen durch einen Prozess der Verhandlung und des Kompromisses zwischen den Mitgliedern der Organisation getroffen werden.

Gemeinschaftsübung: In diesem Spiel übernehmt ihr die Rolle von **Nodes** in einem dezentralen Netzwerk. Euer Ziel ist es, einen **Konsens** für ein Problem zu finden, **ohne einander zu vertrauen**.

- Du spielst die Rolle eines Nodes in einem dezentralen Netzwerk und arbeitest mit anderen zusammen, um einen Konsens für ein Problem zu finden.
- Es kann sein, dass es in der Gruppe böswillige Akteure gibt, die versuchen werden, den Prozess in die Irre zu führen oder zu sabotieren.
- Als **guter Akteur** ist es dein Ziel, mit anderen zusammenzuarbeiten, um Informationen zu überprüfen und einen Konsens zu erzielen.

Die Zukunft ist dezentral: Die Ermächtigung von Gemeinschaften und Individuen

- Als böswilliger Akteur ist es dein Ziel, die Gruppe in die Irre zu führen, aber auf subtile Art und Weise.
- Das Ziel des Spiels ist es, die Probleme und Vorteile von dezentralen Systemen zu verstehen und zu lernen, wie man Informationen verifiziert, einen Konsens erreicht und bösartiges Verhalten erkennt.
- Ihr werdet in kleine Gruppen eingeteilt und erhaltet ein Problem, das ihr in einer bestimmten Zeit lösen müsst.

Denkt daran, dass ihr euch in einem dezentralen System nicht einfach auf die Antworten der anderen Gruppenmitglieder verlassen könnt. Ihr müsst die Richtigkeit der Informationen überprüfen und durch Diskussion und Zusammenarbeit zu einem Konsens kommen.

4.3 Transaktionen sind nur Handelsvereinbarungen

Willkommen auf der dezentralen mikronesischen Insel Yap! Sie ist ein wenig abgelegen, aber faszinierend, weil die Menschen eine besondere Art von Währung verwenden, die „Rai-Steine“. Ein Merkmal, das sie zu einer großartigen Form des Geldes macht, ist ihre Knappheit. Die Gesamtzahl der Rai-Steine ist begrenzt, was bedeutet, dass sie *nicht einfach reproduziert oder inflationiert werden* können wie Fiat-Währungen. Dieses feste Angebot trägt dazu bei, dass die Kaufkraft der Rai-Steine im Laufe der Zeit erhalten bleibt, und macht sie zu einem zuverlässigen Wertaufbewahrungsmit- tel. Diese Rai-Steine sind wie riesige Münzen, mit denen man auf der Insel Dinge kaufen kann. Allerdings können sie eine *Tonne* wiegen. Rai-Steine können einen regelrecht zerquetschen, sodass es etwas unpraktisch ist, sie mit sich herumzutragen. Wie können die Menschen also Rai-Steine als Zahlungsmittel verwenden, ohne sie physisch von einem Ort zum anderen bringen zu müssen?



4.3.1 Vertrauen oder nicht vertrauen

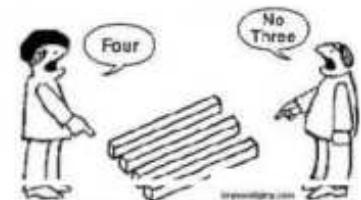
Auch wenn der US-Dollar jetzt die offizielle Währung der Insel Yap ist, sind die Rai-Steine immer noch eine Art von Geld. Im Gegensatz zum Dollar werden die Rai-Steine auf der Insel Yap nicht von einer einzigen Behörde kontrolliert oder in Banken gelagert. Stattdessen beruhen die Transaktionen auf mündlichen Überlieferungen und Vertrauen, wobei die Menschen ihre eigenen Aufzeichnungen darüber führen, wem welche Steine gehören.

Dieses System hat sowohl Vorteile als auch Nachteile. Einerseits ermöglicht es ein gewisses Maß an Unabhängigkeit von einer zentralen Behörde. Andererseits kann es aber auch zu Unstimmigkeiten und Betrugsversuchen führen. Und warum?

Dezentralisierung ist in kleinen Gruppen leicht zu erreichen. Das Leben ist einfach, da es weniger Personen gibt, die koordiniert werden müssen; es ist oft möglich, dass jeder ein Mitspracherecht bei Entscheidungsprozessen hat und dass diese Entscheidungen relativ schnell umgesetzt werden können. Je größer eine Gruppe wird, desto schwieriger wird es, eine Einigung zu erzielen und die Entscheidungen effektiv umzusetzen.



- Stell dir vor, du hast ein Feld voll mit reifem Mais, der geerntet werden muss. Du brauchst Hilfe, also gehst du zu deiner Nachbarin Anna und bietest ihr ein Geschäft an: Wenn sie dir bei der Maisernte hilft, gibst du ihr dafür einen 10-kg-schweren Stein. Anna stimmt zu, und am nächsten Tag arbeitet sie zusammen mit dir auf den Feldern und hilft dir, den Mais zu ernten und einzubringen. Am Ende des Tages schüttelt ihr euch die Hände, und anstatt ihr den Stein physisch zu übergeben, zeigst du ihr einfach, dass ihre Bezahlung (der Rai-Stein) in deinem Garten liegt.
- Von diesem Zeitpunkt an seid *ihr beide damit einverstanden*, dass der Stein nun Anna gehört. Diese Art von **Transaktion**, bei der kein Geld von einer Person zur anderen als Zahlungsmittel übergeben wird, sondern ein *physischer Gegenstand* als **Symbol für den Wert** verwendet wird, ist auf der Insel Yap üblich und wird seit Jahrhunderten als eine Form von Währung verwendet.
- Fünf Jahre später beschließt du, den Rai-Stein als dein Eigentum zu beanspruchen. Du legst der Gemeinde Beweise dafür vor, dass der Stein seit Generationen in deiner Familie weitergegeben wurde und dass du der rechtmäßige Besitzer bist.
- Anna erinnert sich jedoch an die Vereinbarung, die ihr beide getroffen habt, und liefert den Beweis, indem sie Zeugen des Austauschs zu einer Aussage mitbringt. Sie behauptet, der Stein gehöre rechtmäßig ihr, da er ihr als Gegenleistung für ihre Hilfe bei der Ernte gegeben worden sei.
- Einige Mitglieder der Gemeinschaft könnten deiner Forderung zustimmen, indem sie auf die Tradition und die Geschichte des Besitzes des Steins durch deine Familie verweisen. Andere könnten sich jedoch auf Annas Seite stellen und auf eure Vereinbarung verweisen und die Tatsache, dass sich der Stein seit fünf Jahren in ihrem Besitz befindet (bildlich gesprochen), ohne dass andere Mitglieder der Gemeinschaft Einwände hatten. Zu den Faktoren, die berücksichtigt werden könnten, gehören die Geschichte und die Tradition des Besitzes, die Bedingungen der Vereinbarung zwischen dir und Anna und alle relevanten Beweise oder Argumente. Keine sehr solide Lösung, oder?



Wie können sich also Tausende von Fremden auf eine Wahrheit einigen, ohne dass jemand das letzte Wort hat? Das ist eine Frage, die die Menschen seit langem beschäftigt, und es ist eine wichtige Frage, über die man nachdenken sollte. Es hat sich herausgestellt, dass das Internet uns geholfen hat, eine Lösung für dieses Problem zu finden. Die Lösung heißt **Blockchain**.

4.3.2 Lasst uns Vertrauen gegen Regeln tauschen

Stell dir vor, du und deine Freunde sind in einem Gruppenchat, in dem ihr untereinander Dinge kaufen und verkaufen könnt. Jeder Kauf wird in einem gemeinsamen Dokument festgehalten, das alle sehen können, und der Kontostand jeder Person wird aktualisiert. Dieser Chat verwendet ein digitales Kassenbuch, um alle getätigten Transaktionen zu erfassen. Das Kassenbuch ist wie ein Buch mit Aufzeichnungen, das jeder sehen kann.

Die Zukunft ist dezentral: Die Ermächtigung von Gemeinschaften und Individuen

In einem dezentralen System wie diesem haben alle Teilnehmer eine Kopie des Kassenbuchs. Das macht es für eine Person oder Gruppe schwierig, Informationen unbemerkt zu ändern. Es ist wie eine Sicherheitsmaßnahme, die sicherstellt, dass die Aufzeichnungen korrekt sind und niemand schummeln kann. Dies ähnelt der Funktionsweise einer **Blockchain**.

Statt sich auf persönliche Beziehungen und subjektive Interpretationen von Vertrauen zu verlassen, kann ein dezentralisiertes System effektiv funktionieren, wenn es *auf einer Reihe klarer, transparenter Regeln beruht, denen jeder zustimmt. Auf diese Weise können Entscheidungen getroffen und Konflikte auf faire und objektive Weise gelöst werden, ohne dass man sich auf das Vertrauen der einzelnen Parteien verlassen muss.* Das ist vielleicht nicht so romantisch wie Vertrauen, aber es ist eine viel zuverlässigere Methode, um sicherzustellen, dass ein dezentrales System reibungslos funktioniert.

- Wenn es auf der Insel Yap unumstößliche Regeln und schriftliche Aufzeichnungen über alle Transaktionen zwischen den Mitgliedern gäbe, hätte der Konflikt zwischen dir und Anna vermieden werden können. Diese Regeln und Aufzeichnungen hätten allen Mitgliedern des Dorfes klar gemacht, was ihre Rechte und Pflichten sind.

Aber ist es wirklich so einfach? Nicht wirklich. Es gab viele Versuche und Irrtümer, bevor sich die Blockchain-Technologie tatsächlich durchsetzen konnte.

- Was sind die genauen Regeln, die befolgt werden müssen?
- Wer macht diese Regeln?
- Warum werden die Menschen die Regeln befolgen wollen?
- Wie werden die Regeln im Netzwerk verteilt?
- Was wird passieren, wenn jemand gegen die Regeln verstößt?
- Wie können die Regeln später geändert oder aktualisiert werden?
- Wie werden die Regeln durchgesetzt, um sicherzustellen, dass sie von allen eingehalten werden?
- Wie können die Regeln gestaltet werden, sodass sie für jeden im System klar und leicht auffindbar sind?

4.4 Die Entfesselung der Macht der Blockchain: Eine Technologie revolutioniert die Zukunft

Trotz zahlreicher Rückschläge fand eine sehr rätselhafte Person (oder eine Gruppe von Personen) schließlich den Schlüssel zur Entwicklung einer bahnbrechenden Methodik für die Welt des Handels und der Finanzen. Dieses Meisterwerk machte es unglaublich einfach, Transaktionen zu verfolgen und zu überprüfen, und rationalisierte den Prozess des Austauschs von Geld, Waren und anderen Vermögenswerten. Mit seinem innovativen Ansatz und seiner fortschrittlichen Technologie hat dieses System die Art und Weise, wie wir über wirtschaftliche Transaktionen denken, revolutioniert und sie schneller, sicherer und effizienter als je zuvor gemacht.



Eine **Blockchain** ist ein dezentralisiertes digitales Kassenbuch, das alle Transaktionen auf mehreren Computern sicher und transparent aufzeichnet und verifiziert.



Kapitel 4

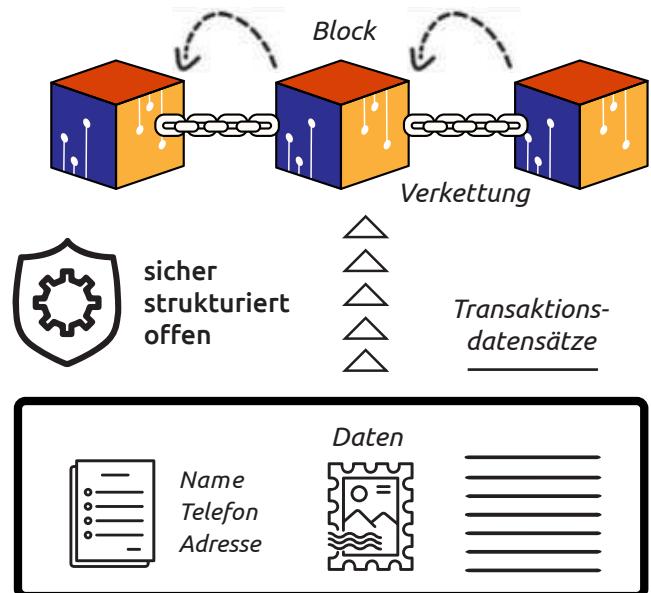
Eine **Blockchain** ist wie ein Geschichtsbuch. Jede Seite (oder „**Block**“) enthält eine Liste von Ereignissen (**Transaktionen**). Wenn mehr Dinge passieren, müssen wir dem Buch neue Seiten (Blöcke) hinzufügen. Jeder kann das Buch kostenlos lesen, aber nur spezielle Helfer (**Miner**) können neue Seiten hinzufügen. Sie stellen sicher, dass das, was geschrieben steht, wahr ist. Wenn etwas im Buch steht, kann es nicht mehr geändert oder gelöscht werden. Es ist eine dauerhafte Aufzeichnung aller **Transaktionen**, die auf der **Blockchain** stattgefunden haben.

- In einer **Blockchain** gibt es keine zentrale Autorität (wie einen Autor, einen Herausgeber oder einen Redakteur), die die darin gespeicherten Informationen bearbeiten, löschen oder ändern kann, weshalb sie im Vergleich zu einer traditionellen zentralen Datenbank als eine sichere und zuverlässige Methode der Datenaufbewahrung gilt.



Wenn kein **Konsens** unter den Helfern (**Minern**) über die Gültigkeit der Seiten (**Blöcke**) besteht, werden sie abgelehnt und nicht in die **Blockchain** aufgenommen.

Was ist eine Blockchain?
Alle Aufzeichnungen von Aktionen in der **Blockchain** werden als **Transaktionen** bezeichnet.



Doch um die **Blockchain** zu verstehen, müssen wir den Kontext, in dem sie existiert, begreifen. Auch wenn viele der Meinung sind, dass die **Blockchain** als eigenständige Innovation nützlich ist, so ist ihre eigentliche Gründungsrolle doch einzigartig: die Schaffung eines unveränderlichen Kassenbuchs und damit einer dezentralen, vertrauenslosen Form des Geldes. Um die **Blockchain** zu verstehen, müssen wir **Bitcoin** als Ganzes verstehen.



Kapitel 5

Die Zukunft des Geldes: Eine Einführung in Bitcoin

5.0 Der geheimnisvolle Schöpfer von *Bitcoin*:

Die Identität von Satoshi Nakamoto und sein Whitepaper

5.1 Erläuterung von Bitcoin und *Bitcoin* in diesem Buch

5.1.1 Was ist Bitcoin? Was ist *Bitcoin*?

5.1.2 Was ist der Unterschied zwischen Bitcoin und *Bitcoin*?

5.1.3 Warum mit Bitcoin beschäftigen, wenn man es sich nicht leisten kann?

5.1.4 Woraus besteht Bitcoin?

5.1.5 Warum ist Bitcoin gutes Geld?

5.1.6 Was geht mich das an?

5.1.7 Wie BENUZT man Bitcoin?

5.1.8 Wie kann man Bitcoin VERSENDEN oder AUSGEBEN?

5.1.9 Wie ERHÄLT man Bitcoin?

5.1.10 Kann *Bitcoin* abgeschaltet werden?

5.1.11 Wie behält die Blockchain den Überblick darüber, wer welche Bitcoin ausgibt?

5.1.12 Wie gelangen neue Bitcoin in das Netzwerk?

5.1.13 Was ist eine Bitcoin-Transaktion?

5.1.14 Sind Bitcoin-Transaktionen sicher?

5.2 Wer ist wer und was ist was in der *Bitcoin*-Welt?

5.3 Ablauf einer *Bitcoin*-Transaktion

5.3.1 Gemeinschaftsübung: *Bitcoin*-Transaktionen in Aktion

5.4 Wodurch erhält Bitcoin seinen Wert?



Die Zukunft des Geldes: Eine Einführung in Bitcoin



Sieh dir das folgende Video an:
„What is Bitcoin?
A Simple Explanation“
von 3Blue1Brown.
Du kannst jederzeit zu
den wichtigsten Stellen
zurückkehren,
da es unterteilt ist.

<https://youtu.be/bBC-nXj3Ng4>



Bitcoin ist ein revolutionäres digitales System, das sichere und transparente Finanztransaktionen ohne die Notwendigkeit einer zentralen Behörde ermöglicht.

5.0 Der geheimnisvolle Schöpfer von Bitcoin: Die Identität von Satoshi Nakamoto und sein Whitepaper

Satoshi Nakamoto ist das Pseudonym der unbekannten Person oder Gruppe von Personen, die **Bitcoin** geschaffen und die erste Blockchain-Datenbank implementiert hat.

Im Jahr 2008 veröffentlichte Satoshi ein Dokument namens „Bitcoin Whitepaper“, in dem er detailliert erklärte, was **Bitcoin** ist und wie es funktioniert. Er teilte es mit der Online-Community von Technik-Enthusiasten, die als Cypherpunks bekannt sind, und es erlangte schnell Aufmerksamkeit für seinen innovativen Ansatz für digitale Währungen.



Satoshi Nakamotos Ziel für **Bitcoin** war es, eine dezentrale digitale Währung zu schaffen, die für jeden mit einer Internetverbindung zugänglich ist, mit transparenten und fairen Transaktionen, die permanent in einem sicheren, verteilten Kassenbuch (der Blockchain) aufgezeichnet werden.

Aber hier ist der Haken: Niemand weiß, wer Satoshi Nakamoto wirklich ist. Die Identität von Satoshi bleibt bis heute ein Rätsel und macht ihn zu einer der faszinierendsten und kryptischsten Figuren in der Welt der Technologie.

- Man schätzt, dass Satoshi Nakamoto etwa eine Millionen **Bitcoin** besitzt, was ihn zu einem der reichsten Menschen der Welt machen würde, wenn seine Identität bekannt würde.
- Man geht davon aus, dass Satoshi Nakamoto japanischer Muttersprachler ist. Die ursprüngliche **Bitcoin**-Software und das Whitepaper wurden zwar in perfektem Englisch verfasst, aber einige der Kommentare im Code sind auf Japanisch geschrieben.
- Satoshi Nakamoto hat zu seiner Zeit nur ein paar hundert Forenbeiträge und E-Mails verfasst, aber die meisten sind immer noch online verfügbar, um einen Einblick in die Gedanken und Beweggründe des **Bitcoin**-Erfunders zu geben.



- Es ist auch möglich, dass es sich bei Satoshi Nakamoto um eine Gruppe von Personen und nicht nur um eine einzelne Person handelt.
 - In den Anfangstagen von *Bitcoin* war Satoshi Nakamoto in der Community recht aktiv, beantwortete Fragen und half bei der Lösung von Problemen. Allerdings verschwand er/sie 2011 plötzlich und seitdem hat man nichts mehr von ihm/ihr/ihnen gehört.
 - Über die wahre Identität von Satoshi Nakamoto wurde viel spekuliert, und im Laufe der Jahre haben mehrere Personen behauptet, der echte Satoshi zu sein. Keine dieser Behauptungen konnte jedoch schlüssig bewiesen werden.

Obwohl Satoshi der Hauptarchitekt hinter *Bitcoin* war, hat er nicht allein gearbeitet. Es gab zweifelsohne einen großen Beitrag und Unterstützung von einflussreichen Persönlichkeiten in der Technik und Kryptographie, einschließlich Wei Dai und Nick Szabo.

Obwohl er mit Herausforderungen wie technischen Problemen und Skepsis in der Gemeinschaft konfrontiert war, inspirierte seine Schöpfung die Entwicklung vieler anderer Technologien und fand breite Akzeptanz. Trotz der Kontroversen, mit denen es konfrontiert war, bleibt Bitcoin der König in der Welt der Kryptowährungen. Die letzte bekannte Nachricht von Satoshi war die Zusicherung, dass das Projekt bei dem Softwareentwickler Gavin Andresen „in guten Händen“ sei.

Verschwörungen und Mysterien um Bitcoin



Bitcoin ist die Idee einer mysteriösen unbekannten Person oder Gruppe, bekannt als „**Satoshi Nakamoto**“. Bis heute weiß niemand, wer die Person(en) hinter **Bitcoin** ist (sind).

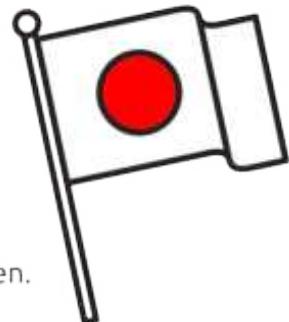
Auf Japanisch

- „*Satoshi*“ bedeutet übersetzt „klar denkend; schlagfertig; weise“.
 - „*Naka*“ kann „innen“ oder „Beziehung“ bedeuten.
 - „*Moto*“ wird definiert als „der Ursprung; die Ursache; das Fundament; die Basis“.

Aus diesem Grund glauben einige, dass die Übersetzung darauf hinweist, dass **Bitcoin** von der CIA (Central Intelligence Agency) geschaffen wurde.

Weitere Verschwörungstheoretiker
glauben, dass vier Unternehmen
dahinter stecken:

Satoshi = Samsung & Toshiba
Nakamoto = Nakamichi & Motorola



Die Zukunft des Geldes: Eine Einführung in Bitcoin

5.1 Erläuterung von Bitcoin und Bitcoin in diesem Buch

Am 17. Mai 2010 fand der erste bekannte Tausch von **Bitcoin** gegen Waren statt. Lazlo Hanyecz kaufte zwei Pizzen für 10.000 BTC. Wie hat er das gemacht?

Im Großen und Ganzen ähnelt **Bitcoin** dem traditionellen Geld, aber man kann es nicht anfassen und es existiert nur im Internet.

Um **Bitcoin** zu verwenden, muss man ein Programm auf seinen Computer herunterladen. Wenn man das Programm ausführt, stellt es eine Verbindung zu anderen Computern her, auf denen das Programm ebenfalls läuft. Sie teilen eine Datei, die Blockchain genannt wird und eine große Liste aller jemals getätigten **Bitcoin**-Transaktionen ist.

5.1.1 Was ist Bitcoin? Was ist Bitcoin?



Bitcoin (orange): Es ist das digitale Bargeld, das über das **Bitcoin-Netzwerk** läuft.

Es handelt sich um eine Währung, mit der man online Zahlungen senden und empfangen kann. Sie wird „digital“ genannt, weil **Bitcoin** im Gegensatz zu traditionellen Währungen wie dem US-Dollar oder dem Euro, die physische Währungen sind, die man in der Hand halten kann, nur über das Internet verwendet werden kann.

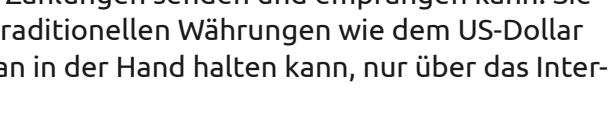


Bitcoin (violett): Es ist alles andere; das System, das Netzwerk, die Software, die Regeln, die Gemeinschaft... Satoshis Schöpfung.

Das **Bitcoin-Netzwerk** besteht aus Computern aus der ganzen Welt, die zusammenarbeiten, um Transaktionen zu verarbeiten und zu überprüfen. Diese Transaktionen werden in der Blockchain registriert.

Die **Regeln** für die Nutzung von **Bitcoin** sind in der Software implementiert, mit der das **Bitcoin-Netzwerk** betrieben wird. Sie werden von allen Teilnehmern des Netzwerks anerkannt und sind so gestaltet, dass jeder **Bitcoin** auf faire und vorhersehbare Weise nutzt.

Die Gemeinschaft der Menschen, die **Bitcoin** nutzen und unterstützen, besteht aus Einzelpersonen, Unternehmen und Organisationen auf der ganzen Welt. Sie sind diejenigen, die das Netzwerk funktionsfähig halten, indem sie die Währung nutzen und unterstützen, die Software ausführen, mit der das Netzwerk betrieben wird, und zur Entwicklung des Netzwerks beitragen.

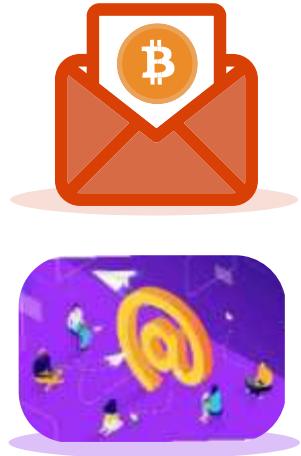




Kapitel 5

5.1.2 Was ist der Unterschied zwischen **Bitcoin** und **Bitcoin**?

Eine Möglichkeit, die Beziehung zwischen **Bitcoin** und dem **Bitcoin-Netzwerk** zu betrachten, ist die Beziehung zwischen einer E-Mail und dem Internet. So wie eine E-Mail eine Nachricht ist, die über das Internet gesendet und empfangen wird, ist **Bitcoin** eine digitale Währung, die über das **Bitcoin-Netzwerk** übertragen und empfangen wird. Das Internet bietet die Infrastruktur für das Senden und Empfangen von E-Mails, während das **Bitcoin-Netzwerk** die Infrastruktur für die Übertragung und den Empfang von **Bitcoin** bereitstellt.



5.1.3 Warum mit **Bitcoin** beschäftigen, wenn man es sich nicht leisten kann?

Hast du schon einmal darüber nachgedacht, **Bitcoin** zu benutzen, wurdest aber durch den hohen Preis einer ganzen Einheit abgeschreckt? Keine Sorge, du bist nicht allein! Die gute Nachricht ist, dass du für die Nutzung nicht gleich einen ganzen **Bitcoin** kaufen musst. Genauso wie du einen Bruchteil eines Dollars durch Münzen erhälst, kannst du auch einen Bruchteil eines **Bitcoin** kaufen. Ein **Bitcoin** ist in 100 Millionen Einheiten, **Satoshis** genannt, teilbar, sodass du jede beliebige Menge **Bitcoin** kaufen kannst, sogar eine kleine Menge. Jetzt, da du weißt, dass du **Bitcoin** im Wert von nur 1 Cent kaufen kannst, lass uns die Möglichkeiten dieser digitalen Währung erkunden!

Satoshi	Bitcoin
1	0,00000001
10	0,00000010
100	0,00000100
1000	0,00001000
10000	0,00010000
100000	0,00100000
1000000	0,01000000
10000000	0,10000000
100000000	1,00000000



Das Symbol für **Bitcoin** ist **BTC** oder **฿**, ähnlich wie ein Dollar USD oder **\$** ist, und die Abkürzung für **Satoshis** ist **Sats**.

Die Umrechnung ist **1 BTC = 100.000.000 Sats**.

- Nehmen wir zum Beispiel an, du möchtest einen Apfel kaufen, der 1,40 Dollar kostet, hast aber nur **0,00008 Bitcoin**. Lass dich von dem kleinen Betrag nicht abschrecken! Wenn du den Laden nach dem Bezahlen verlässt und deinen Kontostand auf deinem Handy überprüfst, wirst du höchstwahrscheinlich feststellen, dass du noch ein paar Sats übrig hast.

5.1.4 Woraus besteht **Bitcoin**?

- Nichts, was man physisch anfassen kann, wie eine Banknote oder einen Dollarschein. Es sind digitale Währungseinheiten, die im **Bitcoin-Netzwerk** als Eigentumsnachweis existieren.

Die Zukunft des Geldes: Eine Einführung in Bitcoin

- So wie jede Dollarnote ihre eigene EINZIGARTIGE Seriennummer hat, die zur Identifizierung und zum Schutz vor Fälschungen verwendet wird, und jede Person ihre eigene ID hat, entspricht jede **Bitcoin**-Transaktion einem einzigartigen **Bitcoin**- „Fingerabdruck“, der dabei hilft, den **Bitcoin** und seine Transaktionsgeschichte zu identifizieren.



= 79054025255fb1a2

Seriennummer: Es handelt sich um eine einzigartige Kombination aus elf Zahlen und Buchstaben, die zweimal auf der Vorderseite der Banknote erscheint. Jede Banknote hat eine eindeutige Seriennummer.

Bitcoin-Transaktion: Jede **Bitcoin**-Transaktion hat einen einzigartigen digitalen Fingerabdruck.

- Im heutigen virtuellen Zeitalter ist es möglich, dass Dinge real und wertvoll sind, auch wenn sie keine physische Form haben.

5.1.5 Warum ist **Bitcoin** gutes Geld?

Eigenschaft	Warum Bitcoin gutes Geld ist.
langlebig	Es handelt sich um eine digitale Währung, die nicht der physischen Abnutzung ausgesetzt ist – wie Gold.
transportabel	Es kann leicht gespeichert und digital übertragen werden, sodass man es bequem überallhin mitnehmen kann – wie Bargeld, nur besser.
einheitlich	Alle Bitcoin sind gleich viel wert, unabhängig davon, wo sie verwendet werden oder wer sie besitzt – wie Bargeld, nur besser.
akzeptiert	Jeden Tag akzeptieren mehr Menschen auf der ganzen Welt Bitcoin als Zahlungsmittel – wie Bargeld, nur besser.
knapp	Der Gesamtvorrat an Bitcoin ist begrenzt, nicht mal 21.000.000 um genau zu sein, was ihn wertvoll und begehrswert macht – wie Gold, nur besser.
teilbar	Es kann in kleinere Einheiten, Satoshis genannt, unterteilt werden, was kleinere Transaktionen ermöglicht. Theoretisch ist ein Bitcoin , da es digital ist, unendlich teilbar – wie Bargeld, nur besser.

5.1.6 Was geht mich das an?

Schnellere und günstigere Zahlungen	Man kann innerhalb von Minuten Geld in die ganze Welt senden, und das zu extrem niedrigen Gebühren.	Finanzielle Inklusion	2,5 Milliarden Menschen ohne Bankverbindung sind in der Lage, über ein Telefon oder einen Computer Zugang zu Geld zu bekommen.	Mehr Privatsphäre	Bitcoin -Transaktionen sind öffentlich, aber deine Identität ist es nicht.	Blockchain-Technologie	Die Technologie hinter Bitcoin wird die Zukunft vieler verschiedener Branchen bestimmen.
-------------------------------------	---	-----------------------	--	-------------------	---	------------------------	---



5.1.7 Wie BENUTZT man Bitcoin?

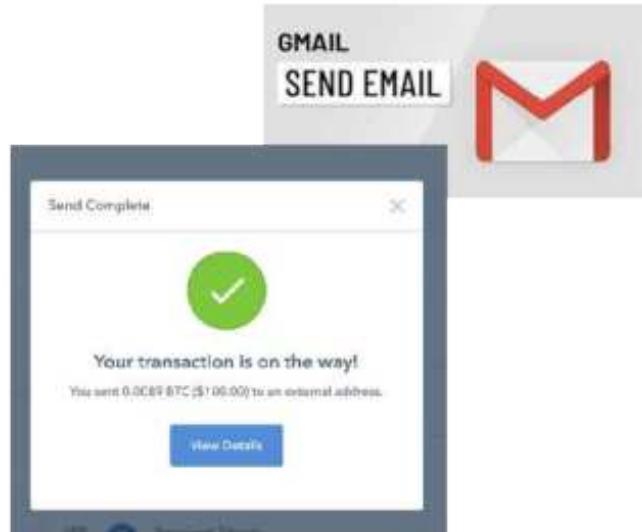
Um **Bitcoin** zu benutzen, musst du eine digitale Brieftasche (Wallet) auf deinem Computer oder Telefon einrichten. Du kannst deine Wallet verwenden, um **Bitcoin** zu verwahren, zu senden oder von anderen Personen zu empfangen, oder sogar, um Dinge online zu kaufen.

5.1.8 Wie kann man Bitcoin VERSENDEN oder AUSGEBEN?

Alles, was du brauchst, ist eine Internetverbindung.

- **Der Vorgang des Versendens von Bitcoin**

ist genauso wie das Versenden einer E-Mail. Um eine E-Mail zu senden, öffnest du dein E-Mail-Programm, gibst die E-Mail-Adresse des Empfängers ein, schreibst eine Nachricht und klickst auf Senden. Um **Bitcoin** an jemanden zu senden oder **Bitcoin** auszugeben, wenn du etwas im Tausch kaufst, öffnest du deine **Bitcoin**-Wallet, gibst die **Bitcoin**-Adresse des Empfängers ein, gibst den **Bitcoin**-Betrag ein, den du senden (oder ausgeben) möchtest, und klickst auf Senden.



5.1.9 Wie ERHÄLT man Bitcoin?

Um **Bitcoin** zu erhalten, kannst du sie entweder online kaufen, sie als Geschenk von jemandem oder als Bezahlung für Waren oder Dienstleistungen annehmen oder sie mit Hilfe eines Computers „schürfen bzw. minen“ (hart für sie arbeiten). Sobald du sie erhalten hast, speicherst du sie (bzw. den Zugang zu ihnen) in einer „Wallet“.

5.1.10 Kann Bitcoin abgeschaltet werden?

Regierungen können versuchen, den Menschen die Nutzung von **Bitcoin** zu erschweren, aber es ist schwierig, das Netzwerk komplett abzuschalten. Das liegt daran, dass **Bitcoin** dezentralisiert ist, was bedeutet, dass es keine zentrale Firma oder Organisation gibt, die es kontrolliert. Stattdessen ist die Software quelloffen, was bedeutet, dass jeder die Software herunterladen, verwenden und auf seinem eigenen Computer ausführen kann.

Regierungen können versuchen, den Zugang zu **Bitcoin** zu beschränken, aber das ist ähnlich wie die Art und Weise, wie Regierungen versuchen, den Zugang zum Internet zu kontrollieren. Menschen können Tools wie VPNs verwenden, um diese Beschränkungen zu umgehen. Außerdem kann **Bitcoin** aufgrund seiner digitalen Natur relativ leicht versteckt werden. Für Regierungen ist es viel schwieriger, **Bitcoin** ausfindig zu machen und zu beschlagnahmen, als physische Vermögenswerte wie Gold oder Immobilien zu finden und zu beschlagnahmen.

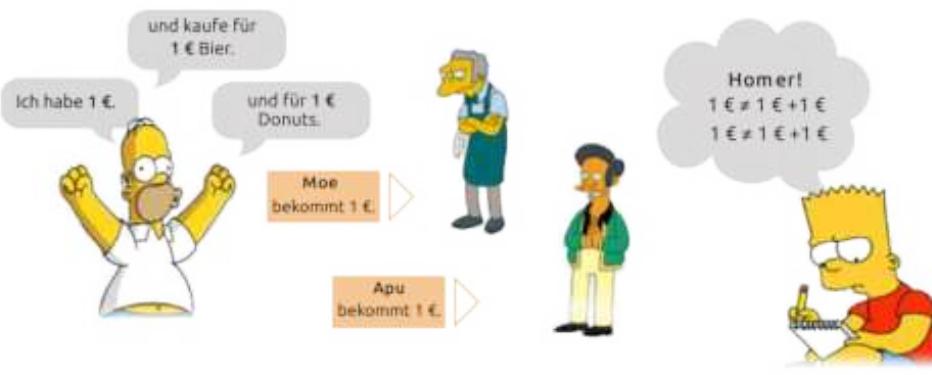
Obwohl es in einigen Ländern illegal ist, haben die Menschen weiterhin Zugang zum **Bitcoin-Netzwerk**. Darüber hinaus haben einige Länder versucht, **Bitcoin** zu kontrollieren, indem sie ihre eigenen digitalen Zentralbankwährungen geschaffen haben, was zu unterschiedlichen Ergebnissen führen könnte. Einige Menschen könnten das neue zentralisierte System akzeptieren und sich daran anpassen, während andere es ablehnen und eher dezentralisierte Lösungen wie **Bitcoin** weiter nutzen könnten.

Die Zukunft des Geldes: Eine Einführung in Bitcoin

5.1.11 Wie behält die Blockchain den Überblick darüber, wer welche Bitcoin ausgibt?

Man kann einen Dollarschein nicht zweimal ausgeben. **Bitcoin** stellt auf ähnliche Weise sicher, dass man dieselbe digitale Münze nicht zweimal ausgeben kann.

Vor **Bitcoin** war es möglich, Transaktionen über ein Netzwerk von Computern zu senden, aber es gab ein Problem: Leute konnten widersprüchliche Transaktionen senden, z. B. indem sie versuchten, dieselbe Münze zweimal auszugeben. Das nennt man „Doppelausgabe“.



Bitcoin löst dieses Problem, indem es alle Computer im Netzwerk zusammenarbeiten lässt. Wenn eine neue Transaktion gesendet wird, wird sie an alle Computer gesendet, die sie im Speicher halten, bevor sie sie in eine permanente Datei (die Blockchain) schreiben.

Dieser Prozess wird „Mining“ genannt und stellt sicher, dass keine doppelt ausgegebenen Transaktionen in die Datei geschrieben werden. Es ist wie ein großer Wettbewerb, bei dem niemand betrügen kann, sodass deine **Bitcoin** immer sicher sind.

So erreicht **Bitcoin** einen Konsens, ohne dass ein einziger Faustschlag erfolgt!

In regelmäßigen Abständen fügt einer der Computer alle Transaktionen, die er im Speicher hat, der Datei hinzu. Dann teilt er die aktualisierte Datei mit allen anderen Computern im Netz. Alle Computer einigen sich darauf, welche Transaktionen gültig sind und welche nicht, und entfernen alle widersprüchlichen Transaktionen aus ihrem Speicher.

5.1.12 Wie gelangen neue Bitcoin in das Netzwerk?

Um Miner für ihre harte Arbeit zu bezahlen oder zu belohnen, werden sie jedes Mal, wenn sie einen neuen Block zur Blockchain hinzufügen, mit neu geprägten **Bitcoin** entschädigt. Derzeit erhalten Miner 6,25 BTC für jeden Block, den sie minen.

5.1.13 Was ist eine Bitcoin-Transaktion?

Eine **Bitcoin**-Transaktion ist eine Übertragung des Eigentums an bestehenden **Bitcoin**-Einheiten auf einen neuen Eigentümer. Doch anstatt tatsächliche Münzen zu übertragen, aktualisieren alle Nodes im Netzwerk ihre lokale Kopie des öffentlichen Kassenbuchs, um die Änderung der Eigentumsverhältnisse widerzuspiegeln. (Erinnere dich an die Rai-Steine! Dies ist nur eine fortschrittlichere Version, bei der das Kassenbuch externalisiert und nicht im Gedächtnis behalten wird, sodass es von jedem eingesehen werden kann).



- Mark und Tobi wollen 1 BTC austauschen. Um dies zu verstehen, ist es wichtig zu wissen, dass es bei **Bitcoin** keine physischen Münzen gibt, sondern nur Aktualisierungen der Blockchain, die dann in den Wallets der beiden beteiligten Parteien auftauchen.
- Wenn Mark 1 BTC an Tobi senden will, nennt man das eine Peer-to-Peer-Transaktion, weil der Wert direkt von Mark an Tobi geht. Aber Tobi erhält nicht wirklich eine „digitale Münze“ von Mark. Stattdessen aktualisieren alle Nodes im Netzwerk ihre lokale Kopie des öffentlichen Kassenbuchs, wodurch das Eigentum an dem **Bitcoin** von Marks Adresse auf Tobis Adresse übergeht.
- Eine **Bitcoin**-Transaktion ist einfach eine signierte Nachricht, die Mark an das Netzwerk sendet und die dann von vielen Nodes validiert wird. Die Nachricht durchläuft mehrere Schritte, z. B. wird sie von einigen der Full-Nodes aufgegriffen, validiert und dann weitergegeben, bis alle Nodes im Netzwerk sie unabhängig voneinander validiert haben.



Die Signatur ist eine digitale Darstellung der Transaktionsdetails, einschließlich des gesendeten **Bitcoin**-Betriebs, der Adresse des Absenders (Mark) und der Adresse des Empfängers (Tobi).



Zweck der digitalen Signatur



Eine Signatur bestätigt, dass die Nachricht (Dokument oder E-Mail) vom Absender stammt und NICHT verändert wurde.

Stell dir vor, dass alle existierenden **Bitcoin** in digitalen Tresoren aufbewahrt werden, jeder mit einer anderen Menge an BTC und einer Geschichte, wie sie dorthin gekommen sind. Jeder Tresor hat einen Besitzer. Deshalb muss er mit einer Adresse identifizierbar sein. Adressen werden durch ein digitales Schloss mit zwei verschiedenen Schlüsseln geschützt, wie Passwörter für ein Konto. Wenn ein Tresor **Bitcoin** enthält, kann sein Besitzer ihn mit seinem privaten Schlüssel öffnen und eine beliebige Menge **Bitcoin** auf einen anderen Tresor übertragen.

Aus der Sicht von Tobi: Um den **Bitcoin** zu erhalten, muss er dem Absender (Mark) seine Adresse mitteilen, wo der **Bitcoin** eingezahlt werden kann.

Aus Marks Sicht: Um seinen **Bitcoin** auszugeben, muss er auf seinen privaten Schlüssel zugreifen, damit er freigeschaltet werden kann.

Die Zukunft des Geldes: Eine Einführung in Bitcoin

5.1.14 Sind Bitcoin-Transaktionen sicher?

Die Transaktionsdetails, wie die Adressen von Absender und Empfänger und der überwiesene Betrag, sind auf der Blockchain öffentlich einsehbar, aber das Eigentum an den übertragenen **Bitcoin** wird durch den Einsatz von Kryptographie verifiziert.

Was ist Kryptographie?



Kryptographie ist eine Methode, Informationen geheim zu halten, indem man sie in einem Code versteckt.



- Bei der Verschlüsselung werden Informationen in einen speziellen Code eingebettet, so dass sie ohne die richtige Entschlüsselungsmethode für niemanden lesbar sind. Dies ist vergleichbar mit dem Verschließen eines Tresors, den nur die Person mit dem richtigen Schlüssel oder der richtigen Kombination öffnen kann.
- Bei der Entschlüsselung hingegen werden die verschlüsselten Informationen wieder lesbar gemacht, so als würde man einen Tresor aufschließen und die darin enthaltenen Informationen lesen können.

Nehmen wir zum Beispiel an, Roman und Tom wollen eine Nachricht vor jemandem namens Moritz verstecken. Sie vereinbaren, einen geheimen Schlüssel zu verwenden, um die Nachricht zu verschlüsseln, bevor sie sie sich gegenseitig schicken. Sie könnten eine einfache Methode verwenden, wie z. B. jeden Buchstaben der Nachricht im Alphabet nach unten zu verschieben, sodass A zu B wird, B zu C, und so weiter. Nur wer den Schlüssel hat, kann die Nachricht entschlüsseln, sodass sie für Moritz unlesbar wird. Obwohl diese Methode heute nicht als sicher gilt, veranschaulicht sie das Prinzip der Kryptographie mit privaten Schlüsseln.

Wie löst man das Freimaurer-Alphabet

Beim Lösen des Freimaurer-Alphabets erhält der Spieler eine verschlüsselte Nachricht und eine Chiffre. Um die Nachricht zu entschlüsseln, muss der Spieler das Symbol der verschlüsselten Nachricht auf der Chiffre finden, um dann den entschlüsselten Buchstaben zu finden.

- Beispiel einer verschlüsselten Nachricht:



A	B	C	J	K	L	S	T	U	W	X	Y	Z
D	E	F	M	N	O							
G	H	I	P	Q	R							



Wie funktioniert die Kryptographie bei Bitcoin-Transaktionen?

Bei der herkömmlichen Kryptographie mit privaten Schlüsseln müssten Tom und Roman zunächst einen geheimen Schlüssel, z. B. ein Passwort, austauschen. Tom würde dann diesen Schlüssel verwenden, um seine Nachricht zu verschlüsseln, bevor er sie an Roman sendet. Roman, der den geheimen Schlüssel ebenfalls kennt, würde dann denselben Schlüssel verwenden, um die Nachricht zu entschlüsseln und sie zu lesen.

Moritz könnte die Nachricht jedoch auch abfangen und denselben Schlüssel verwenden, um die Nachricht zu entschlüsseln und sie zu lesen. Bei dem **Public-Key-Verschlüsselungsverfahren** (oder auch asymmetrisches Kryptosystem), das bei Bitcoin-Transaktionen verwendet wird, haben Tom und Roman jeweils zwei Schlüssel: einen **öffentlichen (Public Key)** und einen **privaten Schlüssel (Private Key)**. Tom kann den **öffentlichen Schlüssel** von Roman verwenden, um seine eigene Nachricht zu verschlüsseln, bevor er sie (an Tom) sendet. Nur Toms **privater Schlüssel** kann die Nachricht entschlüsseln. Moritz, der Toms **privaten Schlüssel** nicht hat, könnte die Nachricht nicht lesen, selbst wenn er sie abfängt.

Neben der Verschlüsselung von Nachrichten kann die Public-Key-Kryptographie auch für **digitale Signaturen** verwendet werden. Eine digitale Signatur ist eine Möglichkeit, die Authentizität einer Nachricht zu beweisen, ähnlich wie eine schriftliche Unterschrift auf einem physischen Dokument. Um eine digitale Signatur zu erstellen, würde Tom **seinen privaten Schlüssel** verwenden, um **seine Signatur zu verschlüsseln**. Roman verwendet dann Toms **öffentlichen Schlüssel**, um sie zu entschlüsseln und zu überprüfen, ob sie tatsächlich von Tom gesendet wurde.

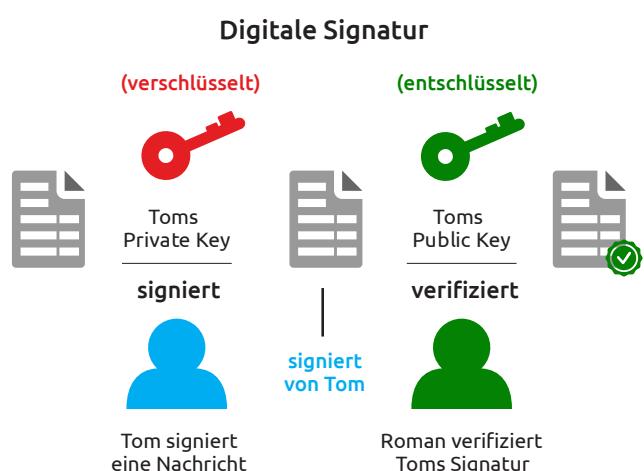
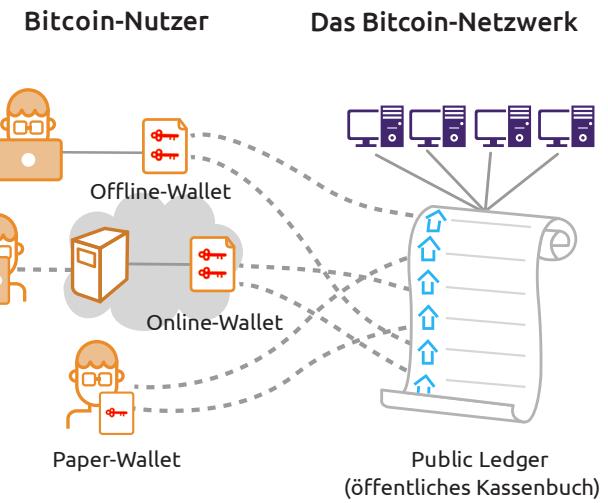


Public-Key-Verschlüsselungsverfahren (für jede Transaktion zwischen zwei Benutzern):

Jeder Nutzer hat zwei Schlüssel: einen **privaten Schlüssel**, der geheim gehalten wird, und einen **öffentlichen Schlüssel**, der **mit anderen geteilt** werden kann.

Der **private Schlüssel** dient als eine Art Identifikation und Eigentumsnachweis, der bestätigt: „**Diese Adresse gehört mir und ich habe die Kontrolle darüber.**“

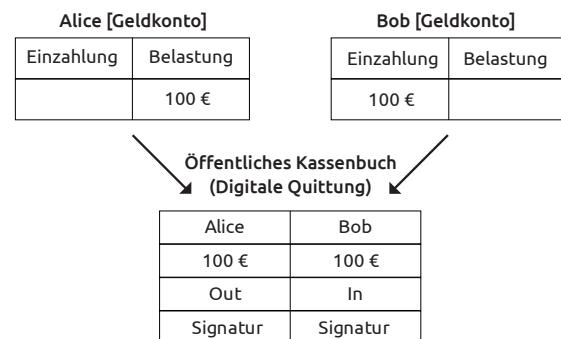
Digitale Signaturen werden erstellt, um die einzelnen Transaktionen zu identifizieren.



Die Zukunft des Geldes: Eine Einführung in Bitcoin

Der Hauptvorteil der Public-Key-Kryptographie gegenüber der Private-Key-Kryptographie besteht also darin, dass sie eine sichere Kommunikation ermöglicht, ohne dass Sender und Empfänger zunächst einen geheimen Schlüssel austauschen müssen, der von einer dritten Partei abgefangen werden könnte.

- Bei **Bitcoin**-Transaktionen wird ein bestimmter **Bitcoin**-Betrag direkt auf das Konto einer anderen Person überwiesen.
 - Du würdest nicht wollen, dass jemand einfach das Geld stiehlt, das dir dein Freund über Venmo geschickt hat, weil die Zahlungsmethode unsicher ist, oder?
- Die Verschlüsselung ist eine Möglichkeit, wichtige Informationen auf ihrem Weg durch das Netz vor böswilligen Akteuren zu schützen, von denen einige, wie z. B. Hacker, die Gelder stattdessen auf ihr Konto umleiten könnten.
- Um die **Transaktionsdetails** bei **Bitcoin** sicher und geschützt zu halten, wird als zusätzliche Schutzmaßnahme jeder Transaktion eine **EINZIGARTIGE Signatur** hinzugefügt. Diese Signatur wirkt wie ein Geheimcode, der sicherstellt, dass niemand einen Teil der Transaktion ändern kann, ohne dass die Software dies erkennt und als ungültig markiert.



Vergleich von **Bitcoin**-Transaktionen mit traditionellen Bankgeschäften

- Im traditionellen Bankwesen wird eine PIN zur **Authentifizierung** von Transaktionen verwendet, ähnlich wie ein **privater Schlüssel** verwendet wird, um Transaktionen in Blockchains zu **signieren**.

Eine einfache Analogie für diesen Prozess wäre eine Person, die ihre Bankkontonummer mit einem privaten Pin (privater Schlüssel) abruft und dann ihre eigene persönliche Unterschrift (einzigartige Signatur) auf einem Online-Scheck (digitale Währung) verwendet, um einer anderen Person (einem anderen Nutzer) Geld zu senden (eine Transaktion durchzuführen). So wie die Unterschrift einer Person auf einem Scheck ihre Identität bestätigt und die Transaktion autorisiert, bestätigt die digitale Unterschrift mit einem privaten Schlüssel die Identität und autorisiert die Transaktion der digitalen Währung.





5.2 Wer ist wer und was ist was in der Bitcoin-Welt?

Die Schlüsselrollen im Netzwerk

Es gibt drei Haupttypen von Teilnehmern im *Bitcoin-Netzwerk*:

- 1 *Miner* sind Computer im *Bitcoin-Netzwerk*, die neue Transaktionen in die Blockchain schreiben und verifizieren, indem sie neue Blöcke an die Blockchain anhängen. Miner werden mit *Bitcoin* für ihre Arbeit belohnt!
- 2 *Nodes* sind Computer im *Bitcoin-Netzwerk*, die Blockchain-Transaktionen und Blöcke speichern und verifizieren. Nodes werden nicht für ihre Arbeit belohnt.
- 3 Die *Entwickler* sind für die Wartung und Verbesserung der *Bitcoin*-Software (d. h. des Codes) verantwortlich. Sie stellen sicher, dass jeder Computer im Netzwerk die Regeln befolgt und reibungslos funktioniert.

Insgesamt arbeiten diese drei Gruppen zusammen, um das *Bitcoin-Netzwerk* am Laufen zu halten und sicherzustellen, dass es sicher und dezentralisiert bleibt.

- Nutzer sind normale Personen, die Bitcoin verwenden. Sie senden und empfangen *Bitcoin* über ihre *Wallets* und können auch Käufe tätigen oder *Bitcoin* in andere Währungen umtauschen.
- Börsen ermöglichen es den Nutzern, *Bitcoin* zu kaufen, zu verkaufen und zu handeln, und erleichtern Transaktionen im Netzwerk. Allerdings spielen die Börsen keine direkte Rolle beim Betrieb des *Bitcoin-Netzwerks* selbst.

Immer noch ein wenig verwirrt? Die Hauptakteure werden erneut vorgestellt, wobei wir unsere Analogie verwenden, in der das *Bitcoin-Netzwerks* mit einem Transportsystem verglichen wird.

- Die Miner sind wie *automatische Mautstellen* oder *Buchhalter*.

- Sie sind für die Buchhaltung zuständig. Sie registrieren jedes Auto, das vorbeifährt, und erheben Gebühren. Sie überprüfen auch, ob die vorbeifahrenden Autos (Bitcoin-Transaktionen) nicht gestohlen sind, abgelaufene Nummernschilder haben oder von Fahrern ohne Lizenz oder betrunken gefahren werden.
- Dieses Verfahren trägt dazu bei, dass das Autobahnssystem (*Bitcoin-Netzwerk*) sicher und effizient ist, und hilft, Kollisionen oder Betrug zu verhindern.



Die Zukunft des Geldes: Eine Einführung in Bitcoin

- Nodes kann man sich als *Raststätten* entlang der Straßen vorstellen.
 - So wie ein Rastplatz ein Ort ist, an dem man anhalten, etwas essen oder eine Toilette benutzen kann, ist ein Node in einem Blockchain-Netzwerk ein Punkt, an dem Transaktionen verarbeitet, validiert und gespeichert werden.
 - Genauso wie Raststätten über Ruhezonen und Parkplätze verfügen, haben Nodes ihre eigenen Warteräume (mempool), in denen verifizierte Transaktionen verweilen können, bevor sie auf der Blockchain weitergeführt werden.
 - Raststätten erheben keine Gebühren für deinen Aufenthalt oder die Nutzung des Standortes.
-
- Entwickler sind wie die *Ingenieure*, die das Straßennetz planen und bauen.
 - Sie sind für die Wartung und Verbesserung der Infrastruktur des Netzes zuständig, z. B. für die Behebung von Problemen oder das Hinzufügen neuer Funktionen.



Eine Bitcoin-Wallet ist wie eine *Garage* für dein Auto. So wie eine Garage ein sicherer Ort ist, an dem du dein Auto aufbewahrst, wenn es nicht in Gebrauch ist, ist eine *Bitcoin-Wallet* ein sicherer Ort, an dem du deine *Bitcoin* aufbewahrst.





- Nehmen wir an, du besitzt ein **Auto** (einen **Bitcoin**) und möchtest es sicher aufbewahren, wenn du es nicht fährst. Du kannst es in deine **Garage** stellen (eine Bitcoin-Wallet) und die **Tür abschließen** (deine Wallet mit einem Passwort sichern). So ist dein Auto (**Bitcoin**) vor Dieben (Hackern) geschützt. Wenn du dein Auto benutzen willst (dein Bitcoin ausgeben willst), kannst du das Garagentor öffnen und deine Wallet mit einem anderen Passwort entsperren, das benötigt wird, um **das Auto zu starten** und **aus der Garage zu fahren** (eine Transaktion durchzuführen).



Börsen kann man sich wie **Autohäuser** vorstellen. So wie man in einem Autohaus Autos kaufen und verkaufen kann, kann man an einer Börse **Bitcoin** kaufen und verkaufen.

- Wenn du zum Beispiel dein Auto (**Bitcoin**) verkaufen willst, kannst du es zu einem Händler (Börse) bringen, der dir hilft, einen Käufer zu finden.

Betrachten wir **Bitcoin** wie einen Autoverkauf:

Stell dir vor, du, der Nutzer, hast einen wertvollen Vermögenswert, z. B. einen **Bitcoin**, den du verkaufen möchtest. Du bringst ihn zu einer Börse, ähnlich einem Autohaus, um einen Käufer zu finden. Auf dem Weg dorthin passierst du die Nodes des Netzwerks, ähnlich wie bei einer Werkstatt, um sicherzustellen, dass sich dein Vermögenswert vor dem Verkauf in optimalem Zustand befindet. Die Transaktion durchläuft dann einen strengen Überprüfungsprozess mit der Finanzabteilung der Börse, ähnlich den Buchhaltern in einem Autohaus, um sicherzustellen, dass alles korrekt ist und der Verkauf reibungslos abläuft. Sobald der Verkauf abgeschlossen ist, erhältst du die Zahlung in Fiat-Währung, und die Börse nimmt den Vermögenswert in Besitz und überträgt ihn auf ihre Geldbörse. Das Netzwerk verfügt auch über ein Team von Entwicklern, ähnlich wie Ingenieure in einem Autohaus, die an der Verbesserung und Aktualisierung der Funktionen und Technologie von **Bitcoin** arbeiten. Andere Teilnehmer des Netzwerks, wie Händler und Investoren, spielen ebenfalls eine Rolle für das Funktionieren des **Bitcoin-Netzwerk**.

5.3 Ablauf einer **Bitcoin**-Transaktion

Neue **Bitcoin**-Transaktionen werden von Wallets auf der ganzen Welt initiiert, aber es gibt keine zentrale Zahlungsabwicklung. Stattdessen konkurrieren **Miner** auf der ganzen Welt um die **Aufzeichnung** von Transaktionen im Kassenbuch.

Nehmen wir an, Tim schuldet Lena **0,5 BTC** und ist bereit, ihr diese zurückzuzahlen. Beide haben digitale Wallets.

1. Lena gibt ihre **Adresse** an Tim weiter.
2. Tim benutzt seine Wallet-Software, um die Transaktion zu erstellen, die Lenas Adresse, den zu überweisenden Betrag (0,5 BTC) und eine Gebühr für den Miner enthält.

Die Zukunft des Geldes: Eine Einführung in Bitcoin



Wenn Tim auf „Senden“ klickt, verwendet seine Wallet seinen privaten Schlüssel, um 0,5 BTC freizuschalten, denn so „signiert“ er die Transaktion. Allerdings gibt er seinen privaten Schlüssel nicht preis.

- Damit teilt Tim dem Netzwerk mit: „Ich bin der Besitzer dieses Kontos und genehmige den Transfer von 0,5 **Bitcoin** auf Lenas Konto.“

KASSENBUCH (LEDGER)	
Kontoinhaber	Wert
Stefan	2,50
Adam	3,00
Michael	6,00
Tim	1,50
Robert	2,00
Lena	1,75
Daniel	5,25

Bitcoin-Transaktionsanfrage-Nachricht
Tim sendet 0,50 BTC an Lena
Tim → Lena 0,50 BTC

KASSENBUCH (LEDGER)	
Kontoinhaber	Wert
Stefan	2,50
Adam	3,00
Michael	6,00
Tim	1,00
Robert	2,00
Lena	2,25
Daniel	5,25



3. Nachdem die Transaktion *signiert* wurde, wird sie an das Netzwerk übertragen, wo sie von Nodes, Miner genannt, überprüft wird. Die Miner prüfen die Transaktion auf ihre Gültigkeit und stellen sicher, dass Tim über genügend Geldmittel verfügt. Ist dies nicht der Fall, lehnen sie die Transaktion sofort ab.

4. Sobald die Transaktion verifiziert und in einen Block aufgenommen wurde, wird sie der Blockchain hinzugefügt, und das Geld wird an Lenas Adresse überwiesen.

5. Lena kann dann ihren privaten Schlüssel verwenden, um auf das überwiesene Geld in ihrer Wallet zuzugreifen.

Es ist wichtig zu wissen, dass die Transaktion nicht mehr rückgängig gemacht werden kann, sobald sie abgeschlossen wurde.

Nun zu den Details

Nachdem er seine digitale Wallet geöffnet hat, leitet Tim über seine eigene Adresse die Transaktion ein, indem er Lenas Bitcoin-Adresse (ähnlich wie eine Bankleitzahl bei einer herkömmlichen Überweisung) und den zu überweisenden **Bitcoin**-Betrag anfordert und angibt. Tim signiert die Transaktion mit seinem privaten Schlüssel (ähnlich wie beim Zugriff auf ein Konto mit einem privaten Passwort), um die Überweisung zu bestätigen.

My Wallet Be Your Own Bank.

Wallet Home My Transactions Send Money Receive Money Import / Export

Total Transactions	0
Total Received	0,00 BTC
Total Sent	0,00 BTC
Final Balance	0,00 BTC

This is Your Bitcoin Address:
19emjx4vqHPn6ZTsh1ZNbBD7uFZFqWA5Cq
Share this with anyone and they can send you payments.



Bankleitzahl Kontonummer Prüfnummer



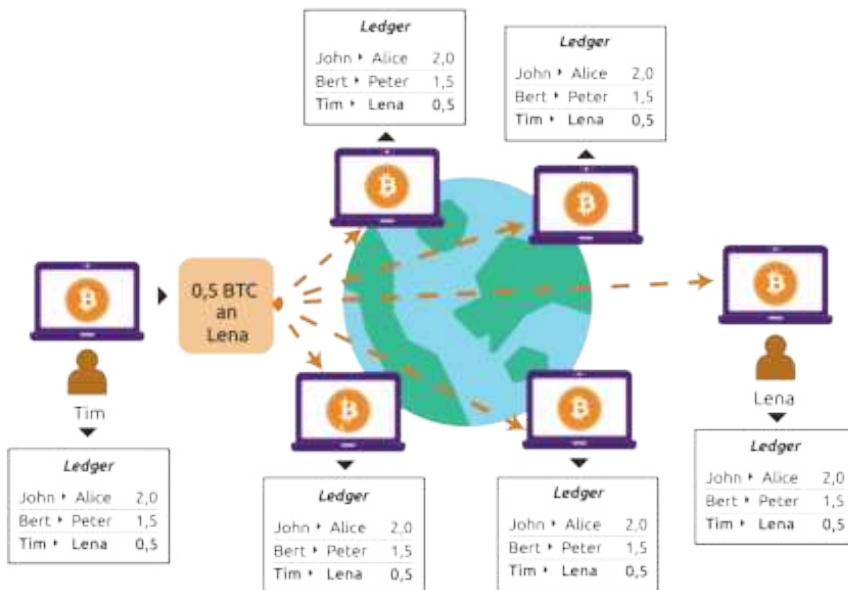
Anschließend wird die Transaktion mit nur einem Mausklick in das Netzwerk übertragen.

Eine Transaktion auf der Blockchain kann man sich wie einen Paketzustellungsprozess vorstellen. Wenn ein Paket zum ersten Mal verschickt wird, ist es nur ein Paket in **einem Postamt** (eine Transaktion, die an einen ersten Node gesendet wird). Das Postamt (Node) prüft die Echtheit des Pakets, und wenn es gültig ist, schickt es es zur weiteren Prüfung an andere Postämter (Nodes) weiter. Das Paket wird von Postamt zu Postamt weitergereicht, bis es jedes Postamt im Netzwerk (alle Nodes in der Blockchain) erreicht. Die Echtheit und Gültigkeit des Pakets wird an jeder Station bestätigt, ähnlich wie eine Transaktion von mehreren Nodes in der Blockchain überprüft wird.

- Lenas eindeutige Adresse wird mit ihrem öffentlichen Schlüssel generiert, um sicherzustellen, dass nur sie Zugang zu den Gel dern hat und diese entsperren kann, ähnlich wie bei einem Puzzle, das nur derjenige lösen kann, der die richtigen Teile hat.



Um die Authentizität der Transaktion zu verifizieren, werden eine digitale Signatur und ein öffentlicher Schlüssel verwendet.



Die digitale Signatur und der öffentliche Schlüssel sind zwei wichtige Teile des Puzzles. Der **öffentliche Schlüssel** wirkt wie ein Ausweis, der sicherstellt, dass Tim der rechtmäßige Besitzer der **Bitcoin** ist. Die **digitale Signatur** beweist, dass Tim die Transaktion autorisiert hat, so als würde er einen Scheck unterschreiben.

	handgeschriebene Unterschrift	Digitale Signatur
Konzept		Digitale Signatur mit asymmetrischer Verschlüsselungs-/Entschlüsselungs-Methode 73207079591743137199 61288414545595292784 33060039936533846924
Problem	wiederverwendbar	Wiederverwendung unmöglich



confirm
 prove
 justify
 check
 inspect
 verify
 substantiate
 clarify
 attest
 authenticate

Die Zukunft des Geldes: Eine Einführung in Bitcoin

Die Nodes im **Bitcoin-Netzwerk** sind wie **Puzzle-Prüfer**. Sie müssen überprüfen, ob alle Teile richtig zusammenpassen. Sie stellen sicher, dass Tim sowohl die **Bitcoin** besitzt als auch die Transaktion autorisiert hat.

Sobald eine Mehrheit der Nodes der Meinung ist, dass das Puzzle korrekt gelöst wurde, wird die Transaktion als legitim angesehen und in eine **Warteschlange** aufgenommen.



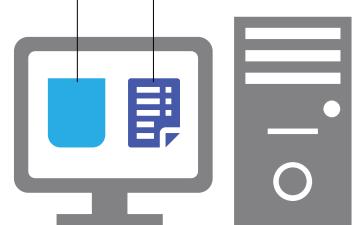
Diese Warteschlange anstehender Transaktionen wird als „**Mempool**“ bezeichnet.

Der **Mempool** ist wie ein Wartebereich für Puzzle, die korrekt gelöst wurden, aber noch nicht zum permanenten Puzzle (Blockchain) hinzugefügt (verkettet) wurden. Er befindet sich in einem anderen Bereich des Speichers eines Nodes als die Blockchain, die bestätigte Transaktionen dauerhaft aufzeichnet.

Ein Node im Bitcoin-Netzwerk

Mempool

Blockchain



Sobald Transaktionen verifiziert sind, müssen sie dauerhaft in der Blockchain gespeichert werden. Eine Gruppe von **Nodes**, die „**Miner**“ genannt werden, konkurrieren darum, sie als erste in die Blockchain aufzunehmen, um eine Belohnung zu erhalten.

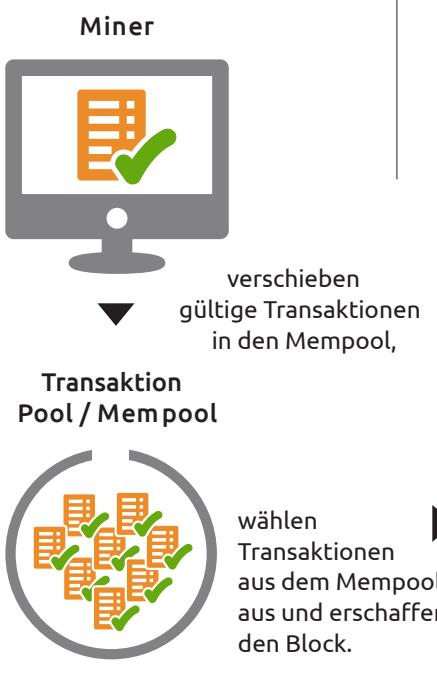
Das sind die Superhelden des **Bitcoin**: die **Miner**! Diese speziellen Computer verwenden ihre Super-Software, um zu überprüfen, dass niemand **Doppelausgaben** tätigt, stiehlt oder versehentlich Geld sendet, das er nicht hat, und sie stellen sicher, dass alle anderen Miner dasselbe tun.

- **Miner** sind wie Puzzle-Kuratoren, sie wählen aus der Warteschlange die Puzzles aus, die zur endgültigen Puzzle-Ausstellung hinzugefügt werden sollen. Dieser Prozess stellt sicher, dass dieselben **Bitcoin** nicht zweimal von derselben Person ausgegeben werden können und dass Transaktionen schnell bearbeitet werden.

Die Miner bewahren eine Kopie der Blockchain auf und vergleichen jede Transaktion mit der Blockchain, um **sicherzustellen**, dass dieselben **Bitcoin** nicht schon vorher ausgegeben wurden. Die Miner fügen der Blockchain nur legitime Transaktionen hinzu, die bestimmte Kriterien erfüllen, wie z. B. die korrekte digitale Signatur und eine ausreichende Geldmenge.

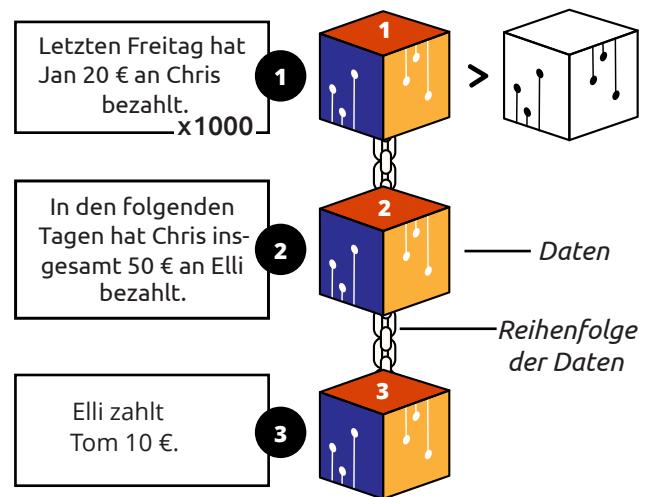


Sobald sie in der Blockchain gespeichert sind, gelten die darin enthaltenen Transaktionen als abgeschlossen und unumkehrbar. Der Austausch von **Bitcoin** von einer **Adresse** zu einer anderen ist damit abgewickelt.

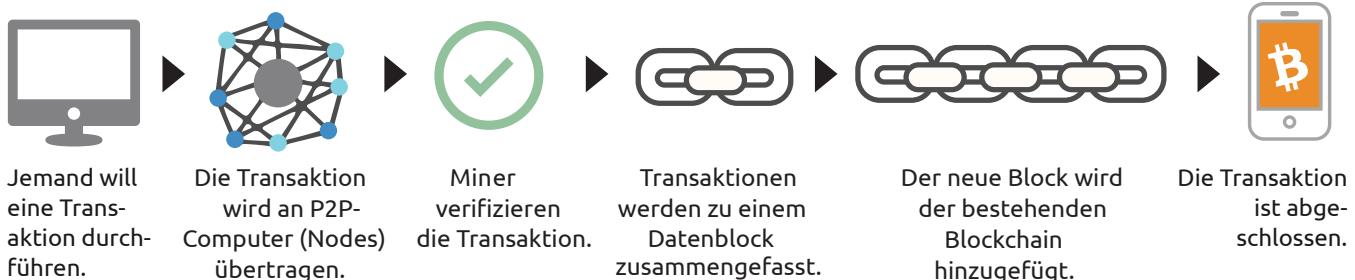


Zusammenfassend lässt sich sagen, dass bei der Nutzung von **Bitcoin** eine Transaktion erstellt, an das Netzwerk gesendet, validiert und bestätigt wird. Dieser Prozess stellt sicher, dass die Transaktion sicher ist und nicht verändert werden kann, was es den Menschen ermöglicht, dem System zu vertrauen, ohne eine zentrale Autorität zu benötigen.

Beispiel einer Transaktion auf einer Blockchain



Ablauf einer Bitcoin-Transaktion



5.3.1 Gemeinschaftsübung: Bitcoin-Transaktionen in Aktion

Miner sind für das Hinzufügen neuer Transaktionen zur Blockchain verantwortlich. Full-Nodes validieren Transaktionen und speichern eine vollständige Kopie der Blockchain. Light-Nodes ermöglichen die Validierung von Transaktionen bei geringerem Speicherbedarf und weniger Berechnungsressourcen.

Gemeinschaftsübung: Nehmen wir an, dass Sender und Empfänger Light-Nodes sind. In Wirklichkeit sind nicht alle Wallets Light-Nodes.

Verinnerliche deine Rolle! Dir wurde eine der folgenden Rollen zugewiesen: **Absender, Empfänger, Node oder Miner.**

Die Zukunft des Geldes: Eine Einführung in Bitcoin

- Die **Absender** sind für die Erstellung und Übermittlung von Transaktionen zuständig.
- Die **Empfänger** sind für den Empfang und die Überprüfung der Transaktionen zuständig.
- Die **Nodes** sind für die Validierung der Transaktionen verantwortlich, indem sie prüfen, ob die Transaktion gültig ist. Dazu überprüfen sie die Transaktion anhand der Regeln des Protokolls und des Konsensmechanismus.
- Die **Miner** sind für das Hinzufügen der Transaktionen zur Blockchain verantwortlich.

1. Als Absender: Erstelle eine Transaktion, indem du folgende Schritte durchführst:

- Schreibe die Anzahl der Geldeinheiten, die du verschicken willst, sowie den Namen oder die Initialen des Empfängers auf einen Überweisungsschein!
- Unterschreibe den Schein mit deinem Namen oder deinen Initialen, wodurch ein privater Schlüssel simuliert wird!
- Übergib den Überweisungsschein und die entsprechende Anzahl Geldeinheiten an den Empfänger!

Sowohl die Nodes als auch die Empfänger müssen die Transaktionen verifizieren:

2. Als Empfänger: Du bist für die Überprüfung der Transaktionen verantwortlich. Gehe wie folgt vor:

- Überprüfe den Transaktionsschein, um sicherzustellen, dass die richtige Anzahl von Geldeinheiten und der Name des Empfängers oder die Initialen notiert sind!
- Zähle die erhaltenen Geldeinheiten und vergleiche sie mit der Anzahl, die auf dem Schein steht!
- Wenn die Geldeinheiten übereinstimmen, mache einen Haken in das Genehmigungsfeld!
- Wenn die Einheiten nicht übereinstimmen oder du Zweifel hast, lehne die Transaktion ab!

gesendete Einheiten	Absender	Signatur des Absenders	Empfänger	Datum & Zeit	Genehmigung des Empfängers

3. Als Node: Überprüfe und validiere Transaktionen. Du bist für die Überprüfung der Gültigkeit der Transaktion zuständig.

- Vergewissere dich, dass die Adresse des Absenders und die Adresse des Empfängers gültig sind!
- Vergewissere dich, dass der Absender über genügend Geldmittel verfügt, um die Transaktion durchzuführen, und dass die Transaktion keine Einheiten doppelt ausgibt!

gesendete Einheiten	Absender	Signatur des Absenders	Empfänger	Datum & Zeit	Genehmigung des Nodes

4. Als Miner: Füge Transaktionen zur Blockchain hinzu. Du bist für das Hinzufügen der Transaktionen zur Blockchain zuständig. Befolge diese Schritte:

- Prüfe die Transaktionen, die von den Empfängern genehmigt und von den Nodes validiert wurden!



- Würfele und vergleiche die Zahlen mit denen des anderen Miners! Der Miner mit der kleineren Zahl wird die Transaktion zur Blockchain hinzufügen.
- Für deine Zeit, Energie und Mühe erhältst du eine Belohnung. Suche dir eine Süßigkeit aus.
- Sobald eine Transaktion der Blockchain hinzugefügt wurde, kann sie nicht mehr geändert oder rückgängig gemacht werden.

5. Behalte dein Guthaben im Auge: Behalte während der gesamten Aktivität dein Guthaben im Auge, indem du die Geldeinheiten in deiner digitalen Wallet zählst!

gesendete Einheiten	Absender	Signatur des Absenders	Empfänger	Datum & Zeit	Genehmigung

6. Diskutiere die gelernten Konzepte mit deiner Klasse!

5.4 Wodurch erhält Bitcoin seinen Wert?

Im Gegensatz zu traditionellen Währungen wie Gold oder Fiat-Geld ist **Bitcoin** digital, dezentralisiert und knapp. Diese Eigenschaften verleihen **Bitcoin** eine Reihe von Vorteilen gegenüber herkömmlichen Geldformen und machen es zu einem wertvollen Wertaufbewahrungsmittel und Zahlungsmittel.

Der Wert von **Bitcoin** ergibt sich aus einer Kombination von folgenden Faktoren:

- Seine Knappheit, da die Gesamtmenge an **Bitcoin**, die jemals hergestellt werden kann, auf nicht mal 21 Millionen begrenzt ist, was es von normalem Geld, das von Regierungen gedruckt werden kann, unterscheidet.
- Seine Nutzbarkeit als dezentralisierte digitale Währung, was bedeutet, dass es von keiner Regierung oder Institution kontrolliert wird und für Transaktionen überall auf der Welt verwendet werden kann.
- Der von Anlegern und Nutzern wahrgenommene Wert, da einige Menschen **Bitcoin** als gute Investition, als Möglichkeit zur Geldaufbewahrung oder als Schutz vor Inflation betrachten.

Wie hoch ist die Marktnachfrage nach Bitcoin und wie beeinflusst sie den Preis?

Die Marktnachfrage nach **Bitcoin** bezieht sich auf die Anzahl der Personen, die bereit sind, **Bitcoin** zu einem bestimmten Preis zu kaufen. Der Preis von **Bitcoin** wird durch die Marktnachfrage, das Angebot und andere wirtschaftliche Faktoren beeinflusst. Wenn die Nachfrage hoch und das Angebot begrenzt ist, steigt der Preis von **Bitcoin** tendenziell an. Umgekehrt sinkt der **Bitcoin**-Preis, wenn die Nachfrage gering ist und ein großes Angebot besteht.

Eines der Hauptargumente gegen **Bitcoin** ist, dass es nicht durch physische Vermögenswerte oder staatliche Garantien abgesichert ist, was es von Natur aus wertlos macht. Mit diesem Argument hat man jedoch die Natur des Geldes falsch verstanden.

Die Zukunft des Geldes: Eine Einführung in Bitcoin

Geld muss nicht durch Sachwerte oder staatliche Garantien abgesichert sein, um wertvoll zu sein; es muss lediglich als Zahlungsmittel und Wertaufbewahrungsmittel allgemein akzeptiert werden. **Bitcoin** erfüllt diese Kriterien und noch einige mehr.

Der praktisch unantastbare Status von **Bitcoin**, der seine Beschlagnahmung erschwert, ist ein wichtiger Faktor für seinen Wert für diejenigen, die autoritäre oder tyrannische Regime fürchten. Dieses Attribut wird von einigen als wertvoller angesehen als die physischen Eigenschaften eines Vermögenswertes.

Schließlich ist **Bitcoin** auch vielseitig verwendbar, da die zugrundeliegende Blockchain-Technologie in verschiedenen Branchen wie der Lieferkette, der digitalen Identität und anderen eingesetzt wird, was es zu einem wertvollen Gut in vielen verschiedenen Branchen macht.

- **Bitcoin** wird als Lösung für die wirtschaftlichen Probleme der Welt angesehen, da es fair, sicher und unbestechlich ist.
- **Bitcoin** wird als digitales Gold bezeichnet, und es wird erwartet, dass die Nachfrage weiter steigen wird, da immer mehr Menschen die Kontrolle über ihr Vermögen übernehmen.
- Auch wenn die Rolle von **Bitcoin** als Zahlungsmittel immer wieder diskutiert wird, ist es wichtig, die bedeutenden Fortschritte anzuerkennen, die in den letzten Jahren gemacht wurden, um die Akzeptanz von **Bitcoin** als praktikable Option für Transaktionen zu erhöhen. Mit dem Aufkommen neuer Technologien und innovativer Zahlungslösungen wird **Bitcoin** zunehmend als praktisches und effizientes Zahlungsmittel angesehen, insbesondere im Bereich der grenzüberschreitenden Transaktionen. Je mehr Unternehmen und Privatpersonen die Vorteile der Verwendung von **Bitcoin** für alltägliche Transaktionen erkennen, desto größer wird sein Potenzial, ein weithin akzeptiertes Zahlungsmittel zu werden.



Kapitel 5



Kapitel 6

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

- 6.0** Vom Neuling zum Profi: Ein Leitfaden für die Bitcoin-Wallet
- 6.1** Der Vorgang des Onboardings und der Sicherung deiner Bitcoin
 - 6.1.1** Gemeinschaftsübung: Selbstverwahrung und richtiger Umgang mit der Wallet
 - 6.1.2** Gemeinschaftsübung: Wie erhalte ich Bitcoin (im Detail)?
 - 6.1.3** Gemeinschaftsübung: Wie sende ich Bitcoin und bezahle für Waren und Dienstleistungen (im Detail)?
- 6.2** On-Chain vs. Off-Chain
- 6.3** Das Lightning-Netzwerk
 - 6.3.1** Eine Lightning-Transaktion
 - 6.3.2** Gemeinschaftsübung: Lightning-Wallet-Staffellauf
 - 6.3.3** Gemeinschaftsübung: Interaktive Lightning-Online-Demo



Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

6.0 Vom Neuling zum Profi: Ein Leitfaden für die Bitcoin-Wallet

Wenn man zum ersten Mal Sats kauft, werden sie auf einem virtuellen Konto gutgeschrieben, ähnlich wie bei der Einzahlung von Geld auf ein Bankkonto.



Der Hauptunterschied besteht darin, dass ein Bankkonto zentralisiert ist und staatlichen Vorschriften unterliegt, während eine **Bitcoin-Wallet** dezentralisiert ist und über ein Netzwerk von **Person zu Person** funktioniert.

- **Bitcoin** hat keinen zentralen Schwachpunkt, aber es ist wichtig, vorsichtig zu sein, denn die **Bitcoin** einer Person können sich im Besitz einer dritten Partei befinden, die sie verwaltet.

• Dieses virtuelle Konto, das oft als „Wallet (Brieftasche)“ bezeichnet wird, ist durch einen **privaten Hauptschlüssel** geschützt, ähnlich wie ein Bankkonto durch *eine persönliche PIN oder ein Passwort* geschützt ist. Genauso wie du die Kontrolle über die Gelder auf deinem Bankkonto hast, kannst du die Sats in deiner Wallet kontrollieren und sie für Einkäufe oder Überweisungen auf andere Konten verwenden.

• Genauso wie ein Schlüsseldienst eine beliebige Anzahl von Schlüsseln erstellen kann, die zum Öffnen von Schlossern verwendet werden können, kann eine **Recovery- oder Backup-Phrase** (oder ein *privater Hauptschlüssel*) verwendet werden, um eine beliebige Anzahl von privaten Schlüsseln zu generieren, die für den Zugriff auf deine Bitcoin-Wallet verwendet werden können. Man könnte sagen, dass eine **Recovery-Phrase** wie ein Schlüsseldienst ist, und die **privaten Schlüssel** sind die Schlüssel, die vom Schlüsseldienst erstellt werden.

12-Word Backup Phrase
dog cat human elephant
bird dolphin snake rat
snail zebra leopard ant



PRIVATE KEYS
Bitcoin 8u924fua9x9vz9e...
Litecoin f7ag9vc89x7as9d...
Ethereum 54aa76d5f7aos8fe...
DASH 54as76d5f7aos8fe...
Decred 87f298f7987dst24f...

Diese Tabelle enthält die beiden Haupttypen von Bitcoin-Wallets, die **selbstverwahrten** und die **verwahrten**. Du kannst die Vorteile und Risiken jedes Wallet-Typs sehen und wer die **Bitcoin** in jedem Fall kontrolliert. Selbstverwahrend bedeutet, dass der Nutzer die privaten Schlüssel besitzt, was bedeutet, dass er seine **Bitcoin** wirklich besitzt, während sie beim zweiten Typ *im Besitz einer dritten Partei sind*.

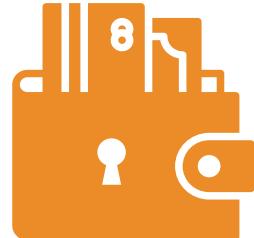
Wallet-Typ	Wer kontrolliert meine Bitcoin?	Vorteile	Risiken
selbst-verwaltete Wallets	Der Nutzer	Vollständige Kontrolle über Gelder und Transaktionen, kein Genehmigungsverfahren oder Einfrieren von Konten, keine Kontrolle durch Unternehmen oder Regierungen, Schutz vor willkürlicher Beschlagnahmung, wie bei der Aufbewahrung von Geld zu Hause.	Keine Wiederherstellung, wenn die Recovery-Phrase verloren geht, weniger Kundensupport, die volle Verantwortung liegt beim Nutzer.
Fremd-verwaltete Wallets	Der Drittanbieter	Einfache Wiederherstellung bei Zugriffsverlust, einfache Kundenbetreuung.	Die Geldmittel sind immer mit dem Internet verbunden, was sie anfälliger für Hackerangriffe und Sicherheitslücken macht.



Kapitel 6

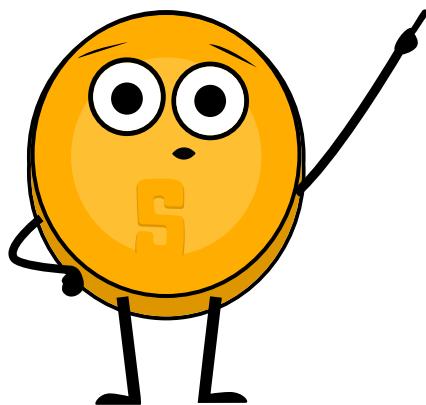
Bei einer **selbstverwalteten Wallet** (die auch als **non-custodial Wallet** bezeichnet wird) besitzt nur du die Schlüssel zur Wallet und hast die volle Kontrolle darüber, was hinein- und hinausgeht. Bei einer fremdverwalteten Wallet hingegen hat eine andere Person den Schlüssel und kann in deinem Namen auf den Inhalt der Wallet zugreifen und ihn verwalten.

- Selbstverwahrung bedeutet, dass man seine eigene Bank ist. Die Transaktionen unterliegen nicht der Kontrolle oder Autorität einer Regierung oder eines Unternehmens, aber es bedeutet auch, dass man die volle Verantwortung für die Sicherheit seiner **Bitcoin** trägt.
- Die Selbstverwahrung stellt sicher, dass Dritte deine **Bitcoin** nicht ohne deine Zustimmung konfiszieren können.
- Die Selbstverwahrung gibt dir in Zeiten der Unsicherheit die Gewissheit, dass deine **Bitcoin** sicher sind.



Es ist wichtig, den richtigen Typ von Wallet für die individuellen Bedürfnisse zu wählen. Manchmal ist es schwer zu unterscheiden, ob es sich um eine fremdverwaltete oder eine selbstverwahrte Wallet handelt. Diese Tabelle zeigt die Unterschiede bei der Installation.

Wallet-Typ	1. Schritt: Wallet auswählen	2. Schritt: Wallet installieren	3. Schritt: Neue Wallet erstellen	4. Schritt: Deine Seed-Phrase sichern	5. Schritt: Wallet benutzen
selbst-verwaltete Wallets	Wähle einen Wallet-Anbieter für die Selbstverwahrung	Befolge die Anweisungen des Wallet-Anbieters	Erzeuge eine Recovery-Phrase und mindestens einen privaten Schlüssel	Bewahre die Recovery-Phrase an einem sicheren Ort auf	Verwende die Wallet, um Bitcoin zu empfangen und zu senden
fremd-verwaltete Wallets	Wähle einen Wallet-Anbieter für die Fremdverwaltung	Befolge die Anweisungen des Wallet-Anbieters	Erstelle ein Konto beim Wallet-Anbieter	entfällt (der Wallet-Anbieter hat den privaten Schlüssel)	Verwende die Wallet, um Bitcoin zu empfangen und zu senden



Bei der Aufbewahrung deiner **Bitcoin** geht es nicht nur darum, wer die Kontrolle darüber hat – es gibt auch viele andere Risiken zu beachten. Deshalb ist es wichtig, eine Lösung für die Aufbewahrung zu finden, die sowohl sicher als auch bequem ist.

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

Wallet-Typ	Beschreibung	Vorteile	Nachteile	Nutzer-Beispiel
Online-Wallet	Eine Wallet, auf die über einen Webbrowser zugegriffen wird.	Zugriff von jedem Gerät mit Internetanschluss. Einfach zu bedienen.	Weniger sicher. Kann gehackt oder kompromittiert werden.	Jemand, der häufig auf seine Wallet zugreifen muss und nicht viel Geld verwahrt.
Mobile-Wallet	Eine Wallet, die auf einem mobilen Gerät installiert ist.	Bequem. Kann von überall aus abgerufen werden.	Kann verloren gehen, wenn das Gerät verlegt, gestohlen oder gehackt wird.	Jemand, der unterwegs Transaktionen durchführen muss und nicht viel Geld aufbewahrt.
Desktop-Wallet	Eine Wallet, die auf einem Desktop-Computer installiert ist.	Sicherer als Online-Wallets. Kann offline verwendet werden.	Kann gehackt werden, wenn der Computer mit Malware infiziert ist.	Jemand, der eine große Menge an Bitcoin aufbewahren möchte und mit einem Desktop-Computer vertraut ist.
Hardware-Wallet	Ein physisches Gerät, das Bitcoin offline speichert.	Sehr sicher. Kann offline verwendet werden.	Wenn das Gerät verloren geht oder gestohlen wird, kann das Geld nicht mehr zurückgeholt werden.	Jemand, der eine große Menge an Bitcoin aufbewahren möchte und bereit ist, für die zusätzliche Sicherheit einer Hardware-Wallet zu bezahlen.
Paper-Wallet	Eine physische Aufzeichnung der privaten und öffentlichen Schlüssel einer Bitcoin-Wallet.	Sehr sicher. Kann offline verwendet werden.	Die physische Aufzeichnung kann verloren gehen oder gestohlen werden.	Jemand, der eine große Menge an Bitcoin aufbewahren möchte und bereit ist, zusätzliche Vorsichtsmaßnahmen zu ergreifen, um die Sicherheit zu gewährleisten.

Vergleiche die Vorteile der verschiedenen Wallets und mache dir bewusst, dass es keine ideale Wallet gibt, die alle Bedürfnisse befriedigt.

- Bei der Auswahl einer Bitcoin-Wallet gibt es einige Dinge, die man beachten sollte:
 - **Sicherheit:** Vergewissere dich, dass die Geldbörse über strenge Sicherheitsmaßnahmen verfügt, z. B. Zwei-Faktor-Authentifizierung und sichere Passwortrichtlinien.
 - **Privatsphäre:** Achte darauf, ob die Geldbörse es dir erlaubt, anonym zu bleiben, oder ob sie persönliche Daten zur Einrichtung eines Kontos verlangt.
 - **Benutzerfreundlichkeit:** Wähle eine Wallet, die einfach zu bedienen und zu handhaben ist, vor allem, wenn du neu im Umgang mit **Bitcoin** bist.
 - **Kompatibilität:** Vergewissere dich, dass die Wallet mit deinem Gerät und deinem Betriebssystem kompatibel ist.
 - **Gebühren:** Vergleiche die von verschiedenen Wallets erhobenen Gebühren, um sicherzustellen, dass du das beste Angebot bekommst.



- **Reputation:** Informiere dich über den Ruf der Wallet und ihres Teams, um sicherzustellen, dass sie vertrauenswürdig ist.
- **Kontrolle:** Einige Wallets geben dir mehr Kontrolle über deine privaten Schlüssel, was ein Sicherheitsvorteil sein kann. Überlege, ob du eine Wallet willst, die dir volle Kontrolle gibt, oder eine, die benutzerfreundlicher ist, aber weniger Kontrolle bietet.

Du kannst dein Guthaben später immer noch auf eine andere Wallet übertragen.

6.1 Der Vorgang des Onboardings und der Sicherung deiner Bitcoin



Onboarding bei **Bitcoin** bezieht sich auf den Prozess des Erwerbs und der Nutzung von **Bitcoin**.

Bevor wir weitermachen, ist es wichtig, dass wir die Schritte für das **Onboarding** lernen und uns mit dem Prozess für den sicheren **Kauf** und die **Sicherung** von **Bitcoin** vertraut machen.

1. **Wähle eine Bitcoin-Börse oder einen Broker:** Es gibt viele verschiedene Plattformen, auf denen du **Bitcoin** kaufen und verkaufen kannst. Wähle eine Plattform, die deinen Bedürfnissen entspricht und seriös ist.
2. **Erstelle ein Konto:** Folge den Anweisungen der Plattform, um ein neues Konto zu erstellen. Dies kann die Angabe persönlicher Daten und die Überprüfung deiner Identität erfordern.
3. **Wähle eine Zahlungsmethode:** Bei den meisten Plattformen kannst du ein Bankkonto, eine Kreditkarte oder eine Debitkarte angeben, um dein Konto aufzuladen. Folge den Anweisungen der Plattform, um deine Zahlungsmethode hinzuzufügen.
4. **Eine Order aufgeben:** Sobald dein Konto eingerichtet und aufgeladen ist, kannst du einen Auftrag zum Kauf von **Bitcoin** erteilen. Die Plattform wird dir ein Preisangebot machen und du kannst die Menge an **Bitcoin** angeben, die du kaufen möchtest.
5. **Bestätige die Transaktion:** Überprüfe die Details deiner Transaktion und **bestätige den Kauf**. Die Plattform wird die Transaktion verarbeiten und die **Bitcoin** werden auf dein Konto auf der Plattform übertragen.
6. **Abheben der Bitcoin:** Wenn du die **Bitcoin** auf eine selbstverwaltete Wallet übertragen möchtest, musst du die **Bitcoin** von der Plattform abheben und an deine Wallet senden. Die Plattform gibt dazu eine Anleitung.

„Not your keys, not your coins“

Dies ist ein beliebtes Sprichwort unter **Bitcoin**-Besitzern. Es bezieht sich auf den Gedanken, dass, wenn man keine direkte Kontrolle über die privaten Schlüssel hat, die mit der Bitcoin-Wallet zusammenhängen, man kein echtes Eigentum an den Geldeinheiten hat.

Der private Schlüssel ist ein Geheimcode, mit dem man auf seine **Bitcoin** zugreifen und sie ausgeben kann.

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

Wenn du deine **Bitcoin** bei einem Drittanbieter-Dienst wie einer Börse oder einer Online-Wallet aufbewahrst, verlässt du dich darauf, dass dieser Dienst deinen privaten Schlüssel sicher verwahrt. Wenn der Dienst gehackt wird oder den Betrieb einstellt, kannst du den Zugriff auf deine **Bitcoin** verlieren.

Das Sprichwort „**Not your keys, not your coins**“ soll dich daran erinnern, dass es wichtig ist, die Kontrolle über deine eigenen privaten Schlüssel zu behalten und sie sicher aufzubewahren. Auf diese Weise kannst du sicherstellen, dass du die volle Kontrolle über deine **Bitcoin** hast und auf sie zugreifen kannst, wann immer du willst.

6.1.1 Gemeinschaftsübung: Selbstverwahrung und richtiger Umgang mit der Wallet

Wenn die Studierenden keine Handys haben, stellt die Lehrkraft jedem ein Handy zur Verfügung. Für diese Übung gibt es zwei Optionen:

Gemeinschaftsübung: 1. Option: Lade eine neue Wallet herunter! Die Studenten sollen die Anweisungen Schritt für Schritt befolgen:

Die Erstellung und Verwendung einer Bitcoin-Wallet

1. Suche nach der App im App Store (iOS) oder im Google Play Store (Android)!
2. Öffne die App! Beim Erstellen der Wallet erhältst du deine 12 oder 24 Wörter umfassende Recovery-Phrase! **Schreibe sie unbedingt auf!** Bewahre sie an einem sicheren Ort auf! Denke daran, dass du, wenn du diese Wortfolge verlierst oder vergisst, nicht auf deine **Bitcoin** zugreifen kannst, wenn du den Zugriff auf deine Wallet verlierst!
3. Anschließend musst du **bestätigen**, dass du deine Recovery- oder Seed-Phrase tatsächlich gespeichert hast. Dazu musst du die Wörter deiner Seed-Phrase in der gleichen Reihenfolge **eingeben**.
4. Als zusätzliche Sicherheitsmaßnahme bieten einige Wallets die Möglichkeit, ein sicheres Passwort zu verwenden.
 - Dein privater Schlüssel und deine erste Bitcoin-Adresse werden von deiner Wallet automatisch für dich erstellt.
5. Verwende deine „Empfangsadresse“, um **Bitcoin** zu empfangen.
Übertrage Bitcoin in deine Wallet.
 - Bei einer selbstverwalteten Wallet kannst du **Bitcoin** nicht immer direkt mit Fiat kaufen, sondern musst sie möglicherweise erst an einer Börse kaufen und transferieren.



**NOT YOUR KEYS
NOT YOUR COINS**

Gemeinschaftsübung: 2. Option: Wallet wiederherstellen (zeitlich begrenzt).

Lade eine Bitcoin-Wallet herunter und füge einige Sats für jeden Studenten hinzu. Gib jedem Studenten ein Blatt mit einer Seed-Phrase, um eine Wallet abzurufen. Die Studenten sollen die Anweisungen Schritt für Schritt befolgen:



1. Wenn du deine Wallet zum ersten Mal startest, siehst du drei Methoden zur Erstellung einer Wallet, tippe auf [**Importiere eine bestehende Wallet**]!
 - Du wirst einen Einführungsbildschirm sehen, tippe auf [**Wiederherstellen mit Recovery-Phrase**]!
2. Gib deine 12/18/24 Wörter der Recovery-Phrase einzeln und in der richtigen Reihenfolge ein!
3. Wenn du fertig bist, drücke auf [**Wiederherstellen**]!
4. Wenn deine Wallet erfolgreich importiert wurde, wird „Import erfolgreich“ angezeigt.

6.1.2 Gemeinschaftsübung: Wie erhalte ich Bitcoin (im Detail)?

Um **Bitcoin** zu erhalten, musst du dem Absender deine **Bitcoin**-Wallet-Adresse mitteilen. Dies ist eine eindeutige Zeichenfolge aus Buchstaben und Zahlen, die deine Wallet repräsentiert und zur Identifizierung im **Bitcoin-Netzwerk** verwendet wird. Du findest deine Wallet-Adresse, indem du dich in deine **Bitcoin**-Wallet einloggst und nach einer Option zum „Empfangen“ oder „Einzahlen“ von **Bitcoin** suchst.

Dann kannst du deine **Bitcoin**-Adresse dem Absender auf eine von mehreren Arten mitteilen:

- **Kopieren und Einfügen der Adresse:** Du kannst die Adresse kopieren, indem du sie markierst und „Kopieren“ auf deiner Tastatur drückst, und sie dann in eine E-Mail oder Nachricht an den Absender einfügen.
- **Teile einen Link zu deiner Bitcoin-Wallet:** Einige **Bitcoin**-Wallets ermöglichen es dir, einen Link zu deiner Wallet zu erstellen, den du mit dem Absender teilen kannst. Der Absender kann dann auf den Link klicken, um deine Wallet aufzurufen und die **Bitcoin** zu senden.
- **Teile einen QR-Code:** Wenn der Absender ein Smartphone mit einer **Bitcoin**-Wallet-App hat, kann er den QR-Code scannen, um deine **Bitcoin**-Adresse zu erhalten.

Sobald der Absender deine **Bitcoin**-Adresse hat, kann er dir die **Bitcoin** schicken, indem er deine Adresse und den Betrag, den er dir schicken möchte, eingibt und die Transaktion einleitet. Die **Bitcoin** werden dann an deine Wallet gesendet und sind sichtbar, sobald die Transaktion im **Bitcoin-Netzwerk** bestätigt wurde. Dies dauert in der Regel ein paar Minuten.

6.1.3 Gemeinschaftsübung: Wie sende ich Bitcoin und bezahle für Waren und Dienstleistungen (im Detail)?

Um **Bitcoin** zu versenden, brauchst du ein paar Dinge: eine **Bitcoin**-Wallet, die **Bitcoin**-Adresse des Empfängers und den Betrag an **Bitcoin**, den du senden möchtest.

1. Öffne deine **Bitcoin**-Wallet!

- Ein SMS-Code wird an deine Telefonnummer gesendet, und du musst ihn in das Dialogfeld eingeben. Wenn du Google 2FA aktiviert hast, musst du alternativ den sechsstelligen Code in der Google-Authenticator-App eingeben.

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

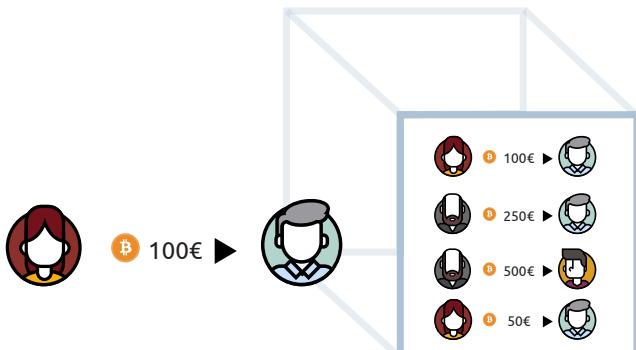
2. Wähle die Funktion „Senden“ oder „Abheben“ und kopiere die Adresse des Empfängers!
 3. Gib die **Bitcoin**-Adresse des Empfängers ein, indem du sie in das Feld „An“ einfügst.
 4. Gib den **Bitcoin**-Betrag, den du senden möchtest, in das Feld „Betrag“ ein.
 5. Überprüfe noch einmal die Adresse des Empfängers und den zu sendenden Betrag.
 6. Bevor du auf **Bestätigen** und **Senden** klickst, empfehlen wir dir, die Transaktionsdetails noch einmal zu überprüfen, um sicherzustellen, dass du die richtige Menge **Bitcoin** an die richtige Wallet-Adresse sendest.
 7. Bestätige die Transaktion und warte darauf, dass das Netzwerk die Transaktion bestätigt.
- Lass uns üben!!! Geh in den Laden, um mit **Bitcoin** ein paar Kleinigkeiten zu kaufen.

6.2 On-Chain vs. Off-Chain

Es ist wichtig zu wissen, dass nicht alle **Bitcoin**-Transaktionen auf der Haupt-**Bitcoin**-Blockchain aufgezeichnet werden. Einige Netzwerke verwenden andere Blockchains, sogenannte Sidechains, um Transaktionen aufzuzeichnen.

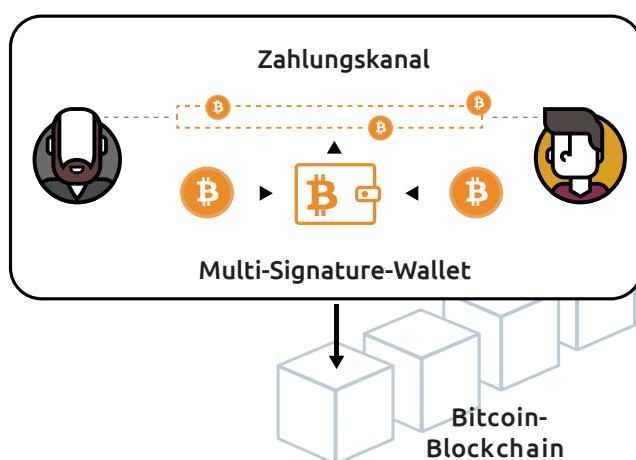
On-Chain-Transaktionen:

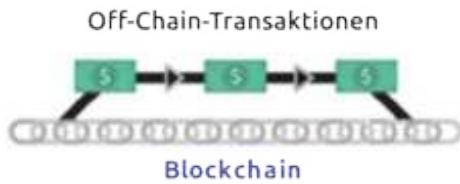
- Dies sind Transaktionen, die direkt auf der **Bitcoin**-Blockchain stattfinden.
- Die Bestätigung dauert etwa 10 Minuten, und die Gebühren hängen von der Größe der Transaktion in Bytes ab.
- Sie sind sicher, können aber langsamer sein.



Off-Chain-Transaktionen (Lightning-Netzwerk):

- Diese Transaktionen finden in einem separaten Netzwerk statt, das auf der **Bitcoin**-Blockchain aufbaut.
- Sie werden schneller und mit geringeren Gebühren abgewickelt.
- Sie werden in der Regel dort eingesetzt, wo Regulierungen und Gesetze ihre Anwendung unterstützen und wo Schnelligkeit und günstige Kosten der Transaktionen eine größere Rolle spielen.
- Im Vergleich zu On-Chain-Transaktionen sind sie jedoch weniger sicher.





Bei Verwendung des Lightning-Netzwerks müssen nur **drei Arten von Transaktionen** an die Blockchain übermittelt werden.

Das **Lightning-Netzwerk** ist ein Skalierungskonzept für **Bitcoin**. Es geht darum, viele **Bitcoin**-Transaktionen aus der Blockchain heraus und in private Kanäle zwischen den Nutzern zu verlagern, aber immer noch auf die Sicherheit der Blockchain zu vertrauen.



Zahlungs-Netzwerk	Bitcoin-Netzwerk	Lightning-Netzwerk
Definition	Ein dezentrales digitales Netzwerk, das Kryptographie zur Sicherung von Finanztransaktionen verwendet.	Ein Second-Layer-Zahlungsprotokoll, das auf der Bitcoin -Blockchain aufbaut und schnellere und günstigere Transaktionen ermöglicht.
Vorteile	- Dezentral und sicher - Keine Rückbuchungen oder Betrug - Kann anonym genutzt werden - Weltweite Akzeptanz	- Schnellere und günstigere Transaktionen - Erhöhte Skalierbarkeit - Off-Chain-Transaktionen belasten die Blockchain nicht
Nachteile	- Langsame Transaktionszeiten - Hohe Gebühren für bestimmte Arten von Transaktionen - Komplex für Anfänger	- Erfordert Vertrauen in die Kanalbetreiber - Noch experimentell und nicht weit verbreitet - Erfordert On-Chain-Transaktionen zum Öffnen und Schließen von Kanälen

6.3 Das Lightning-Netzwerk

Bitcoin ist für sein unveränderliches öffentliches Kassenbuch bekannt, aber für alltägliche Transaktionen wie den Kauf von Kaffee ist es möglicherweise nicht die beste Wahl. Der Prozess, diese Transaktionen an viele Nodes zu senden und sie in einer gemeinsamen Datenbank zu speichern, kann langsam und umständlich sein. Für persönliche oder private Transaktionen ist es besser, Peer-to-Peer-Zahlungskanäle zu nutzen.

Eine bessere Lösung ist ein Skalierungsansatz über mehrere Layer („Ebenen“), wie etwa die Kombination von **Bitcoin** und Lightning-Netzwerk. So können die Nutzer die Ebene auswählen, die ihren Bedürfnissen entspricht. **Bitcoin** ist eine digitale Währung, die dezentralisiert ist, während das Lightning-Netzwerk schnelle, günstige und vertrauliche Zahlungen ermöglicht.

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen



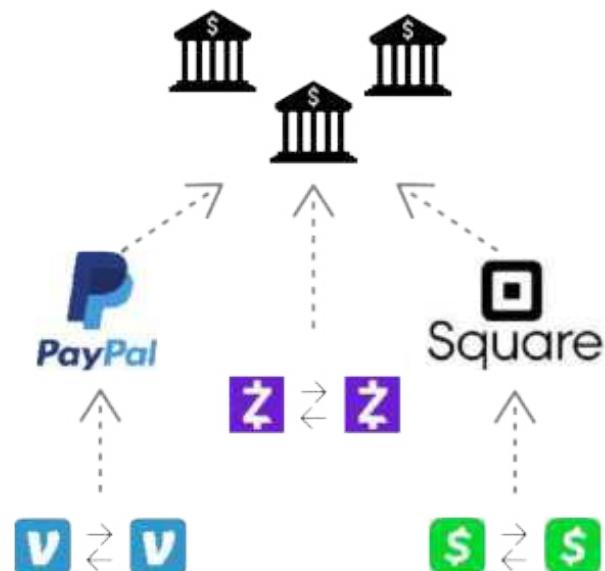
Das Lightning-Netzwerk ist ein Zahlungssystem, das es Nutzern ermöglicht, schnell und kostengünstig Zahlungen mit **Bitcoin** zu senden und zu empfangen. Es funktioniert, indem beide Personen eine gemeinsame Wallet einrichten, in der sie ihre **Bitcoin** speichern, und dann unbegrenzte Transaktionen untereinander durchführen, ohne die Haupt-Blockchain zu berühren. Wenn sie fertig sind, wird der endgültige Kontostand in der Haupt-Blockchain aufgezeichnet.

Lightning arbeitet als separates Netzwerk, das mit der **Bitcoin**-Blockchain verbunden ist, und ist so konzipiert, dass es nahtlos mit **Bitcoin** zusammenarbeitet. Taro, eine neuere Erweiterung von Lightning, ermöglicht nun die Nutzung des Netzwerks für andere Arten von Vermögenswerten, wie z. B. Stablecoins, die es den Nutzern ermöglichen, nahezu sofortige, kostengünstige Zahlungen in einer Währung vorzunehmen, die an traditionelle Fiat-Währungen wie den US-Dollar gebunden ist. Die Zahlungen können unter Umgehung von Intermediären direkt an den Empfänger geleistet werden, wobei die Zahlung in die ursprüngliche Währung umgewandelt wird, bevor sie das Geschäft erreicht.

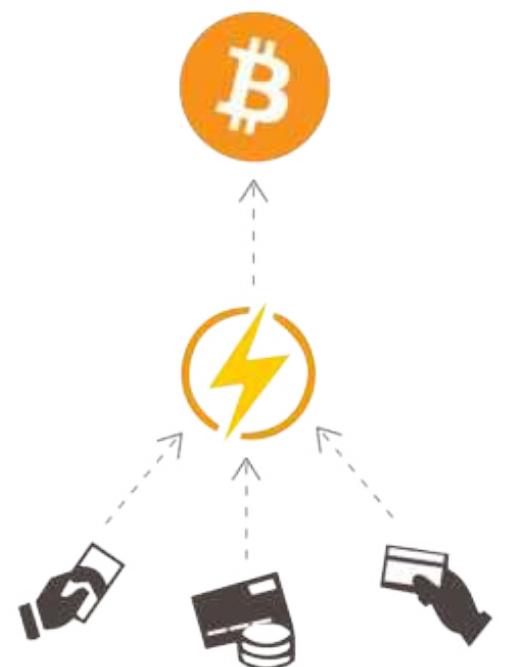
Die Verwendung von Stablecoins im Lightning-Netzwerk für internationale Transaktionen, wie zum Beispiel Überweisungen, bietet mehrere Vorteile:

1. Geringere Kosten: Grenzüberschreitende Transaktionen können aufgrund von Gebühren, die von Banken oder anderen Intermediären erhoben werden, teuer sein. Durch die Verwendung von Stablecoins im Lightning-Netzwerk können diese Gebühren reduziert oder eliminiert werden, wodurch grenzüberschreitende Zahlungen erschwinglicher werden.

Modernes Geldsystem = Geschlossene Netzwerke
Banken bewahren die Endgültigkeit



Bitcoins Geldsystem = Offenes Netzwerk
Bitcoin bewahrt die Endgültigkeit



Das Lightning-Netzwerk bietet die Vorteile digitaler Wallets wie Apple Pay ohne die mit **Bitcoin** verbundene Volatilität des Preises.



2. Höhere Geschwindigkeit: Grenzüberschreitende Transaktionen können bei Verwendung herkömmlicher Methoden mehrere Tage in Anspruch nehmen. Durch die Verwendung von Stablecoins im Lightning-Netzwerk können internationale Transaktionen schnell abgewickelt werden, wodurch sich die für den Abschluss einer Transaktion erforderliche Zeit verkürzt.

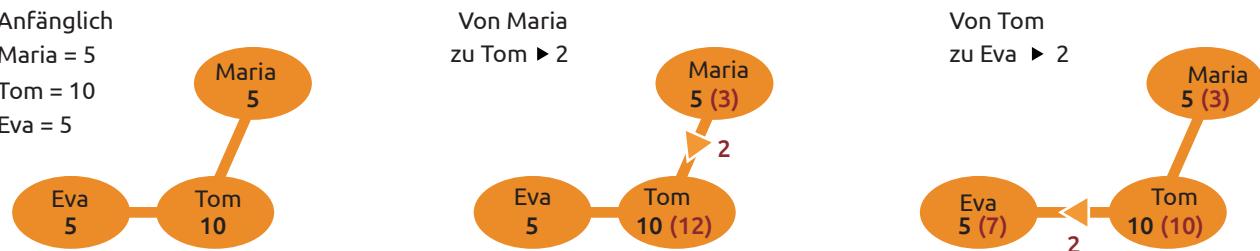
3. Verbesserter Zugang: Für Privatpersonen oder Unternehmen in Ländern mit eingeschränktem Zugang zu traditionellen Bankdienstleistungen kann die Verwendung von Stablecoins im Lightning-Netzwerk eine Möglichkeit bieten, internationale Zahlungen zu tätigen und so den Zugang zu Finanzdienstleistungen zu verbessern.

6.3.1 Eine Lightning-Transaktion

► Beispiel 1

- Maria hat 5 Einheiten einer bestimmten Währung und Eva hat ebenfalls 5 Einheiten. Maria möchte 2 ihrer Einheiten an Eva schicken, also schickt sie 2 Einheiten an Tom. Tom gibt dann die 2 Einheiten an Eva weiter, die nun 7 Einheiten hat. Maria hat nun 3 Einheiten. Und das war's! Die Transaktion ist abgeschlossen.

Der entscheidende Punkt dabei ist, dass Maria und Eva keine Bank oder einen anderen Intermediär einschalten müssen, um die Transaktion abzuwickeln.



- Tom fungiert in diesem Szenario, in dem Maria und Eva einander nicht direkt vertrauen, als Intermediär oder „vertrauenswürdige dritte Partei“. Tom erhält die 2 Einheiten von Maria und gibt sie dann an Eva weiter, womit die Transaktion abgeschlossen ist. Durch den Einsatz von Tom als Intermediär können Maria und Eva die Transaktion ohne eine Bank oder ein anderes zentrales Institut abwickeln, was die Transaktion schneller, billiger und sicherer machen kann. Tom ist ein Schlüsselement in diesem Peer-to-Peer-Transaktionsprozess.

Als Betreiber eines Nodes bzw. Knotenpunkts in einer Lightning-Netzwerk-Transaktion profitiert Tom in mehrfacher Hinsicht:

- 1. Transaktionsgebühren:** Tom erhält für jede Transaktion, die über seinen Node läuft, eine kleine Gebühr, die ihn für die Zeit und den Aufwand entschädigt, die er in die Wartung und den Betrieb seines Nodes investiert.
- 2. Beteiligung am Netzwerk:** Indem er einen Lightning-Node betreibt, beteiligt sich Tom am Netzwerk und trägt dazu bei, dessen Dezentralisierung, Sicherheit und Stabilität zu erhöhen. Dies kann Toms Ruf und Glaubwürdigkeit als zuverlässiger Node-Betreiber erhöhen und ihn zu einem attraktiveren Intermediär für zukünftige Transaktionen machen.

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

3. Wachstum des Netzwerks: Wenn das Lightning-Netzwerk wächst und mehr Menschen es nutzen, wird die Anzahl der Transaktionen, die über Toms Node laufen, wahrscheinlich steigen, was zu höheren Einnahmen aus Transaktionsgebühren führen kann.

4. Erhöhte Netzwerksicherheit: Toms Rolle als Intermediär trägt dazu bei, die Sicherheit des Netzwerks zu erhöhen, indem er eine zusätzliche Schutzebene zwischen Maria und Eva hinzufügt. Dies kann das Vertrauen der Nutzer in das Netzwerk erhöhen, was es für neue Nutzer attraktiver macht und das Wachstum fördert.

Insgesamt kann die Tätigkeit als Node-Betreiber im Lightning-Netzwerk Tom eine stetige Einnahmequelle bieten und ihm die Möglichkeit geben, zum Wachstum und zur Entwicklung des Netzwerks beizutragen.

Zusammenfassend lässt sich sagen, dass On-Chain-Transaktionen langsamer, aber sicherer sind, während Off-Chain-Transaktionen (Lightning-Netzwerk) schneller, aber weniger sicher sind. Man sollte den Kompromiss zwischen Sicherheit und Geschwindigkeit je nach den eigenen Bedürfnissen abwägen.

► Beispiel 2

Mina hat eine große Vorliebe für McDonald's. Sie geht dort jeden Tag zum Frühstück, Mittag- und Abendessen hin! Aber bei so vielen verschiedenen Zahlungsmöglichkeiten ist sie sich nicht sicher, welche die beste Wahl ist. Glücklicherweise hat sie ein wenig über **Bitcoin** und das Lightning-Netzwerk gelernt. Nach einem Vergleich der unten stehenden Tabellen hat Mina keinen Zweifel daran, dass die Lightning-Zahlungsmethode die beste Wahl ist.

Nutzen	Lightning	Traditionelles Bankensystem
Geschwindigkeit	Schnell	Langsam
Transparenz	Transparent	Undurchsichtig
Sicherheit	Sicher	Angreifbar
Transaktionsgebühren	Niedrig	Hoch
Finanzielle Inklusion	Hoch	Begrenzt

Nutzen	Lightning	On-Chain
Skalierbarkeit	Hoch	Niedrig
Privatsphäre	Hoch	Mäßig
Kompatibilität	Hoch	Niedrig
Rechtskonformität	Mäßig	Hoch
Kosteneffizienz	Hoch	Mäßig



Im Durchschnitt
1.700 Transaktionen
pro Sekunde.

Kapazität von
65.000 Transaktionen
pro Sekunde.

Bitcoin On-Chain



Kapazität von
7 Transaktionen
pro Sekunde.

Bitcoin Lightning-Netzwerk



Millionen von
Transaktionen
pro Sekunde.



Mina ist auch ein Fan von schnellen, sicheren und kostengünstigen Transaktionen. Deshalb hat sie sich entschieden, Lightning für ihre Einkäufe bei McDonald's zu nutzen. Mit Lightning kann sie ihre Mahlzeiten noch mehr genießen, da sie weiß, dass ihre Zahlungen sofort, sicher und mit geringen Gebühren abgewickelt werden. Und da das Lightning-Netzwerk die finanzielle Inklusion fördert, kann Mina ihre Mahlzeiten nun auch dann bezahlen, wenn sie sich in einem abgelegenen Gebiet in El Salvador befindet.

Um mit Lightning zu beginnen, lädt Mina zunächst eine Lightning-Wallet auf ihr Smartphone herunter. Dann lädt sie ihre Lightning-Wallet auf, indem sie einige **Bitcoin** von ihrer regulären **Bitcoin**-Wallet an ihre neue Lightning-Wallet sendet. Dieser Vorgang wird als „Aufladen der Wallet“ oder „Aufladen eines Zahlungskanals“ bezeichnet. Mina kann ihre Wallet mit einem beliebigen **Bitcoin**-Betrag aufladen, aber es ist wichtig zu beachten, dass der **Bitcoin**-Betrag, den sie in ihrer Lightning-Wallet aufbewahrt, nicht für ihre On-Chain-Transaktionen verwendet werden kann.

Sobald ihre Lightning-Wallet mit Geld aufgeladen ist, kann sie damit Zahlungen an McDonald's vornehmen. McDonald's hat einen Lightning-Node, sodass Mina einen Zahlungskanal mit dem Restaurant eröffnen kann, indem sie einen Teil ihrer **Bitcoin** von ihrer Lightning-Wallet an eine bestimmte, von McDonald's angegebene Adresse sendet. Dies verschiebt ihre **Bitcoin** von der **Bitcoin**-Blockchain zu einer Off-Chain-Transaktion im Lightning-Netzwerk.



Mit dem offenen Zahlungskanal kann Mina nun bei McDonald's einkaufen, ohne jedes Mal einen neuen Kanal zu eröffnen oder hohe Gebühren zahlen zu müssen. Der Kanal bleibt so lange offen, wie sowohl Mina als auch McDonald's ihn nutzen wollen. Wenn Mina zum Beispiel einen Hamburger für 0,0005 **Bitcoin** kauft, zeigt der Kanal an, dass Mina jetzt 0,9995 **Bitcoin** hat. Und wenn sie am nächsten Tag einen Milchshake für 0,0003 **Bitcoin** kauft, registriert der Kanal, dass Mina jetzt 0,9992 **Bitcoin** hat.

Wenn Mina beschließt, ihr **Bitcoin**-Guthaben für etwas anderes zu verwenden, schließt sie den Kanal, indem sie eine abschließende Transaktion an die **Bitcoin**-Blockchain sendet. Dies geschieht, indem sie eine abschließende Transaktion in ihrer Lightning-Wallet initiiert. Die Transaktion enthält das endgültige Guthaben des Kanals, das von beiden Parteien vereinbart wurde. Die Transaktion wird dann an die **Bitcoin**-Blockchain übertragen und von einem Miner bestätigt. Sobald die Transaktion bestätigt ist, wird der Kanal geschlossen und die verbleibenden **Bitcoin** im Kanal werden an Mina und McDonald's zurückgegeben.

Es ist wichtig zu erwähnen, dass es einige Zeit dauern kann, bis die Schließung eines Kanals in der Blockchain bestätigt wird. Während dieser Wartezeit sind die Gelder noch im Kanal gesperrt und können nicht für On-Chain-Transaktionen verwendet werden. Mina wird eine Benachrichtigung erhalten, sobald die Schließungstransaktion bestätigt ist.

Bitcoin-Wallets: Leitfaden für die Selbstverwahrung und das Lightning-Netzwerk für sichere Transaktionen

6.3.2 Gemeinschaftsübung: Lightning-Wallet-Staffellauf

1. Zunächst musst du eine Lightning-Wallet auf dein Handy oder deinen Computer herunterladen. Es gibt mehrere Optionen für Mobiltelefone, darunter Muun, Blue Wallet, Blink und Eclair, sowie Lightning-App und Zap für Desktop-Computer.
2. Folge den Anweisungen zur Installation der Wallet auf deinem Gerät! Dies kann das Herunterladen der App aus dem App Store oder von Google Play oder das Herunterladen und Installieren der Software von der Website der Wallet beinhalten.
3. Sobald die Wallet installiert ist, öffne sie und folge den Anweisungen, um sie einzurichten! Dazu kann es erforderlich sein, eine neue Wallet zu erstellen oder eine bestehende Wallet wiederherzustellen und sie mit einem Passwort oder einer anderen Form der Authentifizierung zu sichern.
4. Sorge dafür, dass du eine Möglichkeit hast, Satoshis zu erhalten. Dies kann bedeuten, dass du deine Wallet mit einer Empfangsadresse ausstattest oder einen QR-Code scannst, der von deiner Lehrkraft oder einem anderen Mitglied deiner Gruppe bereitgestellt wird.
5. Wenn deine Wallet eingerichtet ist und du bereit bist, Satoshis zu erhalten, wird deine Lehrkraft dir und deiner Gruppe einen Anfangsbetrag an Satoshis zukommen lassen, indem sie sie direkt an deine Wallet schickt.

- A. Das Ziel eurer Gruppe ist es, die Satoshis über das Lightning-Netzwerk von einer Wallet zur nächsten zu bringen, bis sie die letzte Person in der Gruppe erreicht haben.
- B. Um Satoshis an eine andere Person zu senden, öffne deine Wallet und folge den Anweisungen, um eine Zahlung zu tätigen! Du musst die Adresse der Wallet des Empfängers angeben oder einen QR-Code scannen und den Betrag an Satoshis eingeben, den du senden möchtest.
- C. Wenn es eurer Gruppe gelingt, die Satoshis als erste an die letzte Person zu schicken, habt ihr gewonnen! (Und dürft die Satoshis und ein paar Süßigkeiten behalten.)

6.3.3 Gemeinschaftsübung: Interaktive Lightning-Online-Demo

Gemeinschaftsübung: Beginne mit der Erkundung einer der interaktiven Websites, die von der Lehrkraft zur Verfügung gestellt werden. Folge dann den Anweisungen auf der nächsten Seite!

- <https://www.robtex.com/lnemulator.html?conf=A5-5B,B5-5C&send=A2C>
- <https://lnrouter.app/graph/zero-base-fee>





Kapitel 6



1. Konzentriere dich auf die im Unterricht besprochenen Schlüsselkonzepte, einschließlich Zahlungskanäle, Routen und Gebühren!
 2. Notiere dir alle Fragen oder Schwierigkeiten, auf die du beim Erkunden der Website stößt!
 3. Tausche dich mit deiner Gruppe über deine Ergebnisse aus und bespreche alle Fragen und Schwierigkeiten mit der Klasse!
 4. Sei bereit, dich an Diskussionen in der Klasse über das Lightning-Netzwerk und sein Potenzial als Skalierungslösung für Bitcoin-Transaktionen zu beteiligen!



Kapitel 7

Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

- 7.0** Die Beseitigung des Problems der doppelten Ausgaben:
Bitcoins Lösung
- 7.1** Die Nachverfolgung deiner Geldeinheiten
- 7.2** Sicherheit und Geheimhaltung
- 7.3** Der „Mempool“ oder Memorypool:
Der Auffangbehälter für Bitcoin-Transaktionen
 - 7.3.1** Gemeinschaftsübung: In der Warteschleife:
Die unbestätigten Transaktionen des Bitcoin-Netzwerks
- 7.4** Hinter den Kulissen der Blöcke:
Das Geheimnis vom Bitcoin-Scripting
 - 7.4.1** Ein technischer Einblick in Bitcoin-Transaktionen



Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

00001100111000101000101010101100100010101001001100110000011101000101000111110
011010111100100110110001100101110010011010010011100010100100110110111010001100101
101010001101100000101110101000100011100000000111010110111100001010110011110010
1010000101000011

Siehst du die lange Reihe von Einsen und Nullen da oben? Das ist eine Zufallszahl, und wenn wir sie in unser normales Dezimalsystem umwandeln, wird daraus eine Zahl mit mehr als 70 Stellen, das sind sogar mehr Atome als es in unserem Universum gibt! Wir können jedoch ein anderes System verwenden, um diese Zahl auf kürzere Weise darzustellen, und nennen es einen **privaten Schlüssel**.

Das Besondere an diesem privaten Schlüssel ist, dass er einzigartig ist, d. h. er wurde noch nie verwendet und wird nie wieder auftauchen, wenn man diese Seite verlässt oder einen neuen Schlüssel erstellt. Das ist so, als würde man 256 Münzen hintereinander werfen und zweimal genau dasselbe Ergebnis erhalten – unmöglich!

Die Sicherheit von **Bitcoin** hängt davon ab, dass dieser private Schlüssel geheim und schwer zu erraten ist. Wenn jemand anderes ihn in die Hände bekommt oder wenn du ihn verlierst, wirst du dein ganzes Geld für immer verlieren. Bewahre ihn also sicher auf!



Aber wie funktioniert **Bitcoin** eigentlich?
Schau dir das folgende Video an, um es besser zu verstehen!



<https://youtu.be/bBC-nXj3Ng4>

Bisher haben wir etwas über die Geschichte des Geldes und die revolutionäre Idee der Blockchain-Technologie gelernt und uns mit den Grundlagen von **Bitcoin** – der ersten dezentralen digitalen Währung der Welt – beschäftigt. Aber wie verhindert **Bitcoin** Betrug und stellt sicher, dass niemand das gleiche Geld zweimal ausgeben kann?

Die Wahrheit ist, dass man, wenn man jemandem **Bitcoin** schickt, mit seinem privaten Schlüssel sagen muss: „Ja, ich genehmige das.“ Dann sagt das Netzwerk: „Cool, ich überprüfe noch einmal, ob das echt ist“, und schaut sich die Signatur an, um sicherzustellen, dass alles in Ordnung ist, bevor es die **Bitcoin** weiterschickt.

Sign a transaction
Transaction + Private Key = Signature

From Address: Me
Private Key: Enter private key...
To Address: Dale
Digital Signature:
Send transaction with this private key

Verify a transaction
Transaction + Signature = Private Key = Valid

Transaction: Me → Dale 3 BTC
Digital Signature:
Private Key:



Hier kommt die Magie von UTXOs, Public-Key-Kryptographie, Hashing, Scripting und dem Mempool ins Spiel. So wie ein Fingerabdruck sicherstellt, dass niemand anderes deine Identität benutzen kann, stellen Hashes in *Bitcoin* sicher, dass Transaktionen nicht verändert werden können. Skripte sind wie die Regeln für ein Spiel, die sicherstellen, dass Transaktionen bestimmten Bedingungen folgen. UTXOs sind wie die Bausteine eines Puzzles, die den Überblick über das gesamte Geld in deiner virtuellen Brieftasche behalten. Und der Mempool fungiert wie ein Speicherbereich, der sicherstellt, dass alle Transaktionen verifiziert werden, bevor sie der Blockchain hinzugefügt werden. Tauchen wir also ein und entdecken wir, wie *Bitcoin* das Problem der doppelten Ausgaben löst und die Integrität jeder Transaktion in seinem Netzwerk sicherstellt.

7.0 Die Beseitigung des Problems der doppelten Ausgaben: Bitcoins Lösung

Was ist eigentlich das „Problem der doppelten Ausgaben“?

Private und öffentliche Schlüssel sowie *Bitcoin*-Transaktionen werden, wie wir erfahren haben, durch eine Reihe von zufälligen Zahlen und Buchstaben dargestellt, die auf jedem Gerät mit Internetzugang eingesehen werden können.

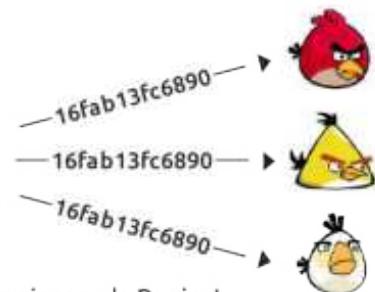


Außerdem werden viele der Informationen im Zusammenhang mit diesen Transaktionen in der Regel in einem numerischen Notationssystem, den Hexadezimalzahlen, übermittelt.

Doppel ausgabe...



Bits sind leichter zu kopieren als Papier!



Dies bedeutet, dass es üblich ist, Zeichenketten mit 64 hexadezimalen Zeichen zu sehen, die aus Buchstaben (A-F) und Zahlen (0-9) bestehen, wie z. B.

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

Wie können wir also verhindern, dass jemand seine *Bitcoin* kopiert und einfügt und sie mehrfach ausgibt, so wie er es mit einer E-Mail oder einem digitalen Foto tun würde?

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

Wie können wir ohne eine zentrale Instanz einen Konsens darüber erzielen, wem welches Geld gehört?

Durch Hashing und Code. Lasst uns das genauer erklären.

Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

Stell dir vor, du hast einen **Bitcoin**, den du deinem Freund als Geburtstagsgeschenk schicken willst. Du sendest den **Bitcoin** an die Adresse deines Freundes, aber dann merkst du, dass du deinem Ex-Freund Geld schuldest und den **Bitcoin** stattdessen an ihn hättest schicken sollen. In einem Moment der Panik beschließt du, hinterhältig zu sein und eine neue Transaktion zu erstellen, um denselben einen **Bitcoin** an deinen Ex-Freund zu schicken. Dies nennen wir eine „doppelte Ausgabe“.

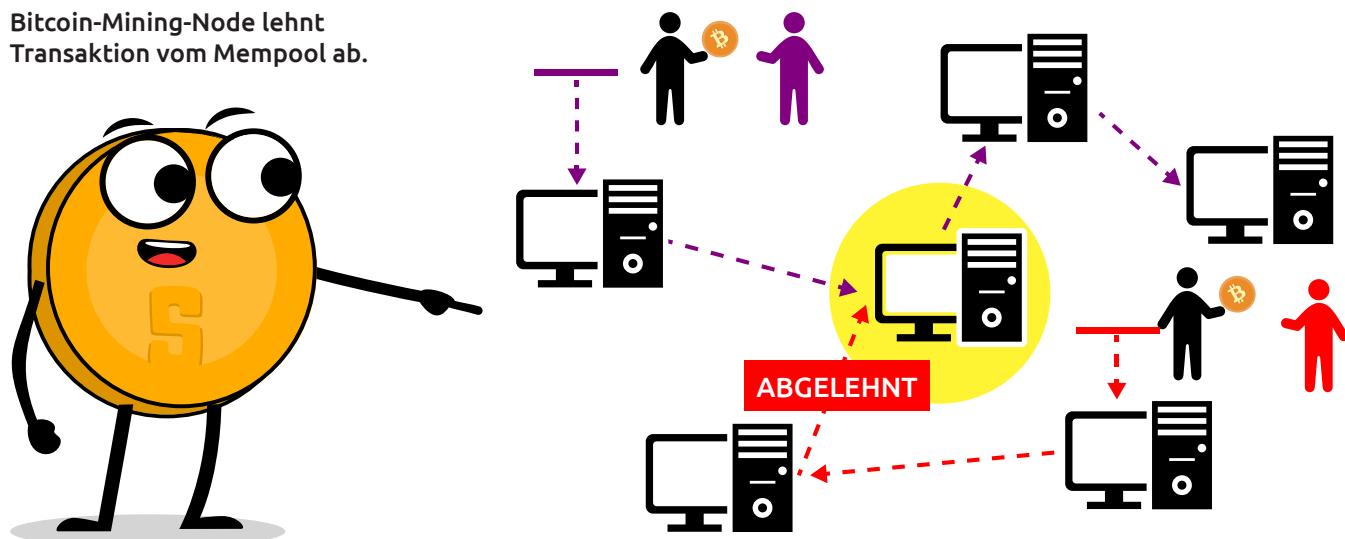
Aber Moment mal, wie kann das Netzwerk das verhindern? Das ist ganz einfach. Die Nodes im Netzwerk erkennen widersprüchliche Transaktionen und lassen nur eine davon zu, basierend auf einer Reihe von Regeln, den sogenannten „**Konsensregeln**“. In diesem Fall ist es wahrscheinlich, dass die Transaktion an deinen Ex-Freund abgelehnt werden würde, da sie nach der ursprünglichen Transaktion an deinen Freund gesendet wurde. Es ist jedoch nur eine Frage des Glücks, welche Transaktion zuerst von einem Miner ausgewählt wird.

Dank der Blockchain ist jeder im Netzwerk in der Lage, sich über den aktuellen Stand des Kassenbuchs zu vergewissern. Dies hilft Doppelausgaben, und Betrug zu verhindern und macht es zu einem sicheren und vertrauenswürdigen System, wie eine digitale Version des „Ehrenkodex“. Wenn du also das nächste Mal **Bitcoin** verschickst, kannst du dich entspannt zurücklehnen, weil du weißt, dass das Netzwerk dir den Rücken freihält.

Wie also löst **Bitcoin** dieses Problem? Nun, lasst es uns herausfinden.

- **Bitcoin** verhindert Doppelausgaben, indem es einen Bestätigungsmechanismus implementiert und ein universelles Kassenbuch (Blockchain) pflegt.
- Die Transaktionen werden der Blockchain in chronologischer Reihenfolge und mit Zeitstempeln hinzugefügt.
- Um doppelte Ausgaben zu vermeiden, wird nur die erste Transaktion, die genügend Bestätigungen erhält (normalerweise 6), in die Blockchain aufgenommen, während die anderen abgelehnt werden.
- Transaktionen auf der Blockchain sind unumkehrbar und können nicht manipuliert werden.

Bitcoin-Mining-Node lehnt Transaktion vom Mempool ab.





Wenn eine Transaktion initiiert wird, kann jeder **Node** sie im Netzwerk in ein paar einfachen Schritten verifizieren:

1. Zunächst prüft der Node, ob die Transaktion ordnungsgemäß mit dem privaten Schlüssel des Absenders signiert ist. Dadurch wird sichergestellt, dass die Transaktion rechtmäßig ist und nicht manipuliert wurde.
2. Als Nächstes prüft der Node, ob der Absender über genügend Geldmittel verfügt, um die Transaktion durchzuführen. Dazu prüft er den Kontostand des Absenders im Kassenbuch der Blockchain.
3. Schließlich validiert der Node auch die **Inputs** und **Outputs** der Transaktion, indem er sicherstellt, dass die Inputs, die in der Transaktion ausgegeben werden, nicht bereits in einer anderen Transaktion ausgegeben wurden und dass die Outputs das Gesamtangebot nicht übersteigen.

Wie wir sehen werden, wird die Kombination aus **Public-Key-Kryptographie** und dem **UTXO-System** (Unspent Transaction Output) in **Bitcoin** verwendet, um die Authentizität von Transaktionen zu überprüfen und Betrug ohne eine zentrale Instanz zu verhindern. Die **Public-Key-Kryptographie** gewährleistet eine sichere Kommunikation und Überweisung von Geldern, während **UTXO** eine Aufzeichnung aller Gelder im Netzwerk führt und Doppelausgaben verhindert.



UTXO, die Abkürzung für „Unspent Transaction Output“, ist einfach eine Aufzeichnung aller im Netzwerk verfügbaren Mittel, die noch nicht ausgegeben wurden.

7.1 Die Nachverfolgung deiner Geldeinheiten

In **Bitcoin** funktionieren Transaktionen so, als würde man einen großen Geldschein in kleinere Scheine aufteilen und diese an verschiedene Personen weitergeben. Das Wechselgeld, das man aus einer Transaktion erhält, wird als nicht ausgegebener Output bezeichnet und kann als Input für eine neue Transaktion verwendet werden. Outputs in **Bitcoin**-Transaktionen können entweder **ausgegeben oder unverbraucht** sein, und ein unverbrauchtes Output wird als wertvoll angesehen, weil es in neuen Transaktionen verwendet werden kann.

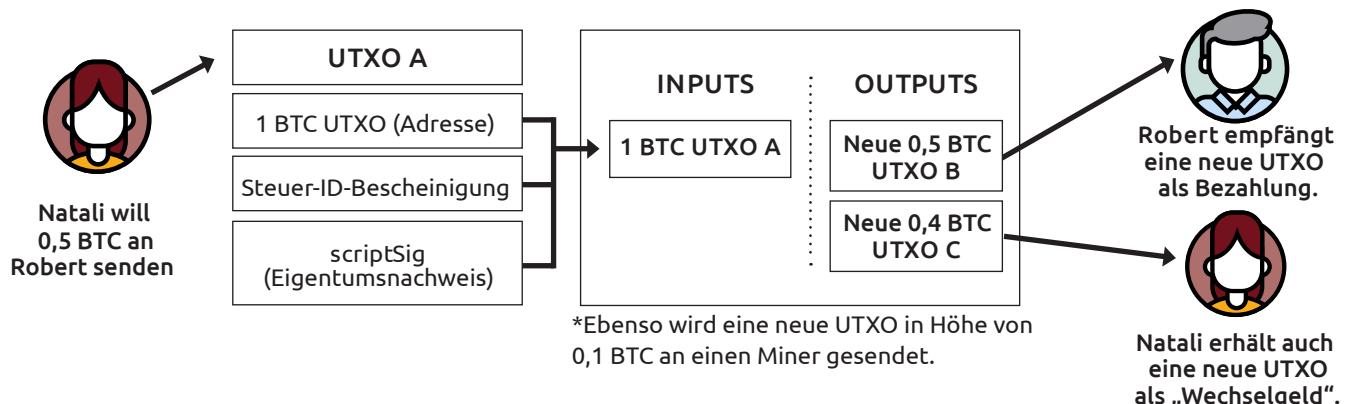
- Stell dir vor, du verwendest mehrere Geschenkkarten, um einen Einkauf zu bezahlen. Die Geschenkkarten aus früheren Transaktionen dienen als Input, und das Wechselgeld, das du erhältst, wird durch eine neue Geschenkkarte mit dem Restbetrag dargestellt. Dies ist vergleichbar mit der Funktionsweise von **Bitcoin**-Transaktionen mit UTXOs.

Was sind UTXOs?

Der Kontostand einer Wallet ist die Summe aller UTXOs eines Nutzers. UTXOs werden verwendet, um den Besitz von **Bitcoin** im Netzwerk zu erfassen. Wenn eine Transaktion durchgeführt wird, werden neue UTXOs erstellt, und wenn eine Transaktion ausgegeben wird, werden bestehende UTXOs verbraucht.

- UTXOs sind wie digitale Münzen in der Welt von **Bitcoin**. Es ist das Wechselgeld, das man zurückbekommt, nachdem man ein paar **Bitcoin** ausgegeben hat.

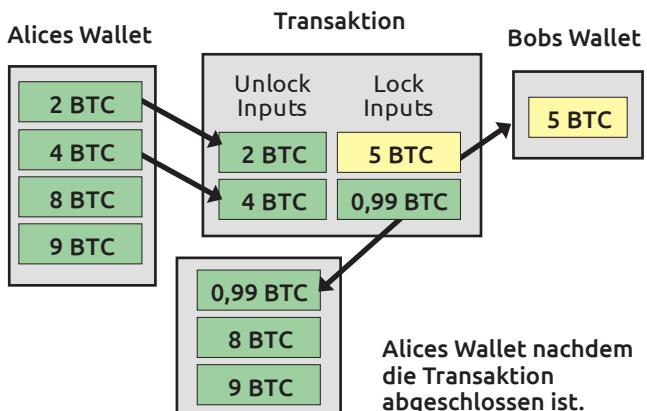
Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs



Die Funktion von UTXOs bei Bitcoin-Transaktionen

Wenn eine Transaktion durchgeführt wird, wird der gesendete **Bitcoin**-Betrag in mehrere Outputs aufgeteilt, von denen jeder mit einer bestimmten Adresse verbunden ist.

- Wenn du **Bitcoin** an jemanden schickst, verwendest du einen oder mehrere Unspent Transaction Outputs (UTXOs) als Quelle der Geldmittel. Diese UTXOs werden, wenn nötig, kombiniert, um einen neuen Output zu erstellen, der dem Empfänger der Transaktion gehört. Dieser neue Output (UTXO) geht dann in das Eigentum des Empfängers über und kann in einer zukünftigen Transaktion als Geldquelle verwendet werden. Diese Kette von UTXOs schafft eine transparente und nachvollziehbare Historie aller **Bitcoin**-Transaktionen auf der Blockchain, beginnend mit dem allerersten Block.



- Wenn jemand zum Beispiel 2 **Bitcoin** senden möchte, aber einen UTXO im Wert von 5 **Bitcoin** hat, wird die Differenz von 3 **Bitcoin** als „Wechselgeld“ an den Absender zurückgeschickt. Dieses Wechselgeld ist ein neuer UTXO für den Absender und kann in einer zukünftigen Transaktion ausgegeben werden.
- In diesem Beispiel schickt Alice Bob 5 **Bitcoin** und behält einen Teil für sich selbst. Sie kombiniert 6 **Bitcoin** aus ihren vier UTXOs, die insgesamt 23 **Bitcoin** ergeben, und sendet 5 an Bob und 0,99 zurück an sich selbst, mit einer 0,01 Gebühr für die Bearbeitung. Die Transaktion wird dann zur Blockchain hinzugefügt, wodurch alle Nodes mit einer Kopie des aktualisierten UTXO-Ledgers aktualisiert werden. Wenn Alice dann versucht, 23 **Bitcoin** in einer separaten Transaktion an Chris zu senden, wird dies von den Nodes abgelehnt, da ein Teil der Outputs bereits ausgegeben wurde.

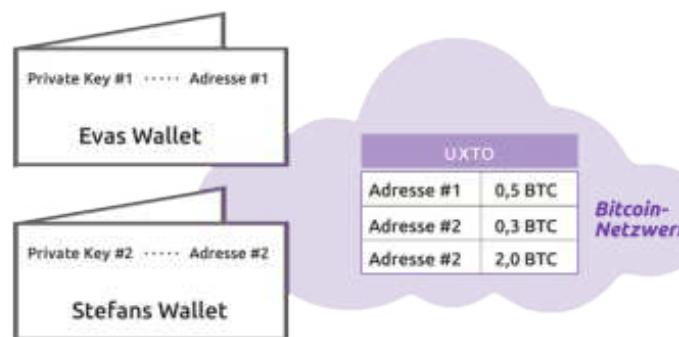
Wenn jemand versuchen würde, einen ausgegebenen Output in seiner Transaktion zu verwenden, würde diese wahrscheinlich von den Nodes im Netzwerk abgelehnt werden. Dies liegt daran, dass diese Nodes eine Kopie desselben Datenbestandes führen und leicht einen Konsens erreichen können, indem sie den Kontostand jeder Adresse überprüfen, bevor sie eine neue Transaktion validieren. Dies gewährleistet die Integrität und Gültigkeit der Transaktionen im Netz.



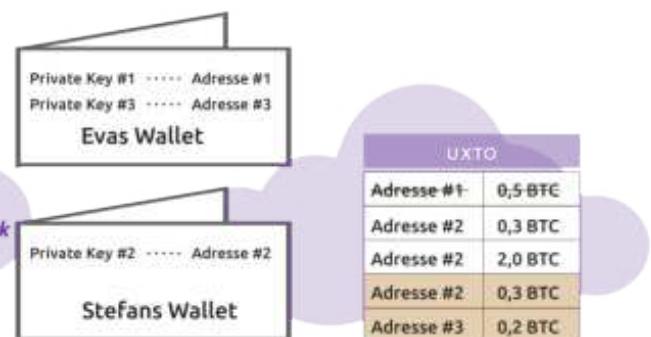
Kapitel 7

Betrachten wir ein anderes Beispiel:

Nur die Person, die den privaten Schlüssel für eine Adresse besitzt, kann auf die in dieser Adresse gespeicherten UTXOs zugreifen. Wenn Eva zum Beispiel einen privaten Schlüssel für Adresse #1 hat, sieht sie 0,5 **Bitcoin** in ihrer Wallet. Wenn Stefan einen privaten Schlüssel für Adresse #2 hat, sieht er 2,0 **Bitcoin** in seiner Wallet.



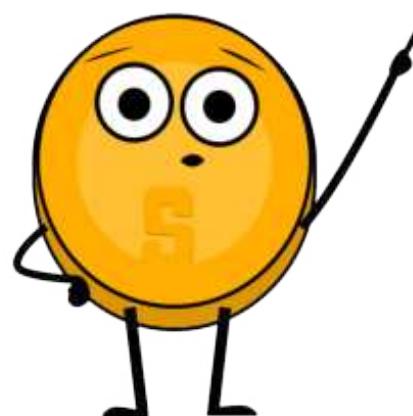
Wenn Eva 0,3 **Bitcoin** an Stefan sendet, generiert ihre Wallet einen neuen privaten Schlüssel und eine neue Adresse (#3). Der ursprüngliche UTXO auf Adresse #1 wird verbraucht und zwei neue UTXOs werden erstellt: einer für Stefans Adresse mit 0,3 **Bitcoin** und einer für Evas neue Adresse mit 0,2 **Bitcoin**. Nachdem diese Transaktion im Kassenbuch erfasst wurde, zeigt Stefans Wallet 2,6 **Bitcoin** und Evas Wallet 0,2 **Bitcoin** an.



Unten sieht man einen Screenshot einer realen Transaktion, bei der es nur einen Input gibt. In einem allgemeineren Fall könnte das Startguthaben jedoch die Summe mehrerer UTXOs sein, die eine Person aus früheren Transaktionen angesammelt hat.



Was kannst du dabei feststellen? Stimmen die Inputs mit den Outputs überein? Kannst du die Details der Transaktion beschreiben? Gibt es einen Zusammenhang zwischen den beiden Screenshots? Und welche Transaktion fand zuerst statt?



Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs



Im Allgemeinen werden verbrauchte Outputs in rot und nicht verbrauchte Outputs in grün angezeigt. Diese Farbcodierung bietet eine visuelle Möglichkeit zur schnellen Identifizierung von verbrauchten und nicht verbrauchten Outputs. Dies kann nützlich sein, um Transaktionen zu verfolgen und den Geldfluss in einer Blockchain zu verstehen.

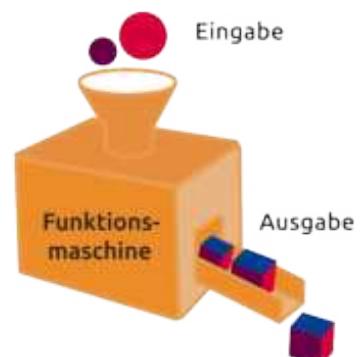
7.2 Sicherheit und Geheimhaltung

Lass dich bitte nicht von den Fachbegriffen und mathematischen Konzepten einschüchtern. Wir verstehen, dass nicht jeder ein Mathematik-Freak ist, aber du wirst dich vielleicht selbst überraschen und sehen, dass selbst die komplexesten Ideen mit ein wenig Anstrengung verstanden werden können.

Was ist eine Funktion, genauer gesagt, was ist eine Einwegfunktion?



Eine Funktion ist wie eine Maschine, die Informationen aufnimmt und sie in etwas Neues verwandelt. Die Informationen, die man der Funktion gibt, werden als **Eingabe** bezeichnet. Die neue Information, die die Funktion erzeugt, wird als **Ausgabe** bezeichnet. Funktionen helfen Computern, Aufgaben zu erledigen und Probleme zu lösen.



Stell dir das wie ein Rezept für die Zubereitung eines Salats vor. Das Rezept (oder die Funktion) sagt dir, welche Zutaten du verwenden und wie du sie zusammenmischen musst, um den Salat zu machen. Du kannst verschiedene Zutaten verwenden, aber das Rezept liefert dir immer den Salat als Ergebnis. Funktionen können dazu beitragen, Dinge einfacher und effizienter zu machen.



Bei diesem Rezept handelt es sich also um eine **Funktion**, die die **Zutaten** als **Eingaben** nimmt und als **Ausgabe** den **gemischten Salat** produziert.



Bei **Bitcoin** werden Funktionen verwendet, um **Transaktionen auszuführen**. Wir wissen bereits, dass Transaktionen bei **Bitcoin** im Wesentlichen Wertübertragungen von einer Adresse zu einer anderen sind. Um eine Transaktion durchzuführen, wird eine Reihe von kryptographischen Funktionen verwendet, um die Transaktion zu validieren und den Status der **Bitcoin**-Blockchain zu aktualisieren, die ein dezentrales Kassenbuch ist, das alle Transaktionen aufzeichnet.

Zu den Funktionen, die bei einer **Bitcoin**-Transaktion genutzt werden, gehören die Überprüfung der Authentizität der Transaktionsdaten, die Überprüfung, ob der Absender über genügend Geldmittel verfügt, und die Aktualisierung der Guthaben der betreffenden Adressen. Sobald eine Transaktion verifiziert und zur Blockchain hinzugefügt wurde, wird sie Teil der permanenten Aufzeichnung aller Transaktionen im Netzwerk.

- Eine **Einwegfunktion** verwendet eine Reihe von Befehlen, um die Informationen zu verarbeiten und sie in etwas **Neues** umzuwandeln, so wie ein Smoothie-Rezept die Zutaten in ein neues Getränk verwandelt. Aber so wie man einen **Smoothie nicht entmischen kann**, um die ursprünglichen Zutaten zurückzubekommen, kann man auch die **Einwegfunktion nicht umkehren**, um die ursprünglichen **Informationen zurückzubekommen**.



Die **Public-Key-Kryptographie**, zu der auch der öffentliche Schlüssel gehört, beruht auf der Verwendung von Einwegfunktionen, die es schwierig machen, den privaten Schlüssel aus dem öffentlichen Schlüssel zu ermitteln. Es ist zwar nicht „unmöglich“, den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen, aber es ist extrem schwierig, und es würde einen enormen Zeitaufwand und eine enorme Rechenleistung erfordern, um diese Aufgabe zu bewältigen.



- Einen privaten Schlüssel aus einem öffentlichen Schlüssel bei **Bitcoin** zu finden, ist wie der Versuch, eine Nadel in einem Heuhaufen zu finden, der so groß wie ein Fußballfeld ist. Die Nadel steht für den privaten Schlüssel und der Heuhaufen für alle möglichen privaten Schlüssel.

Dementsprechend sind Einwegfunktionen so konzipiert, dass sie nicht umkehrbar sind und nicht entschlüsselt werden können.

Was ist eine Hash-Funktion?



Hashing ist wie ein Fingerabdruck für digitale Daten. Dabei wird eine digitale Nachricht in einen Code fester Länge umgewandelt, der als eindeutiger Identifikator dient.

So wie ein Fingerabdruck eine Person identifizieren kann, kann ein Hash eine digitale Information identifizieren. Hashes werden in vielen Anwendungen verwendet, einschließlich **Bitcoin**-Transaktionen.

Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

Die Verwendung von Hashing bei Bitcoin-Transaktionen

Bei **Bitcoin** wird jede Transaktion mit einem Hash versehen, bevor sie in die Blockchain aufgenommen wird. Der Hash fungiert als Signatur für die Transaktion und bestätigt, dass die Transaktion gültig ist und nicht manipuliert wurde. Wenn jemand versucht, auch nur einen einzigen Buchstaben in der Transaktion zu ändern, wird der Hash völlig anders sein und andere auf die Änderung aufmerksam machen.

Die Rolle von Hashing bei der Gewährleistung von Sicherheit

Hashing ist für die Sicherheit des **Bitcoin-Netzwerks** von entscheidender Bedeutung. Durch die Verwendung von Hashes zur Identifizierung von Transaktionen kann das Netzwerk jeden Versuch erkennen, eine Transaktion zu verändern oder zu manipulieren. Dies hilft, Betrug zu verhindern und sicherzustellen, dass alle Transaktionen korrekt in der Blockchain aufgezeichnet werden.

Eine Hash-Funktion ist eine Art von **Einwegfunktion**, die eine Eingabe (bezeichnet als „Information“ oder „Daten“) in eine numerische Darstellung umwandelt, die als „Hash“ bezeichnet wird. Der ausgegebene Hash-Wert ist den Eingabedaten eindeutig zugeordnet, sodass selbst eine kleine Änderung der Eingabedaten zu einem völlig anderen Hash-Wert führt.

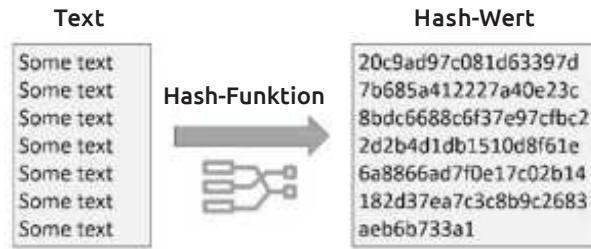


Eine Hash-Funktion ist wie eine geheime Code-Maschine. Sie nimmt eine **Information** auf und verwandelt sie in einen Code.

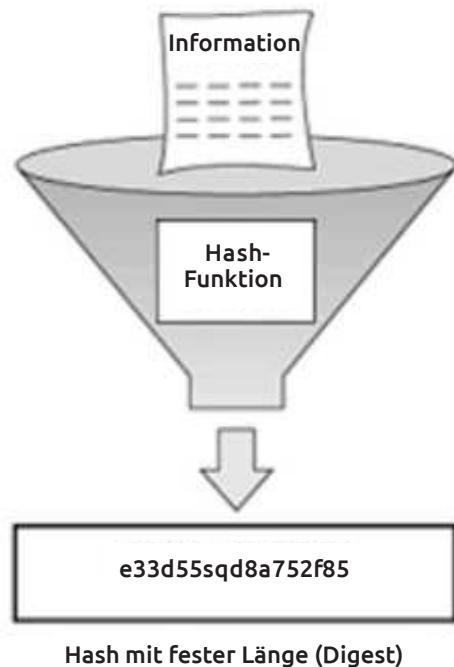
- Der Code sieht für dieselbe Information immer gleich aus. Wenn man die Information auch nur ein wenig ändert, sieht der Code völlig anders aus. Das hilft dem Computer, sich Dinge zu merken und zu prüfen, ob etwas geändert wurde.



<https://tools.keycdn.com/sha256-online-generator>



Daten mit beliebiger Länge



Sofortige Generierung eines SHA256-Hashes aus einer beliebigen Zeichenkette oder einem Eingabewert. Hash-Funktionen werden als Einwegmethoden verwendet.



Kapitel 7



Die Ausgabe, also der Hash, ist immer gleich lang, unabhängig davon, wie lang die ursprüngliche Information war.

Bitcoin verwendet ein paar spezielle Arten von Hash-Funktionen namens SHA-256 und RIPEMD160. Ein paar Beispiele:

- Beachte, dass ein Punkt in der zweiten Eingabe die Ausgabe im Vergleich zur ersten vollständig verändert!
- Die dritte Eingabe ist eine riesige Datei, doch die Ausgabe hat immer noch die gleiche feste Länge wie die beiden anderen.
- SHA256-Hash der Zeichenfolge **hello world**
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- SHA256-Hash der Zeichenfolge **hello world**.
7ddb227315f423250fc67f3be69c544628dfe41752af91c50ae0a9c49faeb87
- SHA256-Hash der herunterladbaren iso-Datei **Ubuntu 18.10**
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

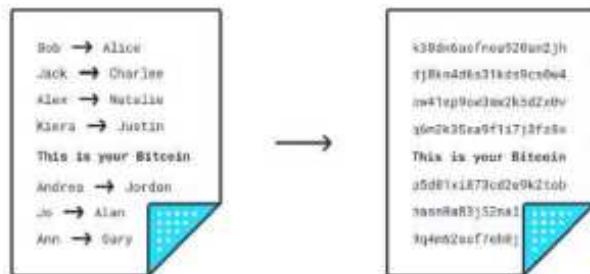
Hashing kann man sich auch als eine Partitur vorstellen, die das Wesentliche eines Musikstücks festhält. Genauso wie eine Partitur eine eindeutige Darstellung eines Musikstücks ist, ist ein Hash-Wert eine eindeutige Darstellung eines Datensatzes. Durch den Vergleich der Partitur eines Musikstücks mit der tatsächlichen Aufführung kann ein Musiker feststellen, ob die Aufführung korrekt ist. In ähnlicher Weise kann man durch den Vergleich des Hash-Werts von empfangenen Daten mit dem ursprünglichen Hash-Wert feststellen, ob die Daten während der Übertragung verändert wurden.



Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

- So wie eine geringfügige Abweichung bei einer musikalischen Darbietung dazu führen kann, dass sie anders klingt, führt selbst die kleinste Veränderung der Originaldaten zu einem anderen Hash-Wert. Dies macht Hashing zu einem wirksamen Mittel, um die Integrität und Authentizität digitaler Informationen zu gewährleisten.

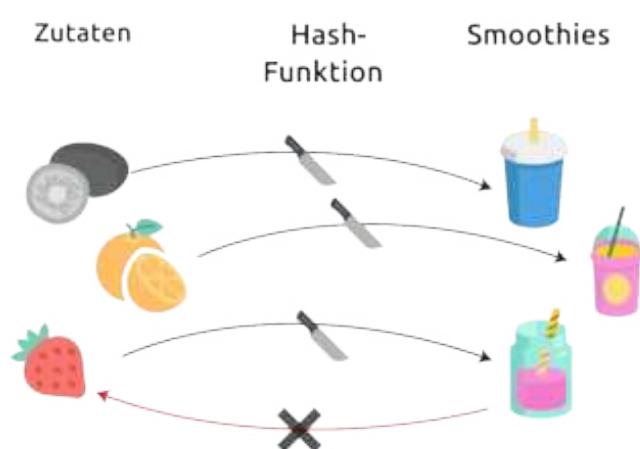
Der Prozess der Verschlüsselung des öffentlichen Schlüssels durch Hashing wird verwendet, um die Sicherheit von Informationen zu verbessern, indem sie in ein unlesbares Format mit fester Länge umgewandelt werden. Bitcoin verwendet die Algorithmen SHA-256 und RIPEMD-160, um öffentliche Adressen zu erzeugen. Die daraus resultierende Ausgabe dient als eindeutige Kennung für den öffentlichen Schlüssel und trägt dazu bei, die Integrität und Sicherheit der in der Blockchain gespeicherten Transaktionen zu gewährleisten. Durch diese **Verschlüsselung** der Informationen wird es für Unbefugte schwieriger, auf die Daten zuzugreifen und sie zu manipulieren.



<https://bitcoinsimulator.duckdns.org/explanation?page=10>

Hashing

Eine Hash-Funktion verarbeitet eine beliebige Eingabe und erzeugt eine Ausgabe mit fester Länge



- **Deterministisch:** Die gleichen Zutaten ergeben immer den gleichen Smoothie.

- **Urbild-Resistenz:** Man kann keine Erdbeere Formen, wenn man einen Smoothie bekommt.

- **Korrelationsresistenz:** Wenn man die Zutaten ein wenig verändert, erhält man einen völlig anderen Smoothie.

- **Kollisionsresistenz:** Es ist schwierig, für einen Smoothie andere Zutaten zu finden, die genau denselben Smoothie ergeben.

- **Schnelligkeit und Überprüfbarkeit:** Wenn man Obst in den Mixer wirft, ist das schnell gemacht, und das Ergebnis ist mit Sicherheit ein Smoothie.



7.3 Der „Mempool“ oder Memorypool: Der Auffangbehälter für Bitcoin-Transaktionen

Was ist der Mempool?

Der Mempool ist wie ein Warteraum für Transaktionen im **Bitcoin-Netzwerk**. Wenn eine Transaktion durchgeführt wird, wird sie zuerst dem Mempool eines Nodes hinzugefügt, bevor sie verifiziert und der Blockchain hinzugefügt wird.

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

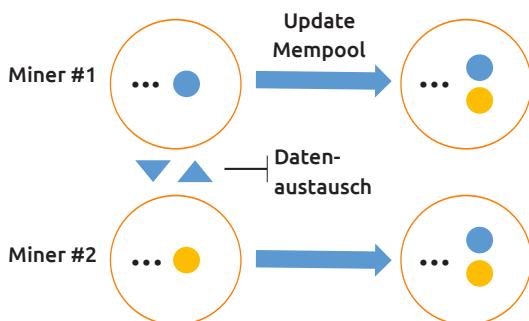
-  tx hsh 6053b699...
fee rate: 3 sat/vB
-  tx hsh bb3b8clfc...
fee rate: 1 sat/vB
-  tx hsh d7c2532a9...
fee rate: 15 sat/vB
-  tx hsh 0ecdd9c6...
fee rate: 2 sat/vB



Wenn ein Node zum ersten Mal eine Transaktion von einem Peer erhält, muss er die Rechtmäßigkeit der Transaktion überprüfen. Niemand möchte fehlerhafte oder betrügerische Transaktionen.



Die Mempool-Synchronisierung ermöglicht es den Nodes, ihre Transaktionen mit anderen Nodes zu teilen, indem sie eine Nachricht mit einer Liste der verifizierten Transaktionen im Mempool senden.



Der Hauptzweck eines Mem pools:

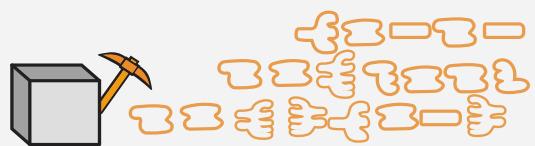
1

Weiterleiten unbestätigter Transaktionen.



2

Bereitstellung von Transaktionen für die Miner.



Accept To Memory Pool (ATMP)

umfasst die Überprüfung von Dingen wie:

- Habe ich diese Transaktion schon?
- Existiert ein Konflikt mit einer anderen Transaktion im Mempool?
- Deckt der **Bitcoin**-Input den **Bitcoin**-Output?
- Belegen die Signaturen, dass die vorherigen Outputs ausgegeben werden können?
- Sind die Gebühren ausreichend?

Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

Wie Transaktionen verifiziert und dem Mempool hinzugefügt werden

Ein **Full-Node** prüft alle Transaktionen, um sicherzustellen, dass sie gültig sind und noch nicht ausgeführt wurden. Wenn eine Transaktion gültig ist, überprüft der Node sie und fügt sie zu seinem Mempool hinzu. Dann teilt er sie mit anderen Nodes, um sie erneut zu überprüfen. Wenn schließlich die Mehrheit zustimmt, wird die Transaktion aus dem Mempool aller Nodes entfernt und dauerhaft in die Blockchain aufgenommen.

Transaktionen im **Bitcoin-Netzwerk** werden aus dem Mempool genommen und bestätigt, wenn sie in einen Block aufgenommen werden, der dann der Blockchain hinzugefügt wird. Es gibt jedoch mehrere Gründe, warum eine Transaktion nach 72 Stunden möglicherweise nicht bestätigt wurde:

- 1. Niedrige Gebühr:** Transaktionen mit einer niedrigen Gebühr werden möglicherweise nicht schnell genug verarbeitet, da die Miner eher Transaktionen mit höheren Gebühren auswählen, um sie in ihre Blöcke aufzunehmen.
- 2. Überlastung des Netzwerks:** Wenn das Netzwerk überlastet ist, kann es zu Verzögerungen bei der Bestätigung von Transaktionen kommen, selbst wenn diese eine hohe Gebühr haben.
- 3. Versuch von Doppelausgaben:** Wenn ein böswilliger Akteur versucht, Doppelausgaben zu tätigen, kann seine Transaktion vom Netz zurückgewiesen werden.
- 4. Falsche oder unvollständige Daten:** Wenn eine Transaktion falsche oder unvollständige Daten enthält, kann sie vom Netzwerk zurückgewiesen werden.
- 5. Fehlerhafte Transaktion:** Wenn eine Transaktion fehlerhaft ist, kann sie vom Netz zurückgewiesen werden.

Um zu vermeiden, dass Transaktionen abgelehnt werden, empfiehlt es sich, eine Gebühr zu wählen, die hoch genug ist, um die zeitnahe Bearbeitung der Transaktion zu gewährleisten, und vor dem Absenden noch einmal zu überprüfen, ob alle Daten der Transaktion korrekt sind.

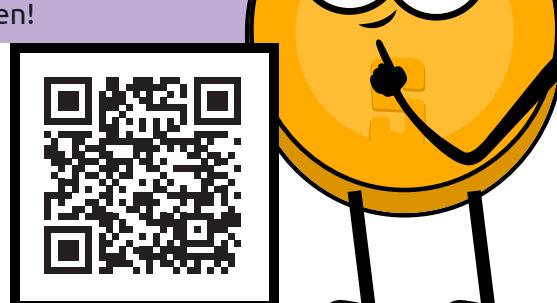


Bei einem **DDoS-Angriff** (Distributed Denial of Service) wird versucht, das Netzwerk für die Nutzer unerreichbar zu machen, indem es mit zu viel Datenverkehr aus mehreren Quellen überlastet wird. Dieser Angriff zielt darauf ab, den normalen Verkehr einer Website oder eines Dienstes zu stören, indem er sie mit fingiertem Datenverkehr überflutet, sodass es für echte Nutzer schwierig oder unmöglich wird, auf die Website zuzugreifen oder die Dienstleistung zu nutzen.

7.3.1 Gemeinschaftsübung: In der Warteschleife: Die unbestätigten Transaktionen des Bitcoin-Netzwerks

Gemeinschaftsübung: Befolge die folgenden Anweisungen!

1. Geh auf die Website <https://bits.monospace.live/>





2. Such dir eine unbestätigte Transaktion aus und klicke sie an!

- Welche Informationen kannst du finden?
- Kannst du nachvollziehen, woher die Bitcoin kommen?
- Wie viele Adressen siehst du? Was bedeutet Input und Output?
- Kannst du die UTXO nachvollziehen? Kannst du erkennen, welche BTC ausgegeben wurden?
- Stimmt der Input mit dem Output überein?
- Fällt für jede Transaktion eine Gebühr an?
- An wen geht die Gebühr? Ist sie angemessen?
- Wer zahlt die Gebühr?
- Kannst du herausfinden, wie viel BTC von einer Adresse zu einer anderen gesendet wurden?

3. Notiere die TxID, den Gebührensatz (fee rate), die Gebühr (fee) und den Gesamtwert der Transaktion auf einem Zettel!

4. Analysiere bei Bedarf weitere Transaktionen und vergleiche sie mit der ersten in Bezug auf den Betrag, die gezahlte Gebühr und der Wahrscheinlichkeit, in den nächsten Block aufgenommen zu werden!

5. Überlege, was es bedeutet, wenn ein Block „gemined“ wird und eine Transaktion „unbestätigt“ ist!

6. Bereite dich darauf vor, diese Beobachtungen und Fragen in der nächsten Unterrichtsstunde zu besprechen!

7.4 Hinter den Kulissen der Blöcke: Das Geheimnis vom Bitcoin-Scripting

Script ist eine Programmiersprache, die in **Bitcoin** verwendet wird, um **Smart Contracts** zu erstellen und **Transaktionen zu automatisieren**. Um Script zu verstehen, ist es hilfreich, es sich als eine Reihe von Anweisungen vorzustellen, die dem **Bitcoin-Netzwerk** sagen, was es mit einer bestimmten Transaktion tun soll.



Ein **Smart Contract** ist ein selbstausführender Vertrag, bei dem die Bedingungen der Vereinbarung zwischen Käufer und Verkäufer direkt in Codezeilen geschrieben sind. Der Code und die darin enthaltenen Vereinbarungen existieren in einem Blockchain-Netzwerk und werden automatisch ausgeführt.

- Stell dir das wie einen Verkaufsautomaten vor! Du wirfst Geld ein, wählst etwas aus, und der Automat gibt die Ware automatisch heraus. Auf die gleiche Weise führt ein intelligenter Vertrag automatisch die Bedingungen der Vereinbarung zwischen zwei Parteien aus, ohne dass Intermediäre wie Anwälte oder Banken erforderlich sind.

Ein Smart Contract könnte zum Beispiel dazu verwendet werden, eine finanzielle Vereinbarung wie ein Darlehen oder eine Anleihe abzubilden. Die Bedingungen der Vereinbarung, wie der Zinssatz und der Rückzahlungsplan, sind in dem Vertrag kodiert. Wenn die vereinbarten Bedingungen erfüllt sind, führt der Vertrag die Bedingungen automatisch aus und überträgt die entsprechenden Geldmittel.

Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

Die entscheidenden Vorteile von Smart Contracts bestehen darin, dass sie transparent, sicher und selbstausführend sind, was dazu beitragen kann, die mit herkömmlichen Vertragsprozessen verbundenen Kosten und Risiken zu verringern. Da sie in einem dezentralisierten Netzwerk existieren, sind sie außerdem resistent gegen Manipulationen oder Eingriffe, was sie zu einer sichereren und vertrauenswürdigeren Methode zur Durchführung von Transaktionen macht.

In ähnlicher Weise verwendet **Bitcoin** Script, um sicherzustellen, dass bestimmte Bedingungen erfüllt sind, bevor eine Transaktion verarbeitet wird.

Andere Blockchain-Netzwerke wie Ethereum unterstützen zwar auch Smart Contracts und programmierbare Transaktionen, verwenden aber andere Programmiersprachen und Ansätze, um die Regeln und Bedingungen für Transaktionen durchzusetzen. Nur **Bitcoin** verwendet Script.

Script ist eine sehr einfache Programmiersprache, die jedoch leistungsfähig genug ist, um eine Vielzahl von Transaktionen zu verarbeiten. Sie kann zum Beispiel verwendet werden, um Transaktionen mit mehreren Signaturen zu erstellen, bei denen mehrere Personen eine Transaktion signieren müssen, bevor sie verarbeitet werden kann, oder um einen Smart Contract zu erstellen, bei dem eine Transaktion automatisch ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind.

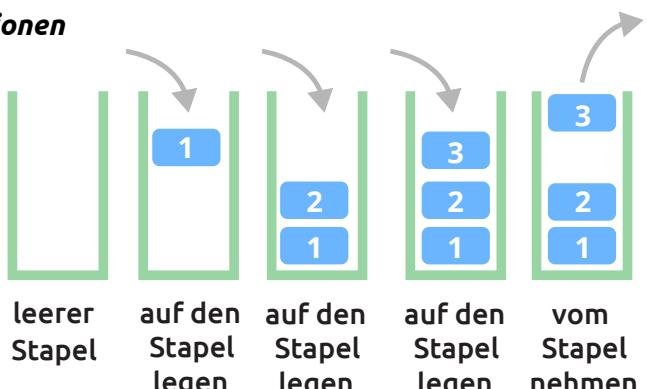
Script mag zwar komplex erscheinen, aber die Grundidee dahinter ist eigentlich ganz einfach. Durch die Verwendung von Script kann das **Bitcoin-Netzwerk** automatisch die Regeln und Bedingungen von Transaktionen durchsetzen, was es zu einem sicheren und effizienten Weg macht, Werte zu übertragen.

Die Verwendung von Scripting bei Bitcoin-Transaktionen

- Stell dir vor, du hast eine Reihe von Münzen und du willst sie in verschiedene Fächer sortieren, etwa so wie Münzen in verschiedene Sparschweine zu stecken! Die Reihenfolge, in der du die Münzen in die Fächer legst, ist dabei entscheidend. Dies ist vergleichbar mit der Art und Weise, wie Satoshis bei einer Transaktion übertragen werden. Die Inputs sind wie eine Reihe von Münzen und die Outputs sind die Fächer, die darauf warten, eine Münze zu erhalten.

Um die Münzen den Fächern zuzuordnen, gehe jede Münze der Reihe nach durch und lege sie in das erste verfügbare Fach. Dies wird als „first-in-first-out“ oder FIFO bezeichnet, was bedeutet, dass die erste Münze in der Reihe in das erste verfügbare Fach gelegt wird, und so weiter.

- Skripte arbeiten mit einem stapelbasierten System, bei dem die Anweisungen in der Reihenfolge ihres Erscheinens abgearbeitet werden, also von oben nach unten. Das Konzept ist vergleichbar mit einem Tellerstapel, bei dem man nur auf den Teller zugreifen kann, der oben auf dem Stapel liegt.

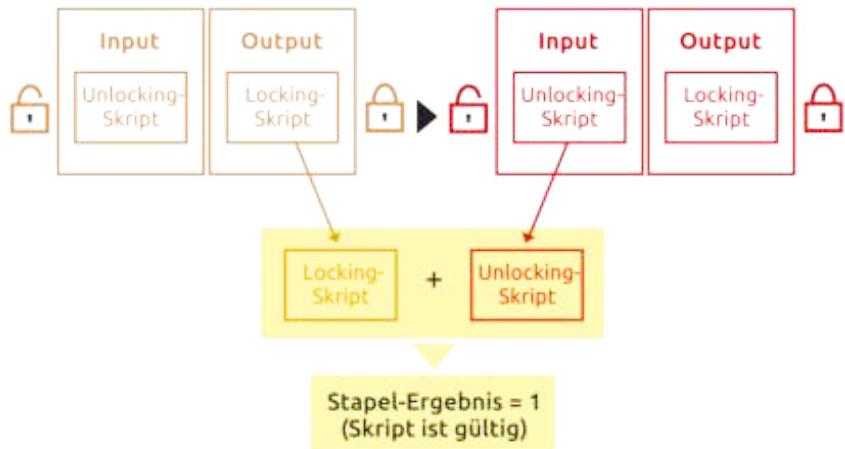




Kapitel 7

Eine einfache **Bitcoin**-Transaktion verwendet mindestens ein „Sperrskript/Locking-Skript“ und ein „Entsperrskript/Unlocking-Skript“, um zu bestimmen, wer auf die Gelde in einer bestimmten Wallet-Adresse zugreifen kann. Das Locking-Skript kann man sich als eine Liste von Anweisungen vorstellen, die beschreibt, wie der Empfänger der Gelder auf diese zugreifen kann, während das Unlocking-Skript die Gelder wieder freigibt.

- Stell dir Script als ein Rezept zum Backen eines Kuchens vor! So wie du die Schritte im Rezept befolgen musst, um den Kuchen zu backen, muss der Computer die Anweisungen in Script in einer bestimmten Reihenfolge befolgen, um das Eigentum an **Bitcoin** zu übertragen.



Durch die Verwendung von Skripten zum Sperren und Ent sperren sowie von privaten und öffentlichen Schlüsseln kann der Besitz und die Übertragung von UTXOs sicher verfolgt und überprüft werden.

7.4.1 Ein technischer Einblick in Bitcoin-Transaktionen

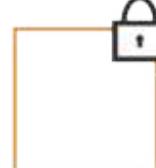
Das Sperrskript enthält die **Adresse des Empfängers** und prüft, ob der richtige private Schlüssel verwendet wurde. Dadurch wird gewährleistet, dass private Schlüssel vertraulich bleiben und sicher geschützt werden können.

Um das Geld freizugeben, muss der Absender den Besitz nachweisen, indem er eine digitale Signatur mit seinem privaten Schlüssel erzeugt und damit den Besitz der Adresse bestätigt.



1EUXSxuUVy2PC5enGXR1a3yxBEjNWMHuem CHECKPRIVATEKEY

Locking-Skript



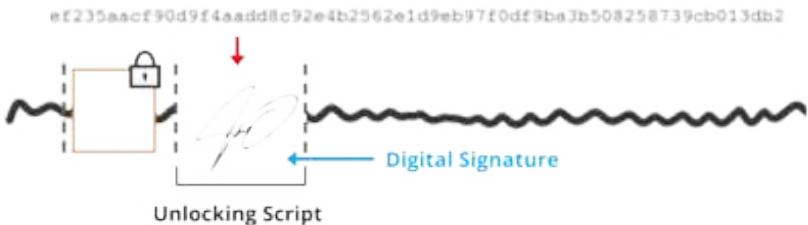
Der Output (**Bitcoin**-UTXO) wurde dieser Adresse (1EUX...) zugeschrieben und gesperrt und nur der richtige private Schlüssel kann ihn entsperren.

Die Geheimnisse der inneren Funktionsweise von Bitcoin: Mathematik, Mempool und UTXOs

Nehmen wir zum Beispiel an, dass du **Bitcoin** an einen Freund schicken willst, aber du willst sicherstellen, dass dein Freund sie erst nach einem bestimmten Datum ausgeben kann. Du kannst **Bitcoin**-Script verwenden, um diese Bedingung zu

definieren, was als „**time-lock** (Zeitsperre)“ bekannt ist. Wenn du die Transaktion erstellst, fügst du ein Skript ein, das die Bedingung der Zeitsperre festlegt. Wenn dein Freund die **Bitcoin** erhält, kann er sie erst ausgeben, wenn das angegebene Datum verstrichen ist.

Bitcoin-Script kann auch verwendet werden, um komplexere Bedingungen für das Tätigen von **Bitcoin**-Ausgaben zu schaffen, wie z. B. Transaktionen mit mehreren Signaturen, bei denen mehrere Parteien eine Transaktion authentifizieren müssen, bevor sie ausgegeben werden kann. Dies kann in Situationen nützlich sein, in denen mehrere Parteien eine Transaktion genehmigen müssen.



CHECKPRIVATEKEY ist eine Funktion, die überprüft, ob die Adresse mit dem richtigen privaten Schlüssel übereinstimmt.



CHECKSIG prüft, ob DIE Transaktion vom Besitzer des privaten Schlüssels genehmigt wurde, der zu dem öffentlichen Schlüssel passt, der zum Signieren der Transaktion verwendet wurde.

Vereinfacht ausgedrückt, trägt Script zur Sicherheit und Zuverlässigkeit von **Bitcoin**-Transaktionen bei, indem es private und öffentliche Schlüssel verwendet, um das Eigentum und die Übertragung von Geldern zu verifizieren. Verschiedene Transaktionsmethoden haben unterschiedliche Sicherheitsniveaus. Einige offenbaren den öffentlichen Schlüssel des Empfängers während der Transaktion, was ihn anfällig für Diebstahl macht, falls der private Schlüssel jemals gehackt wird. Bei anderen bleibt der öffentliche Schlüssel verborgen und bietet ein höheres Maß an Sicherheit.



Kapitel 7



Im nächsten Kapitel werden wir tiefer in den Prozess des Minings und die Rolle der Miner im **Bitcoin-Netzwerk** eintauchen. Wir werden untersuchen, wie sie Transaktionen validieren, neue Blöcke erstellen und Belohnungen für ihre Bemühungen erhalten.

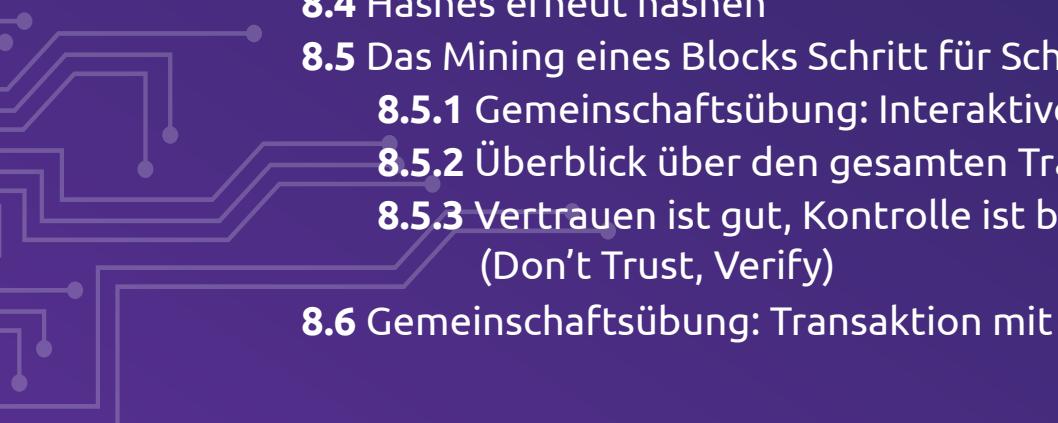
Bleib dabei, um ein umfassendes Verständnis der Funktionsweise des **Bitcoin-Netzwerks** zu erlangen!



Kapitel 8

Eine sichere Kette bauen: Der Prozess des Bitcoin- Minings und seine Rolle in der Blockchain

- 8.0 Die Juwelen der Blockchain: Die Miner und der Mining-Prozess**
- 8.1 Das dynamische Belohnungssystem des Bitcoin-Minings: Blocksubvention, Transaktionsgebühren und Halvings**
- 8.2 Die entscheidende Aufgabe des Bitcoin-Minings: Die Sicherung der Blockchain**
- 8.3 Analyse eines Blocks**
- 8.4 Hashes erneut hashen**
- 8.5 Das Mining eines Blocks Schritt für Schritt erklärt**
 - 8.5.1 Gemeinschaftsübung: Interaktive Mining-Übung**
 - 8.5.2 Überblick über den gesamten Transaktionsvorgang**
 - 8.5.3 Vertrauen ist gut, Kontrolle ist besser (Don't Trust, Verify)**
- 8.6 Gemeinschaftsübung: Transaktion mit UTXOs**



Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

8.0 Die Juwelen der Blockchain: Die Miner und der Mining-Prozess

Die Miner sind die Buchhalter.

- In zentralisierten Systemen werden Buchhalter von Unternehmen bezahlt, um dessen finanziellen Aufzeichnungen im Überblick zu behalten und die Richtigkeit und Vollständigkeit zu gewährleisten.

In ähnlicher Weise werden **Miner** in **Bitcoin** für ihre Arbeit beim Überprüfen und Hinzufügen von Transaktionen zur Blockchain bezahlt und tragen dazu bei, dass das Netzwerk sicher ist und reibungslos funktioniert. Diese Arbeit erfordert den Einsatz von **Rechenleistung** und spezieller Hardware. Das Ziel des Minings ist es, der Blockchain neue Blöcke hinzuzufügen und ihre Sicherheit, Dezentralität und langfristige Lebensfähigkeit zu erhalten.



Die Miner sammeln unbestätigte Transaktionen und bilden damit einen Block. Dann machen sie sich auf die Suche nach dem wertvollen Schlüssel, der den **Platz des Blocks in der Blockchain** sichert.

Der Schlüssel ist ein „**gültiger Blockhash**“, der unter Milliarden anderer versteckt ist und nur mit einem bestimmten, vom Netzwerk festgelegten Schlüssel entschlüsselt werden kann.

- Stell dir einen riesigen Heuhaufen vor, der mit Millionen von Schlüsseln gefüllt ist, von denen jeder einen einzigartigen Blockhash darstellt! Das Netzwerk hat einen bestimmten Schlüssel festgelegt, der einen wertvollen Preis freischalten wird. Die Miner durchsuchen den Heuhaufen und probieren jeden Schlüssel im Schloss aus, aber nur ein Miner wird das Glück haben, den richtigen Schlüssel zu finden.

Der erste Miner, der den korrekten Blockhash findet, sendet ihn zusammen mit dem Block mit Transaktionen an das Netzwerk. Andere Miner überprüfen dann die Lösung, um sicherzustellen, dass sie auch wirklich passt. Wenn die Lösung korrekt ist, wird der Block der Blockchain hinzugefügt, wodurch ein sicheres und öffentliches Kassenbuch entsteht.

Für ihre harte Arbeit werden die Miner auf zwei Arten belohnt: durch die Blocksubvention und Transaktionsgebühren. Die Blocksubvention sind neu generierte **Bitcoin**, die mit jedem zur Blockchain hinzugefügten Block in Umlauf gebracht werden. Transaktionsgebühren hingegen sind kleine **Bitcoin**-Beträge, die die Nutzer dafür bezahlen, dass ihre Transaktionen schneller bearbeitet und vom Miner im Block priorisiert werden. Die Miner können frei entscheiden, welche Transaktionen sie in den Block aufnehmen, den sie minen, und sie bevorzugen oft die Transaktionen mit den höchsten Transaktionsgebühren. Die Summe aus Blocksubvention und Transaktionsgebühren als Blockbelohnung/Blockreward bezeichnet.



Was ist Bitcoin-Mining?

Bitcoin-Mining ist der Prozess, bei dem Transaktionsdaten zu **Bitcoins** öffentlichen Kassenbuch früherer Transaktionen bzw. der Blockchain hinzugefügt werden.

Dieses Kassenbuch früherer Transaktionen wird Blockchain genannt, weil es eine Aneinanderreihung von Blöcken ist. Diese Kette dient dazu, die Durchführung der Transaktionen all dieser anderen Netzwerke zu validieren.

Bitcoin-Nodes verwenden diese technologische Kette, um eine echte **Bitcoin**-Transaktion von dem Versuch zu unterscheiden, bereits ausgegebene Geldeinheiten noch einmal auszugeben.





8.1 Das dynamische Belohnungssystem des Bitcoin-Minings: Blocksubvention, Transaktionsgebühren und Halvings

Satoshi Nakamoto, der Schöpfer von *Bitcoin*, entwickelte eine intelligente Lösung zur dezentralen Verteilung neuer *Bitcoin* über ein Block-Belohnungssystem.



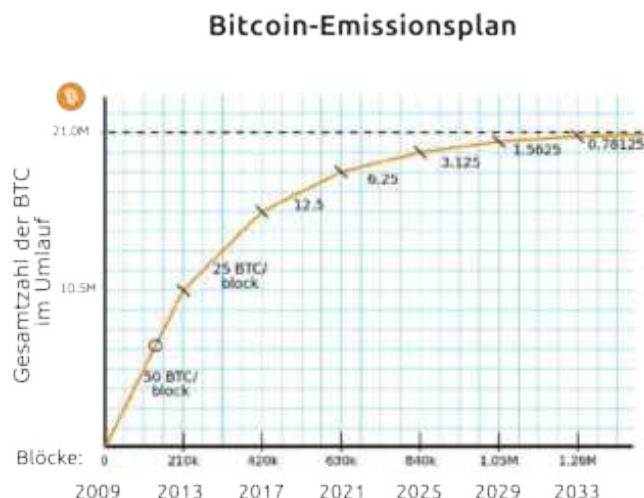
Der Bitcoin-Emissionsplan ist sein Plan für die Schaffung und Freigabe neuer Bitcoin in den Umlauf, der darauf abzielt, die Knappheit von Bitcoin über einen längeren Zeitraum zu erhalten.

In der Anfangszeit von *Bitcoin* erhielten die Miner 50 *Bitcoin* für jeden Block, den sie schürften. Diese Blocksubvention dient als finanzieller Anreiz für Miner, in leistungsstarke Hardware und Strom für ihre Mining-Aktivitäten zu investieren.

Um jedoch das Angebot an neuen *Bitcoin* zu kontrollieren und die Stabilität des Netzwerks aufrechtzuerhalten, halbiert sich die Blocksubvention alle 210.000 Blöcke. Dieser Prozess, der als „Halving“ bekannt ist, reduziert die Menge an neuen *Bitcoin*, die in Umlauf gebracht wird, und schafft weiterhin Anreize für die Miner, das Netzwerk zu sichern und seine Dezentralisierung zu gewährleisten.

- Nehmen wir an, du hast ein Glas, das nur 1000 Bonbons fassen kann. Jeden Tag kannst du 10 Bonbons in das Glas geben. Auf diese Weise werden neue *Bitcoin* geschaffen und durch den Mining-Prozess dem Bestand hinzugefügt. Nach jeweils vier Jahren wird die Menge der Süßigkeiten, die man in das Glas geben kann, jedoch halbiert.

Dies ist vergleichbar mit dem Halving von *Bitcoin*, das die Schaffung neuer *Bitcoin* verlangsamt. Das ultimative Ziel ist es, die Knappheit aufrechtzuerhalten und die Gesamtzahl von *Bitcoin* auf circa 21 Millionen Einheiten zu begrenzen, so wie das Glas nur eine begrenzte Menge an Süßigkeiten fassen kann.



Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

Der Halving-Prozess ist vergleichbar mit der Tatsache, dass Goldminen einen begrenzten Vorrat haben und schließlich immer schwieriger zu finden sind. Heute gibt das *Bitcoin*-Protokoll etwa alle zehn Minuten 3,125 neue BTC an Miner frei, wenn ein Block gemined wird.

Die Tabelle zeigt die Details der nächsten Halbierungsereignisse für *Bitcoin*, einschließlich des Prozentsatzes des Gesamtangebots, der bis zu diesem Datum gemined sein wird, des voraussichtlichen Zeitpunkts des nächsten Halving-Events und der Blocknummer, bei der das Halbierungsereignis voraussichtlich stattfinden wird.

Ereignis	Voraussichtlicher Termin	Block	Blocksubvention	emittierter Anteil in Prozent
fünftes Halving	2028	1.050.000	1,5625	98,4375 %
sechstes Halving	2032	1.260.000	0,78125	99,21875 %
siebentes Halving	2036	1.470.000	0,390625	99,60938 %



Die Umlaufmenge bezieht sich auf die Menge an *Bitcoin*, die derzeit im Umlauf und für den Handel verfügbar ist. Diese Angabe stellt die Gesamtzahl der Einheiten dar, die gemined wurden und sich zu einem bestimmten Zeitpunkt im Umlauf befinden, mit Ausnahme der Einheiten, die möglicherweise für immer gesperrt oder verloren sind.

Je mehr *Bitcoin* gemined werden, um so mehr werden sich die Umlaufmenge und der prozentuale Anteil an der Gesamtmenge erhöhen, bis die Gesamtmenge von 21 Millionen erreicht ist.

Bitcoin: emittierter Prozentsatz der 21-Mio-Gesamtmenge





Die **Inflationsrate** ist die Rate, mit der das zirkulierende Angebot einer Kryptowährung im Laufe der Zeit zunimmt, ausgedrückt als Prozentsatz des Gesamtangebots. Diese Rate wird berechnet als die *Differenz zwischen dem zirkulierenden Angebot und dem maximalen Gesamtangebot (21 Millionen)*, geteilt durch das maximale Gesamtangebot und multipliziert mit 100.

Bei jedem Halving-Event wird die Blocksubvention für die Miner reduziert, wodurch die Emissionsrate neuer **Bitcoin** sinkt. Infolgedessen sinkt die Inflationsrate von **Bitcoin** mit der Zeit, was zu einem Anstieg des **Bitcoin**-Preises führen kann.

Das verringerte Angebot in Verbindung mit der steigenden Nachfrage kann den Preis von **Bitcoin** in die Höhe treiben. Dies kommt nicht nur den frühen Anwendern der Technologie zugute, sondern dient auch als Anreiz für Miner, das Netzwerk weiterhin zu sichern und ihre Rechenleistung und Ressourcen zur Verfügung zu stellen.

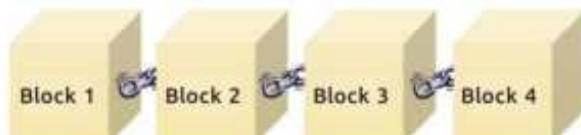
8.2 Die entscheidende Aufgabe des Bitcoin-Minings: Die Sicherung der Blockchain

Was ist ein gültiger Block-Hash in der Blockchain?

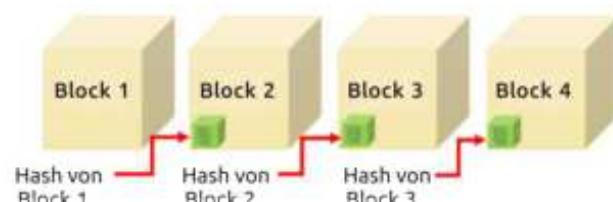
Ein Block-Hash dient als eindeutige Kennung für jeden Block in der Blockchain und hilft, Versuche, vergangene Transaktionen zu verändern, zu erkennen. Die Blöcke in der Blockchain enthalten Transaktionen und bilden eine Kette von Blöcken, beginnend mit dem aller ersten Genesis-Block bis zum jüngsten Block, wodurch eine öffentliche und transparente Aufzeichnung aller Transaktionen entsteht. Der Block-Hash verknüpft jeden Block mit dem vorherigen, sodass jeder die Geschichte jeder Transaktion einsehen kann und die Genauigkeit und Sicherheit der im Netzwerk gespeicherten Daten gewährleistet ist. So wie ein Fingerabdruck eine Person identifiziert, identifiziert der Block-Hash jeden einzelnen Block in der Blockchain.



Der erste **Bitcoin**-Block, der insgesamt 50 **Bitcoin** enthielt, wurde vom Schöpfer von **Bitcoin**, Satoshi Nakamoto, gemined.



Die Blöcke werden miteinander „verbunden“, indem eine bestimmte Beziehung zwischen den Blöcken erzwungen wird. Das heißt, ein Block muss einen „Fingerabdruck“ enthalten, der ein Hash-Wert der Daten des vorherigen Blocks ist. Eine Hash-Funktion kann eine beliebige Nachricht (die Blockinformationen) auf eine feste Größe (z. B. 160 Bit) komprimieren und erzeugt einen Fingerabdruck der Nachricht.



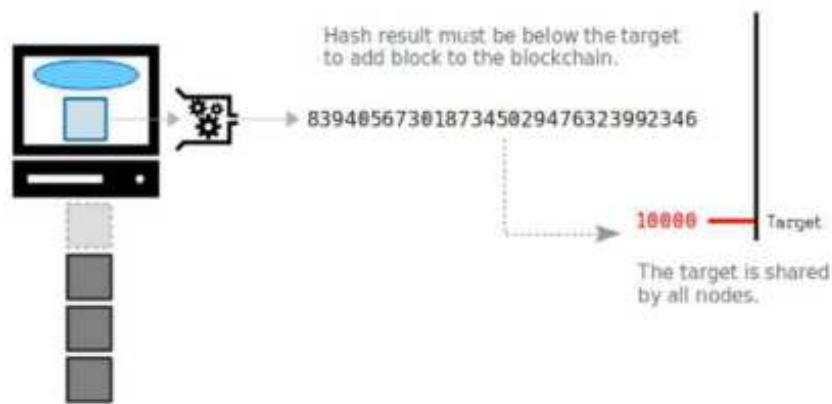
Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

Ein Block-Hash kann zwar zur Überprüfung der Integrität der Daten im Block verwendet werden, gibt aber nicht alle Informationen innerhalb des Blocks preis. Auf die Informationen innerhalb des Blocks kann nur mit Hilfe der kryptographischen Schlüssel zugegriffen werden, die zur Entschlüsselung erforderlich sind. Der Block-Hash ist lediglich ein Mittel, um zu überprüfen, ob die Daten im Block nicht verändert worden sind.

Der Wettstreit um einen Block

Die Miner nehmen an einem Wettbewerb teil, um den Block-Hash zu finden, der mit dem vom Netzwerk festgelegten Ziel (einer speziellen Zahl) übereinstimmt. Der Miner, der den richtigen Block-Hash findet, erhält die Möglichkeit, diesen Block zur Blockchain hinzuzufügen und ihm die entsprechende Hash-ID zuzuweisen. Diese Lösung dient als Nachweis für die Authentizität des Blocks.

- Mining kann mit einem Rennen verglichen werden, bei dem es darum geht, die Ziellinie so schnell wie möglich zu erreichen. Die Zielvorgabe für den Schwierigkeitsgrad (**Difficulty Target**) des Rennens wird in regelmäßigen Abständen angepasst, sodass es schwieriger wird, einen Block zu minen, je mehr Miner an dem Rennen teilnehmen.



- Nehmen wir an, das vom Netzwerk gesetzte Ziel in einer Blockchain ist 1000. Die Miner müssten mit ihren Computern nach einer speziellen Zahl, dem sogenannten Block-Hash, suchen, die kleiner als 1000 ist. Der erste Miner, der einen Block-Hash findet, der kleiner als 1000 ist, darf eine Gruppe von Transaktionen zur Blockchain hinzufügen und wird mit einigen **Bitcoin** belohnt.



Der Schwierigkeitsgrad ist ein Maß dafür, wie schwierig es ist, einen gültigen Block-Hash zu finden, der dem vom Netzwerk gesetzten Ziel entspricht. Er wird regelmäßig angepasst, um sicherzustellen, dass der Blockchain in gleichmäßigem Rhythmus Blöcke hinzugefügt werden. Der Schwierigkeitsgrad wird als Zahl ausgedrückt, und je höher der Schwierigkeitsgrad ist, desto schwieriger ist es, einen Block-Hash zu finden, der der Zielvorgabe entspricht.

- Nehmen wir zum Beispiel zwei verschiedene Hashes:
 - Hash 1: 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
Schwierigkeitsgrad: 1
 - Hash 2: 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
Schwierigkeitsgrad: 2



In diesem Beispiel hat Hash 2 einen höheren Schwierigkeitsgrad als Hash 1, da er mehr Nullen am Anfang erfordert. Das bedeutet, dass es bei einem höheren Schwierigkeitsgrad schwieriger ist, einen Block-Hash zu finden, der dem vom Netzwerk gesetzten Ziel entspricht.

Die Suche nach einem gültigen Block-Hash ist mit einer Menge Computerarbeit verbunden.



Indem er einen gültigen Block-Hash findet, zeigt ein Miner, dass er die Arbeit geleistet hat, die erforderlich ist, um den neuen Block zur Blockchain hinzuzufügen, und er wird in **Bitcoin** für seine Mühe bezahlt. Proof of Work (PoW) ist die Methode, die **Bitcoin** verwendet, um Transaktionen zu validieren und neue Blöcke zur Blockchain hinzuzufügen.

PoW sorgt für die Sicherheit der Blockchain, indem es jedem mit böswilligen Absichten erschwert wird, die Kontrolle zu übernehmen. Das Ziel wird so angepasst, dass alle zehn Minuten ein Block gemined wird, wodurch das Netzwerk noch sicherer wird, da das Ziel immer schwerer zu erreichen ist.

Das vom Netzwerk festgelegte Ziel für das Mining eines bestimmten Blocks könnte beispielsweise folgendermaßen lauten:

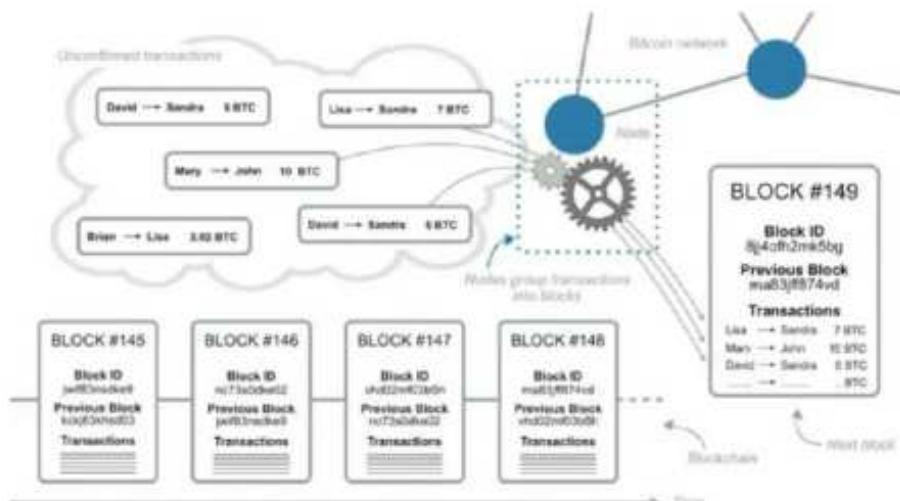
00000000A1m1NgF0RbL0cK5wItHth3hAy5tAcK

Das bedeutet, dass der erste Miner, der einen Hash mit acht führenden Nullen findet, dieses Ziel erreicht und den Block zur Blockchain hinzufügen darf und eine Vergütung in **Bitcoin** erhält.

Die Rolle der Miner

Miner haben in einem Block-chain-Netzwerk eigentlich zwei Aufgaben:
1) die Verifizierung von Transaktionen und
2) das Hinzufügen neuer Blöcke.

Sie sammeln unbestätigte Transaktionen in ihrem Mempool, wählen einen Teil davon aus, um sie in ihren potenziellen Block aufzunehmen, und suchen dann nach dem Block-Hash.



Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

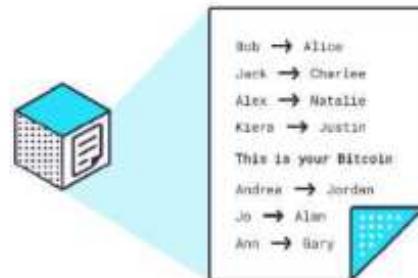
Mehrere Miner können gleichzeitig an der Erstellung neuer Blöcke arbeiten. Der erste Miner, der einen Block-Hash entdeckt, der dem vom Netzwerk gesetzten Ziel entspricht, teilt ihn dem Netzwerk mit, woraufhin die anderen Miner die Transaktionen im potenziellen Block dieses Miners überprüfen, um sicherzustellen, dass sie gültig sind. Wenn die Transaktionen tatsächlich gültig sind, wird der Block zur Blockchain hinzugefügt. Die anderen Blöcke, die von den anderen Minern zu diesem Zeitpunkt erstellt wurden, werden nicht hinzugefügt, sondern verworfen. Dieses Verfahren trägt dazu bei, den Konsens innerhalb des Netzwerks aufrechtzuerhalten und Doppelausgaben zu verhindern.



Ein potenzieller Block ist ein Block von Transaktionen, der für die Aufnahme in die Blockchain in Betracht gezogen wird, aber noch nicht hinzugefügt wurde.

8.3 Analyse eines Blocks

Eine Blockchain besteht aus Blöcken, ähnlich wie Seiten in einem Kassenbuch, in denen neue Transaktionen enthalten sind. Jeder Block hat einen Header mit einer Zusammenfassung der Daten, einem Verweis auf den vorherigen Block und einer eindeutigen Nummer, die **Nonce** oder **einmalig verwendete Nummer** genannt wird, sowie einigen anderen Details. Die Aufgabe der Miner besteht darin, die Header-Informationen bei der Erstellung von potenziellen Blöcken korrekt auszufüllen.

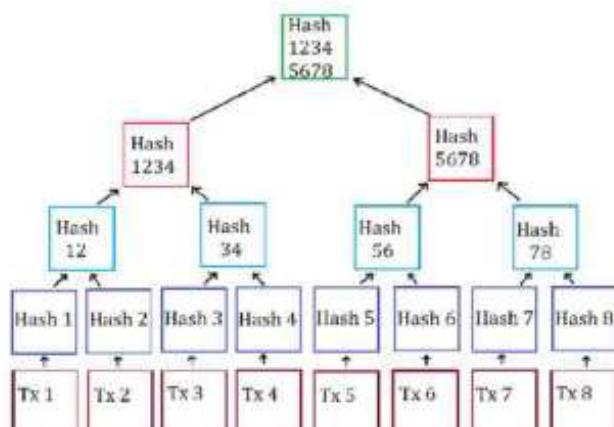


Die Organisation von Transaktionen

Die Miner müssen die Transaktionen in ihren potenziellen Blöcken in einem bestimmten Format anordnen, wobei nur ein Teil der Informationen im Header enthalten ist.



Transaktionen bilden das Rückgrat des **Bitcoin-Netzwerks** und werden durch die Verwendung von **Merkle-Bäumen** effizient und sicher organisiert. Diese Bäume fassen große Datenmengen in einer kompakten Darstellung zusammen und verbessern so die allgemeine Sicherheit und Effizienz des Netzwerks.





Der **Merkle-Root-** bzw. **Merkle-Wurzel-Hash**, der im Header enthalten ist, ist ein einzelner Hash-Wert, der als digitaler Fingerabdruck für alle Transaktionen in einem Block dient. Dies ermöglicht eine effiziente Verifizierung von Transaktionen, ohne dass jede Transaktion einzeln geprüft werden muss, was ihn zu einem wichtigen Bestandteil der Sicherheit und Skalierbarkeit des **Bitcoin-Netzwerks** macht.

Wenn eine Transaktion in einem Block enthalten ist, wird ihr Hash in den **Merkle-Root-Hash** aufgenommen. Wenn sich ein Teil der Daten ändert, wird der endgültige Code anders sein, sodass böswillige Änderungen an den Daten leicht zu erkennen sind. Dies trägt zur Wahrung der Privatsphäre und zum Schutz sensibler Informationen bei, die in jeder Transaktion im Netzwerk enthalten sind.

Wenn ein Hacker versucht, ein einziges Zeichen in einer Transaktion zu ändern, werden die Verifizierungen der nachfolgenden Blöcke fehlschlagen, da jeder Block von den Informationen des vorherigen Blocks abhängt. Die Merkle-Wurzel fungiert als sichere Kette, die alle Transaktionen in einem Block miteinander verbindet und die Genauigkeit und Integrität der Daten im Netzwerk gewährleistet.



Eine Coinbase-Transaktion bei **Bitcoin** ist eine spezielle Art von Transaktion, die in jedem Block der Blockchain enthalten ist. Sie dient zwei Zwecken: Erstens belohnt sie den Miner, der den Block erfolgreich gemined hat, und zweitens bietet sie eine Adresse, um Transaktionsgebühren als Provision zu erhalten.

Diese Transaktion ist auch im Merkle-Baum enthalten. Im Gegensatz zu anderen Transaktionen hat die Coinbase-Transaktion keinen Input, da sie durch den Software-Algorithmus neue Einheiten erzeugt. Stattdessen wird eine neue unverbrauchte Transaktionsausgabe (UTXO) erstellt, die als Input für zukünftige Transaktionen verwendet werden kann.

Die Komponenten eines Blocks: Der Block-Header in der Blockchain



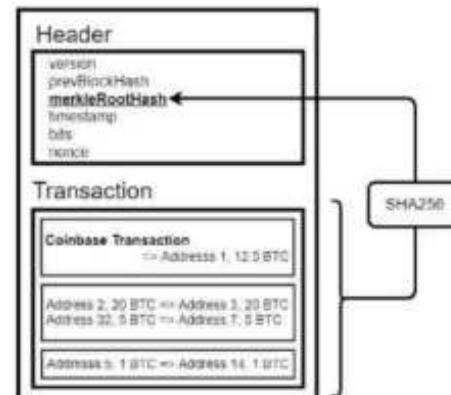
Ein **Block-Header** ist wie der Umschlag eines Buches; er bietet eine Zusammenfassung des Inhalts und wichtige Details eines Blocks.

- **Der Block-Hash:** Der gültige eindeutige Code des Blocks, durch den er identifiziert wird. Ein **Block-Hash** kann verwendet werden, um die Konsistenz der Informationen in einem Block jedes Mal zu überprüfen, wenn der Block oder die darin enthaltenen Informationen überprüft werden.
- **Version:** Dies ist eine Art Kennzeichnung, die angibt, welche Version der Software die Person verwendet hat, die den Block erstellt hat.
- **Vorheriger Block-Hash:** Dies ist der gültige Block-Hash für den Block, der vor dem Block kam, den man gerade betrachtet. Er stellt sicher, dass die Blöcke in der richtigen Reihenfolge sind und dass niemand die vorherigen Blöcke ändern kann, ohne dass dies Auswirkungen auf den aktuellen und alle nachfolgenden Blöcke hat.

Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

Block-Header

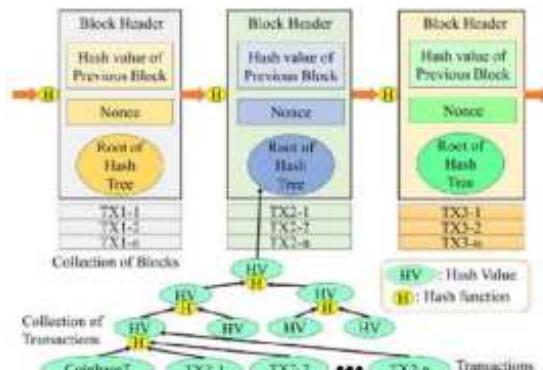
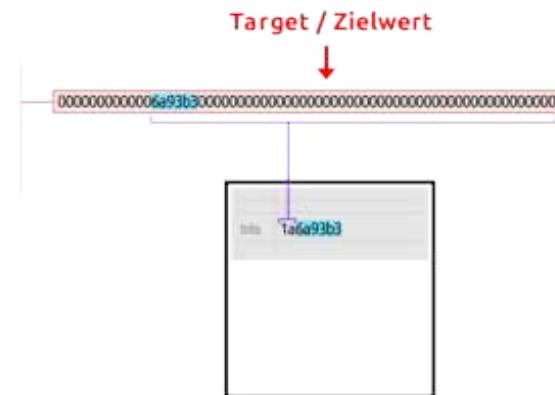
Version	1
vorheriger Block	00
Merkle-Root	ba3ffef2b2b29e5ae2fd4f7186c5c2ad13cf618aa2cde86adacb6229e75b762
Zeitstempel	2012-08-31 11:32:28
Bits	436658110
Nonce	538012418



- Merkle-Root-Hash: SHA256 (Hash(H(1,2),H(3,4,...)), Hash(H(5,6),H(7,8),...)). Dadurch werden bestimmte UTXOs in der Kette aktualisiert.
- Zeit: Dies ist der Zeitpunkt, zu dem die Person, die den Block erstellt hat, mit der Arbeit daran begonnen hat.
- Bits: Dies ist eine Art Code, der angibt, wie schwer es war, diesen Block herzustellen. Er wird auch „Zielwert“ genannt.
- Nonce: Eine Nonce ist eine eindeutige Nummer, die von Minern verwendet wird, um einen neuen Block in einer Blockchain zu erstellen. Miner probieren verschiedene Nonce-Zahlen aus, bis sie eine finden, die ihnen den korrekten Hash-Wert für den Block liefert, was beweist, dass sie die nötige Arbeit geleistet haben, um den Block zu validieren und ihn der Blockchain hinzuzufügen.

Die Nonce-Suche: Die Suche nach der magischen Zahl im Blockchain-Wettstreit

In der Welt der Blockchain hat jeder Block einzigartige Informationen und Sicherheitsmaßnahmen, um Manipulationen zu verhindern. Eine dieser Maßnahmen ist die **Nonce**, eine Zahl, die einmal verwendet wird, um einen einzigartigen potenziellen Block-Hash zu erstellen.



Wenn ein Miner versucht, der Blockchain einen neuen Block hinzuzufügen, muss er die richtige Nonce finden, die einen Hash-Wert erzeugt, der dem vom Netzwerk gesetzten Ziel entspricht. Dazu werden verschiedene Nonce-Werte ausprobiert und durch die Hash-Funktion laufen gelassen, bis der richtige Wert gefunden ist.



Kapitel 8

Denk daran, dass Hash-Funktionen sehr empfindlich auf Änderungen der Eingabe reagieren, was bedeutet, dass schon eine kleine Änderung der Eingabe zu einer völlig anderen Ausgabe führt! Durch die Verwendung eines anderen Nonce-Wertes können die Miner also sicherstellen, dass jeder Block, den sie minen, einen einzigartigen Hash-Wert hat.

Die Nonce ist nur eine der Komponenten des Block-Headers, zusammen mit anderen wichtigen Informationen wie dem Zeitstempel und dem vorherigen Block-Hash. Sobald alle Informationen im Block-Header zusammengehasht wurden, entsteht der **potenzielle Block-Hash-Wert**. Der Miner, der den Hash-Wert findet, der dem vom Netzwerk gesetzten Ziel entspricht, gewinnt das Rennen und darf den Block in die Blockchain aufnehmen.

Wie wir unten sehen, wurde MiPrimerBitcoin für Block 7 mit 1 BTC für die Berechnung des korrekten Block-Hashes belohnt, den das Netzwerk zu diesem Zeitpunkt (21/1/23) benötigte. Zusätzlich kassierte MPB Gebühren von den Transaktionen, die in dem Block enthalten waren. Die **Nonce**, die schließlich den **Gewinner-Hash** ergab, war 354.

Version		6bb6b273f34fcwf6d6
Previous Block ID		b804ef5a3f57479d6t
Merkle Root		ea22f1d48c61e52dd6
Time		7975b4b
Bits		
Nonce = 1		
Version		c488f7bc6249e19e8
Previous Block ID		a72de0106ba79fcf613
Merkle Root		ab709340219b7fc500b
Time		8e6fd87
Bits		
Nonce = 12590		
Version		00000000002418e19
Previous Block ID		a9972de6100fe72d1b
Merkle Root		13a07f034802796f1c6
Time		8d1d9f7
Bits		
Nonce = 2307		

Finding the correct nonce such that the block hash meets the target hash requirements

Block 7			Block 8		
Miner: MiPrimerBitcoin			Miner: MiPrimerBitcoin		
Accepted			Accepted		
2 Transactions			4 Transactions		
New Block Reward	MiPrimerBitcoin	1 BTC	MiPrimerBitcoin	jim	0.03 BTC
MiPrimerBitcoin	Marc	0.2 BTC	MiPrimerBitcoin	Roby	0.04 BTC
7a3bab002a...	7f11b513...		7a3bab002a...	425318058...	
			MiPrimerBitcoin	Delia	0.003 BTC
			7a3bab002a...	8bc94011...	
Hash of the previous Block:			Hash of the previous Block:		
0bb6b273f34fcwf6d6b804ef5a3f57479d6t			00000000002418e19a9972de6100fe72d1b		
Nonce: 354	Hash:		Nonce: 231	Hash:	
000bf0718fa7001bd677945833c7967e29f74646420ba46327fe?			000bf0718fa7001bd677945833c7967e29f74646420ba46327fe?		

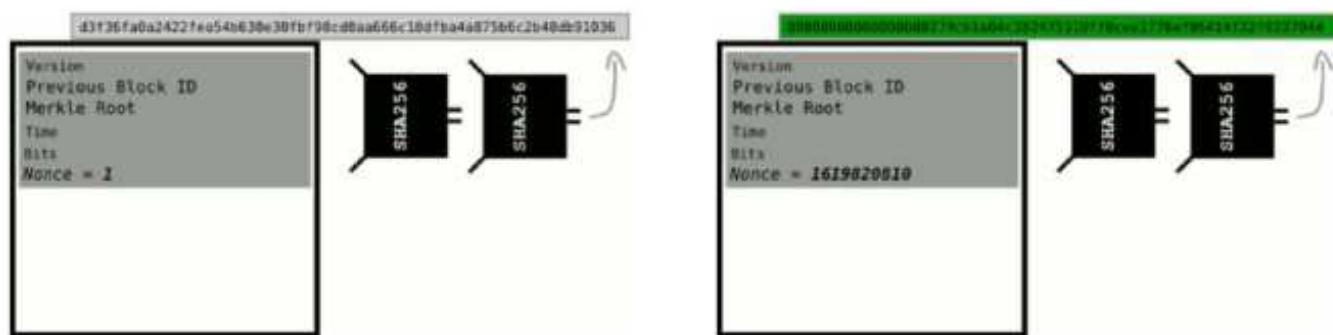


Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

8.4 Hashes erneut hashen

Wie lange brauchen Miner, um einen gültigen Hash zu finden? Und wie schnell können sie die Nonce-Werte während ihres Berechnungsprozesses ändern?

Im folgenden Beispiel benötigte ein Miner 1619820810 Wiederholungen, um einen Hash-Wert mit der erforderlichen Anzahl von Nullen zu finden. Der Miner, dem es gelang, den richtigen Nonce-Wert zu finden, fügte den Block zur Blockchain hinzu und bildete damit einen sicheren und unveränderlichen Teil der Kette.



Die Hashrate ist ein Maß für die Rechenleistung des Netzwerks und die Geschwindigkeit, mit der Miner Nonce-Berechnungen durchführen können, die zur Ermittlung des korrekten Block-Hashes verwendet werden.

Je mehr Rechenleistung ein Miner hat, desto schneller kann er diese Berechnungen durchführen, was ihm einen Vorteil im Mining-Prozess verschaffen kann. Mit zunehmender Hashrate des Netzwerks steigt jedoch auch die Schwierigkeit, neue **Bitcoin** zu minen, wodurch es für alle Miner schwieriger wird, den richtigen Block-Hash zu finden.

- So wie Sportler ihre Ausrüstung aufrüsten, um schneller zu laufen, investieren Bitcoin-Miner in spezielle Computer-Hardware, um ihre Hashrate zu erhöhen und Blöcke effizienter zu minen. Je mehr sie in Ressourcen investieren, desto größer sind ihre Chancen, die Ziellinie als Erster zu erreichen.
- Die Hashrate kann mit der Geschwindigkeit des Läufers verglichen werden. Je leistungsfähiger die Maschine des Miners ist, desto höher ist die Hashrate, und desto schneller kann er minen. Wie bei einem Rennen ist eine hohe Geschwindigkeit jedoch keine Garantie für einen Sieg, wenn das Schwierigkeitsziel auf eine höhere Stufe eingestellt wurde. Die Miner müssen ihre Ausrüstung ständig aufrüsten und ihre Hashrate verbessern, um der Konkurrenz voraus zu sein und eine Chance zu haben, einen Block zu minen und das Rennen zu gewinnen.



Der Prozess, den korrekten Hash-Wert durch Ändern der Nonce zu finden, wird als Mining bezeichnet!



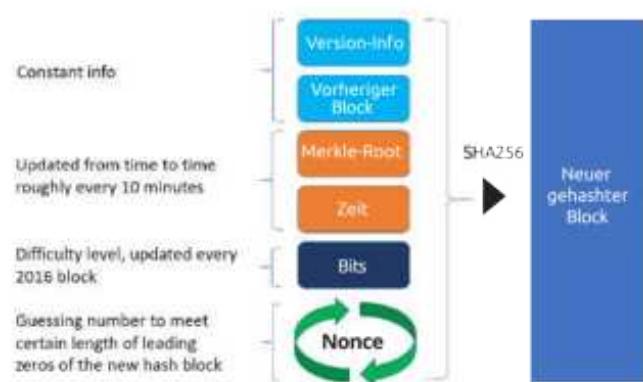
Wenn wir über einzelne Miner und die gesamte Netzwerkgröße sprechen, verwenden wir unterschiedliche Dezimal-Präfixe, was verwirrend sein kann.

Die wichtigsten Hash-Bezeichnungen sind wie folgt:

- **Bitcoin**-Mining-Maschinen hashen in Terahash pro Sekunde (TH/s).
- Die gesamte Hashrate des Netzwerks wird in Exahash pro Sekunde (EH/s) angegeben.

Bitcoin-Hashrate:
1,1 Exahash / Sekunde
Ein Hash / Sekunde
Ein Kilohash = 1.000 Hashes
Ein Megahash = 1.000.000 Hashes
Ein Gigahash = 1.000.000.000 Hashes
Ein Terahash = 1.000.000.000.000 Hashes
Ein Petahash = 1.000.000.000.000.000 Hashes
Ein Exahash = 1.000.000.000.000.000.000 Hashes

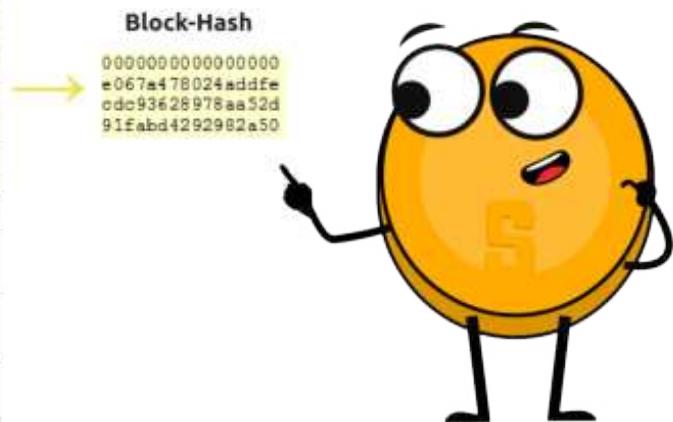
Bitcoin-Block-Hashing



Der Block-Hash kann als Proof of Work bezeichnet werden

Zusammenfassend lässt sich sagen, dass die Miner etwa alle zehn Minuten einen Wettlauf um einen gültigen Block-Hash austragen. Sie beginnen damit, alle Daten aus ihren potenziellen Blöcken zu nehmen (die in den Block-Headern übersichtlich zusammengefasst sind), hashen sie ein zweites Mal zu einem einzigen Hash und vergleichen die Ausgabe mit einem vom Netzwerk festgelegten Ziel-Hash-Wert. Ist der erzeugte Block-Hash-Wert zu hoch, passt der Miner die Nonce an und versucht es erneut. Dieser Vorgang wird Billionen Mal pro Sekunde wiederholt, bis ein erfolgreicher Miner schließlich einen Hash-Wert findet, der dem Zielwert des Netzwerks entspricht.

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344c0e19fa6b2b92b3a19c8efbadc141787
timestamp	350b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
	...



Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain



Unabhängig davon, wie viel oder wie wenig Mining-Hash-Power eingesetzt wird, wird durchschnittlich alle zehn Minuten ein Block gemined.

- Wenn die Gesamt-Hashrate sinkt, sinkt der Schwierigkeitsgrad, um es den Minern zu erleichtern, neue **Bitcoin** zu minen.
 - Dies trägt dazu bei, die Rate, mit der neue **Bitcoin** gemined werden, konstant zu halten.
- Die Schwierigkeitsanpassung erfolgt anhand einer Formel, die die durchschnittliche Zeit berücksichtigt, die für das Mining der vorherigen 2016 Blöcke benötigt wurde.
 - Wenn die durchschnittliche Zeit für das Mining von 2016 Blöcken weniger als 14 Tage beträgt, wird der Schwierigkeitsgrad erhöht.
 - Wenn die durchschnittliche Zeit für das Finden von 2016 Blöcken mehr als 14 Tage beträgt, wird der Schwierigkeitsgrad gesenkt.



Die **Emissionsrate** bezieht sich auf die Rate, mit der neue Einheiten zum zirkulierenden Angebot hinzugefügt werden, oft durch Mining. Diese Rate kann durch verschiedene Faktoren beeinflusst werden, darunter Veränderungen der Hashrate des Netzwerks, die Anzahl der geschürften Blöcke und Halving-Events, die die Anzahl der Einheiten, die pro Block gewonnen werden können, reduzieren.

8.5 Das Mining eines Blocks Schritt für Schritt erklärt

Das Mining eines Blocks im **Bitcoin-Netzwerk** umfasst mehrere Schritte:

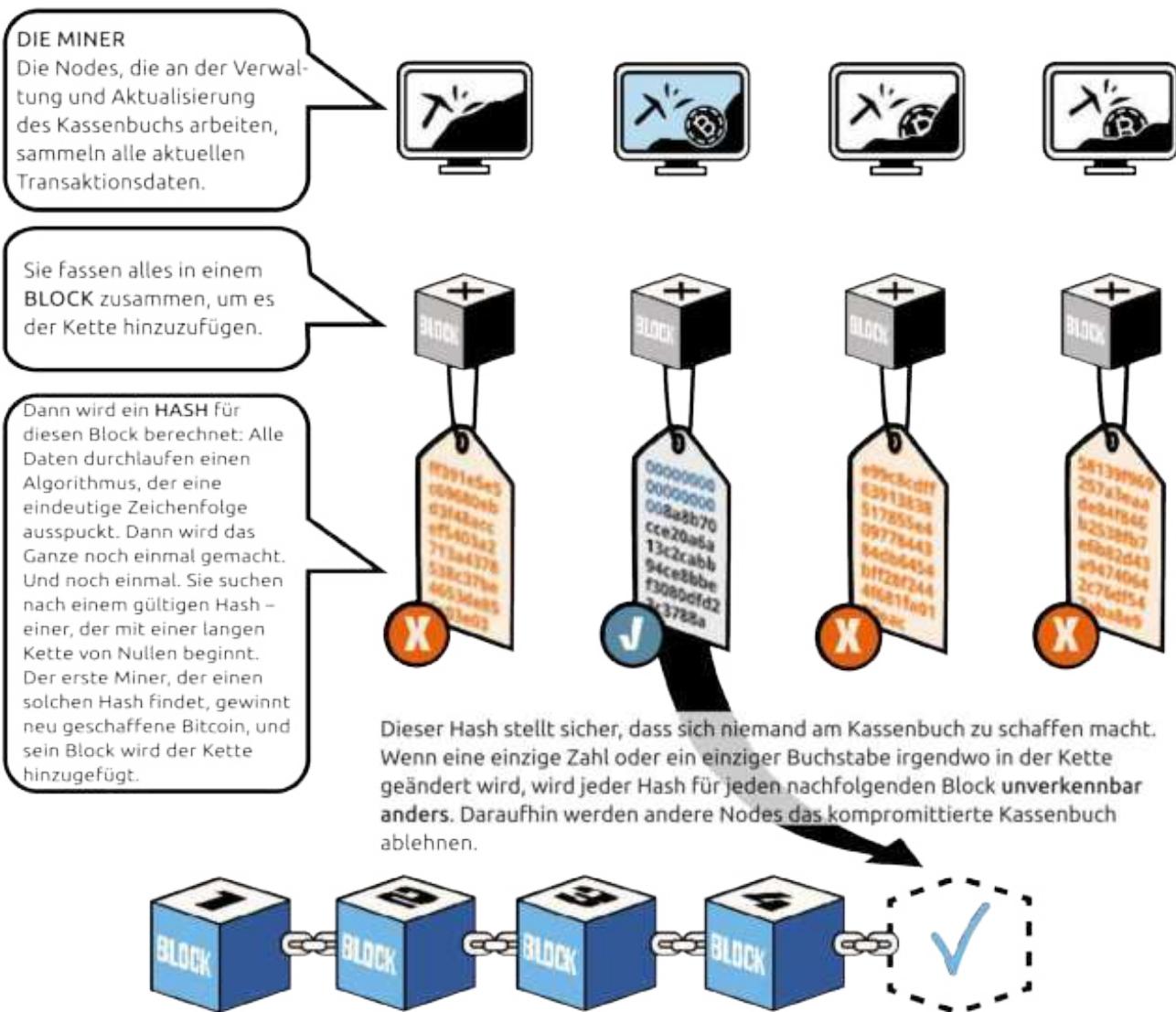
1. Neue Transaktionen werden ans Netzwerk gesendet, von den Nodes aufgenommen und überprüft.
2. Von den unbestätigten Transaktionen im **Mempool** werden einige ausgewählt. Transaktionen mit höheren Gebühren werden vorrangig behandelt.
3. Diese Transaktionen werden dann in einem **Merkle-Tree** organisiert und zusammen mit dem **Hash des vorherigen Blocks**, einem **Zeitstempel** und einer **Nonce** in einen **potenziellen Block** aufgenommen.
4. Die Miner konkurrieren um die Lösung eines mathematischen Rätsels, das auf den Informationen im Block basiert, einschließlich der Transaktionen und einer Zufallszahl.
5. Bei dem Rätsel geht es darum, eine bestimmte Zahl (den „Hash“) zu finden, die in Kombination mit den Blockdaten einen Wert ergibt, der kleiner als eine Zielzahl ist.



Mit anderen Worten: Die Miner verwenden den **Proof of Work**, um den **Nonce**-Wert so lange anzupassen, bis ein Hash erzielt wird, der die **festgelegten Schwierigkeitsanforderungen** erfüllt.



Kapitel 8



6. Der Miner, der als erster den korrekten Hash gefunden hat, sendet ihn an das Netzwerk, und die anderen Miner überprüfen die Lösung, um zu sehen, ob sie tatsächlich korrekt ist.

7. Wenn die Lösung verifiziert wird, wird der Block der Blockchain hinzugefügt.



Der gesuchte Block wird zur Verifizierung an das Netzwerk weitergeleitet. Sobald er von anderen Minern verifiziert wurde und das Netzwerk einen Konsens erzielt hat, wird der Block als letzter bzw. neuster Block in der Kette zur Blockchain hinzugefügt.



<https://yogh.io/block/0000000000003f9c14c33d90574dee123950e62dff44100ad2f59c29b5b4e709/>

Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

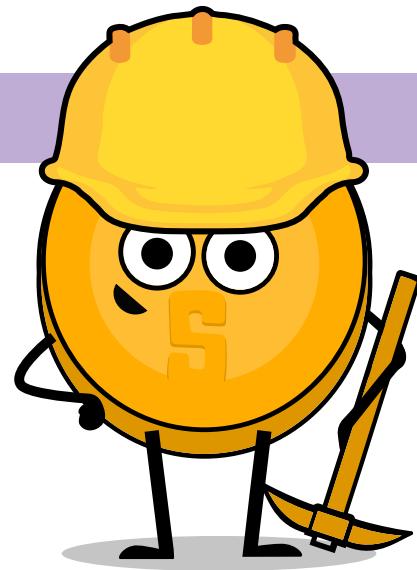
8. Der Miner, der den Block erfolgreich gemined hat, wird mit neu geschaffenen **Bitcoin** aus der Coinbase-Transaktion und den Transaktionsgebühren aus den enthaltenen Transaktionen belohnt.
9. Der neue Block wird Teil der unveränderlichen und transparenten Aufzeichnung aller Transaktionen in der Blockchain. Der Block-Hash und die darin enthaltenen Informationen werden verwendet, um die Blockchain zu aktualisieren, und der Prozess beginnt mit dem nächsten Block von vorn.

8.5.1 Gemeinschaftsübung: Interaktive Mining-Übung

Gemeinschaftsübung: Befolge die folgenden Anweisungen!

1. Besuche die Website!
<https://chainflyer.bitflyer.jp/>

2. Überprüfe die verschiedenen Elemente, die auf der Seite angezeigt werden, einschließlich der letzten Blöcke, der bestätigten Transaktionen, der Anzahl der Transaktionen, der Speichernutzung und des ungefähren Werts des gesamten Blocks!



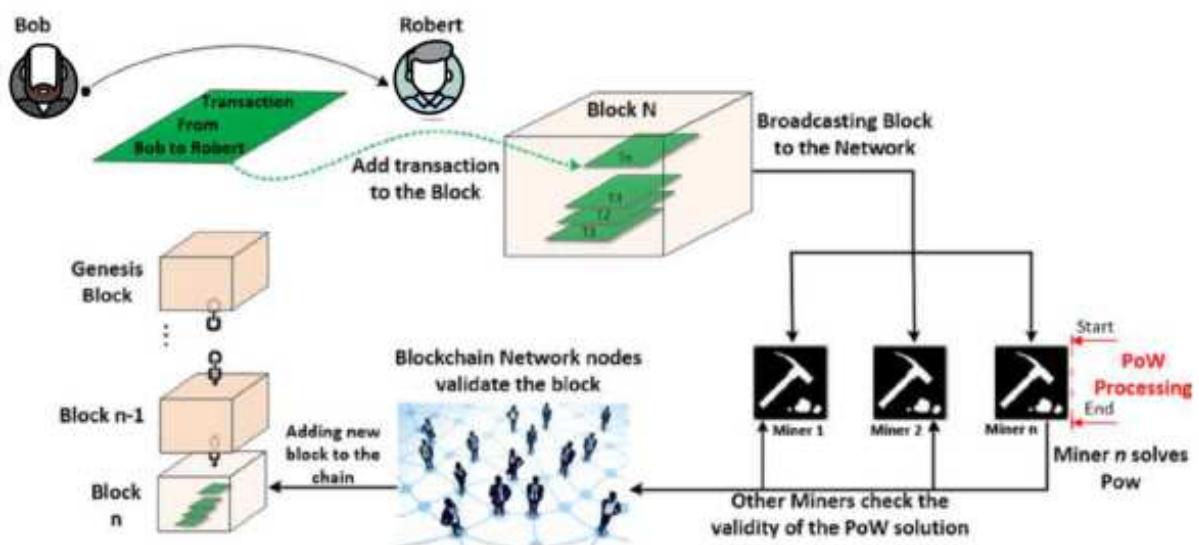
Beantworte folgende Fragen:

- Welcher war der letzte geschürfte Block?
- Wie viele Transaktionen waren in diesem Block enthalten?
- Wie hoch ist der Gesamtwert, der in **Bitcoin** gehandelt wird?
- Wie groß war der Block in Megabyte?
- Mit wie vielen Nullen beginnt die Nonce des Blocks?
- Wie viel hat der Miner insgesamt verdient?
- Wie hoch war der Gesamtwert der Gebühren, die der Miner für das Hinzufügen der Transaktionen zum Netzwerk erhalten hat?
- Wähle eine der Transaktionen mit dem höchsten Wert in diesem Block! Auf wie viele BTC-Wallets wurde der Betrag verteilt?



8.5.2 Überblick über den gesamten Transaktionsvorgang

1. Ein Benutzer möchte **Bitcoin** an einen anderen Benutzer senden. Er erstellt eine Transaktion mit den Details der Sendung, einschließlich des zu sendenden **Bitcoin**-Betriebs, der Adresse des Absenders und der Adresse des Empfängers.
2. Der Nutzer verwendet dann seinen privaten Schlüssel, um die Transaktion zu verschlüsseln. Dieser private Schlüssel ist eine Art Geheimcode, den nur der Nutzer kennt und mit dem er nachweisen kann, dass er derjenige ist, der er vorgibt zu sein.
3. Die verschlüsselte Transaktion wird an das Netzwerk der **Bitcoin**-Nodes gesendet.



4. Die Nodes überprüfen die Transaktion anhand des öffentlichen Schlüssels des Absenders, der in der Blockchain verfügbar ist. Sie prüfen, ob die Signatur gültig ist und ob der Absender über genügend **Bitcoin** verfügt, um die Transaktion durchzuführen.
5. Die Nodes fassen dann die verifizierten Transaktionen zu einem Block zusammen.
6. Der Block wird dann an das Netzwerk der **Bitcoin**-Miner weitergeleitet.
7. Miner verwenden einen komplexen mathematischen Algorithmus, um ein Rätsel zu lösen, was als „Mining“ bezeichnet wird. Sobald für das Rätsel eine Lösung gefunden wurde, wird sie der Blockchain hinzugefügt und der Block in die Kette aufgenommen.
8. Sobald der Block zur Blockchain hinzugefügt wird, gilt die Transaktion als abgeschlossen und der Empfänger kann mit seinem eigenen privaten Schlüssel auf die **Bitcoin** zugreifen.



Zusammenfassend lässt sich sagen, dass der Absender die Transaktion mit seinem privaten Schlüssel erstellt und verschlüsselt, die Nodes die UTXOs der Transaktion mit dem öffentlichen Schlüssel des Absenders verifizieren und die Miner die verifizierte Transaktion zur Blockchain hinzufügen. Der Empfänger kann dann mit seinem privaten Schlüssel auf die **Bitcoin** zugreifen. Sobald ein Block geschürft wurde, gelten alle darin enthaltenen Transaktionen als bestätigt, und die UTXOs, die als Input für diese Transaktionen verwendet wurden, gelten als verbraucht und werden nicht mehr verwendet.

Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

8.5.3 Vertrauen ist gut, Kontrolle ist besser (Don't Trust, Verify)

In der Welt der Kryptowährungen ist der Satz „Don't trust, verify“ eine Erinnerung daran, Transaktionen immer selbst zu verifizieren, anstatt sich auf andere zu verlassen, etwa auf eine zentrale Behörde oder einen Vermittler. Das **Bitcoin-Netzwerk** besteht aus einem dezentralen Netzwerk von Nodes, das es den Nutzern ermöglicht, Transaktionen selbst zu verifizieren.

Es gibt jedoch Szenarien, die dazu führen können, dass Transaktionen rückgängig gemacht werden, z. B. **Doppelausgaben**, **verwaiste Blöcke** und **Reorganisation**. Um die Sicherheit von Transaktionen zu erhöhen, wird empfohlen, sechs Bestätigungen oder sechs Blöcke, die die betreffende Transaktion einschließen, abzuwarten, bevor man sie als endgültig betrachtet. Je mehr Bestätigungen eine Transaktion hat, desto sicherer wird sie, da die Wahrscheinlichkeit, dass sie rückgängig gemacht wird, sinkt. Die Anzahl der erforderlichen Bestätigungen kann je nach Anwendungsfall und gewünschtem Sicherheitsniveau variieren.

- **Doppelausgabe:** Bei einem Double-Spend-Angriff versucht ein böswilliger Akteur, denselben **Bitcoin** zweimal auszugeben, indem er das Netzwerk so manipuliert, dass seine zweite Ausgabe des selben **Bitcoin** als gültig akzeptiert wird. Wenn ein Miner oder eine Gruppe von Minern, die mehr als 50 % der Hash-Leistung des Netzwerks kontrollieren (bekannt als 51%-Angriff), eine Double-Spend-Transaktion bestätigen, könnte diese zu einem Block hinzugefügt und als gültig betrachtet werden, wodurch die ursprüngliche Transaktion effektiv rückgängig gemacht wird.
- **Verwaiste Blöcke:** Wenn zwei Miner zur gleichen Zeit einen neuen Block finden, kann das Netzwerk vorübergehend beide akzeptieren. Wenn einer der Blöcke später um weitere Blöcke erweitert wird, erkennt das Netzwerk diese Kette als die Hauptkette an und der andere Block wird zu einem verwaisten Block, der nicht mehr Teil der Hauptblockchain ist. Die Transaktionen, die in dem verwaisten Block enthalten sind, gehen nicht verloren und werden in einen späteren Block aufgenommen, wenn sie weiterhin gültig bleiben.



Ein verwaister Block bei **Bitcoin** ist ein gültiger Block, der nicht in der längsten Kette enthalten ist, die als Hauptkette gilt.

- **Reorganisation:** Dies könnte theoretisch passieren, wenn ein neuer Block zur Blockchain hinzugefügt wird und dadurch die bestehende Kette durch eine andere ersetzt wird. Wenn eine Transaktion in einem Block enthalten ist, der sich nicht mehr auf der Hauptkette befindet, würde sie als ungültig betrachtet und die Transaktion würde rückgängig gemacht werden.

TRANSACTION

3748e7346577f81ab0d15a351d9a0018a93790b4a636f38a613b393750

Pending (5 Confirmations) Amount sent 6.42932025 BTC Received Time 2023-02-24 09:20:03 UTC

TRANSACTION

3748e7346577f81ab0d15a351d9a0018a93790b4a636f38a613b393750

8 Confirmations Amount sent 6.27633484 BTC Received Time 2023-02-24 09:20:03 UTC



8.6 Gemeinschaftsübung: Transaktion mit UTXOs

Gemeinschaftsübung: Befolge die folgenden Anweisungen!

1. Werde dir deiner Rolle bewusst: Dir wurde eine der folgenden Rollen zugewiesen: Absender, Empfänger, Node oder Miner.

- Als **Absender** bist du für die Erstellung und Übermittlung von Transaktionen verantwortlich.
- Als **Empfänger** bist du für den Empfang und die Überprüfung von Transaktionen verantwortlich.
- Als **Node** bist du für die Validierung der Transaktionen und die Einhaltung der Regeln verantwortlich.
- Als **Miner** bist du für die Überprüfung und das Hinzufügen der Transaktionen zur Blockchain verantwortlich, wobei du Belohnungen für deine harte Arbeit erhältst.

2. Wenn du der **Absender** bist, erstelle eine Transaktion! Gehe dazu folgendermaßen vor:

- Nimm ein Transaktionsformular und fülle die folgenden Felder aus:
 - Input UTXO: 20 BTC
 - Output UTXO: 10 BTC an die Adresse des Empfängers
 - Output UTXO: 1 BTC an die Adresse des Miners
 - Change UTXO: 9 BTC an deine Adresse
 - Signatur: Deine Unterschrift simuliert einen privaten Schlüssel.
- Gib das Transaktionsformular und die entsprechende Anzahl von Geldeinheiten an den Empfänger weiter!

3. Wenn du der **Empfänger** bist, überprüfe die Transaktionen! Gehe wie folgt vor:

- Überprüfe das Transaktionsformular, um sicherzustellen, dass die richtige Anzahl von Geldeinheiten und der Name oder die Initialen des Empfängers eingetragen sind!
- Zähle die erhaltenen Geldeinheiten und vergleiche sie mit der Anzahl der Einheiten, die auf dem Transaktionsformular vermerkt sind!
- Wenn die Geldeinheiten übereinstimmen, kreuze das Zustimmungsfeld auf der UTXO-Tabelle an, die gemeinsam genutzt wird und für alle in der Klasse zugänglich ist!
- Wenn die Geldeinheiten nicht übereinstimmen oder du Zweifel hast, lehne die Transaktion ab und schreibe den Grund in die UTXO-Tabelle!

4. Wenn du ein **Node** bist, validiere Transaktionen: Als Node bist du für die Validierung der Transaktionen verantwortlich, indem du die Gültigkeit der Transaktion anhand der Regeln des Protokolls und des Konsensmechanismus überprüfst.

- Vergewissere dich, dass die Adresse des Absenders und die des Empfängers gültig sind!
- Vergewissere dich, dass der Absender über genügend Geldmittel verfügt, um die Transaktion abzuschließen, indem du anhand des UTXO-Diagramms überprüfst, ob die als Input für die Transaktion verwendeten UTXOs tatsächlich existierten und nicht schon vorher ausgegeben worden sind!
- Vergewissere dich, dass bei der Transaktion keine Geldeinheiten doppelt ausgegeben werden, indem du dir das UTXO-Diagramm ansiehst!

Eine sichere Kette bauen: Der Prozess des Bitcoin-Minings und seine Rolle in der Blockchain

5. Wenn du ein **Miner** bist, füge Transaktionen zur Blockchain hinzu! Als Miner bist du für das Hinzufügen der Transaktionen zur Blockchain verantwortlich. Befolge diese Schritte:

- Prüfe die Transaktionen, die von den Empfängern genehmigt und von den Nodes validiert wurden!
- Würfele und vergleiche die Zahlen mit denen der anderen Miner! Der Miner mit der kleineren Augenzahl (unter 25) fügt die Transaktion zur Blockchain hinzu.
- Für deine Zeit, Energie und Mühe erhältst du eine Belohnung ...1 BTC.
- Sobald eine Transaktion der Blockchain hinzugefügt wurde, kann sie nicht mehr geändert oder rückgängig gemacht werden.

6. Behalte dein Guthaben im Auge: Behalte während der gesamten Aktivität dein Guthaben im Auge, indem du die Geldeinheiten in deiner digitalen Wallet zählst!

7. Diskutiere mit deinen Klassenkameraden und deiner Lehrkraft über die gelernten Schlüsselkonzepte!



Kapitel 8



Kapitel 9

Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

9.0 Warum Bitcoin?

9.1 Die Zukunft von Bitcoin

9.1.1 Der Lindy-Effekt

9.2 Bitcoin ist mehr als nur digitales Geld

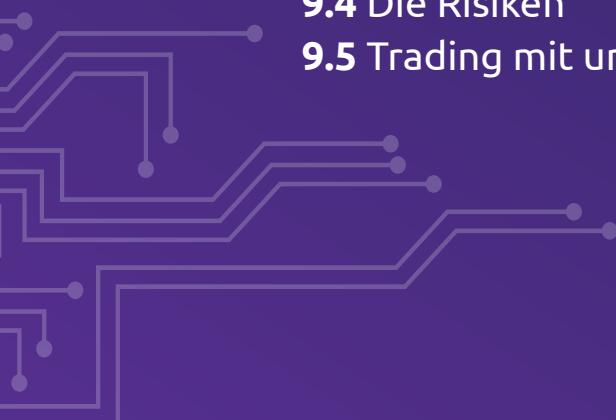
9.3 Die Probleme und Herausforderungen

9.3.1 Das regulatorische Umfeld für Bitcoin

9.3.2 Der Energieverbrauch beim Bitcoin-Mining

9.4 Die Risiken

9.5 Trading mit und Investieren in Bitcoin



Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

9.0 Warum Bitcoin?

Bitcoin ist ein Wendepunkt in der Finanzwelt, insbesondere in Teilen der Welt, in denen das traditionelle Bankensystem nicht funktioniert. In armen Regionen sind die traditionellen Banken aufgrund der hohen Kosten für die Einhaltung von Vorschriften oft nicht bereit, auf die Bedürfnisse der Menschen einzugehen. Infolgedessen hat ein erheblicher Teil der Bevölkerung keinen Zugang zu wichtigen Finanzdienstleistungen. Außerdem sind grenzüberschreitende Überweisungen in Länder wie El Salvador nicht nur teuer, sondern auch langwierig. Die mit diesen Transaktionen verbundenen Gebühren und die Verzögerungen bei der Bearbeitung können für diejenigen, die auf diese Gelder für ihren täglichen Bedarf angewiesen sind, verheerend sein. Darüber hinaus haben Menschen ohne Bankverbindung keinen Zugang zu Investitionen und Vermögenswerten, um sich gegen die Inflation zu schützen, was ihre finanzielle Unsicherheit weiter verstärkt. In Anbetracht dieser Probleme bietet **Bitcoin** eine Lösung, die den unmittelbaren Bedürfnissen dieser Bevölkerungsgruppen gerecht wird. Es ermöglicht einen schnellen und effizienten Geldtransfer ohne Intermediäre und zu einem Bruchteil der Kosten. Darüber hinaus bietet es den Menschen in bankenlosen Bevölkerungsgruppen eine Möglichkeit, Werte zu speichern und sich vor Inflation zu schützen.

9.1 Die Zukunft von Bitcoin



Die „Hyperbitcoinisierung“ ist eine theoretische Zukunft, in der **Bitcoin** die dominierende globale Währung wird. Das würde bedeuten, dass **Bitcoin** von jedem, überall und für alles verwendet wird – vom Kauf des Kaffees über das Bezahlen von Rechnungen bis hin zum Kauf eines Hauses.

Das wachsende Interesse von Milliardären, Ländern und Regierungen an **Bitcoin** verdeutlicht die potenziellen Auswirkungen einer breiten Akzeptanz von **Bitcoin** auf Wirtschaft und Gesellschaft. Hier sind einige der Vorteile einer hyperbitcoinisierten Welt:

1. Eine Revolution auf dem Remissen-Markt: Der Remissen-Markt umfasst die Überweisung von Geldern von einer Partei zur anderen, oft über internationale Grenzen hinweg. Trotz sinkender Kosten sind Rücküberweisungen im Vergleich zu inländischen Banküberweisungen nach wie vor relativ teuer, insbesondere bei kleineren Beträgen. **Bitcoin** hat das Potenzial, den Rücküberweisungsmarkt zu revolutionieren, indem es die Kosten durch sein Layer-2-Protokoll Lightning-Netzwerk auf nahezu Null reduziert. Das Lightning-Netzwerk bietet schnelle und kostengünstige Transaktionen, wodurch es sich gut für den Geldtransfermarkt eignet und die hohen Kosten und andere Herausforderungen im Zusammenhang mit Geldüberweisungen, wie z. B. langsame Abwicklungszeiten und eingeschränkte Geschäftszeiten, bewältigt.

2. Eine selbstverwaltete Zukunft: Eine selbstverwaltete Zukunft ist eine Zukunft, in der der Einzelne die volle Kontrolle über seine eigene digitale Identität und sein Vermögen hat. Sie könnte zu mehr finanzieller Integration, Privatsphäre und Sicherheit führen und dem Datenschutz bei Transaktionen einen höheren Stellenwert einräumen.



3. Veränderungen in der Geldpolitik: Sollte sich *Bitcoin* auf breiter Basis durchsetzen, könnte es die Fähigkeit von Regierungen in Frage stellen, die Geldmenge durch traditionelle geldpolitische Instrumente zu kontrollieren, was zu Veränderungen in der geldpolitischen Steuerung und Umsetzung führen könnte. *Bitcoin* könnte auch die finanzielle Inklusion, Gleichberechtigung und Chancen erhöhen und die Möglichkeiten von Regierungen und Finanzinstituten zur Manipulation der Wirtschaft verringern.

4. Ein verlässliches Wertaufbewahrungsmittel: Die digitale Knappheit von *Bitcoin* macht es zu einem zuverlässigen Wertaufbewahrungsmittel, was mehr Menschen dazu ermutigen könnte, es als Mittel zum Sparen für die Zukunft zu nutzen.

5. Verbesserte Transparenz und Rückverfolgbarkeit: Die fälschungssichere und unveränderliche Aufzeichnung aller Transaktionen in der Blockchain könnte die Transparenz und Rechenschaftspflicht in verschiedenen Branchen und Sektoren erhöhen.

6. Verbesserte Cybersecurity: Die dezentrale Struktur von *Bitcoin* macht es weniger anfällig für Hackerangriffe und Datenschutzverletzungen, was die allgemeine Sicherheit verbessert.

7. Verringerung des CO2-Fußabdrucks und Förderung erneuerbarer Energien: Indem sie den Prozess des Bitcoin-Minings nachhaltiger und umweltfreundlicher gestalten, können Miner dazu beitragen, den CO2-Fußabdruck zu verringern und die Nutzung erneuerbarer Energiequellen zu fördern. Dies steht im Einklang mit wichtigen ESG-Aspekten (ESG – Environmental, Social and Governance / Umwelt, Soziales und Verwaltung).

9.1.1 Der Lindy-Effekt



Der Lindy-Effekt ist eine einfache Theorie, die besagt, dass je länger es etwas gibt, desto wahrscheinlicher ist es, dass es auch in Zukunft Bestand haben wird. Diese Theorie kann auf viele Dinge angewendet werden, auch auf *Bitcoin*.

Bitcoin, eine dezentralisierte digitale Währung, die es seit 2009 gibt, ist ein Paradebeispiel für den Lindy-Effekt in Aktion. Obwohl *Bitcoin* im Laufe der Jahre mit zahlreichen Herausforderungen konfrontiert wurde, darunter technologische Veränderungen, Sicherheitsverletzungen und staatliche Regulierungen, hat seine Popularität weiter zugenommen und es wurde von einer wachsenden Zahl von Unternehmen als Zahlungsmittel angenommen.

Den Test der Zeit meistern



Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

Einer der Hauptgründe für die Langlebigkeit und die anhaltende Nutzung von **Bitcoin** ist sein dezentraler Charakter. Dies bedeutet, dass es als sicheres und transparentes Finanzsystem ohne die Notwendigkeit von Intermediären funktioniert, was es für Personen attraktiv macht, die finanzielle Privatsphäre und Kontrolle wertschätzen. Darüber hinaus hat auch die Fähigkeit von **Bitcoin**, als sicheres Wertaufbewahrungsmittel zu funktionieren, zu seiner wachsenden Beliebtheit und Akzeptanz beigetragen.

Ein weiterer Faktor, der zur Langlebigkeit von **Bitcoin** beiträgt, ist sein Widerstand gegen Veränderungen und Wettbewerb. Änderungen an den Konsensregeln des Netzwerks erfordern die Zustimmung der Mehrheit der Nutzer zu dem Update, was es schwierig macht, einen Konsens zu erreichen, und dazu führt, dass nur Updates, denen die überwältigende Mehrheit der Netzwerkeinnehmer zustimmt, umgesetzt werden. Hinzu kommt, dass trotz der Existenz vieler konkurrierender Kryptowährungen bisher keine in der Lage war, mit der Langlebigkeit von **Bitcoin** mithalten oder das gleiche Maß an Netzwerkeffekten zu erreichen.

Die Hashrate von **Bitcoin** ist im Laufe der Jahre exponentiell angestiegen, und auch die Verbreitung des Minings hat sich ausgeweitet. Die Zahl der Nutzer, die sich dem **Bitcoin-Netzwerk** anschließen, hat ebenfalls exponentiell zugenommen. Schätzungsweise 140 bis 190 Millionen Nutzer sind inzwischen Teil des Netzwerks. Diese Faktoren in Verbindung mit der anhaltenden Beliebtheit und Nützlichkeit von **Bitcoin** deuten darauf hin, dass **Bitcoin** auch in Zukunft verwendet und Vertrauen genießen wird.

9.2 Bitcoin ist mehr als nur digitales Geld

Bitcoin hat aus verschiedenen Gründen an Popularität gewonnen, nicht nur als Mittel zum Geldverdienen. Einige Nutzer werden von der Idee angetrieben, ein Finanzsystem zu schaffen, das frei von zentraler Kontrolle ist, während andere einfach finanziell profitieren wollen.

Bitcoin ermöglicht auch die Erstellung einzigartiger **digitaler Artefakte**, die als **Satoshi-Inscriptions** bekannt sind. Diese Inscriptions, die Text, Bilder, Videos, Audio und Software enthalten können, werden auf der **Bitcoin**-Blockchain gespeichert, was sie unveränderlich, sicher und dezentral macht. Die eindeutige Identifizierung eines jeden Satoshis wird durch Ordinals ermöglicht. Im Gegensatz zu traditionellen NFTs benötigen diese Inscriptions keine separate Infrastruktur oder Token, was ihre Sicherheit und Dezentralität weiter erhöht.

Die Kombination von **Bitcoin** und Künstlicher Intelligenz kann für verschiedene Anwendungen wie den Handel mit Kryptowährungen, Sicherheit und Marktanalysen genutzt werden.

Das **Lightning-Netzwerk** von **Bitcoin** hat schnellere und sicherere Finanzzahlungen möglich gemacht. Atomic Swaps ermöglichen es beispielsweise, eine Kryptowährung gegen eine andere zu tauschen, ohne dass ein Intermediär benötigt wird. RSK, eine Plattform, die auf der **Bitcoin**-Blockchain aufbaut, ermöglicht auch die Erstellung von Smart Contracts und dezentralen Anwendungen, was neue Möglichkeiten, was auf **Bitcoin** aufgebaut werden kann, eröffnet.

Da diese Technologien weiter entwickelt und verbessert werden, sind für die Zukunft spannende Entwicklungen zu erwarten.



9.3 Die Probleme und Herausforderungen

Bitcoin Core ist eine leistungsfähige und weit verbreitete Implementierung des **Bitcoin**-Protokolls.

1. Skalierbarkeit: Wenn die Zahl der Nutzer und Transaktionen im Netzwerk wächst, kann die Menge der Daten, die von den Nodes gespeichert und verarbeitet werden müssen, recht groß werden. Dies kann die Validierung von Transaktionen verlangsamen und es neuen Nutzern erschweren, dem Netzwerk beizutreten.

2. Datenschutz: Während **Bitcoin**-Transaktionen pseudonym sind, ist die Blockchain öffentlich zugänglich, was bedeutet, dass Dritte die Möglichkeit haben, die Geldströme zu verfolgen und die Nutzer zu identifizieren. Es gibt einige Lösungsvorschläge für dieses Problem, wie z. B. die Verwendung von **Coin-Mixing** und **Stealth-Adressen**, die jedoch noch nicht weit verbreitet sind.

3. Benutzerfreundlichkeit: Für den Durchschnittsnutzer kann der Prozess der Einrichtung und Nutzung eines Full-Nodes recht technisch und entmutigend sein. Eine Vereinfachung der Benutzererfahrung und eine bessere Zugänglichkeit für einen größeren Personenkreis könnten dazu beitragen, die Akzeptanz zu erhöhen.

4. Dezentralisierung: Der aktuelle Konsens-Algorithmus von **Bitcoin** ist ein **Proof-of-Work**-Algorithmus, der von spezialisierten und großen Mining-Farmen betrieben werden kann. Dies kann zu einer Konzentration der Mining-Leistung und einer Bedrohung für die Dezentralisierung und Sicherheit des Systems führen.

5. Sicherheit: Obwohl **Bitcoin Core** quelloffen ist, was bedeutet, dass der Code von jedem einge-sehen werden kann, ist es immer noch möglich, dass Bugs oder Schwachstellen in den Code eingeschleust werden. Die kontinuierliche Überprüfung und Verbesserung der Sicherheit der Software kann dazu beitragen, die Nutzer vor möglichen Angriffen zu schützen. Wenn ein Angreifer zum Beispiel einen privaten Schlüssel generiert, der einer großen Anzahl von **Bitcoin** gehört, könnte er diese **Bitcoin** stehlen.

Insgesamt ist **Bitcoin Core** zwar ein solides Stück Software, aber kontinuierliche Entwicklung und Forschung sind unerlässlich, um diese Verbesserungsmöglichkeiten anzugehen und sicherzustellen, dass das Netzwerk sicher, dezentralisiert und weit verbreitet bleibt.

9.3.1 Das regulatorische Umfeld für Bitcoin

Der Kryptowährungsmarkt war in den letzten Jahren mit zahlreichen Herausforderungen konfrontiert, darunter der Zusammenbruch von FTX im Jahr 2022 und der Absturz der Stablecoins TerraUSD und LUNA zu Beginn desselben Jahres, was zu erheblichen Verlusten und einem Rückgang des Vertrauens der Anleger führte. Zu den Risiken, die mit Investitionen in Kryptowährungen verbunden sind, gehören Volatilität, Schwierigkeiten bei der Bewertung von Vermögenswerten, Verwahrungsrisiken, nicht registrierte Vermögenswerte und Anbieter, die außerhalb des regulatorischen Rahmens operieren, sowie unvorhersehbare Regulierungen.

Die Regulierung von Kryptowährungen, einschließlich **Bitcoin**, ist ein Thema, das von Regierungen und Finanzaufsichtsbehörden weltweit diskutiert wird. Während einige Kryptowährungen verboten haben, haben andere versucht, sie in einer Weise zu regulieren, die ein Gleichgewicht zwischen Innovation und Verbraucherschutz herstellt. Der Vorsitzende der US-Börsenaufsicht SEC, Gary Gensler,

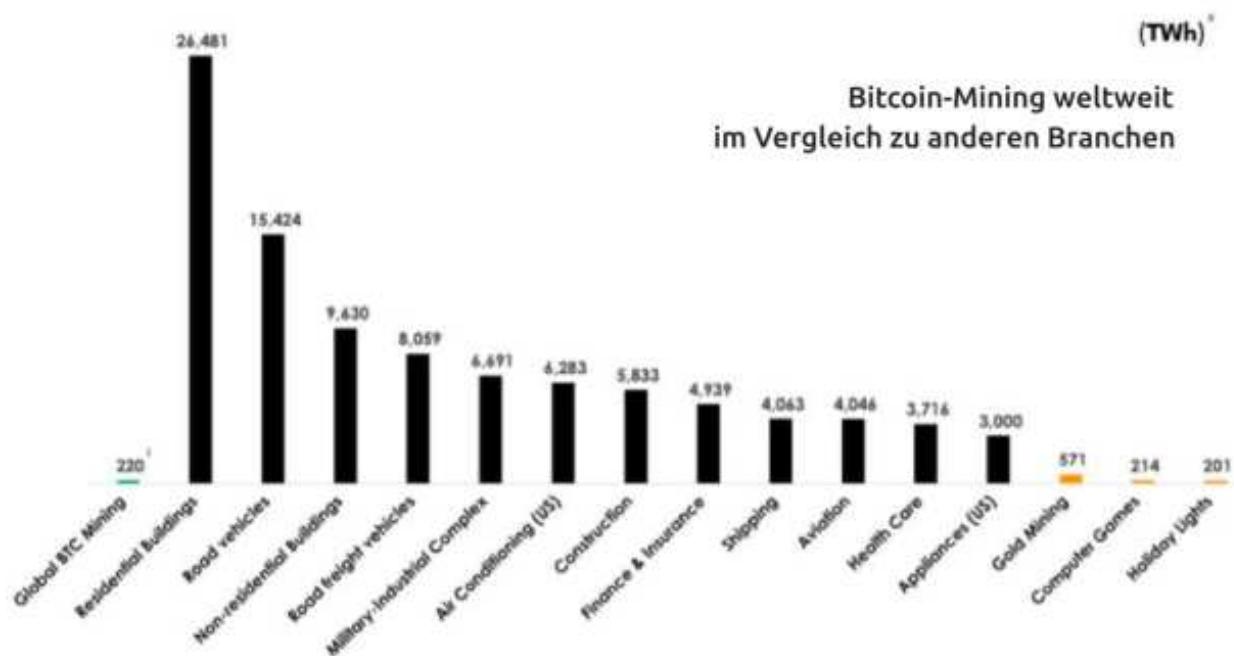
Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

erklärte kürzlich, dass die Regulierung des Kryptowährungsmarktes näher rückt und dass *Bitcoin* als Ware betrachtet werden wird. Nach Angaben der SEC weisen viele Token auf dem Markt die wesentlichen Merkmale von Wertpapieren auf und werden in die Zuständigkeit der SEC fallen, während *Bitcoin* als Ware unter die Aufsicht der Commodity Futures Trading Commission (CFTC) fällt. Die SEC hat noch viel zu tun, um umfassende Gesetze zum Schutz der Anleger einzuführen. Diese Entscheidung des SEC-Vorsitzenden wird von einigen Anlegern als positiv angesehen, was die Erwartung allmählich steigender Preise weckt. Trotz der derzeitigen Marktvolatilität betrachten einige Anleger dies als Kaufgelegenheit und glauben an die Zukunft digitaler Währungen als grenzenlose, dezentralisierte, fälschungssichere und nicht konfiszierbare Form von Geld.

9.3.2 Der Energieverbrauch beim Bitcoin-Mining

Das Bitcoin-Mining verbraucht viel Energie, etwa 79 Terawattstunden pro Jahr. Dies bedeutet jedoch nicht zwangsläufig, dass es eine Energieverschwendug oder schädlich für die Umwelt ist. Bitcoin-Mining kann dazu beitragen, ungenutzte Energiekapazitäten zu nutzen, insbesondere an abgelegenen oder unzugänglichen Orten. Außerdem wird der Großteil des Bitcoin-Minings mit erneuerbarer Energie wie Wasserkraft, Sonnenenergie, Windkraft und Erdwärme betrieben. Dies trägt dazu bei, die Produktion und Erforschung dieser Energiequellen rentabler zu machen. Darüber hinaus bietet das Bitcoin-Mining Sicherheit für das *Bitcoin-Netzwerk* und ermöglicht den Menschen den Zugang zu sicherem und zugänglichem Geld.

Es ist jedoch wichtig, zu wissen, dass der Energieverbrauch durch den Wettbewerb zwischen den Minern bestimmt wird, nicht durch die Anzahl der Transaktionen. Der Prozess der Validierung der digitalen Signatur, der nur einen kleinen Teil des Minings ausmacht, verbraucht nur wenig Energie. Der Energieverbrauch beim Bitcoin-Mining ist zwar hoch, aber nicht so hoch wie in anderen Branchen wie dem traditionellen Finanzsystem oder der Goldgewinnung und dem Recycling. Miner nutzen auch zunehmend saubere und erneuerbare Energiequellen wie Erdwärme und Wasserkraft, um ihren Mining-Betrieb zu betreiben.





Der Schlüssel zur Verringerung der Umweltauswirkungen liegt in der Förderung der Nachfrage nach grüner Energie, und das Wachstum der Branche führt zu Innovationen bei der Erzeugung sauberer Energie und zur Verringerung der Umweltverschmutzung. Es ist auch wichtig, zu wissen, dass die von den Minern genutzte Energiequelle einen großen Einfluss auf die Umweltbelastung hat. Mit der Weiterentwicklung der Technologie und der Industrie nutzen immer mehr Miner erneuerbare Energiequellen wie Wasser-, Sonnen- und Windenergie, was die Umweltauswirkungen erheblich verringert.

9.4 Die Risiken

Bitcoin kann große Freiheit bieten, aber es ist wichtig, daran zu denken, dass mit großer Macht auch große Verantwortung einhergeht. Die Verwendung von **Bitcoin** birgt Risiken. Es ist daher wichtig, diese Risiken zu verstehen und proaktive Schritte zu unternehmen, um sein Geld zu schützen.

- 1. Volatilität:** Der Wert von **Bitcoin** kann sehr volatil sein und sich in kurzer Zeit stark verändern, was zu erheblichen Verlusten für Anleger führen kann.
- 2. Fehlende Regulierung:** **Bitcoin** wird nicht von Regierungen oder Finanzinstituten reguliert, was bedeutet, dass es kaum eine Aufsicht zum Schutz der Verbraucher gibt.
- 3. Sicherheitsrisiken:** Bitcoin-Börsen und -Wallets können gehackt und gestohlen werden, was für die Nutzer zum Verlust von Geldern führen kann.
- 4. Betrug:** Es gibt viele Betrügereien im Zusammenhang mit **Bitcoin**, die für Investoren zum Verlust von Geldern führen können.
- 5. Illegale Aktivitäten:** **Bitcoin** wurde für illegale Aktivitäten wie Geldwäsche und den Kauf illegaler Waren im Dark Web verwendet.
- 6. Mangelndes Verständnis:** **Bitcoin** ist komplex und kann für den Durchschnittsbürger schwer zu verstehen sein, was zu einer schlechten Entscheidungsfindung und potenziellen Verlusten führen kann.
- 7. Mangel an Akzeptanz:** **Bitcoin** ist als Zahlungsmittel nicht allgemein akzeptiert, was seine Nützlichkeit im Alltag einschränkt.
- 8. Technische Risiken:** **Bitcoin** unterliegt technischen Risiken wie Bugs und Fehlern, die zu Problemen und möglicherweise zu einem Wertverlust führen können.
- 9. Quantencomputer:** Quantencomputer könnten möglicherweise die Sicherheit von **Bitcoin** gefährden, indem sie die Verschlüsselung brechen, die zur Sicherung von Transaktionen und Wallets verwendet wird.



Das Quantencomputing ist eine Methode für Computerberechnungen, die sich von der Arbeitsweise der meisten heutigen Computer unterscheidet. Anstelle von „Ein“- und „Aus“-Zuständen wie bei herkömmlichen Computern werden bei Quantencomputern „Qubits“ verwendet, die sich in vielen Zuständen gleichzeitig befinden können. Dadurch sind Quantencomputer bei bestimmten Arten von Berechnungen potenziell viel schneller als herkömmliche Computer.

Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

10. Digitale Bedrohungen: Hacker können deine Internetverbindung missbrauchen, um auf deine privaten Schlüssel und sensiblen Daten zuzugreifen, z. B. durch gehackte Software-Wallets, das Anklicken bösartiger Links oder Spyware-Betrügereien.

11. Social-Engineering-Betrug: Betrüger können dich dazu verleiten, Transaktionen zu bestätigen, indem sie sich als Kundendienstmitarbeiter ausgeben oder ein falsches Gefühl des Vertrauens erwecken. Daher ist es wichtig, vorsichtig zu sein und deine Seed-Phrase nicht weiterzugeben.

12. Blind Signing: Mangelnde Transparenz kann zu Blind Signing führen, bei dem du Transaktionen zustimmst, ohne die Details vollständig zu verstehen. Daher ist es wichtig, dass du dich über die neuesten Beträgerien informierst und eine Wallet wählst, die alle Transaktionsdetails anzeigt.

13. 51%-Angriff: Ist eine potenzielle Sicherheitsbedrohung für das *Bitcoin-Netzwerk* und tritt auf, wenn ein einzelner Miner oder eine Gruppe von Minern mehr als 50 % der gesamten Rechenleistung oder Hashrate des Netzwerks kontrolliert. Dies ermöglicht es ihnen, die Kontrolle über das Netzwerk zu übernehmen und möglicherweise die Blockchain zu manipulieren, indem sie entweder verhindern, dass neue Transaktionen hinzugefügt werden, oder Transaktionen zu ihren Gunsten verändern.

Wenn ein Angreifer erfolgreich einen 51%-Angriff durchführt, könnte er *Bitcoin* doppelt ausgeben, d. h. er könnte dieselben *Bitcoin* mehr als einmal ausgeben. Dies würde es ihnen ermöglichen, effektiv *Bitcoin* zu stehlen oder Betrug im Netzwerk zu begehen. Die Durchführung eines 51%-Angriffs ist jedoch unglaublich schwierig und kostspielig, da er die Kontrolle über eine beträchtliche Menge an Rechenleistung erfordert würde, und die Kosten, die mit der Beschaffung dieser Leistung verbunden sind, könnten die potenziellen Gewinne aus dem Angriff überwiegen.

Es ist wichtig, anzumerken, dass das *Bitcoin-Netzwerk* noch nie auf diese Weise erfolgreich angegriffen wurde, aber die Möglichkeit eines 51%-Angriffs ist immer gegeben und unterstreicht, wie wichtig es ist, sicherzustellen, dass das Netzwerk dezentralisiert und sicher bleibt.

Um deine *Bitcoin* sicher zu schützen, verwende eine Offline-Wallet, lies alle Transaktionsdetails und informiere dich ständig über die neuesten Bedrohungen! Lasse nicht zu, dass Unwissenheit und ein falsches Gefühl von Vertrauen dein hart verdientes Vermögen gefährdet!

Obwohl das Quantencomputing für die Sicherheit von *Bitcoin* durchaus ein Risiko darstellt, darf man nicht vergessen, dass es sich immer noch um eine spekulative Bedrohung handelt und es ungewiss ist, ob und wann sie Realität wird. Ein 51%-Angriff auf *Bitcoin* ist bedenklich, aber er wäre kostspielig und für den Angreifer nicht sehr vorteilhaft. Effizientere und kostengünstigere Angriffsmethoden, wie DDoS, wären für einen rational agierenden Akteur, der Betrug begehen will, wahrscheinlicher.

9.5 Trading mit und Investieren in Bitcoin

Wenn es darum geht, in Kryptowährungen zu investieren, ist *Bitcoin* die sichere und zuverlässige Wahl, die mit den Werten und Prinzipien einer dezentralisierten Zukunft übereinstimmt.



Markttrends beziehen sich auf die allgemeine Richtung, in die sich der Markt bewegt. Von einem bullischen Trend spricht man, wenn sich der Markt in einem Aufwärtstrend befindet. Dies ist in der Regel mit dem Optimismus der Anleger und der Erwartung verbunden, dass die Preise weiter steigen werden. Im Gegensatz dazu spricht man von einem bärenischen Trend, wenn sich der Markt auf einem Abwärtstrend befindet, der durch niedrigere Höchst- und Tiefststände gekennzeichnet ist. Dies ist in der Regel mit dem Pessimismus der Anleger und der Erwartung verbunden, dass die Kurse weiter fallen werden.

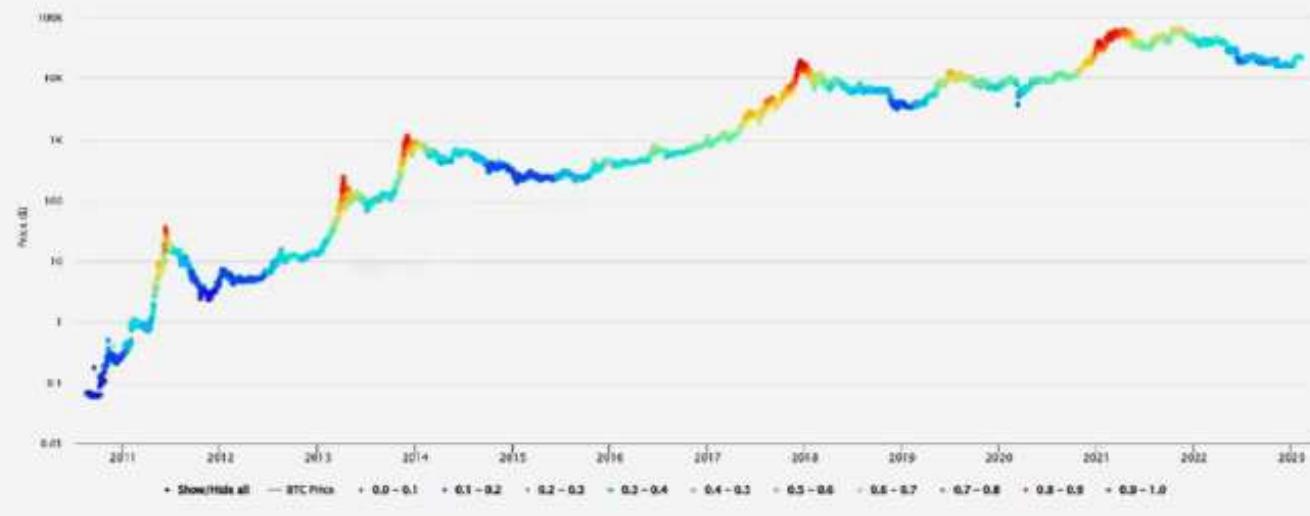
Die technische Analyse ist keine exakte Methode, und die Ergebnisse der Vergangenheit sind nicht immer ein Indikator für künftige Ergebnisse. Sie sollte in Verbindung mit anderen Analyseformen, wie der Fundamentalanalyse und der Markttimmung, verwendet werden, um fundierte Handels- und Anlageentscheidungen zu treffen.

Das von Benjamin Cohen erstellte **Risk-Metric-Diagramm** ist eine schnelle und intuitive Methode, um die Markttimmung zu verstehen und potenzielle Kauf- oder Verkaufschancen für **Bitcoin** einzuschätzen. Dieses Diagramm zeigt den Preis der Vermögenswerte an und weist einen farbkodierten Wert zu, um das mit diesem Preis verbundene Risiko darzustellen. Die Risikowerte reichen von 0 bis 1, wobei dunklere rote Farben für ein höheres Risiko und dunklere blaue Farben für ein geringeres Risiko stehen.

Der Zweck der **Risikomatrix** besteht nicht darin, Höchst- oder Tiefststände des Marktes vorherzusagen, sondern vielmehr darin, Bereiche zu identifizieren, die langfristig für Käufe oder Verkäufe attraktiv sein könnten. Ein niedriger Risikowert deutet darauf hin, dass **Bitcoin** unterbewertet ist und eine Kaufgelegenheit darstellt, während ein hoher Risikowert darauf hindeutet, dass er überbewertet ist und eine Verkaufsgelegenheit darstellt.

Farbe des Bitcoin-Preises – aufgeschlüsselt nach Risikostufen

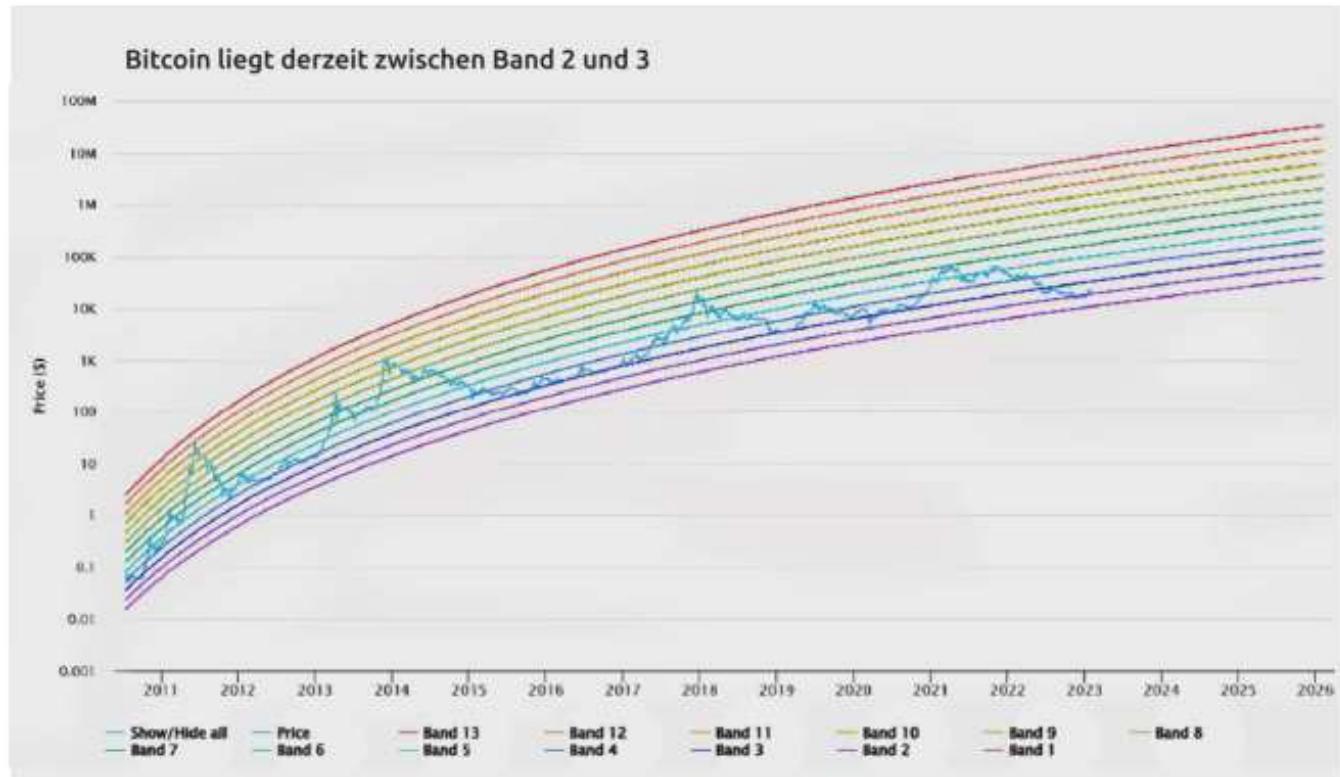
Aktueller Risikowert: 0,374, Konfidenzniveau: 9



Der **logarithmische Marktpreis** ist eine Methode zur Visualisierung der Preisbewegungen eines Vermögenswerts, wie z. B. **Bitcoin**, im Laufe der Zeit. Bei diesem Ansatz wird eine logarithmische Skala auf der y-Achse verwendet, um das exponentielle Wachstum, das häufig bei Vermögenspreisen zu beobachten ist, besser widerzuspiegeln.

Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

Der logarithmische Marktpreis wird verwendet, um die Preisbewegungen von **Bitcoin** im Laufe der Zeit zu verfolgen und potenzielle Spitzen und Akkumulationszonen zu identifizieren. Die Marktzyklen, auf die im Beispiel Bezug genommen wird, sind Perioden des Preisanstiegs und -rückgangs, und die Regenbogenbänder werden verwendet, um das relative Ausmaß dieser Preisbewegungen zu veranschaulichen.



Der logarithmische Marktpreis kann nützlich sein, um potenzielle Akkumulationszonen oder Zeiträume zu identifizieren, in denen der Preis relativ niedrig ist und eine gute Gelegenheit zum Kauf bietet. Im Beispiel werden die Zonen zwischen Band 3 und 4 als gute Akkumulationszeiträume für die Marktzyklen 3 und 4 identifiziert.



Marktzyklen bei **Bitcoin** beziehen sich auf das wiederkehrende Muster von Wachstum und Schrumpfung des Preises und der Marktaktivität. Es ist gekennzeichnet durch Zeiten der Spekulation und des Hypes, gefolgt von Korrektur und Konsolidierung. Einige Analysten argumentieren, dass die Zyklen stark mit den Halving-Events korrelieren.

Es ist wichtig, zu beachten, dass der logarithmische Marktpreis zwar wertvolle Erkenntnisse liefern kann, aber nur eines von vielen Instrumenten ist, die zur Analyse von Markttrends und Preisbewegungen verwendet werden können, und in Verbindung mit anderen Analysemethoden eingesetzt werden sollte, um ein umfassenderes Verständnis des Marktes zu erlangen. Hinzu kommt, dass sich die Marktbedingungen ständig ändern und die Performance der Vergangenheit keine Garantie für zukünftige Ergebnisse ist.

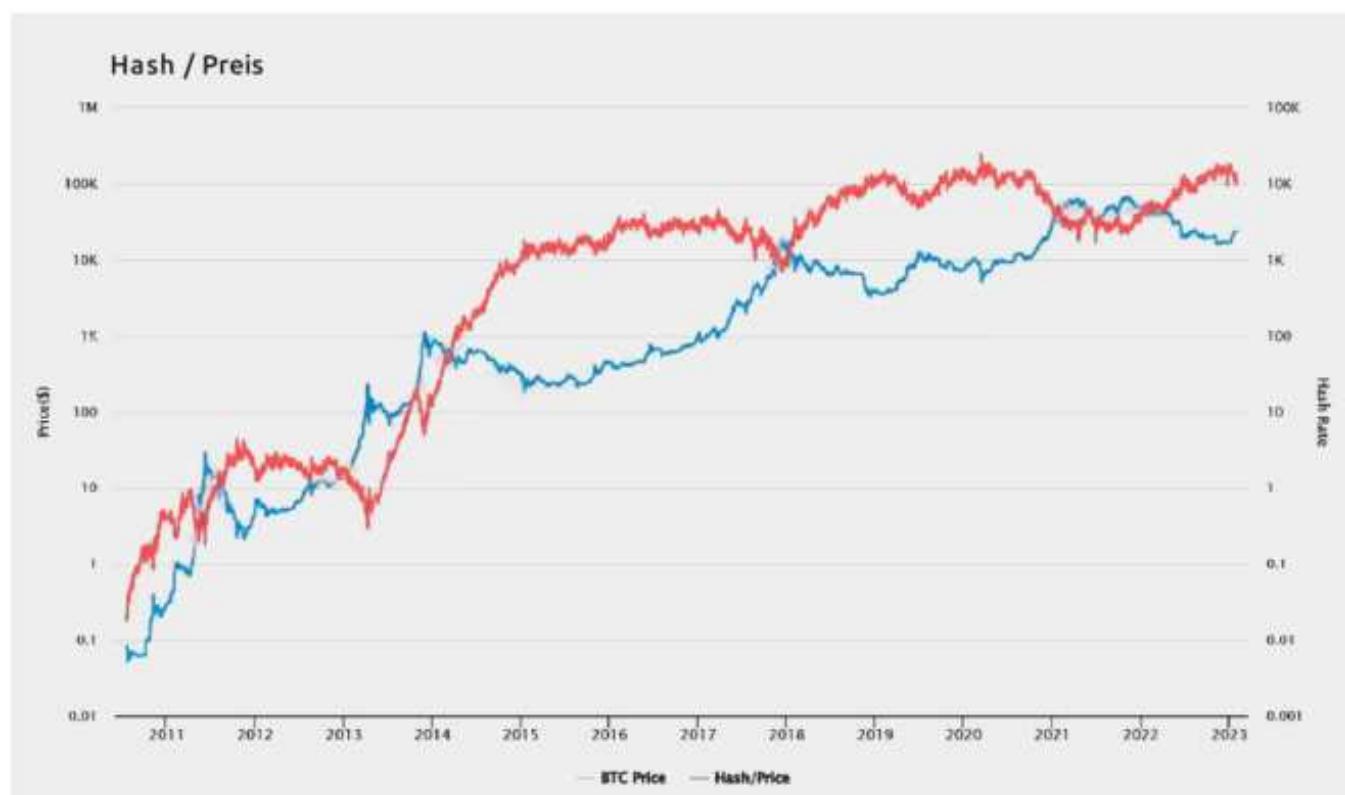


Das Hash/Preis-Verhältnis und das Preis/Hash-Verhältnis sind Metriken, die verwendet werden, um das Wachstum des **Bitcoin**-Preises und das Wachstum der Rechenleistung des **Bitcoin-Netzwerks**, oder der Hashrate, zu vergleichen. Diese Metriken werden verwendet, um die Beziehung zwischen den beiden zu verstehen, und wie Veränderungen in einem die andere beeinflussen können.

Wenn der Preis von **Bitcoin** schneller steigt als die Hashrate, sinkt das Verhältnis Hash/Preis und das Verhältnis Preis/Hash steigt. Das bedeutet, dass der Preis von **Bitcoin** schneller steigt als die Rechenleistung des Netzwerks, was auf eine erhöhte Nachfrage nach **Bitcoin** hindeuten könnte.

In der Nähe lokaler Höchststände, wenn der **Bitcoin**-Preis schnell steigt, kann es jedoch zu einem plötzlichen Rückgang des Hash/Preis-Verhältnisses kommen. Dies liegt daran, dass das Preiswachstum das Wachstum der Rechenleistung übersteigt, was zu einem Rückgang des Hash/Preis-Verhältnisses führt.

Wenn andererseits sowohl die Hashrate als auch der Preis von **Bitcoin** mit denselben Relationen sinken oder steigen, bleiben die Verhältnisse konstant. Das bedeutet, dass die Rechenleistung des Netzwerks und der Preis von **Bitcoin** mit der gleichen Rate wachsen.



Warum der innere Wert von Bitcoin mehr ist als nur heiße Luft

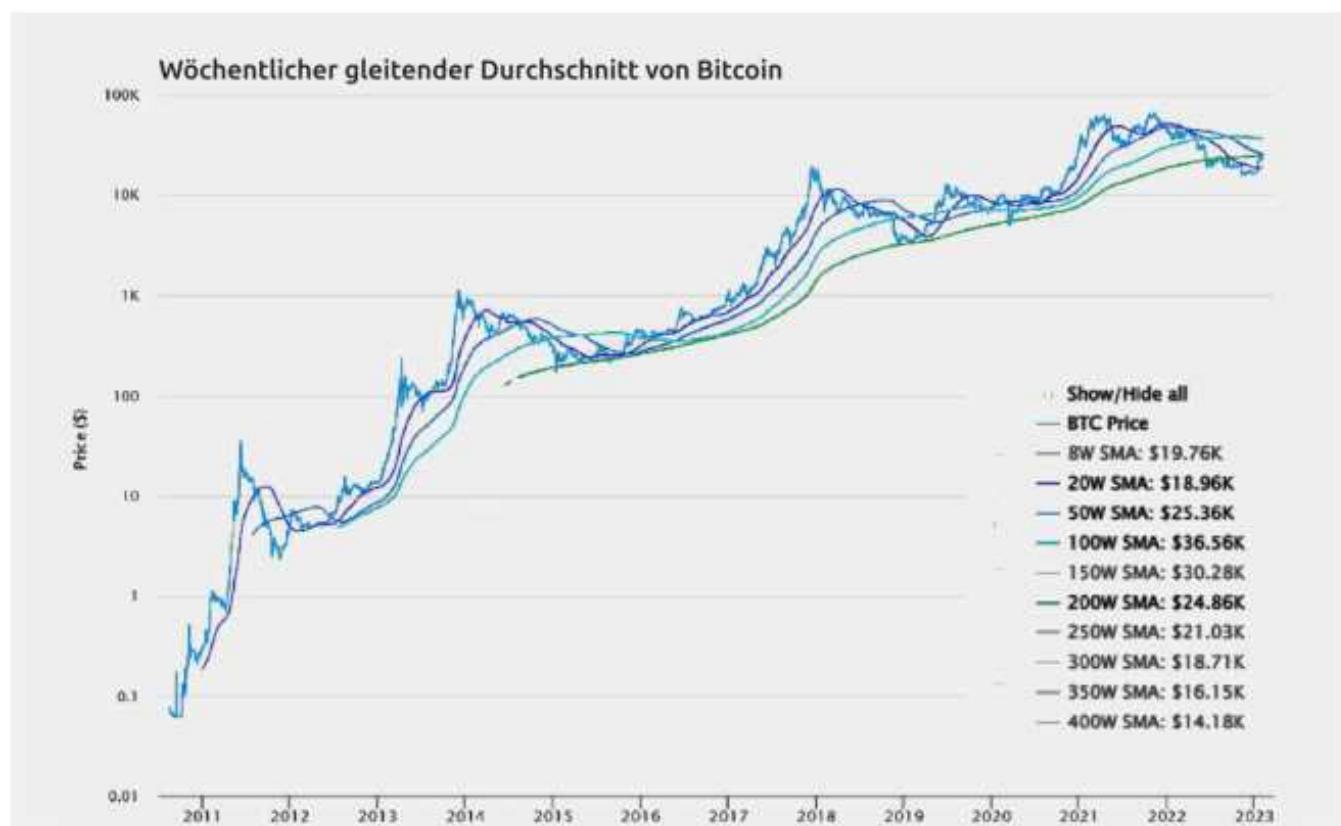
Wenn die Hashrate des *Bitcoin-Netzwerk* schneller ansteigt als der Preis von *Bitcoin*, steigt das Hash/Preis-Verhältnis und das Preis/Hash-Verhältnis sinkt. Dies könnte darauf hindeuten, dass das Netzwerk sicherer und fähiger wird, Transaktionen zu verarbeiten, was sich in Zukunft positiv auf den *Bitcoin*-Preis auswirken könnte.

Trendlinien werden verwendet, um einen aktuellen Markttrend zu erkennen. Sie werden durch die Verbindung von zwei oder mehr Kurspunkten gebildet und dienen dazu, ein Unterstützungs- oder Widerstandslevel anzudeuten. Eine Trendlinie, die nach oben geneigt ist, gilt als bullisch, während eine Trendlinie, die nach unten geneigt ist, als bärisch gilt.

Gleitende Durchschnitte werden verwendet, um die Volatilität des Kurses eines Wertpapiers über einen bestimmten Zeitraum zu verringern. Sie werden berechnet, indem die Schlusskurse eines Wertpapiers über eine bestimmte Anzahl von Zeiträumen addiert und dann durch die Anzahl der Zeiträume geteilt werden. Ein gleitender Durchschnitt kann dazu verwendet werden, die Richtung eines Trends zu ermitteln und Kauf- und Verkaufssignale zu generieren. Das *Dollar-Cost-Averaging* (DCA, z. Dt. Durchschnittskosteneffekt) unter kurzfristigen gleitenden Durchschnitten wie dem 100-Wochen- und dem 50-Wochen-SMA kann mehr Einstiegspunkte bieten, jedoch kurzfristig zu Verlusten führen.



Dollar-Cost-Averaging (DCA, z. Dt. Durchschnittskosteneffekt) ist eine Strategie, bei der in regelmäßigen Abständen ein fester Geldbetrag in einen bestimmten Vermögenswert investiert wird, unabhängig von dessen Kurs.





Das Ziel von DCA ist es, die Auswirkungen der Marktvolatilität auf ein Anlageportfolio zu verringern, indem die Käufe über einen längeren Zeitraum verteilt werden, anstatt alles auf einmal zu kaufen.

- Ein Anleger kann zum Beispiel beschließen, jeden Monat 100 Euro in einen Kryptowährungswert zu investieren. Wenn der Preis des Vermögenswerts hoch ist, wird der Anleger weniger Einheiten kaufen, und wenn der Preis niedrig ist, wird der Anleger mehr Einheiten kaufen. Im Laufe der Zeit kann dieser Ansatz zu niedrigeren durchschnittlichen Kosten pro Einheit des Vermögenswerts führen und somit die Auswirkungen kurzfristiger Preisschwankungen verringern.

DCA kann für eine Vielzahl von Anlagen verwendet werden, darunter Aktien, Anleihen und Rohstoffe, und wird häufig für Personen empfohlen, die gerade erst mit dem Investieren beginnen und das Risiko der Marktvolatilität minimieren möchten.

Es ist wichtig, zu beachten, dass DCA weder einen Gewinn garantiert noch vor Verlusten in einem rückläufigen Markt schützt und mit gründlicher Recherche und Marktanalyse kombiniert werden sollte. Außerdem sollten Anleger ihre eigenen finanziellen Ziele und ihre Risikotoleranz berücksichtigen, wenn sie sich für die beste Anlagestrategie entscheiden.

Indikatoren wie der **RSI** und der **MACD** werden verwendet, um überkaufte und überverkaufte Bedingungen und potenzielle Trendänderungen zu erkennen. Der RSI vergleicht das Ausmaß der jüngsten Gewinne mit den jüngsten Verlusten, um überkaufte und überverkaufte Bedingungen zu ermitteln. Der MACD wird berechnet, indem der exponentielle gleitende Durchschnitt (EMA) der 26-Periode vom EMA der 12-Periode subtrahiert und dann ein 9-Tage-EMA des Ergebnisses eingezeichnet wird. Er wird verwendet, um Veränderungen der Dynamik und des Trends zu erkennen.

Es ist wichtig, zu beachten, dass diese Kennzahlen nur eines von vielen Instrumenten sind, die zur Analyse von Markttrends und Preisbewegungen verwendet werden können, und dass sie in Verbindung mit anderen Analysemethoden eingesetzt werden sollten, um ein umfassenderes Verständnis des Marktes zu erhalten. Außerdem ändern sich die Marktbedingungen ständig und die Performance der Vergangenheit ist keine Garantie für zukünftige Ergebnisse.



Kapitel 10

Von Bits zu Bitcoin: Das Zusammensetzen des Puzzles

10.0 Nur ein paar Fakten, ein paar Witze ...
und der Fachjargon

10.1 Richtlinien für die Einreichung und Bewertung
der Abschlussarbeit von Mi Primer Bitcoin



Von Bits zu Bitcoin: Das Zusammensetzen des Puzzles

10.0 Nur ein paar Fakten, ein paar Witze ... und der Fachjargon



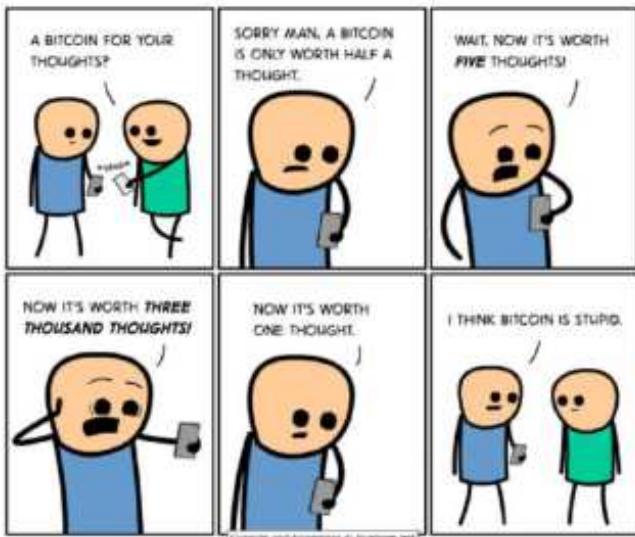
Das *Bitcoin-Netzwerk* ist leistungsfähiger als 500 Supercomputer zusammen.



Rückerstattungen sind bei *Bitcoin*-Transaktionen nicht möglich.



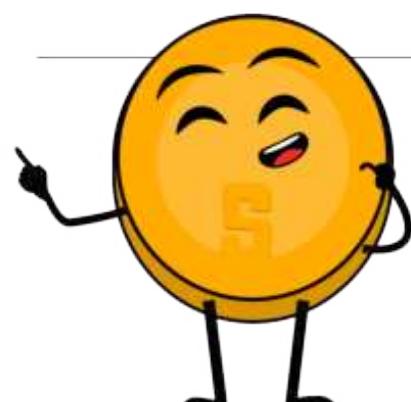
Kapitel 10



Wie viele Miner braucht man, um eine Glühbirne zu wechseln?

– *Eine Million.*

Ein Miner, der sie wechselt, und 999.999 Miner, die im Kreis laufen, um zu bestimmen, wer es tun darf.



Von Bits zu Bitcoin: Das Zusammensetzen des Puzzles

10.1 Richtlinien für die Einreichung und Bewertung der Abschlussarbeit von Mi Primer Bitcoin

Einleitung:

Die Abschlussarbeit des Mi Primer Bitcoin-Kurses ist ein ein- bis zweiseitiges Essay mit dem Titel „Warum Bitcoin?“, in dem man erklären soll, was **Bitcoin** ist, wie es funktioniert und auf welche Weise es die heutige Welt verändert.

Anforderungen:

- Der Aufsatz sollte mindestens eine Seite und höchstens zwei Seiten lang sein, mit doppeltem Zeilenabstand und Schriftgröße 12.
- Der Aufsatz sollte in korrektem Deutsch und frei von Grammatik- und Rechtschreibfehlern verfasst sein.
- Der Aufsatz sollte eine Einleitung, einen Hauptteil und eine Schlussfolgerung enthalten.

Zu behandelnde Themen:

- Erkläre, was **Bitcoin** ist und schreibe etwas über seine Geschichte!
- Erkläre, wie **Bitcoin** funktioniert, einschließlich seiner Hauptmerkmale wie Dezentralisierung, Transaktionen und Mining!
- Erläutere mindestens zwei Möglichkeiten, wie **Bitcoin** die Art und Weise, wie die Welt heute funktioniert, verändert! Verwende Beispiele und Belege, um deine Antwort zu untermauern!

Alternativprojekt:

Diejenigen, die eine praktische Erfahrung bevorzugen, können an der letzten Übung (Bitcoin-Simulator) mit dem **Bitcoin-Blockchain-Simulator-Tool** teilnehmen:
<https://bitcoinsimulator.duckdns.org/blockchain?chain=public>

Hier erstellst du eine neue Wallet und erhältst einen privaten Schlüssel, mit dem du einen Block minen, Transaktionen signieren, eine private Blockchain erstellen und einen 51%-Angriff durchführen kannst.



<https://bitcoinsimulator.duckdns.org/blockchain?chain=public>

Bewertungskriterien:

Die folgenden Kriterien werden zur Bewertung deiner Abschlussarbeit herangezogen:

- Klare Erklärung, was **Bitcoin** ist und wie es funktioniert.
- Verwendung von Beispielen und Belegen zur Untermauerung deiner Antwort.
- Kohärenz und Gliederung des Aufsatzes.
- Korrekte Anwendung von Grammatik und Rechtschreibung.
- Relevanz und Tiefe der Erörterung zum Thema.



Kapitel 10

Einreichung:

Die Abschlussarbeit muss bis zu dem im Lehrplan angegebenen Termin im Word- oder PDF-Format per E-Mail an den Kursleiter geschickt werden. Verspätete Einreichungen werden nicht akzeptiert.

Schlussfolgerung:

Die Abschlussarbeit ist eine Gelegenheit für dich, dein Verständnis von *Bitcoin* und seinem Einfluss auf die Welt zu zeigen. Der Aufsatz sollte deine Fähigkeit demonstrieren, Informationen zu analysieren und zusammenzufassen und sie in einer klaren und präzisen Weise zu präsentieren.

Viel Glück bei deiner Abschlussarbeit!

Weiterführende Quellen

Weiterführende Quellen

Warum sollte man Bitcoin benutzen?

- **Hard Money** (ca. 30 Minuten):

Dieser Film untersucht die Geschichte des Geldes und wie Bitcoin in das aktuelle Finanzsystem passt. Er geht auf die Probleme mit traditionellen Fiat-Währungen ein und zeigt, wie Bitcoin eine Lösung bietet.

- „**Why Bitcoin**“ von Wiz:

Dieser Artikel gibt einen Überblick über die Vorteile der Verwendung von Bitcoin als Währung und Wertaufbewahrungsmittel. Er hebt die dezentrale Natur von Bitcoin hervor und wie sie eine größere finanzielle Freiheit und Sicherheit ermöglicht.

- „**The Bullish Case for Bitcoin (Das bullische Argument für Bitcoin)**“ von Vijay Boyapati:

In diesem Artikel wird dargelegt, warum Bitcoin ein wertvoller Vermögenswert ist und warum er das Potenzial hat, eine dominierende globale Währung zu werden. Der Autor geht auf die technischen und wirtschaftlichen Aspekte von Bitcoin ein, die es zu einer guten Investitionsmöglichkeit machen.

- „**Why Bitcoin matters**“ von Aleks Svetski (ca. 1 Stunde):

In diesem Video geht es um die Bedeutung von Bitcoin als dezentraler digitaler Vermögenswert und wie er das aktuelle Finanzsystem beeinflussen kann. Der Erzähler erkundet das Potenzial von Bitcoin, Menschen auf der ganzen Welt finanzielle Freiheit zu bringen.

Was ist Bitcoin?

- „**What is Bitcoin**“ von Greg Walker:

Dieser Artikel bietet eine umfassende Erklärung dessen, was Bitcoin ist, einschließlich seiner Geschichte, Technologie und wie er sich von traditionellen Währungen unterscheidet.

- „**Bitcoin – The Genesis**“ von RT (ca. 30 Minuten):

Dieses Video behandelt die Entstehung und die Anfänge von Bitcoin. Es untersucht die Beweggründe des mysteriösen Schöpfers Satoshi Nakamoto und wie sich das Konzept von Bitcoin entwickelt hat.

- „**Understanding Bitcoin**“ von BJ Dweck (ca. 1 Stunde 30 Minuten):

In diesem Video werden die technischen Aspekte von Bitcoin und seine Funktionsweise ausführlich erläutert. Der Erzähler behandelt Themen wie die Blockchain, das Mining und den dezentralen Charakter von Bitcoin.

Weiterführendes Lernen

- **The Bitcoin Standard** (ca. 1 Stunde 40 Minuten):

Dieses Hörbuch erforscht den wirtschaftlichen und historischen Kontext, der zur Entstehung von Bitcoin führte. Es behandelt die Vorteile einer dezentralisierten Währung und das Potenzial von Bitcoin, ein globaler Standard zu werden.

- „**Intro to Bitcoin Austrian Thought**“ (ca. 1 Stunde):

Dieser Audiovortrag behandelt die Österreichische Schule der Nationalökonomie und wie sie sich auf das Konzept von Bitcoin bezieht. Er bietet einen detaillierten Einblick in die wirtschaftlichen Prinzipien hinter Bitcoin und wie sie mit dem österreichischen Denken übereinstimmen.



- Alex Gladstein** Check Your Financial Privilege
- Alex Swan** Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications
- Amanda Cavaleri** Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide
- Anita Posch** Learn Bitcoin: Become Financially Sovereign
- Eric Yakes** The 7th Property: Bitcoin and the Monetary Revolution
- Jeff Booth** The Price of Tomorrow: Why Deflation is the Key to an Abundant Future
- Jimmy Song** The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future
- Nik Bhatia** Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies
- Robert Breedlove** Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money

Dalia Platt – Curriculum & Content Creator
dplatt@miprimerbitcoin.io
@dalia_platt

Glossar

51%-Attacke: Eine Art von Angriff auf ein Blockchain-Netzwerk, bei dem eine einzelne Instanz oder Gruppe einen Großteil der Rechenleistung des Netzwerks kontrolliert, was es ihr ermöglicht, Transaktionen zu manipulieren und das Netzwerk möglicherweise zu stören.

Altcoin-Saison: Eine Zeitspanne, in der alternative Kryptowährungen erhebliche Preissteigerungen erleben, oft aufgrund von erhöhtem Investoreninteresse und Akzeptanz.

Altcoins: Digitale Währungen außer Bitcoin.

Angebot und Nachfrage: Der wirtschaftliche Grundsatz, dass der Preis einer Ware oder Dienstleistung durch das Zusammenspiel von angebotener und nachgefragter Menge bestimmt wird.

Atomic Swap: Ein Peer-to-Peer-Tausch von einer Kryptowährung gegen eine andere, ohne dass eine zentrale Börse oder ein Vermittler erforderlich ist.

Auktion: Ein Verfahren, bei dem Waren oder Vermögenswerte an den Meistbietenden verkauft werden.

Bestätigung: Der Prozess, bei dem eine Transaktion vom Netzwerk verarbeitet wird und es sehr unwahrscheinlich ist, dass sie rückgängig gemacht wird. Das Verfahren, bei dem „Miner“ die Echtheit von Transaktionen mit ihrer Computerhardware und -software verifizieren. Es wird empfohlen, mindestens sechs Bestätigungen abzuwarten, um Doppelausgaben verzubeugen.

BIP: Bruttoinlandsprodukt, der Gesamtwert der in einem Land in einem bestimmten Zeitraum produzierten Waren und Dienstleistungen.

Bitcoin: Eine digitale Währung/ein digitales System, das es Menschen ermöglicht, sich gegenseitig Geld zu schicken, ohne eine Bank zu benutzen.

Block-Explorer: Ein Hilfsmittel zum Anzeigen und Erforschen der Blockchain, mit dem Benutzer einzelne Blöcke, Transaktionen und Wallet-Adressen anzeigen können.

Block-Prämie: Der Betrag an neuen Bitcoin, der an Miner für das Hinzufügen eines neuen Blocks zur Blockchain vergeben wird.

Blockchain: Eine öffentliche Aufzeichnung aller durchgeföhrten Bitcoin-Transaktionen.

BTC: Die für Bitcoin verwendete Einheit. Eine digitale Währung, mit der gehandelt werden kann oder Käufe getätigt werden können.

Cold Storage / Cold Wallet / Offline-Wallet: Eine Methode zur Offline-Speicherung von Bitcoin, ohne die Risiken von Hackern oder anderen Online-Bedrohungen.



Dezentralisierung: Die Verteilung von Macht und Kontrolle über ein Netzwerk anstelle einer zentralen Autorität.

Dezentralisierte autonome Organisation (DAO): Eine Organisation oder ein Netzwerk, das durch Smart Contracts (intelligente Verträge) gesteuert wird und auf einer Blockchain läuft, ohne eine zentrale Behörde oder Verwaltungsstruktur.

Dezentrales Finanzwesen / Decentralized Finance (DeFi): Eine Bewegung innerhalb der Kryptowährungsbranche zur Schaffung dezentraler Finanzprodukte und -dienstleistungen, die auf einer Blockchain basieren.

Dezentrales System: Ein System, in dem die Macht oder Kontrolle auf mehrere Instanzen verteilt ist.

Digitaler Vermögenswert (Asset): Eine digitale Repräsentation von Wert, die gehandelt oder als Wertaufbewahrungsmittel verwendet werden kann, wie z. B. Bitcoin.

Distributed Ledger / Verteiltes Kassenbuch: Eine Datenbank, die über ein Netzwerk von Computern verteilt ist, anstatt an einem zentralen Ort gespeichert zu sein.

Doppelte Übereinstimmung der Bedürfnisse: Das Phänomen, dass zwei Parteien in einer Tauschwirtschaft sowohl das haben, was die andere Partei will, als auch das wollen, was die andere Partei hat.

Doppelausgabe: Wenn eine Person versucht, ihre Bitcoin an zwei verschiedene Empfänger gleichzeitig auszugeben.

Dust- / Staub-Transaktion: Eine Transaktion, bei der eine sehr kleine Menge Bitcoin gesendet wird, die zu gering ist, um wirtschaftlich rentabel zu sein.

Entwertung: Die Verringerung des Wertes einer Währung, oft durch Verringerung des Edelmetallanteils einer Münze.

FOMO: Fear of missing out (Angst, etwas zu verpassen), ein Begriff, der das Gefühl der Angst oder des Bedauerns beschreibt, dass man eine gewinnbringende Gelegenheit auf dem Kryptowährungsmarkt verpasst.

FUD: Fear, uncertainty, and doubt (Angst, Ungewissheit und Zweifel), ein Begriff, der zur Beschreibung negativer Gerüchte oder Informationen verwendet wird, die eine Marktpanic oder einen Rückgang des Marktes verursachen können.

Geld- und Fiskalpolitik: Die Politik einer Zentralbank bzw. einer Regierung, die die Geldmenge und die Zinssätze in einer Volkswirtschaft beeinflusst.

Geldmenge: Die Gesamtmenge des im Umlauf befindlichen Geldes in einer Volkswirtschaft.

Handelspaar: Ein Satz von zwei Währungen oder Vermögenswerten, die an einer Kryptowährungsbörse gegeneinander gehandelt werden können.

Hard Fork: Eine Änderung des Bitcoin-Protokolls, die eine neue Version der Blockchain erzeugt, die nicht mit der vorherigen Version kompatibel ist (z. B. Bitcoin Cash).

Hardware-Wallet: Ein physisches Gerät zur Speicherung privater Schlüssel und zur Verwaltung von Kryptowährungen, das im Vergleich zu Software-Wallets mehr Sicherheit bietet.

Hash-Funktion: Eine mathematische Funktion, die Eingabedaten beliebiger Größe entgegennimmt und eine Zeichenkette fester Größe ausgibt, die häufig in der Kryptographie und Blockchain-Technologie verwendet wird.

Hashrate: Eine Möglichkeit, die Rechenleistung des Bitcoin-Netzwerks zu messen.

HODL: Ein Begriff, der in der Kryptowährungs-Community verwendet wird, um zu beschreiben, dass man Kryptowährungen langfristig hält, anstatt sie zu verkaufen oder zu handeln.

Hot-Wallet / Online-Wallet: Eine Bitcoin-Wallet, die mit dem Internet verbunden ist und einen einfachen Zugriff auf Bitcoin ermöglicht.

Importe: Waren und Dienstleistungen, die in einem anderen Land hergestellt und auf dem heimischen Markt verkauft werden.

Initial Coin Offering (ICO): Eine Fundraising-Methode, bei der eine neue Kryptowährung an Investoren im Austausch gegen eine etabliertere Kryptowährung, wie z. B. Bitcoin, verkauft wird.

Kapitalverkehrskontrollen: Beschränkungen für den grenzüberschreitenden Geldverkehr.

Kaufkraft: Die Fähigkeit des Geldes, Waren und Dienstleistungen zu kaufen.

Konsensmechanismus: Eine in der Blockchain-Technologie verwendete Methode zur Validierung von Transaktionen und zur Gewährleistung der Integrität der Blockchain.

Kryptowährungsbörse: Eine Plattform, auf der Nutzer Kryptowährungen kaufen, verkaufen und gegen andere Vermögenswerte wie Fiat-Währung oder andere Kryptowährungen handeln können.

Kryptowährungs-Wallet: Ein Softwareprogramm, das private Schlüssel speichert und es Benutzern ermöglicht, ihre Kryptowährung zu senden, zu empfangen und zu verwalten.



Kryptographie: Ein Zweig der Mathematik, der zur Entwicklung sicherer Systeme beiträgt.

Layer-1-Protokoll: Die grundlegende Schicht eines Blockchain-Netzwerks, die die grundlegenden Aspekte des Konsenses, der Transaktionsvalidierung und der Datenspeicherung regelt.

Layer-2-Protokoll: Eine sekundäre Schicht, die auf einem Layer-1-Blockchain-Netzwerk aufbaut und häufig zur Verbesserung der Skalierbarkeit, Geschwindigkeit und Funktionalität verwendet wird.

Ledger / Kassenbuch: Eine Aufzeichnung der Finanztransaktionen.

Lightning-Netzwerk: Ein Layer-2-Zahlungsprotokoll, das schnellere und billigere Bitcoin-Transaktionen ermöglicht, indem es Off-Chain-Kanäle für kleinere Transaktionen nutzt.

Merkle-Baum / Hash-Baum: Eine baumartige Datenstruktur, die in der Bitcoin-Blockchain verwendet wird, um die Integrität großer Datenmengen effizient zu überprüfen.

Mining-Pool: Eine Gruppe von Minern, die zusammenarbeiten, um ihre Chancen zu erhöhen, neue Blöcke zu finden und Bitcoin zu verdienen.

Mining: Der Prozess der Durchführung von mathematischen Berechnungen für das Bitcoin-Netzwerk mit Computer-Hardware, um Transaktionen zu bestätigen und die Sicherheit zu erhöhen.

Multi-Signatur(Multisig)-Wallet: Eine Wallet, die mehrere Signaturen oder Genehmigungen erfordert, bevor eine Transaktion ausgeführt werden kann, was zusätzliche Sicherheit und Kontrolle bietet.

Multi-Signatur: Ein Sicherheitsmerkmal, das mehr als einen privaten Schlüssel erfordert, um eine Bitcoin-Transaktion zu autorisieren.

Netzwerk: Eine Gruppe von miteinander verbundenen Akteuren.

Node: Ein Computer oder Gerät, das mit dem Bitcoin-Netzwerk verbunden ist und an der Überprüfung und Übertragung von Transaktionen mitwirkt.

Node-Netzwerk: Ein Netzwerk von verbundenen Computern oder Geräten, die das Bitcoin-Netzwerk unterstützen und aufrechterhalten.

Non-Fungible Token (NFT): Eine Art von digitalem Asset, das ein einzigartiges oder einmaliges Objekt darstellt, das oft zur Darstellung von Kunst, Sammlerstücken oder anderen einzigartigen Objekten verwendet wird.

Nonce: Eine Zufallszahl, die zu einem Block-Header hinzugefügt wird, um einen Hash zu erstellen, der dem Schwierigkeitsziel entspricht.

Öffentliche Blockchain: Eine Blockchain, an der sich jeder beteiligen und Transaktionen verifizieren kann, wodurch sie dezentralisiert ist.

Öffentliche/r Schlüssel / Bitcoin-Adresse: Ein öffentliches Passwort/eine öffentliche Nummer, um Bitcoin zu empfangen.

Orphan Block (verwaister Block): Ein Block, der nicht in der Hauptkette der Blockchain enthalten ist, weil er durch eine längere konkurrierende Kette ungültig gemacht wurde.

Paper-Wallet: Eine gedruckte Kopie der privaten und öffentlichen Schlüssel eines Benutzers, die zurweil er durch eine längere konkurrierende Kette ungültig gemacht wurde.

Peer-to-Peer (P2P): Ein dezentralisiertes Netzwerk, in dem die Teilnehmer direkt miteinander interagieren und nicht über eine zentrale Behörde.

Peg (Anbindung): Ein fester Wechselkurs zwischen zwei Währungen, bei dem die eine an den Wert der anderen gekoppelt ist.

Private Blockchain: Eine Blockchain, die von einer einzigen Organisation kontrolliert wird, anstatt dezentralisiert zu sein.

Private Key / Privater Schlüssel: Ein geheimer Datensatz, der das Recht einer Person, Bitcoin von einer bestimmten Wallet auszugeben, durch eine kryptographische Signatur nachweist.

Proof of Stake (PoS): Ein Konsensmechanismus, der in einigen Blockchain-Netzwerken verwendet wird und bei dem die Nutzer einen bestimmten Betrag an Kryptowährung besitzen müssen, um an der Validierung von Transaktionen teilzunehmen.

Proof of Work (PoW): Ein Konsensmechanismus, der von den Nutzern einen gewissen Rechenaufwand verlangt, um am Netzwerk teilnehmen zu können.

Public Key / Öffentlicher Schlüssel: Eine eindeutige Kennung für den Empfang von Bitcoin, die durch einen mathematischen Prozess aus dem privaten Schlüssel eines Benutzers abgeleitet wird.

Public Ledger / Öffentliches Kassenbuch: Eine dezentrale Datenbank, die eine öffentliche Aufzeichnung aller Transaktionen im Bitcoin-Netzwerk führt.



Recheneinheit (Unit of Account): Eine Standardmaßeinheit, die verwendet wird, um den Wert von Waren und Dienstleistungen auszudrücken.

Recovery Phrase / Seed Keyword: Eine Reihe von 12, 18 oder 24 Wörtern, die verwendet werden können, um mehrere Paare von privaten und öffentlichen Schlüsseln zu erzeugen. Diese können verwendet werden, um eine Bitcoin-Wallet wiederherzustellen.

Reservequote: Der Anteil der Einlagen, den eine Bank als Reserven halten muss.

Restriktives Bankwesen: Beschränkungen oder Begrenzungen von Bankdienstleistungen oder des Zugangs zu Bankdienstleistungen.

Satoshi Nakamoto: Das Pseudonym, das von dem/den anonymen Schöpfer(n) von Bitcoin verwendet wird.

Satoshi: Die kleinste Einheit von Bitcoin, die 1/100.000.000 eines Bitcoins entspricht. Er ist nach dem Schöpfer von Bitcoin, Satoshi Nakamoto, benannt.

Satoshis pro byte (sat/b): Eine Einheit, die verwendet wird, um die Höhe der Bitcoin-Transaktionsgebühr zu messen, die pro Byte der Transaktionsdaten gezahlt wird.

Schulden: Geld, das einem anderen geschuldet wird.

SegWit (Segregated Witness): Ein Upgrade des Bitcoin-Protokolls, das die Art und Weise ändert, wie Daten auf der Blockchain gespeichert werden, und so eine höhere Kapazität und niedrigere Transaktionsgebühren ermöglicht.

Sidechain: Eine Blockchain, die mit einer anderen Blockchain verbunden ist und die Übertragung von Vermögenswerten oder Informationen zwischen den beiden Ketten ermöglicht.

Signatur: Ein mathematischer Mechanismus, der es ermöglicht, Eigentum zu beweisen.

Smart Contract: Ein selbstausführender Vertrag, bei dem die Bedingungen der Vereinbarung in einen Code geschrieben sind.

Soft Fork: Eine Änderung des Bitcoin-Protokolls, die mit älteren Versionen der Software rückwärtskompatibel ist.

Stablecoin: Eine Art von Kryptowährung, die darauf ausgelegt ist, einen stabilen Wert beizubehalten, indem sie häufig an eine Fiat-Währung oder einen anderen Vermögenswert gekoppelt ist.

Tauschhandel: Der Austausch von Waren und Dienstleistungen ohne die Verwendung von Geld.

Token: Eine auf einer Blockchain geschaffene Werteinheit, die häufig zur Darstellung eines bestimmten Vermögenswerts oder Nutzens innerhalb eines bestimmten Ökosystems verwendet wird.

Tokenization (Tokenisierung): Der Prozess der Erstellung einer digitalen Repräsentation eines Vermögenswerts oder einer Vermögensklasse auf einer Blockchain, die Bruchteilseigentum und Übertragbarkeit ermöglicht.

Transaktionsgebühr: Ein kleiner Bitcoin-Betrag, der vom Absender einer Transaktion gezahlt wird, um den Minern einen Anreiz zu geben, die Transaktion in einen Block aufzunehmen und der Blockchain hinzuzufügen.

Transaktions-ID: Eine Zeichenfolge aus Zahlen und Buchstaben, die die Details einer Bitcoin-Überweisung (z. B. den gesendeten Betrag, die Adressen des Absenders und des Empfängers und das Datum der Überweisung) in der Bitcoin-Blockchain anzeigt.

Transaktion: Die Übertragung von Bitcoin von einer Adresse zu einer anderen im Bitcoin-Netzwerk.

Trustless / Vertrauensfrei: Ein System oder eine Transaktion, die kein Vertrauen in eine dritte Partei oder einen Vermittler erfordert. Stattdessen verlässt es sich auf die Sicherheit und Transparenz der zugrunde liegenden Technologie.

Unbanked (ohne Bankkonto): Einzelpersonen oder Gemeinschaften ohne Zugang zu traditionellen Bankdienstleistungen.

Volatilität: Der Grad der Veränderung des Preises eines Vermögenswerts im Laufe der Zeit.

Wal: Eine Person oder Organisation, die eine beträchtliche Menge an Kryptowährungen besitzt und in der Lage ist, die Marktpreise durch große Transaktionen zu beeinflussen.

Wallet-Adresse: Eine eindeutige Kennung, die zum Senden und Empfangen von Bitcoin im Bitcoin-Netzwerk verwendet und normalerweise als eine Kette von Buchstaben und Zahlen dargestellt wird.

Wallet-Backup: Eine Kopie der privaten Schlüssel und der Recovery Phrase/Seed Keywords einer Bitcoin-Wallet, die verwendet werden kann, um den Zugang zur Wallet wiederherzustellen, falls das Original verloren geht oder gestohlen wird.

Wallet: Ein virtuelles Behältnis für Bitcoin, das einer physischen Geldbörse ähnelt und einen oder mehrere private Schlüssel enthält, mit denen man die Bitcoin ausgeben kann, die ihm in der Blockchain zugewiesen sind.



Warenwert: Gegenstände, die an und für sich einen Wert haben und als Tauschmittel verwendet werden, wie Gold oder Silber.

Warenkorb: Eine Sammlung von Waren oder Dienstleistungen, die zur Messung der Entwicklung der Lebenshaltungskosten verwendet wird.

Wechselkurs: Der Wert einer Währung im Verhältnis zu einer anderen.

White-Hat-Hacker: Ein ethischer Hacker, der seine Fähigkeiten einsetzt, um Schwachstellen in Computersystemen und Netzwerken zu erkennen und zu beheben.

Whitepaper: Ein Dokument, das das Problem und die Lösung erklärt, die ein Blockchain-Projekt oder eine Kryptowährung anstrebt.

Wiederverwendung von Adressen: Die Praxis, dieselbe Bitcoin-Adresse für mehrere Transaktionen zu verwenden.

XBT und BTC: Abkürzungen für Bitcoin.

Zahlungsmittel: Gegenstände oder Systeme, die im Austausch gegen Waren und Dienstleistungen weithin akzeptiert werden.

Zentralbank (Federal Reserve): Eine staatliche Institution, die die Geldpolitik eines Landes verwaltet.

Zentralisierung: Die Konzentration von Macht oder Kontrolle in einer einzigen Instanz.

Zentralisiertes System: Ein System, in dem die Macht oder die Kontrolle in einer einzigen Instanz konzentriert ist.

Zeitwert des Geldes: Der Grundsatz, dass Geld in der Gegenwart mehr wert ist als in der Zukunft.

Zwei-Faktor-Authentifizierung (2FA): Eine Sicherheitsmaßnahme, die zwei Authentifizierungsmethoden erfordert, normalerweise ein Passwort und einen separaten Code oder ein Gerät, um auf ein Konto zuzugreifen oder eine Transaktion abzuschließen.

Warum ist es wichtig, etwas über Bitcoin zu lernen?

1. Was ist *Bitcoin* und wie funktioniert es?

Bitcoin ist eine dezentralisierte digitale Währung, die unabhängig von einer Zentralbank funktioniert. Sie ermöglicht Peer-to-Peer-Transaktionen ohne Intermediäre, was sie zu einer revolutionären Technologie in der Finanzbranche macht. Um die potenziellen Auswirkungen und den Nutzen zu verstehen, ist es wichtig, zu wissen, wie sie funktioniert.

2. Was macht *Bitcoin* einzigartig und wertvoll?

Bitcoin ist einzigartig, weil es in einem dezentralisierten Netzwerk funktioniert, was Bitcoin resistent gegen staatliche Eingriffe und Manipulationen macht. Außerdem gibt es nur einen begrenzten Vorrat, der auf etwa 21 Millionen begrenzt ist, was es ähnlich wie Gold knapp und wertvoll macht. Das Wissen um diese Eigenschaften hilft, sein Potenzial als Wertaufbewahrungsmittel und Investition zu verstehen.

3. Welche Auswirkungen kann *Bitcoin* auf die Finanzindustrie haben?

Die breite Akzeptanz von *Bitcoin* hat das Potenzial, die traditionellen Finanzsysteme zu stören und das Monopol der Zentralbanken in Frage zu stellen. Es bietet auch neue Möglichkeiten für Investitionen und finanzielle Eingliederung, insbesondere für Personen in Ländern mit instabilen Währungen. Das Verständnis der potenziellen Auswirkungen von Bitcoin auf die Finanzindustrie ist für jeden, der sich für Finanzen und Technologie interessiert, von entscheidender Bedeutung.



EL SALVADOR

