Kryptowährungen

Funktionsweise, Chancen und Risiken

Hausarbeit

Autor: Hannes Frey

Betreuer: Roland Kiefer

Stuttgart, den 31.05.2021

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Zusammenfassung

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1 Einleitung

Seit der Erfindung des Internets in den 90er Jahren befindet sich die Welt im digitalen Wandel. Das World Wide Web bietet Funktionen, die vor 20 Jahren als unvorstellbar galten, und das enorme Wachstumspotential der Technik ist noch lange nicht ausgeschöpft. Im Jahre 2009 ist diesem Zweig auch eine digitale Währung entsprungen und diese begleitet uns seither: Die Bitcoin. Doch bei dieser einen Währung ist es nicht geblieben, denn in den vergangenen Zwölf Jahren haben sich tausende weitere dazu gesellt und eine eigene Ökonomie erschaffen, die das Potenzial einer digitalen Revolution besitzt. Kryptowährungen haben es dabei zuletzt wieder vermehrt in die Abendnachrichten geschafft, sei es wegen neuer Allzeithochs oder Kursabstürzen.[1]

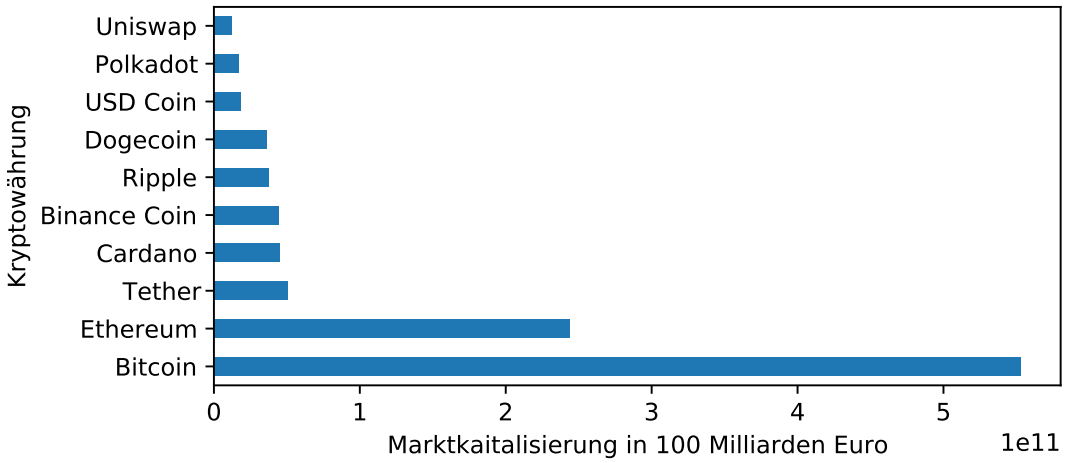

Abbildung 1: Marktkapitalisierung der Zehn größten Krytowährungen in Euro [2]

In der folgenden Arbeit werden Funktionsweise, Chancen und Risiken sowie die wirtschaftliche Bedeutung von Kryptowährungen genauer behandelt, die Geschichte der Entwicklung wird explizit nicht thematisiert.

2 Funktionsweise

Die Technologie, die viele Kryprowährungen und im besonderen Bitcoin auszeichnet, ist als Blockchain bekannt. Wie der Name bereits vermuten lässt, handelt es sich dabei um eine „Kette“aus „Blöcken“in denen beispielsweise jegliche Transaktionen unter Zuhilfenahme von kryptographischen Mechanismen gespeichert sind. [3] Die Blockchain ermöglicht es zudem, Daten nicht zentral speichern zu müssen, sonder diese dezentral in einem Peer to Peer (P2P) Netzwerk abzulegen. In einem solchen Netz arbeiten alle Rechner, die Teil dessen sind, gleichberechtigt zusammen. Zu unterscheiden sind unterschiedliche Kryprowährungen meist in anderen Technologien,denn so setzt Bitcoin beispielsweise zu Verifizierung der Transaktionen auf „Proof-of-Work“, wohingegen andere „Proof-of-Stake“nutzen. Weiter ist auch bemerkbar, dass Protokolle von Kryptowährungen die maximale Menge an in Umlauf befindlicher Geldmenge begrenzt können oder mal bestimmte Inflations- oder Deflationspolitik vorsehen. [4]

2.1 Blockchain am Beispiel Bitcoin

Wie oben bereits beschrieben, verbirgt sich hinter dem Konzept der Blockchain ein Peer-to-Peer Netzwerk, und die Blockchain ermöglicht es so einen gemeinschaftlichen Konsens zu finden, ohne eine dritte zentrale Partei, wie eine Bank oder eine Regierung zu benötigen. Abbildung 2 und 3 zeigen diese Unterschiede anschaulich.

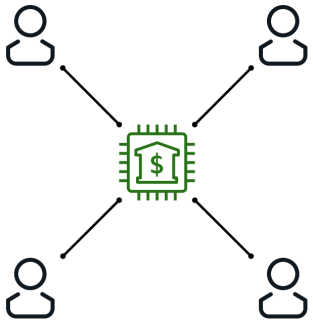

Abbildung 2: Bank als Zentrale Drittpartei

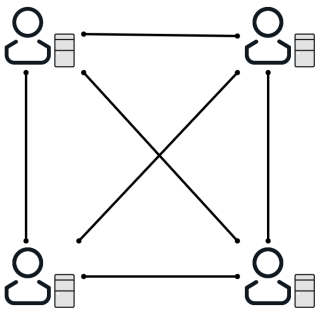

Abbildung 3: Dezentrales Peer-to-Peer Netzwerk

Vergleicht man beide Modelle, so werden alle zentral gespeicherten Daten einer Bank wie Kontostände und Überweisungen ebenso in einer Blockchain gespeichert, nur liegen dort die Datenbanken vielfach kopiert auf allen Rechnern des Netzwerkes vor. Wichtig ist zu erwähnen, dass es sich hierbei nicht um Kopien im geläufigen Sinne handelt, sondern, da es keine Originaldatenbank gibt, jede dieser Kopien den anderen gegenüber gleichwertig ist. Da in der Blockchain alle Transaktionen gespeichert sind, fungiert das Netzwerk somit als globales und kollektives Buchführungssystem, wodurch es zudem unmöglich ist Bitcoins zu vervielfachen oder zu fälschen. [5]

Jeder Nutzer des Netzes ist dabei als Client anzusehen und besitzt als solcher ein Wallet, das eine digitale Analogie zur Geldbörse darstellt. In dieser Wallet jedoch sind jedoch keine Coins aufbewahrt, vielmehr ist in der Wallet ein Schlüssel gespeichert, durch welchen man zugriff auf alle Bitcoin erhalten kann, die man bisher Empfangen hat. Betätigt nun ein Client eine Transaktion, so wird diese per „Best-Effort“-Prinzip an alle im Netzwerk befindlichen „Miner“weitergeleitet. Diese kümmern sich darum, die Transaktionen zu bestätigen und in den nächsten Block der Blockchain einfließen zu lassen.

Um dabei sicherzustellen, dass nur der rechtmäßige Besitzer die Informationen über gewollte Transaktionen seiner Bitcoins an Miner senden kann, verwendet das Protokoll der Bitcoin digitale Signaturen. Zum Zuge kommt ein asymmetrisches kryptographisches Verfahren, das mit privaten und öffentlichen Schlüsseln arbeitet, wobei beide Schlüssel nichts anderes als Zahlenkombinationen sind. Zur besseren Lesbarkeit dieser werden sie mehrmals gehashed um am Ende eine 34 stellige Zeichenkombination zu erhalten. Der private Key ist nur dem Besitzer bekannt und wird verwendet, um die eigenen Transaktionen mittels einem speziellen Algorithmus zu signieren. Der öffentliche Key ist, wie der Name bereits verrät, für jeden einsehbar und dient zur Überprüfung der Signatur einer abgesendeten Transaktion, denn ein privater und öffentlicher Schlüssel gehören immer zusammen. Somit lässt sich immer feststellen, ob bei einer Transaktion Absender und Besitzer übereinstimmen.(siehe Abb.4) [3][6]

Wurde nun, wie tausendfach täglich, eine gültige Transaktion abgesendet, nimmt

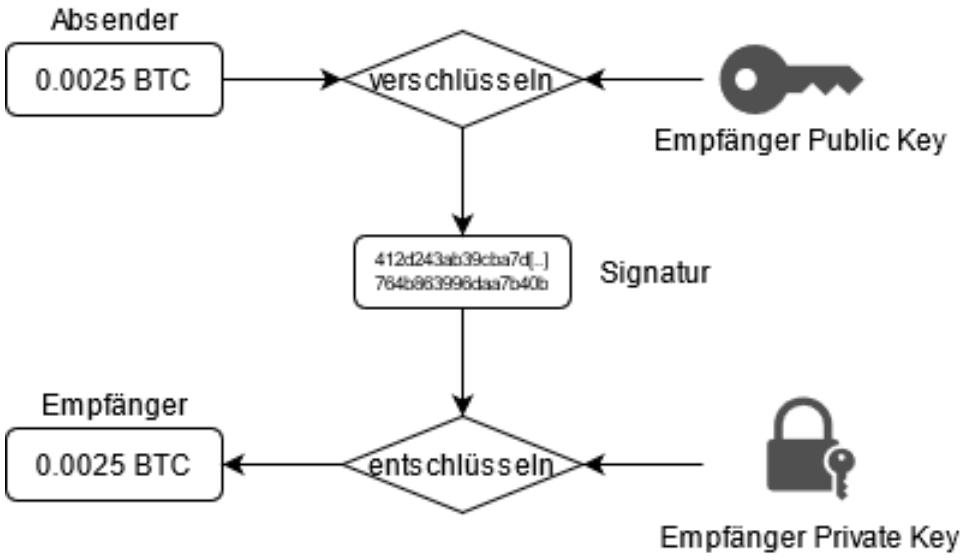

Abbildung 4: Asymmetrische Kryptographie am Beispiel einer Bitcoin Transaktion [7]

ein Miner diese in seine Version der Blockchain auf. Hier spielt nun die Dezentralisation eine große Rolle, denn alle Miner konkurrieren insgesamt darum, dass ihrer Version der Blockchain zu vertrauen ist und diese zur Fortsetzung der Blockchain verwendeter werden soll. Jeder Block der Bitcoin Blockchain hat dabei in etwa die Größe von Einem Megabyte, und ungefähr alle 10 Minuten wird der Blockchain ein neuer Block angehängt. Bevor dies allerdings geschieht, muss der Block zunächst „gefunden“. Im Wettkampf untereinander stellt jeder Miner zunächst seinen Block mit allen getätigten Transaktionen zusammen, und nutzt diesen dann zusammen mit zufälligen Zahlen, genannt Block Header, als Eingabe in den SHA256-Algorithmus. Ziel ist es dann durch ausprobieren verschiedenster Block-Header in der Ausgabe des Algorithmus eine bestimmte Anzahl an Nullen voranstehend zu haben. Die Genaue Anzahl an Nullen hängt dabei von der Gesamtmenge an Rechenleistung im Netz ab, denn sie ist variabel und passt sich automatisch an, um ungefähr bei Zehn Minuten Rechenzeit pro Block zu bleiben. [8]

Wurde von einem Miner dann eine Korrekte Zahl gefunden verkündet dieser es im Netzwerk und die restlichen Geräte überprüfen den Hash des Blocks mit Hilfe des

Block-Headers und zudem, ob auch alle Transaktionen im Block korrekt sind. Ist er gültig, übernehmen sie ihn. Als Belohnung für die geleistete Rechenarbeit erhält der Miner, dessen Block übernommen wird, als Belohnung eine vordefinierte Menge Bitcoin, die vorher noch nicht existierten, und zudem die Summe aller Transaktionsgebühren der im Block enthaltenen Transaktionen.

Um Manipulationen von Transaktionen in früheren Blöcken zu verhindern, beinhaltet ein Block immer auch den Hash des vorherigen Blocks. Ändert man also den Inhalt eines früheren Blocks, so ändert sich damit auch dessen Hash, und der aller darauf folgenden Blöcke in einen ungültigen Hash. Diese „Verkettung“aller Blöcke führt zu dem Namen Blockchain. [5]

2.2 Proof of Work vs Proof of Stake

Das oben beschriebene Konzept, wie es beispielsweise von den Kryptowährungen Bitcoin und Litecoin angewandt wird, nennt sich auch „Proof-of-Work“(PoW), denn für die Verifizierung der Legitimität (Proof) von Transaktionen müssen Berechnungen (Work) durchgeführt werden. Welche Ausmaße das aufgrund der Lukrativität des Bitcoin schürfen angenommen hat, verdeutlicht Abbildung 5.

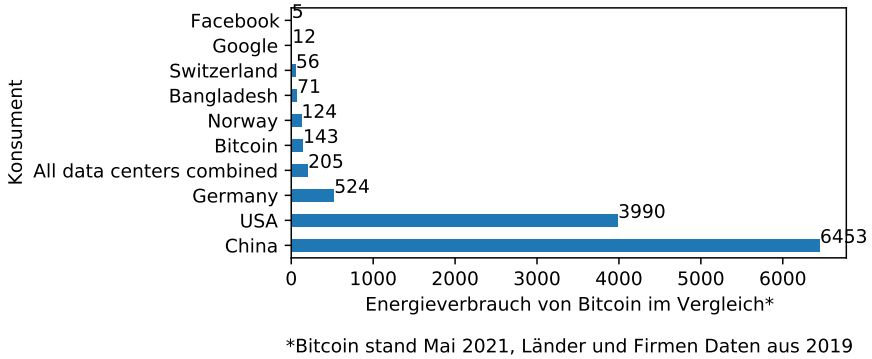

Abbildung 5: Stromverbrauch des Bitcoin-Netzwerkes im Vergleich zu anderen Konsumenten [9]

Wie sich unschwer erkennen lässt übersteigt der Energiebedarf des Bitcoin Minings inzwischen sogar den ganzer Länder, und im Vergleich zu IT-Riesen ist deren Energieverbrauch marginal. Da inzwischen in jeder Gesellschaftlichen Schicht jedoch klar wird, dass wir eine kommende Katastrophe die durch immer steigende Temperaturen dringlichst zu verhindern haben, wird die Kritik immer lauter. Ein Lösungsvorschlag hierbei lautet Proof-of-Stake, denn anders als bei PoW werden hier keine Berechnungen mehr benötigt. Es handelt sich dabei weitgehend um das selbe Konzept, nur dass anstelle des Arbeitens Sicherheiten in Form des jeweiligen Coin hinterlegt werden müssen und über den Zeitraum des Minings eingefroren bleiben. Mit diesem Anteil an eingefrorener Währung validiert ein Nutzer dann ebenso die Transaktionen für einen Block. Wer aus dem Pool aller Miner im Endeffekt ausgewählt wird, den Block zu validieren ist dabei in einem zuvor festgelegtem Algorithmus beschrieben und sollte möglichst Zufällig sein. Je nach Implementierung bekommen die Miner dann beispielsweise die transaktionsgebühren alles Transaktionen des verifizierten Block oder etwa jähliche Zinsen auf die eingefrohrenen Coins. [3]

2.3 Ethereum und Smart Contracts

Ethereum belegt gemessen an der Marktkapitalisierung den zweiten Platz aller Kryptowährungen, weswegen sich ein kurzer Blick hierauf lohnt. Im Vergleich zu Bitcoin scheint Ethereum zunächst sehr ähnlich zu sein, denn beide Protokolle verwenden eine Blockchain in Kombination mit Proof-of-Work, doch Ethereum ist mehr als eine reine Kryptowährung. In erster Linie ist Ethereum eine Plattform für die Entwicklung dezentraler Apps über sogenannte Smart Contracts. Ein solcher Smart Contract kann dabei von einem dezentralen Wahlsystem, über Kredite und Versicherungen bis hin zu Crowdfunding reichen. Hier ist auch von Vorteil, dass Ethereum Transaktionen deutlich schneller und günstiger verarbeiten kann als in Bitcoin. Der Konsens des Ethereum-Netzwerks ist zudem auf der Seite des Wechsels zu einem System dass auf Proof-of-Stake aufbaut, Test-Netzwerke sind bereits am laufen und der Wechsel des Hauptnetzes

soll noch 2021 stattfinden. [3]

3 Chancen und Risiken

4 Konsequenzen

4.1 Heutiges Geldsystem

Literatur

[1] Tim Schredder. *Das Neue Geld, Bitcoin, Kryptowährungen und Blockchain verständlich erklärt.* München: Piper, 2018.

[2] *CoinMarketCap.com*. URL: https://coinmarketcap.com/de/ (besucht am 01. 06. 2021).

[3] Krijn Soeteman. *Kryptowährungen für Dummies*. Weinheim: Wiley, 2019.

[4] Tobias Wenger und Kim Oliver Tokarski. *Kryptowährungen, Eine empirisch-qualitative Analyse von Kryptowährungen gegenüber dem traditionellen Währungssystem*. Weinheim: Wiley, 2019.

[5] J Rosenberg. „Kryptowährungen". In: *Z Herz- Thorax- Gefäßchir* 33 (Apr. 2019), 139–146.

[6] *Binance, Was ist eine digitale Signatur?* URL: https://academy.binance.com/de/articles/what-is-a-digital-signature (besucht am 03. 06. 2021).

[7] *Coincierge, Public Keys und Private Keys*. URL: https://coincierge.de/wallets/ (besucht am 03. 06. 2021).

[8] Vincent Schlatt u. a. „BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE". In: (Jan. 2019).

[9] *Bitcoin Devours More Electricity Than Many Countries*. URL: https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin/ (besucht am 03. 06. 2021).

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die Zitate deutlich kenntlich gemacht zu haben.
Ich erkläre weiterhin, dass die vorliegende Arbeit in gleicher oder ähnlicher Form noch nicht im Rahmen eines anderen Prüfungsverfahrens eingereicht wurde.

Stuttgart, den 4. Juni 2021 Hannes Frey