Universität Leipzig

Fakultät für Mathematik und Informatik
Institut für Informatik

Bitcoin (BTC) als digitale Währung

- Potential als nachhaltiges Zahlungsmittel -

Seminararbeit

Leipzig, September, 2021

vorgelegt von

Dähnert, Florian
Informatik – Master

Dozenten: Prof. Dr. Hans-Gert Gräbe
Ken Pierre Kleemann

Inhaltsverzeichnis

Abkürzungsverzeichnis

E-Geld	Elektronisches Geld
Nonce	number used only
P2PKH	Pay-To-Public-Key-Hash
TXID	Transaktions-Hash
UTXO	unspent transaction output

1 Einleitung

Das Thema der Nachhaltigkeit ist aus unserem Alltag nicht mehr wegzudenken. In den Medien wird immer wieder auf die Notwendigkeit eines nachhaltigen Lebens für unsere Zukunft und die unseres Planeten hingewiesen, so dass dieser Anspruch schlussendlich nicht nur bei den Unternehmen und Firmen, sondern auch bei jedem einzelnen Bürger angekommen ist. Offensichtlich liegt mit der Forderung nach einem solchen Lebensstil ein breites Ansatz- und Handlungsspektrum vor. Die zunehmende Digitalisierung bietet hier Potenziale für alle Lebensbereiche des Menschen. Darunter fällt im Bereich der Ökonomie auch die Zahlung mit sogenannten Kryptowährungen wie Bitcoin, Dogecoin und Ether.
In der vorliegenden Arbeit soll Bitcoin als System und als Zahlungsmittel näher in Bezug auf seine Potentiale für Nachhaltigkeit betrachtet werden.

Bitcoin ist mehr als nur eine Kryptowährung. Bitcoin ist ein System, eine mögliche Alternative und vielleicht der Beginn eines neuen Zeitalters im Währungsbereich.
Unter dem Pseudonym Satoshi Nakamoto wurde 2008 ein Whitepaper veröffentlicht, welches eine Alternative zum bisherigen Währungsstandard aufzeigen sollte. In Anbetracht der damaligen globalen Banken- und Finanzkrise wurde mit Bitcoin ein System angestrebt, wodurch ohne zentrale Instanz, ohne Vertrauen in einen Vertragspartner Geld transferiert werden sollte. Nicht nur die Währung Bitcoin, sondern die Funktionsweise des Systems Distributed Ledger Technologies, waren als revolutionär einzustufen. Transaktionen sollten digital und - ähnlich dem Konzept von Bargeld - dezentral verlaufen. Die Überprüfung auf Rechtmäßigkeit der einzelnen Überweisungen geht nicht mehr von einzelnen Instanzen aus, sondern erfolgt über eine breite Masse an natürlichen Personen aus unserer Gesellschaft. Jeder der über einen Bitcoin-Node (Zugang) und die dazu benötigten Hardware-Ressourcen verfügt, kann eine Bewertung der getätigten Transaktionen teilen. Der Konsens dieser Bewertungen bestimmt dann über die Richtigkeit der Überweisung. Zudem kann nachvollzogen werden, ob eine ausreichende Liquidität des Senders besteht.
Die Arbeit mit dem System unterliegt strengen Regeln, die Nakamoto bereits in seinem Whitepaper von 2008 festgehalten hat, beispielsweise für das Mining und die Blockzusammenstellung (vgl. Nyumbayire 2021). Damit Regelverstöße und mögliche Manipulationsversuche minimiert werden können, werden Protokolle und Daten über den Verlauf redundant auf die

einzelnen lokalen Speichermedien der Teilnehmer des Netzwerkes gespeichert. Die Funktionsweise von Bitcoin wird im dritten Kapitel erläutert.

Die Vision von Nakamoto ist die Schaffung eines digitalen Bargelds, anonym und dezentral. 13 Jahre nach der Veröffentlichung des Whitepapers soll mit der vorliegenden Arbeit ein Resümee der Potenziale von Bitcoin in Bezug auf Nachhaltigkeit gezogen werden. Dazu soll erörtert werden, ob Bitcoin (Währung) in den nächsten Jahren eine mögliche Alternative für die Zahlung mit Bargeld darstellt.

Wie bereits erwähnt ist Bitcoin als Begriff zweideutig. Zum einen wird das System beschrieben, zum anderen die Währung. Daher werden zunächst die Grundlagen von Geld und Währung dargestellt. Anschließend soll die Funktionsweise des Systems erläutert werden. Im Anschluss daran werden Eigenschaften von Bitcoin und die Begriffe ideales und solides Geld geklärt. Abschließend werden Unterschiede im Vergleich mit herkömmlichen Zahlungs- und Abwicklungssystemen aufgezeigt und das Potential von Bitcoin als alternatives Zahlungsmittel bewertet.

2 Einordnung und Definition von Währung

Bevor in die Grundlagen von Bitcoin als Kryptowährung eingeführt werden kann, bedarf es hier einer Definition des Währungsbegriffes, um eine Einordnung von Kryptowährung vornehmen zu können.

Unter dem Begriff der Währung wird das „hoheitlich geordnete Geldwesen eines Staates oder Währungsgebietes einschließlich aller Regelungen zur Sicherung der Geldwertstabilität [verstanden], weshalb der Begriff Währung auch für den Namen der Geldeinheit (Geld) steht.“ (Manger-Nestler 2020). Wir können in unserem Alltag zwischen verschiedenen Formen von Geld unterscheiden: neben dem Bargeld in Form von Münzen und Banknoten gilt auch elektronisches Geld und Zentralbankgeld als Teil unserer Währung (vgl. Wohlmann 2020: 304 f.).
In der Literatur ist dabei noch keine Einigkeit darüber erzielt wurden, ob die sogenannten Kryptowährungen als Zahlungsmittel oder Bezahlverfahren einzuordnen ist (vgl. ebd.: 305).
Wohlmann (2020) definiert diese jedoch als „digitales Bargeld“ (vgl. ebd.:305), da die Transaktionen auf einer Dezentralisierung beruhen. Weitere Merkmale des Bargeldes weisen einen

engen Zusammenhang mit dem zu untersuchenden Bitcoin als Kryptowährung auf. Wie bereits erwähnt war es die Intention von Nakamoto, eine Währungsart zu erschaffen, die auf Pseudonymität und Dezentralität basiert. Ähnlich der Verwendung von Bargeld, kann es ohne zentrale Instanz genutzt werden. Eine Nachverfolgung von Banknoten ist nur bedingt über die Seriennummer möglich. Dabei sind nur Ausgeber und letzter Empfänger bekannt. Bei Bankmünzen ist es nahezu ausgeschlossen die Übertragung zwischen den Besitzern nachzuvollziehen, da kein eineindeutiges Identifikationsmerkmal vorliegt. Es benötigt kein Vertrauen in ein System oder in eine Instanz, um den Wert des Geldes zu verifizieren.
Aufgrund dieser Merkmale wird Bargeld auch als eine Art Peer-to-Peer-System bezeichnet (vgl. Wohlmann 2020: 304) und steht eng im Zusammenhang mit dem Erscheinungsbild der Kryptowährung, welche in Kapitel 3 ausführlicher aufgegriffen wird.

Eine digitale Transferierung von Geld, die sich in ihrer Nutzung auch durch die andauernde Corona-Pandemie verstärkt hat, ist das Elektronische Geld, kurz E-Geld. Jedes Geld, welches über eine E-Geld-Karte, auch Giro- oder Kreditkarte genannt oder über Bankinstituten (Online Banking) transferiert wird, wird dem E-Geld zugewiesen. In einem zentralen Dateisystem eines Bankinstituts ist ein bestimmter Wert (Kontostand), welcher sich aus Haben und Soll ergibt, hinterlegt. Um hier die „Manipulation“ von Geld in Form von Doppelausgaben zu vermeiden, bedarf es einer Kontrollinstanz, welche in der Regel die Banken selbst stellen. Fehlerhafte Transaktionen können somit korrigiert oder aufgeklärt werden.

Die Regulierung von Geldbeständen ist Aufgabe der Zentralbanken. Dabei sind Zentralbanken nationale oder supranationale Institutionen. Beispielsweise stellt die Deutsche Bundesbank eine von der Regierung losgelöste Einrichtung dar, welche die Bewahrung der Geldwert- und Preisniveaustabilität verfolgt. In anderen Ländern, wie beispielsweise China, ist die Zentralbank (People´s Bank of China) von der Staatsregierung weisungsgebunden. Dennoch verfolgen diese Institutionen ähnliche Ziele. Zudem sind sie verantwortlich für die Ausgabe von Bargeld und E-Geld, welches nur an Geschäftsbanken übermittelt wird. Vor diesem Hintergrund wird diese Währungsart als Zentralbankgeld bezeichnet.

Die letzte Währungsart, die hier vorgestellt werden soll, die sogenannten Kryptowährungen, fallen in der gewählten Kategorisierung aus den genannten Gründen in den Bereich „Sonstiges“

(vgl. Wohlmann 2020: 306). Heutzutage existiert bereits eine Vielzahl an Kryptowährungen. Neben Bitcoin sind Ether und Dogecoin als Hauptvertreter zu erwähnen.
Im Wirtschaftslexikon von Gabler werden Kryptowährungen als „digitale (Quasi-)Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem“ (Bendel 2021) definiert. Nähere Ausführungen dazu folgen in Kapitel 3.

Wenn Kryptowährungen mit den anderen vorgestellten Währungsarten verglichen werden, können, besonders in Bezug auf Bargeld, viele Parallelen aufgedeckt werden. Der Begriff Peer-to-Peer, der bereits im Zusammenhang mit dem Bargeld verwendet wurde, entstammt dem informationstechnologischen Netzwerksystem und findet auch bei Kryptowährungen wie Bitcoin Anwendung. Daher wird hier auch von digitalem Bargeld gesprochen.
Sowohl bei Kryptowährung als auch bei Bargeld genügt der Besitz als hinreichende Legitimation. Im Gegensatz dazu bedarf es für die Legitimation von E-Geld der Identifikation des Zahlenden, um eine Gewährleistung der Rechtmäßigkeit und Liquidität sicherzustellen.

3 Grundlagen Bitcoin

In diesem Kapitel soll eine Definition des Sachverhaltes erfolgen. Dabei wird auf die Funktionsweise von sicheren Transkationen mit Bitcoin und die Bedeutung von „Blockchain“ eingegangen.

Häufig wird der Begriff „Bitcoin“ genutzt, ohne dabei inhaltlich zu differenzieren. Dennoch beinhaltet er nicht nur den „Coin“, welcher gehandelt und transferiert wird, sondern auch das geschaffene System aus der Idee von Nakamoto. Wenn nachfolgend in der vorliegenden Seminararbeit explizit auf den Coin verwiesen werden soll, wird dieser mit dem von Onlinehandelsbörsen benutzen Akronym *BTC* abgekürzt. Wenn Inhalte des Systems besprochen werden sollen, wird der Begriff *Bitcoin* genutzt.

3.1 BTC als das erste digitale Geld

Bitcoin stellt den Versuch dar, ein System - entgegen der globalen hegemonial-zentralisierten Ordnung - zu entwickeln, welches als elektronisches Peer-to-Peer-„Bargeld“ mit einer globalen Community als Knotenpunkt (Nodes) arbeitet (vgl. Ammous 2019: 286). Die Verantwortung soll

nicht mehr in der Hand einer einzigen zentralen Institution liegen. Nakamoto verdeutlichte seine Intention für ein derartiges System in einem Artikel vom 11. Februar 2009: „*The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. "* (Nakamoto 2009). Damit beruft er sich auf diverse Vertrauensbrüche in der Geschichte der Geldpolitik. Dass es sich dabei um ein aktuelles Problem handelt, beweist der Absturz des venezolanischen Bolivar, der im Zeitraum von 2009 bis 2019 eine Abwertung von 2:1 Bolivar/US-Dollar auf 250.000:1 erfuhr (vgl. Pritzker 2020: 9). Das Grundproblem ist hier, dass die venezolanische Zentralbank nicht losgelöst vom Staat agieren kann und bei wirtschaftlichen Schwierigkeiten die entsprechende Inflation in Kauf genommen wird.
Aus diesem Grund stellte Nakamoto die folgenden Anforderungen an sein System: Entkoppelt von Staat und Zentralbank stellt Bitcoin eine distribuierte Software dar, die eine Wertübertragung in einer Währung, hier BTC, ermöglicht, die vor unerwarteter Inflation geschützt ist. Bitcoin automatisiert Methoden einer Zentralbank und macht diese vorhersehbar und nicht veränderbar, indem der Konsens der Community eine Kopie des Open-Source-Code besitzt. Ammous beschreibt Bitcoin als erste mögliche Lösung für Probleme der Verkäuflichkeit, Solidarität und Souveränität (vgl. Ammous 2019: 229). Diese Begriffe werden in Kapitel 4 näher erläutert.

3.2 Bitcoin als System

In diesem Abschnitt soll eine BTC-Transaktion exemplarisch funktional und technisch vorgestellt werden, Aufgaben einzelner Akteure erläutert, sowie Algorithmen und Kryptografien benannt werden.

3.2.1 Transaktion - Senden

Wie bereits erwähnt, ist Bitcoin ein Peer-to-Peer Netzwerk, d.h. es befinden sich endlich viele Mitglieder im Netzwerk, welche untereinander verbunden sind. Dabei ist zu unterscheiden, ob als Full-Node oder als Miner im Netzwerk agieren werden soll. Für das Transferieren von BTC-Einheiten sind nur Full-Nodes authentifiziert, wobei Transaktionsanfragen auch von außerhalb des Netzwerkes durch sogenannte „lightweight clients" an die Full-Nodes gestellt werden können. Somit muss keine vollständige Kopie der Blockchain heruntergeladen werden.

Blockchain bietet dem Bitcoin als Technologie die Eliminierung der Notwendigkeit auf Dritte zu vertrauen. Dritte stehen hier im Zusammenhang als Vermittler für (Krypto-) Währungstransaktionen. Blockchain ist keine schnelle, günstige und effiziente Lösung für derartige Transaktionen. Sie bringt jedoch den Vorteil mit, dass ohne Vermittlungsrolle globale Transaktionen getätigt werden können. Im Sinne der Blockchain werden Blöcke mit Transaktionsdaten untereinander referenziert und dezentral gespeichert.

Unabhängig davon, ob ein Light- oder Full-Node betrieben wird, wird die Erstellung eines Wallets, ähnlich einem Bankkonto, benötigt. Heutzutage sind Wallets hierarchisch deterministisch (vgl. Schmidt-Ott 2021). Das heißt, dass bei der Erstellung über eine Software oder Anwendung das Wallet zunächst nur über eine *Seed Phrase* verfügt. Aus dieser Zeichenfolge (12-24 Wörter) können Private-Keys, anschließend Public-Keys und Public-Adressen konstruiert werden (vgl. ebd.). Innerhalb der Wallet können verschiedene Konten mit Private- und Public-Key erzeugt werden. Der Privat-Key ist in diesem Sinne das Passwort des Kontos und der daraus erstellte Public-Key ist die Kontenbezeichnung. Mit diesen Informationen kann auf das Konto zugegriffen werden. Im Laufe der Bitcoin-Entwicklung wurden Public-Addresses integriert, mit denen eine höhere Sicherheitsstufe erreicht werden konnte. Für das Empfangen von Bitcoin ist die Herausgabe des Public-Keys somit nicht mehr notwendig. Die Public-Address wird über den Public-Key gehasht. Unter Hashing versteht man einen Prozess, der einen beliebigen Datenstrom bzw. Zeichenfolge in einen Datensatz fester Größe umwandeln kann. Die Besonderheit ist dabei, dass der neue Datensatz nicht umkehrbar ist. Das heißt, der Algorithmus impliziert eine Einwegsfunktion und somit ist ausgeschlossen, dass mit dem Hashwert als Ergebnis nicht auf sein Urbild zurückgeschlossen werden kann. Es gibt keine Möglichkeit, um den Input nachzuvollziehen. Sobald ein Zeichen im Ausgangsdatenstrom verändert wurde, verändert sich das gesamte Endergebnis. Dabei muss erwähnt werden, dass hiermit ein allgemeines Problem im Kryptodesign vorliegt, da verschiedene Inputs zu einem identischen Output führen können, was als Hash-Kollision bezeichnet wird. Die Wahrscheinlichkeit hierfür ist jedoch sehr gering, da mit SHA-256 aus 2^{256} eindeutigen Hash-Werten gewählt werden kann. In dem nachfolgenden Auszug ist diese Dimension der möglichen Hash-Werte dargestellt.

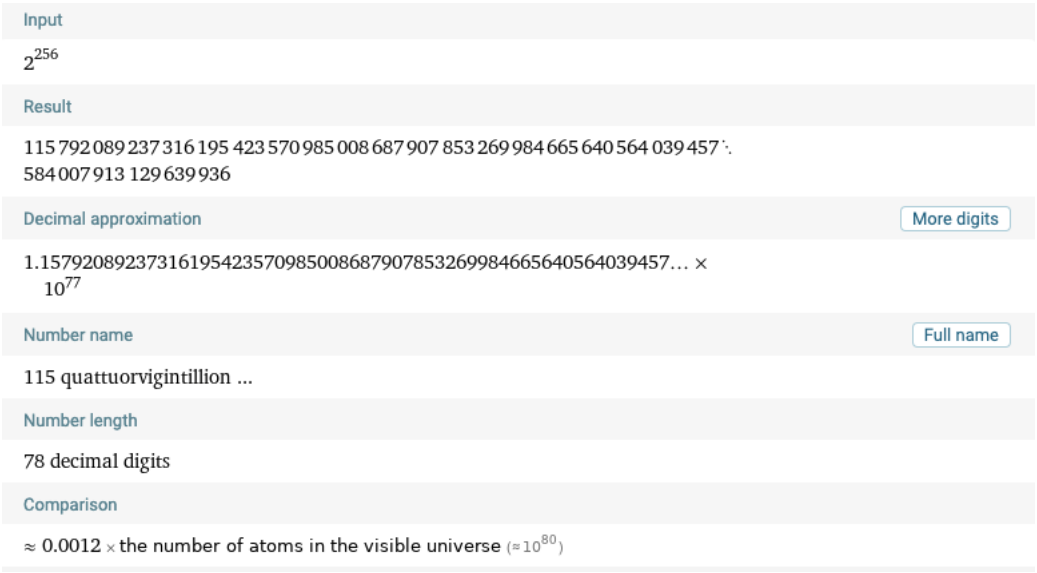


Abbildung 3.1: Mögliche eindeutige Hash-Werte mit SHA-256

Aufgrund dieser hohen Anzahl ist der für Bitcoin genutzte Algorithmus SHA-256 nahezu Preimage – und Kollisionsresistent. Preimage bezeichnet in diesem Zusammenhang, dass der Algorithmus nicht auf das Urbild zurückzuschließen lässt, es sei denn, man kann die Ausgabe einer Eingabe zuordnen, da dieser Algorithmus deterministisch arbeitet. Die Rechenleistung heutiger Computer ist jedoch nicht in der Lage, zeitnah die Menge der Möglichkeiten abzugleichen.

Das Hashing von Private-Key auf Public-Key erfolgt über die Einwegsfunktion mittels standardgemäßen Pay-To-Public-Key-Hash (P2PKH). Eine Rückverfolgung ist in diesen Hash-Dimensionen nahezu unmöglich.

Sobald eine Transaktionsanfrage zweier übereinstimmender Parteien vorliegt, codiert der Empfänger seine Public-Address mit dem Algorithmus base58-Check zu einem String, welcher jetzt über eine Adressversionsnummer, eine Fehlererkennungsprüfsumme und eine Public-Address verfügt (vgl. bitcoin.org 2021). Diese Bitcoin-Adresse wird dann dem Sender übergeben. Dieser decodiert den String, um den ursprünglichen Hash-Wert, die Public-Adresse, zu erhalten. Der Sender hat nun verschiedene Möglichkeiten eine Transaktion zu formulieren. Standardmäßig wird die Überweisung P2PKH-Transaktion verfasst. Diese beinhaltet eine eindeutige Versionsnummer, eine Eingabe, sowie eine Ausgabe und eine Sperrzeit (vgl. Rybarczyk 2018). In der Eingabe werden alle *unspent transactionen outputs* (UTXO) aufgelistet, die der Höhe der Transaktion entweder entsprechen oder sie übersteigen. Wenn beispielsweise 18 BTC überwiesen werden sollen und der Sender bisher nur zwei Gutschriften in Höhe von jeweils 10 BTC erhalten

hatte, werden beide in voller Höhe in der Eingabe als UTXO hinterlegt. Der Restbetrag in Höhe von 2 BTC wird nach Abschluss der Transaktion an die Bitcoin-Adresse des Senders als UTXO zurücküberwiesen.
Neben den UTXO beinhaltet die Eingabe außerdem eine Sequenznummer und ein Entsperrungsskript ScriptSig mit einer digitalen Signatur und einem öffentlichen Schlüssel.
Die Ausgabe wiederum enthält den eigentlichen Überweisungswert. Zudem ist hier das Script-PubKey vorzufinden, welches BTCs sperrt, während diese an den nächsten Empfänger weitergegeben werden. ScriptPubKey und ScriptSig arbeiten komplementär (vgl. Mycryptopredia 2018). Beide Skripte werden nacheinander ausgeführt, wenn der Empfänger seine BTCs weiter an jemand anderen (Empfänger 2) versenden möchte. Zunächst werden die BTCs vom Empfänger 1 mit den Bedingungen des ScriptSig entsperrt, um diese als UTXO in die Eingabe aufzunehmen und sie wiederum mit dem Script-PubKey zu versperren. Dieser Prozess ist eine Sicherheitsmaßnahme vom System, damit nicht autorisierte Teilnehmer die BTCs auf dem Transaktionsaktionsweg abfangen und für sich benutzen können. Abschließend wird die gesamte Transaktion durch den Sender unterzeichnet, hier wird vorrangig die secp2561-Signatur genutzt. Full-Nodes geben anschließend ihre Transaktionsnachricht an das Netzwerk frei. Darauf folgt das sogenannte Mining, die Erstellung von Transaktionsblöcken und deren Verkettung.

3.2.2 Transaktion – Mining

Der Begriff des Minings ist spätestens nach dem Bekanntwerden der globalen Knappheit an Grafikkarten populär geworden. Der Markt reguliert sich nur sehr langsam, da die Miner-Community stetig wächst.
Mining bezeichnet einerseits ein Validierungsverfahren und andererseits das Hinzufügen und Verketten von Transaktionsdaten in Blöcken. Bevor ein Block jedoch veröffentlicht werden kann und somit die Kette der Blöcke erweitert wird, ist zunächst die Blockbildung notwendig. Ein Block besteht grundsätzlich aus zwei Teilen: Block-Header und Transaktion.
Im Block-Header befinden sich die Metadaten: Hashwert des Vorgängerblocks, ein Zeitstempel und das Hashergebnis des Merkle-Baums (root-hash). Letzteres ist eine Zusammenfassung und Berechnung von Transaktionshashes (TXID) einzelner Transaktionen.
Die für den Block-Header notwendige *Nonce* (number used once), wird durch die Miner berechnet. Dafür ist das System an verschiedene Bedingungen gekoppelt. Es ist vorgesehen, dass ein Block ungefähr aller 10 Minuten veröffentlicht werden kann. Hintergrund ist die

vorprogrammierte Ausgabe von Blockprämien bis zum Jahr 2140. Neue Bitcoins werden ausschließlich durch das Mining erstellt und durch einen Verkauf über die Miner in den Umlauf gegeben. Da die Anzahl der Miner im Netzwerk jedoch nicht konstant ist, können Blöcke in unterschiedlicher Zeit veröffentlicht werden, mitunter zwischen 1 bis 12 Minuten. Um annähernd dem gewünschten Standard zur Veröffentlichung der Blocks von 10 Minuten zu entsprechen, wurde ein sogenanntes *Difficulty Adjustment* eingeführt, welches den Gültigkeitsbereich für den zu lösenden Hash-Wert vorgibt. Da das Netzwerk schwankende Mitgliederzahlen hat, die an einen aktiven Mining-Prozess teilnehmen, muss die Blockproduktion be- oder entschleunigt werden, indem die Vorgabe im Miningprozess anhand der führenden Nullen variiert. Eine automatische Anpassung erfolgt systemseitig ungefähr aller 14 Tage auf Grundlage der Gesamtrechenleistung, die dem System aktuell zur Verfügung steht. Das Problem hierbei ist die zeitliche Verzögerung, wie anhand der roten Kurve in der nachfolgenden Grafik veranschaulicht werden soll.

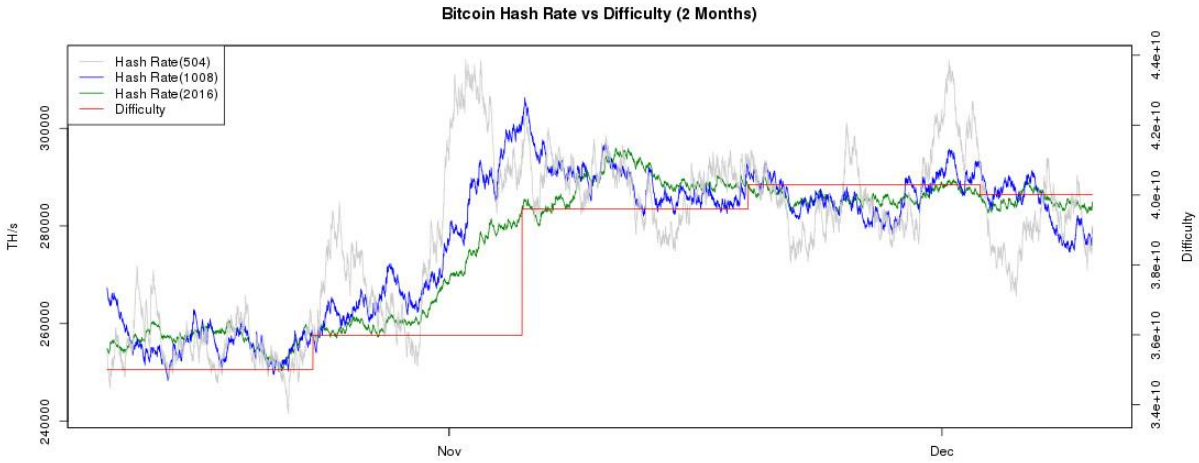


Abbildung 3.2: Vergleich Hashrate und Schwierigkeitsanpassung (cryptomining-blog.com 2014)

Die Schwierigkeitsanpassung ist eine bewährte Technologie für schwer erzeugbares Geld, wie dem Bitcoin (vgl. Ammous 2019: 237). Es verhindert das Abschweifen von dem Emissionszeitplans und sollte in der Theorie den Stock-to-Flow, den prognostizierten Marktwert, nicht stark beeinflussen (vgl. Ledesma 2021).

Das nachfolgende Beispiel soll diesen Vorgang verdeutlichen, indem beispielhaft ein System vorgegeben ist, welches eine Nullstelle zu Beginn des Hash erfordert.

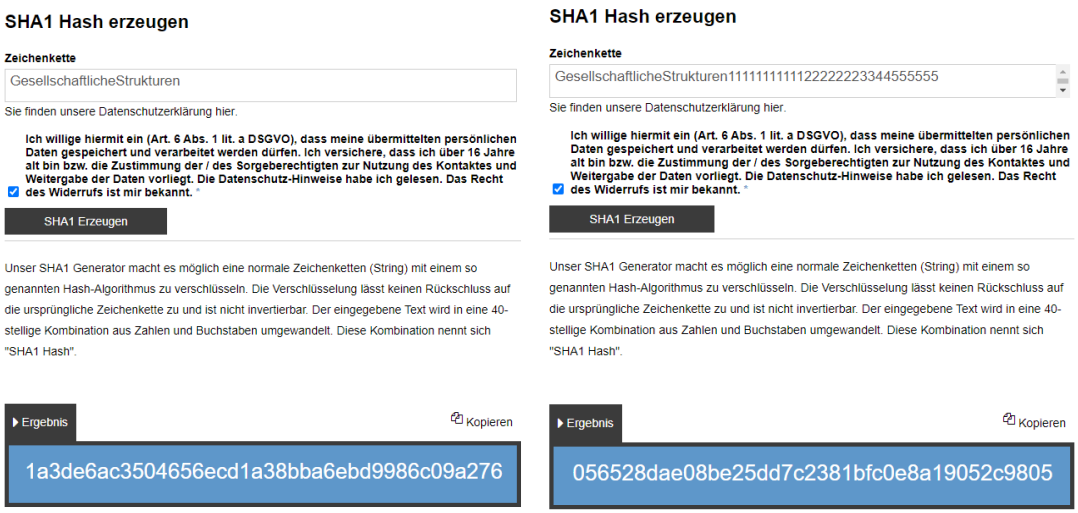


Abbildung 3.3: Mining-Prozess - vereinfachtes Beispiel

Um nun einen gewünschten Hash mit einer Null zu generieren, benötigt man die Zeichenkette „GesellschaftlicheStrukturen11111111111222222233445555555". Dabei entspricht „11111111111222222233445555555" der *„Goldenen Nonce",* da diese Zeichenkette gemeinsam mit den Daten des Blocks zu einem Hash im Gültigkeitsbereich führt.
Die Vorgabe der Nullen ist immer eine Mindestangabe. Falls im Beispiel ein Hash berechnet werden würde, der 2 führenden Nullen aufweist, würde dieser auch als gültig angesehen werden. Weiterhin wurde im obigen Beispiel mit dem Algorithmus SHA-1 gearbeitet. In Bitcoin wird standardgemäß der Algorithmus SHA-256 angewendet (vgl. Pritzker 2020: 31 f.), der einen noch größeren Umfang an möglichen Konstellationen besitzt.
Zusammengefasst ist Mining kein reiner Berechnungsprozess, sondern fungiert nach dem Prinzip des *Trail-and-Error* (vgl. Centieiro 2020). Gemeinsam mit den Blockdaten und einen vorgegeben Gültigkeitsbereich werden immer wieder verschiedene Noncen getestet, bis diese zu einem positiven Ergebnis führen.

Nach dem Hinzufügen der richtigen Nonce im Block-Header gilt der Block als vollständig und wird im Netzwerk an die Full-Nodes gesendet, die in letzter Instanz die Überprüfung des Arbeitsaufwandes übernehmen. Dazu hashen die Full-Nodes die Nonce mit den Metadaten aus dem Block. Sobald mehr als 50% der Full-Nodes den gleichen End-Hash bestätigen, gilt dieser Block als wahrheitsgemäß. Der Block, welcher eine maximale Größe von einem Megabyte aufweisen darf, wird jetzt in die Blockchain geschrieben. Tritt der Fall ein, dass verschiedene Miner Blöcke gleichzeitig veröffentlichen, kommt es zum Chain-Split (vgl. Pritzker 2020: 63 f.). Dabei

wird die Blockkette desjenigen Miners verfolgt, der nachweislich einen größeren Arbeitsaufwand hatte. Die Transaktionen aus den sogenannten verwaisten Blöcken werden wieder als *unspent transaction* deklariert und für eine andere Blockbildung genutzt (vgl. ebd.: 64).

Die erhaltenen BTCs können vom Empfänger nur entsperrt werden, wenn dieser den Output als Input einer neuen Transaktion benennt und die Bedingungen des erstellten *Signatur-Skript (scriptSig),* durch die Benutzung des *öffentlichen Schlüssels (PublicKey),* erfüllt. Damit gilt die Transaktion als abgeschlossen.
Hierbei wird nach dem Trail-and-Error-Prinzip vorgegangen, d.h. nach jeder Berechnung wird geprüft, ob der Wert dem Gültigkeitsbereich entspricht. Bei Nichtentsprechen wird eine neue Berechnung angestoßen. Im Fall von Bitcoin wird immer wieder eine neue Nonce in Verbindung mit den statischen Metadaten des Blocks gewählt. Das sogenannte *Proof-of-Work* ist kein Ergebnis aus der Entwicklung von Bitcoin, sondern wurde bereits 1993 erfunden (vgl. Pritzker 2020: 28).

Der Proof-of-Work geht mit einem hohen Stromverbrauch einher (vgl. Busch et al. 2021). Um diesen zu decken, gibt das System nach einer erfolgreichen Aufnahme in die Blockchain, ein sogenanntes *Block-Reward* aus (vgl. cvj.ch o.D.). Anfänglich belief sich der Betrag auf 50 BTC pro Block. Dieser Wert reduzierte sich aufgrund des Emissionszeitplans auf nur noch 6,25 BTC (vgl. Pritzker 2020: 44). Voraussichtlich 2024 oder nach 210.000 neuen Blöcken führt das System eine Halbierung (*Halving*) der Blockprämie aus (vgl. Pritzker 2020: 44 ff.). Dies hängt mit der begrenzten Anzahl an BTC zusammen, die ausgegeben werden können. BTC sind insgesamt auf 21 Millionen Coins begrenzt und können nur geschürft werden. Das Halving ist notwendig, um langfristig, bis in das Jahr 2140, neues Geld, auszugeben. Zukünftig wird daher vermehrt auf Transaktionsgebühren gesetzt, denn die Kosten für Hard- und Software und Stromverbrauch, können in wenigen Jahren voraussichtlich nicht mehr mit der Blockprämie allein gedeckt werden. Daher besteht die Option, bei jeder Transaktion eine eigens festgelegte Gebühr (engl.: Fee) zu erheben.

3.2.3 Eigenschaften

In diesem Abschnitt wird Bitcoin bezüglich der Eigenschaften Effizienz, Sicherheit, Autonomie und Volatilität untersucht. Dabei sollen bereits Anhaltspunkte für die spätere Diskussion – Bitcoin als Alternative für derzeitige Währungen – erarbeitet werden.

Bitcoin wird als sehr ineffizient eingestuft (vgl. Cox 2021). Die Effizienz wird durch diverse Faktoren, wie beispielsweise das Handelssystem oder auch die ökologische Bilanz bestimmt. Letzteres steht heutzutage noch immer sehr in der Kritik (vgl. ebd.). Schätzungsweise verbrauchen allein die Miner so viel Strom, wie die gesamten Niederlande im jährlichen Vergleich (vgl. Bocksch 2021). Dabei ist jedoch der Betrieb der Computer der Full-Nodes, die ebenfalls als Prüfer relevant sind, noch nicht einberechnet wurden. Als Alternative zum bisherigen Verfahren *Proof-of-Work* wird vorgeschlagen, Konzepte des *Proof-of-Stake* oder *Proof-of-Authority* einzubinden (vgl. Mitra 2021). Diese entsprechen jedoch nicht der Idee der Dezentralisierung.
Zusätzlich dazu, wurde das Handelssystem in seiner Anwendung für den Durchschnittsverbraucher noch als zu komplex eingeschätzt. So war Bitcoin anfänglich aufgrund weniger Gebrauchsinformationen den Kreisen der Informatiker und der Kryptografiker vorbehalten. Dieser Umstand wurde in den letzten Jahren jedoch berücksichtigt, sodass Transaktionen heute benutzerfreundlich über Apps gesteuert werden können.

Im Bereich der Sicherheit, speziell der Datensicherheit, ist Bitcoin aufgrund der Irreversibilität der Transaktionsdaten als sehr sicher einzuschätzen. Daten werden redundant dezentral gespeichert. Mitglieder (Nodes und Miner) müssen jederzeit einen aktuellen Stand der Blockchain vorweisen, um zugreifen zu können. Die regelgerechte Abwicklung der Transaktionen bedarf nicht dem Vertrauen einer Gegenpartei, sondern nur dem Vertrauen in ein technisches Protokoll. Bitcoin ist daher Open-Source, damit Prozesse verstanden und nachvollzogen werden können. Eine Grauzone der Sicherheit von Bitcoin stellt jedoch der rechtliche Umgang außerhalb des Systems dar. Es gibt bisher keinen Gesetzesentwurf, um beispielsweise geschädigte Personen zu schützen. Erschwert wird dies durch den Umstand, dass Kryptowährungen in den meisten Ländern nicht als Währung anerkannt sind und eine internationale Aufklärung in der Regel problematisch ist. Nutzer von Kryptowährungen agieren eigenverantwortlich. Bei Verlust des Primärschlüssels und dem dazugehörigen Wallet, kann nach deutschem Recht kein Schadensanspruch gestellt werden. Bei dem Erwerb von BTCs über Exchange-Plattformen kann bisher

nur „auf die allgemeinen Grundsätze der vorvertraglichen Rücksichtnahmepflichten gemäß § 311 Absatz 2 und § 241 Absatz 2 BGB“ (Dethloff 2018) zurückgegriffen werden.

Eine weitere Eigenschaft von Bitcoin ist die Autonomie. Darunter soll das Fehlen einer zentralen Institution und die Unabhängigkeit vom Bankensektor verstanden werden (vgl. Wohlmann 2020: 314) Das System Bitcoin kann autark im Bezug zu anderen Banken betrieben werden, es ist sozusagen ein in sich geschlossenes Konstrukt. Die vollständige Autonomie ist spätestens bei Ein- und Auszahlungen von BTCs und bei den immer beliebteren Off-Chain-Transkationen aufgehoben.
Zusammengefasst ist Bitcoin hier so zu beurteilen, dass eine vollständige Autonomie - entsprechend der Idee des Erfinders Nakamoto - anfänglich realisiert werden konnte, aber aufgrund der steigenden Zahl der Nutzer nicht mehr realisierbar ist. Dies ist auf die Vielzahl der Transaktionen zurückzuführen, die getätigt werden.

Bitcoin muss sich zudem mit einer weiteren negativen Wirtschaftsentwicklung befassen, der sehr hohen Volatilität (vgl. Ammous 2019: 258). Volatilität gibt die Standardabweichung für die Kursschwankungen an (vgl. ebd.: 258). Die zwei nachfolgenden Grafiken sollen vergleichend - bezogen auf die Währung Euro – demonstrieren, dass BTC viel höhere Kursamplituden aufzeigt als der US-Dollar als Beispiel für eine etablierte Währung.

Abbildung 3.4: Kursentwicklung BTC-Euro 2020/21 (finanzen.net 2021)

Abbildung 3.5: Kursentwicklung US-Dollar-Euro 2020/21 (finanzen.net, 2021)

Betrachtet man die Entwicklungen des letzten Jahres, schwankte der US-Dollar gerade einmal um ungefähr 5%. Dementgegen unterlagen BTCs Schwankungen von mehr als 430%.

4 Solides und ideales Geld

In Kapitel 2 wurden bereits die vier Währungstypen thematisiert und dabei wurde festgestellt, dass Kryptowährungen eine unterschiedliche Akzeptanz in verschiedenen Ländern haben. In Deutschland beispielsweise, zählen Kryptowährungen zu Sonstigen Währungen.
Das Ziel der Arbeit ist es, darzustellen, ob sich BTC als sichere Währung, vergleichbar mit dem Euro, eignet und sich dementsprechend etablieren kann. Dazu folgt an dieser Stelle eine Einführung in die Begriffe des *idealen* und *soliden Geldes*, um eine Vergleichbarkeit herzustellen. BTC sollte diesen Merkmalen entsprechen, um als alternative Währung bestehen zu können.
Bei den folgenden Ausführungen handelt es sich um eine bloße theoretische Darstellung des Konstruktes. Der Verfasser unterlässt hierbei bewusst eine persönliche Bewertung und vernachlässigt den Einfluss wirtschaftlicher Aspekte.

Solides Geld ist aufgrund seiner Verkäuflichkeit und seiner Wertstabilität vor allem in der freien Marktwirtschaft beliebt (vgl. Ammous 2019: 101 f.). Diese Eigenschaften teilen heutzutage bereits die verbreitetsten Währungen, was beispielsweise in Kapitel 3.2.3 mit der Volatilität des US-Dollar, gezeigt wurde. Zudem sollte eine Übertragbarkeit auf andere Personen und Währungen, sowie die Teilbarkeit über Skalen, möglich sein (vgl. ebd.: 101 f.). Ein weiteres Merkmal soliden Geldes ist, dass autoritäre Institutionen die Geldmenge nicht manipulieren und auch

keine Vorschrift zur Verwendung geben können (vgl. ebd.: 102). Um größere Rezessionen oder gar Krisen zu vermeiden, muss mit diesem Geld eine wirtschaftliche Kalkulation möglich sein.

Auf diesen Eigenschaften baut das ideale Geld auf. Sie werden jedoch um das Merkmal der Limitierung der Geldmenge erweitert. Das bedeutet, dass es keinen Staat oder keine Zentralbank gibt, die die Geldmenge eigenständig erhöht. Somit ist sichergestellt, dass die Währung bzw. das Geld einer absoluten Knappheit unterliegt, was Entwertung/Inflation verhindert.

Zusammengefasst sollte BTC, um als eigenständige Währung gelten zu können, also die folgenden Eigenschaften besitzen: Wertstabilität, zukunftssichere Kalkulation, Teilbarkeit und freie Verwendung.
BTC verhindert mit der festgelegten Summe an Coins Inflationen, es sind jedoch hohe Volatilitäten beobachtbar.

5 Diskussion – Bitcoin als sichere und nachhaltige Währung?

Nachdem nun die Grundlagen zu den Bereichen Geld, Währung, Währungspolitik und Bitcoin als Zahlungssystem dargestellt wurden, soll nun eine zusammenfassende Bewertung folgen. Dabei soll unter dem Schwerpunkt der Nachhaltigkeit, vor allem das Potential von BTCs als alternatives Zahlungsmittel im Vergleich zu herkömmlichen Währungen und Zahlungswegen betrachtet werden. Diese Diskussion erscheint notwendig, da Bitcoin zwar schon seit einigen Jahren veröffentlicht wurde, aber dennoch mit nur einem geringen Anteil am ökonomischen Geschehen teilhat. Dies erscheint verwunderlich, da mit Kryptowährungen eine vermeintlich sichere und flexible Alternative zu Bargeld oder Online-Banking vorliegt. Um hier eine fundierte Bewertung abgeben zu können, dienen die theoretischen Grundlagen der Kapitel 2 bis 4 als Basis.

5.1 Vor- und Nachteile des Systems Bitcoin

Neben der Dezentralisierung stellt vor allem das Vertrauen in ein offenes und schwer zu veränderliches System, anstelle des Vertrauens von Dritten, einen Vorteil von Bitcoin dar, da diese „von Natur aus eine zusätzliche Sicherheitslücke“ (Szabo 2001) bieten. Bitcoin selbst bietet viele

Sicherheitsaspekte. „Die Natur von Bitcoin ist so, dass nach der Veröffentlichung der Version 0.1 das Kerndesign für immer in Stein gemeißelt wurde“. (übersetzt aus Engl., Satoshi 2010) Dahinter verbirgt sich die Konstanz des Systems, denn eine Systemänderung ist nur durch den Konsens möglich. Versuchte Manipulationen können auf diese Art minimiert werden.
Weiterhin sind Transaktionen und Zugänge zu Wallets besonders gesichert. Die dafür angewandte asymmetrische Kryptografie mit Privat- und Public-Key ist das zentrale operative Merkmal von Bitcoin, welches die Verifikation der genannten Funktionen ermöglicht.

In diesem Zusammenhang stellt die Effizienz ein umstrittenes Thema heutiger Zahlungs- und Abwicklungssysteme dar. Das Arbeiten mit Transaktionen auf mehreren Instanzen benötigt viel Arbeitszeit und ist in gewisser Weise ein erhöhter Kostenfaktor. Kontenabgleiche und mögliche Doppelausgaben (engl. Double Spending) könnten durch das Konstrukt Bitcoin umgangen werden. Mit dem global verteilten Peer-to-Peer-System sind Ländergrenzen aufgehoben, sodass Überweisungen zeitnah und kostengünstig getätigt werden können. Aufgrund der dezentralen Steuerung des Systems und der Transaktionsmechanismen, ist Bitcoin in den genannten Punkten als deutlich effizienter einzustufen als herkömmliche Zahlungs- und Abwicklungssysteme, wie beispielsweise Deutsche Bank und PayPal.

Weiterhin ist die ökologische Bilanz von Systemen, Prozessen und Produkten ein aktuell relevantes Thema, welches aufgrund der akuten Klimakrise in den Mittelpunkt rückt. 75% aller Bitcoin-Minen- Betreiber nutzen bereits teilweise Strom aus erneuerbaren Energien (vgl. Busch et al. 2021). 39% der Miner arbeiten vollständig mit grünem Strom (vgl. ebd.). Viele davon haben ihre Minen in den Skandinavischen Ländern errichtet, da durch die Nutzung von Wasser- und Windkraft ausreichend Strom zur Verfügung steht, ohne diese Ressourcen der Gesellschaft zu entziehen und die Kosten gering sind.
Hierzu liefert der Wirtschaftswissenschaftler Saifedean Ammous im gesellschaftlich-politischen Hinblick ein weiteres Argument:

> *„Die Frage, ob Bitcoin Strom verschwendet, ist im Kern ein Missverständnis über die grundsätzlich subjektive Natur von dem, was man unter Wert versteht. Strom wird weltweit in großen Mengen zur Deckung des Bedarfs der Verbraucher erzeugt. Die Beurteilung, ob dieser Strom verschwendet wurde oder nicht, liegt einzig im Ermessen des Verbrauchers(,) der dafür bezahlt. Menschen, die bereit sind, für ihre Transaktionen die*

Betriebskosten des Bitcoins-Netzwerks zu übernehmen, finanzieren im Grunde diesen Stromverbrauch, d.h. der Strom wird zur Befriedigung der Verbraucherbedürfnisse erzeugt und wurde somit nicht verschwendet. Funktional gesehen ist der PoW (Anm. Proof-of-Work) die bisher einzige von Menschen erschaffene Methode, um hartes digitales Geld zu erschaffen. Wenn die Nutzer der Meinung sind, dass es sich lohnt, für den PoW zu bezahlen, dann ist der Strom nicht verschwendet worden."
(Ammous 2019: 301)

Der Fokus auf den gesellschaftlichen Nutzen als einzigen Bezugspunkt wird jedoch als kritisch erachtet. Weiterhin zeigt sich, dass die Proof-of-Work-Methode im direkten Vergleich mit anderen Transaktionsverfahren einen erhöhten Strombedarf aufweist.

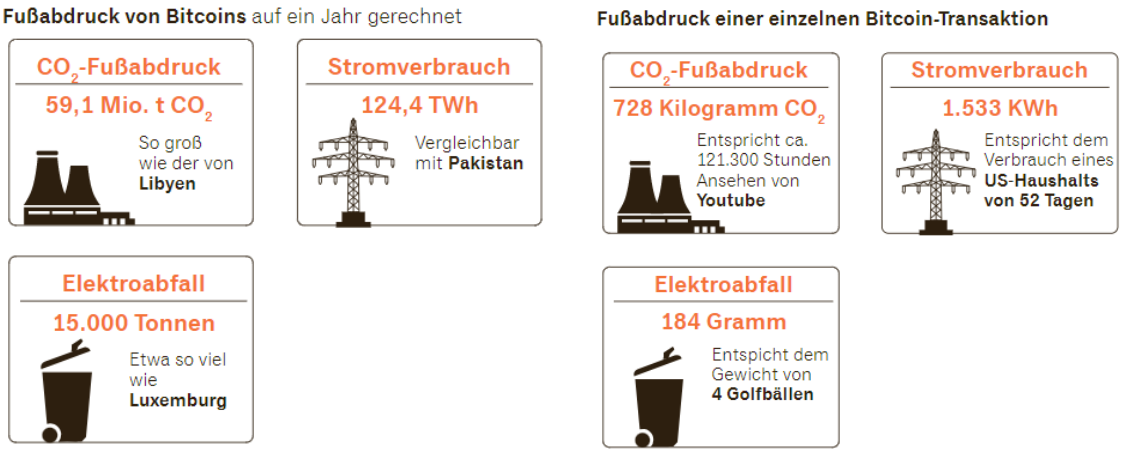


Abbildung 5.1: Vergleichdaten zum Stromverbrauch von Bitcoin (Busch et al. 2021)

Proof-of-Work bietet Funktionen und Sicherheiten an, die andere Methoden bisher nicht in diesem Umfang bieten können. Beispielweise kann mit Proof-of-Stake Strom eingespart werden, allerdings würde somit nicht mehr der Idee der vollkommenen Dezentralität entsprochen werden. Daher wird das System in naher Zukunft voraussichtlich nicht wesentlich verändert werden.

Doch der erhöhte Energieverbrauch des Systems stellt nicht den einzigen Nachteil dar.
Nationale sowie internationale Zahlungsdienstleister unterliegen grundsätzlich einer Rechtsform. Bitcoin gehört weder einer Gesellschaft noch einer Institution an. Natürliche und juristische Personen können demnach nicht benannt werden. Es ist lediglich eine Software, die durch

das Agieren von Mitgliedern betrieben werden kann. Im weitesten Sinne könnte man die Community als Organisation für das Transferieren von Coins benennen. Da sich BTCs dahingehend in einer juristischen Grauzone bewegen, scheint beispielsweise der Ersatz im Schadensfall problematisch. Es gibt keine eindeutige Rechtsprechung für Kryptowährungen bei dem Eintreten von Diebstählen, Insolvenzen und Manipulation.

Im vorherigen Abschnitt wurde erneut auf den Sicherheitsaspekt der Verifikation mittels asymmetrischer Kryptografie hingewiesen. Die Schlüssel bestehen aus einer 78-stelligen Zeichenfolge, als Ergebnis eines SHA-256 Hashes. Im Vergleich zu einem gewöhnlichen Kontenzugriff, zu dem Kontonummer und Pin/Passwort gehört, sind diese Schlüssel also deutlich schwieriger zu behalten. Ein Verlust des Schlüssels ist somit wahrscheinlicher.
Im Vergleich dazu, können bei einer Bank oder anderen Zahlungsdienstleistern, mit einer entsprechenden Legitimation der eigenen Person, neue Zugangsdaten beantragt werden. Bei Bitcoin ist dieser Weg ausgeschlossen. Die Wallets sind nicht mehr zugänglich und die BTCs sind eingefroren. Allgemein stellt der Verlust oder die Zerstörung von BTC ein großes Problem für das System dar. Aufgrund der absoluten Knappheit können keine Coins nachproduziert werden. Nach Angaben von Investopedia sollen bereits über 20% der erzeugten BTCs verloren gegangen sein (vgl. Reiff 2019). Dies hat negative Auswirkungen auf die Liquidität und das Transaktionsvolumen.
Bitcoin gilt in der Realwirtschaft bereits als relevant und verbreitet, jedoch auch als anfälliges Ökosystem (vgl. Sharma 2021). Zusätzlich scheint die Nachweisbarkeitspflicht über den Besitz eines Wallets schwierig. Bei Verlust des Primär-Schlüssels und des Seed Phrase, kann keine eindeutige Identität zum Wallet mehr zugeordnet werden.

5.2 Vor- und Nachteile der Währung BTC

Die bisherige Erörterung bezog sich vorrangig auf das System Bitcoin. Im Folgenden soll daher Bitcoin als Währungsmittel fokussiert werden. BTC waren zuletzt vor allem bei Regierungen, Anlegern und Spekulanten thematisiert. Daher werden die Aspekte von dem Autor stärker gewichtet, die mit der Währung in Verbindung stehen.

BTC wird als digitales Bargeld angesehen. Der Vorteil im Vergleich zu anderen Währungen liegt nicht darin, Barzahlzahlungen zu ersetzen, sondern darin, sie unabhängig vom Standort durchführen zu können. Anhand der Transaktionszahlen konnte ein deutlicher Zugang an Bitcoin-Überweisungen festgestellt werden. Die gesellschaftliche Akzeptanz für Kryptowährungen, insbesondere für BTCs, nahm zu und führt dazu, dass Unternehmen diese „Währung" bereits annehmen. Das bekannteste Beispiel dafür ist Tesla. Erste Zentralbanken äußersten sich zur möglichen Benutzung von BTCs als Reservewährung[1], wenn die Wertstabilität vergleichbar mit dem des Euro und US-Dollars sein sollte (vgl. Ammous 2019: 289). Dies würde weiteres Vertrauen in eine neuartige Währung für die Gesellschaft geben.

Es wurde bereits angemerkt, dass BTC ein absolut knappes Gut ist und dass das System durch die Blockprämie vorgibt, dass voraussichtlich mit Abstufen der Prämien im Jahr 2140 keine neuen Coins produziert werden. Theoretisch können somit ca. 21 Millionen BTCs geschürft werden. Allerdings sind bis zum Jahr 2050 bereits 20 Millionen BTCs ausgegeben, wodurch ein Ende des ursprünglichen kalkulierten Minings vorher eintreten wird. Die Ursache für diese Verzerrung ist, dass die Schwierigkeitsanpassung kein präziser Prozess ist, sondern eine Kalibrierung. In der Regel sollte aller 10 Minuten ein Block gebildet werden. Demnach ist nur eine geringe Standardabweichung vom System vorgesehen. Aufgrund der variablen Zahl der Miner, kann mit der Schwierigkeitsanpassung nicht immer rechtzeitig reagiert werden.
So entfiel der chinesische Minermarkt, nachdem die Regierung ein Verbot aussprach (vgl. Neuhaus 2021). Dieser Rückgang wurde erst 14 Tage später registriert. Sollte ein solcher Fall erneut eintreten und die Miner somit keine Block-Rewards im klassischen Sinne mehr erhalten, bedarf es der Umstellung auf Transaktionsgebühren. Diese würden weitaus höher ausfallen als die bisherigen. Ob die Gesellschaft für ihre Pseudonymität hohe Gebühren in Kauf nimmt, wird sich zeigen.

Neben der unpräzisen Schwierigkeitsanpassung haben sich im Laufe der Zeit zwei weitere Probleme ergeben. Zum einen wird das Mining in den nächsten Jahren nicht mehr so attraktiv sein, wie heute, denn anhand des Stock-to-Flow-Modells ist der berechnete Marktpreis bereits durchaus höher als der heutige.

[1] Reservewährungen werden verwendet, um Konten zwischen Zentralbanken zu begleichen, um den Marktwert der eigenen Währung zu verteidigen.

Abbildung 5.2: Stock-to-Flow-Modell - Prognostizierter Marktwert (finance.yahoo.com 2021)

Dazu folgen höhere Kosten für Strom, weniger Blockprämien durch das Halving und teurere Hardware. Zudem nahm die Konkurrenz in den letzten Monaten stark zu.
Zum anderen benötigt das System bei Zuwachs der täglich durchgeführten Transaktionen Skalierungsmöglichkeiten. Bitcoin selbst kann nur 120 Millionen Transaktionen pro Jahr durchführen. Im Vergleich dazu kann Visa 100 Milliarden Transaktionen pro Jahr tätigen. Wenn Bitcoin diese Dimensionen erreicht, dann müsste jeder Node 800 Megabyte an Daten aller 10 Minuten laden. In einem Jahr würden ungefähr 42 Terabyte an Daten zusammenkommen, wodurch für Privatpersonen zu hohe Kosten entstehen würden. Der einzige Spielraum für eine sinnvolle Skalierung ist die Verwendung von Off-Chain-Transaktionen und sogenannten Mikrotransaktionen. Andere Optimierungsansätze sind noch in Diskussion bzw. Gegenstand der Forschung.

Ein weiterer Vorteil ist auf politischer Ebene zu finden. Banken kontrollieren Konten und Depots, Regierungen kontrollieren wiederum die Banken. Eine solche Konstellation ist bei Bitcoin auf politischer Ebene ausgeschlossen, da keine zentralen Autoritäten dominant sind. Die chinesische Regierung konnte im genannten Beispiel lediglich das Betreiben von „Minen“ unterbinden, nicht den Zugriff auf diverse Wallets und auch nicht auf das Transaktionsgeschehen. Zudem besteht vorwiegend in Entwicklungsländern das Problem, dass Regierungen großen Einfluss auf Zentral-, Geschäfts- und Privatbanken haben. Ammous behauptet, dass eine Regierung immer die Geldproduktion monopolisieren wollen würde und einer zu starken Versuchung ausgesetzt sei, sich an der Erhöhung der Geldmenge zu beteiligen (vgl. Ammous 2019: 244).

Nakamoto hingegen garantiert mit seinem System ein geringes Angebotswachstum, vor dem Hintergrund mit Bitcoin ein absolut knappes Gut geschaffen zu haben. Zudem erweisen sich die gute Kaufkraft, die Teilbarkeit und Gruppierung von Bitcoin als Eigenschaften von solidem Geld. Neben der begrenzten Auflage von BTCs zeigt Bitcoin mit der unmöglichen Nachproduktion von BTCs weitere Funktionen von idealem Geld. Diese Eigenschaften haben die derzeit existenten Währungen nicht. Vor allem in Ländern mit einer angespannten Währungspolitik wäre ein Einsatz von Bitcoin angebracht.

Nakamoto definierte sein System folgendermaßen: "*A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution*." (Nakamoto 2008: 1). Dabei intendierte er ein Zahlungs- und Abwicklungssystem auf Grundlage eines eigenen Systems, mit eigener Währung - vergleichbar mit einem Binnenmarkt.
Seit ungefähr 2017 gibt es den Bitcoin-Hype, wodurch dessen Marktwert drastisch gestiegen ist. Dieses Jahr erreichte Bitcoin zwischenzeitlich die Marke von 64.000 US-Dollar (vgl. finanzen.net 2021). Diese Entwicklung beruht auf Spekulationen, da Bitcoin nicht mehr nur das Cash-Flow-System mit der eigenen Währung, sondern vielmehr eine Wertanlage darstellt. Das BTC-Angebot bis zum Jahr 2140 nur noch um 11,48% (Zahlen aus August 2021) steigen, während andere Ressourcen und Währungen dahingehend in den nächsten 25 Jahren deutlich zunehmen werden: Gold um 52%, der japanische Yen um 64%, die Schweizer Franken um 169%, der US-Dollar um 272%, der Euro um 286% und das britische Pfund um 429% (vgl. Ammous 2019: 248). Da somit die Angebotswachstumsrate von BTC in absehbarer Zeit unter der von Gold liegt, bewirkt diese Angebotsbeschränkung jetzt schon eine deutlich erhöhte Nachfrage als Wertaufbewahrungsmittel. Normalweise würde mit zunehmender Akzeptanz und Beliebtheit ein Zahlungsabwicklungssystem exponentielle Anstiege in der Anzahl der Transaktionen verzeichnen, dies ist bei Bitcoin jedoch nicht der Fall. Experten sprechen hier von einem „Beweis, dass BTC als Wertanlage genutzt wird" (Ammous 2019: 255). Weiterhin bekräftigen Aussagen, die BTC als „geeignetste Technologie zum Sparen" bezeichnen (vgl. ebd.: 255) und das Mitmischen von sogenannten Bitcoin-Wale[2] die Stellung von BTC als Anlageinstrument. Einer der populärsten Bitcoin-Wale ist Elon Musk mit seiner Firma Tesla. Musk kaufte im Namen von dem

[2] Im Kryptobereich werden „Wale" als solche Anleger bezeichnet, die große Mengen einer Kryptowährung halten. Wenn diese Anleger große Mengen an Coins kaufen oder verkaufen, schlägt es große „Wellen" im Kurs.

Automobilhersteller Tesla große Mengen an BTCs auf, zu der Zeit, als deren Aufschwung begann und die Coins zu entsprechend niedrigen Preisen erstanden werden konnten. Musk nutzte seine Bekanntheit und seinen Einfluss via Twitter, um BTC zu etablieren:

Abbildung 5.3: Tweet zur Verkündigung von BTC als Zahlungsmittel bei Tesla (via Twitter - Elon Musk 2021)

Jedoch wurde die Bezahlung von Tesla-Automobilien mit BTC zeitnah eingestellt, da das System Bitcoin für Zahlungsabwicklungen zu viele Ressourcen verbrauchen würde.

Abbildung 5.4: Tweet zur Rücknahme von BTC als Zahlungsmittel für Tesla-Fahrzeuge (via Twitter - Elon Musk 2021)

Anleger reagierten darauf, wodurch es zu einem Absturz des Marktpreises von BTC kam. Hier wurde weniger die Transaktionsmethode in Frage gestellt, sondern vielmehr die Zukunft von Bitcoin und BTC. Medien berichteten zudem, dass Musk vor dem Absetzen des Tweets zahlreiche Bitcoins verkauft hätte und sich innerhalb von wenigen Wochen, um einen dreistelligen Millionenbetrag bereichern konnte (vgl. Jahn 2021).

Dieses Beispiel zeigt, dass die Wertinstabilität des BTCs ein großes Problem darstellen würde, wenn es als Währung eingestuft werden sollte. Die Vorteile des Bitcoins in Form von Eigenschaften des idealen Geldes können somit bisher nicht genutzt werden.

5.3 Missbrauch und Monopolisierung

Außerhalb dieser Argumentation sollen hier noch zwei weitere Themen angeführt werden, die im Zusammenhang von Bitcoin und Nachhaltigkeit berücksichtigt werden sollen: kriminelle Geschäfte und Monopolisierung von Minern.

Kriminelle Transaktionsgeschäfte werden mit Bargeld, durch Überweisungen mit falschen Identitäten oder über das Darknet getätigt. Letzteres findet meist nur über einen Server statt und ist daher begrenzt. Bei allen drei Verfahren besteht eine Anonymität bzw. Pseudonymität. Politisch wurde diesbezüglich bereits im Bereich des Bargeldes reagiert. Es stellte sich heraus, dass die 500 Euro Scheine häufig genutzt wurden, um illegalen Geschäften nachzugehen. Frankreich will künftig eine Bargeldobergrenze einführen, um dagegen vorzugehen (vgl. fondsprofessionell.de 2021). Bitcoin eröffnet den Kriminellen jedoch neue Türen, um ihren Transaktionsgeschäften nachzugehen. Mit der umworbenen Pseudonymität können Geschäfte global, ohne Preisgabe der Identität, durchgeführt werden, solange keine weiteren Schnittstellen involviert sind. Schnittstellen können hier beispielsweise Exchange-Plattformen, Onlinehändler oder Adressen sein, die persönliche Daten erfordern. Sobald Euro auf einer Exchange-Plattform in BTC eingetauscht werden sollen, müssen Kreditkartendaten hinterlegt werden. Nichtsdestotrotz nutzen viele Kriminelle den Weg über Bitcoin. Die Verfolgung der Zahlungswege ist möglich, kann jedoch nicht garantiert werden.

Das zweite Problem, welches hier angesprochen werden soll, ist die mögliche Monopolisierung von Minern. Meist wird die Zusammenarbeit im Team als effizienter eingestuft, so auch beim

Mining. Über die Jahre hinweg wurden daher immer mehr sogenannte Pools gegründet, d.h. Rechenleistungen werden gekoppelt, um eine größere Anzahl an Proof-of-Work-Aufgaben in kürzerer Zeit lösen zu können. Die Blockprämien werden dann der Rechenleistung entsprechend aufgeteilt. Die eigentliche Gefahr dabei ist die Tatsache, dass wenn ein Pool zu groß wird oder sogar einen Anteil von über 50% vom Miningprozess übernimmt, Transaktionen ungleich behandelt werden können. Es kann zum Ausschluss von bestimmten Transaktionen oder zu einer ständigen Bevorzugung von Transaktionen kommen, bei denen die zusätzlichen Gebühren am höchsten sind.
Dieser Vorgang verhindert das Veröffentlichen von Blöcken durch andere Miner, da die Wahrscheinlichkeit, dass der Pool die Goldene Nonce auch gefunden hat, sehr groß ist. Zudem wird vom System nur die Blockkette verfolgt, die nachweislich die größte Rechenleistung vorweisen kann: der Pool. Deswegen ist das Netzwerk auf einen Zuwachs angewiesen, damit die Rechenressourcen ausgewogen verteilt bleiben. Umso größer das Netzwerk wird, desto unwahrscheinlicher wird eine solche Monopolisierung.

5.4 Zusammenfassung

Insgesamt weist Bitcoin also sowohl als System, als auch als digitale Währung (BTC) zahlreiche Vorteile auf. Dazu zählen vor allem die Effizienz und die erweiterte Sicherheit durch den Verzicht auf Dritte. Auch die bereits vorherrschende gesellschaftliche Akzeptanz und die politische Unabhängigkeit können als positive Merkmale eingeschätzt werden.
Dem gegenüber stehen jedoch auch schwerwiegende Kritikpunkte, vor allem im Bereich der Nutzerfreundlichkeit. Dazu zählt einerseits die ungünstige rechtliche Lage im Schadensfall und die fehlende Möglichkeit der Wiederherstellung eines verlorenen Schlüssels. Weiterhin stellt die eingeschränkte Reproduktion und die schwankende Volatilität ein Problem dar, welches Bitcoin als offiziell anerkannte Währung verhindert.

6 Fazit

Der Verzicht auf eine zentrale Autorität bei digitalem Bargeld bedingt gleichzeitig die Verknappung des Coins. Mit der Verknappung wird wiederum ein Gut erschaffen, welches als Anlageninstrument verwendet wird. Bei einer absoluten Knappheit, wie Bitcoin es vorgibt, wird der

Coin, wie Gold behandelt. Heutiges Bargeld besitzt zwar einen Wert, die Kosten für die Herstellung belaufen sich jedoch um ein Vielfaches geringer. Zudem kann Bargeld aufgrund der geringen Kosten nachproduziert werden.
Daraus lässt sich schlussfolgern, dass sich Bitcoin als Anlagegut manifestiert hat. Die Nutzung als anerkannte Währung ist jedoch aufgrund der hohen Volatilität und der geringen Liquiditätssumme als problematisch und somit als unwahrscheinlich einzuschätzen. Im Regelfall würde in diesem Fall die Angebotsmenge der Währung zentral-autoritär erhöht werden. Bei Bitcoin fehlt diese Instanz jedoch.

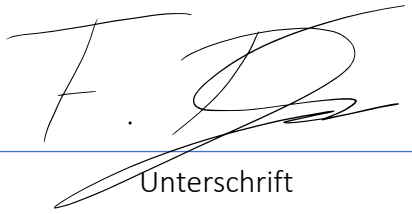
Insgesamt bietet Nakamoto also ein System, welches Transaktionen nachhaltig, im Sinne von kostengünstig und dezentral, ermöglichen soll. Dagegen spricht jedoch, dass es bisher als wenig benutzerfreundlich eingestuft werden muss und die benötigten Ressourcen nicht für die Nachhaltigkeit des Produktes sprechen.
Zusammenfassend stellt Bitcoin also in seiner aktuellen Form keine hinreichende Alternative zu Bargeld und herkömmlichen elektronischem Geld dar, da vor allem Aspekte der Nachhaltigkeit und des gesellschaftlichen Nutzens dagegensprechen.

7 Selbstständigkeitserklärung

Ich versichere eidesstattlich, die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt zu haben. Alle wörtlichen und sinngemäßen Entlehnungen sind unter genauer Angabe der Quelle kenntlich gemacht.

Die Satzung der Universität Leipzig zur Sicherung guter wissenschaftlicher Praxis vom 17. April 2015 habe ich zur Kenntnis genommen und bei der Erstellung dieser Arbeit beachtet.

Leipzig, 11.09.2021



Unterschrift

Literaturverzeichnis

Ammous, Saifedean (2019): Der Bitcoin-Standard – die dezentrale Alternative zum Zentralbankensystem, Rheinfelden, Deutschland: Aprycot Media.

Bendel, Prof. Dr. Oliver (2021): Definition: Was ist Kryptowährung, wirtschaftlexikon.gabler, [online] https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160 [abgerufen am 27.04.2021].

bitcoin.org (2021): Transactions, bitcoin.org [online] https://developer.bitcoin.org/devguide/transactions.html [aufgerufen am 12.08.2021].

Bocksch, René (2021): Bitcoin verbraucht mehr Strom als die Niederlande, statista, [online] https://de.statista.com/infografik/18608/stromverbrauch-ausgewaehlter-laender-im-vergleich-mit-dem-des-bitcoins/ [abgerufen am 14.08.2021].

Busch, Alexander, Holtermann, Felix, Müller, Mareike (2021): Der Traum vom grünen Bitcoin: So will die Kryptobranche ihr schmutziges Image loswerden, in Handelsblatt, [online] https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/report-der-traum-vom-gruenen-bitcoin-so-will-die-kryptobranche-ihr-schmutziges-image-loswerden/27251340.html [aufgerufen am 24.08.2021].

Centieiro, Henrique (2020): Bitcoin Proof of Work, levelup.gitconnected, [online] https://levelup.gitconnected.com/bitcoin-proof-of-work-the-only-article-you-will-ever-have-to-read-4a1fcd76a294 [aufgerufen am 25.06.2021].

Cox, Jeff (2021): Yellen sounds warning about „extrem inefficient“ bitcoin, cnbc, [online] https://www.cnbc.com/2021/02/22/yellen-sounds-warning-about-extremely-inefficient-bitcoin.html [abgerufen am 14.08.2021].

cryptomining-blog (2014): Bitcoin Hash Rate vs Difficulty (2 month), cryptomining-blog, [online] https://cryptomining-blog.com/wp-content/uploads/2014/12/current-bitcoin-hashrate-difficulty-chart.jpg [aufgerufen am 26.06.2021].

cvj.ch (o.D.): Block Reward, cvj, [online] https://cvj.ch/glossary/block-reward/ [abgerufen am 15.08.2021].

Dethloff, Ingo M (2018): Kryptowährung und ICO – Schadensersatz bei Verlust? – Urteil zur Erlaubnispflicht, anwalt, [online] https://www.anwalt.de/rechtstipps/kryptowaehrung-und-ico-schadensersatz-bei-verlust-urteil-zur-erlaubnispflicht_151139.html [aufgerufen am 15.08.2021].

finance.yahoo.com (2021): Bitcoin - Stock-to-Flow-Model, finance.yahoo, [online] https://finance.yahoo.com/news/going-bitcoin-cryptocurrency-following-price-192509907.html [aufgerufen am 15.08.2021].

finanzen.net (2021), finanzen, [online] https://www.finanzen.net/devisen/bitcoin-euro/chart [aufgerufen am 28.08.2021].

fondsprofessionell.de (2021): Kampf gegen Geldwäsche: Paris pocht auf strenge Bargeld-Obergrenze, fondsprofessionell, [online] https://www.fondsprofessionell.de/news/vertrieb/headline/kampf-gegen-geldwaesche-paris-pocht-auf-strenge-bargeld-obergrenze-209092/ [aufgerufen am 28.08.2021].

Grandt, Dr. Michael: Gibt es noch „sichere“ Währungen: Der Schweizer Franken, proaurum, [online] https://proaurum.ch/aktuellwichtig/grandt-sichere-waehrungen-teil2 [aufgerufen am 25.05.2021].

Jahn, Thomas (2021): Tesla sendet mit dem schnellen Bitcoin-Verkauf ein gefährliches Signal, in Handelsblatt, [online] https://www.handelsblatt.com/meinung/kommentare/kommentar-tesla-sendet-mit-dem-schnellen-bitcoin-verkauf-ein-gefaehrliches-signal/27135936.html [aufgerufen am 15.08.2021].

Krawisz, Daniel (2013): The Proof-of-Work Concept, nakamotoinstitute, [online] https://nakamotoinstitute.org/mempool/the-proof-of-work-concept/ [abgerufen am 26.08.2021].

Ledesma, Lyllah (2021): Bitcoin Stock-to-Flow Model, Rooted in 'Hard Money' Narrative, Goes Off Course, finance.yahoo, [online] https://finance.yahoo.com/news/bitcoin-stock-flow-model-rooted-153030252.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&.html [aufgerufen am 12.08.2021].

Manger-Nestler, Prof. Dr. Cornelia (2020): Währung, gabler-banklexikon, [online] https://www.gabler-banklexikon.de/definition/waehrung-62457/version-375520 [aufgerufen am 28.08.2021].

Mitra, Rajarshi (2021): Proof of Work (Arbeitsnachweis) vs. Proof of Stake (Anteilsnachweis) Grundlegende Anleitung für das Mining, blockgeeks, [online] https://blockgeeks.com/guides/de/proof-of-work-arbeitsnachweis-vs-proof-of-stake-anteilsnachweis/ [abgerufen am 10.04.2021].

Mycryptopedia (2018): scriptPubKey & scriptSig Explained, mycryptopedia, [online] https://www.mycryptopedia.com/scriptpubkey-scriptsig/ [aufgerufen am 10.06.2021].

Nakamoto, Satoshi (2009): Bitcoin open source of implementation of p2p currency, satoshinakamoto, [online] http://satoshinakamoto.me/2009/02/11/bitcoin-open-source-implementation-of-p2p-currency/#selection-51.0-51.224 [aufgerufen am 26.06.2021].

Neuhaus, Andreas (2021): Bitcoin fällt unter 37.000 Dollar – China will gegen Krypto-Mining vorgehen, in Handelsblatt, [online] https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrungen-bitcoin-faellt-unter-37-000-dollar-china-will-gegen-krypto-mining-vorgehen/27213882.html [aufgerufen am 15.08.2021].

Nyumbayire, Christian (2021): The Nakamoto Consensus, interlogica, [online] https://www.interlogica.it/en/insight-en/nakamoto-consensus/ [abgerufen am 26.04.2021].

Pritzker, Yan (2020): Bitcoin entdecken – Wie die Technologie hinter dem ersten knappen und dezentralisierten Geld funktioniert, Rheinfelden, Deutschland: Aprycot Media – Held & Troendle GbR.

Reiff, Nathan (2019): 20% of All BTC is Lost, Unrecoverable, Study Shows, investopedia, [online] https://www.investopedia.com/news/20-all-btc-lost-unrecoverable-study-shows/ [aufgerufen am 25.06.2021].

Rybarczyk, RJ (2018): Bitcoin P2PKH Transaction Breakdown, medium, [online] https://medium.com/coinmonks/bitcoin-p2pkh-transaction-breakdown-bb663034d6df [aufgerufen am 10.06.2021].

Satoshi: Transactions and Scripts (2010): DUP HASH160 ... EQUALVERIFY CHECKSIG (Eintrag im Bitcoin-Forum vom 17.06.2010), bitcointalk, [online] https://bitcointalk.org/index.php?topic=195.0 [aufgerufen am 10.06.2021].

Schmidt-Ott, Markus (2021): Wie funktioniert eine Wallet?, finanzfluss, [online] https://www.finanzfluss.de/bitcoin-handbuch/wie-funktioniert-eine-wallet/ [aufgerufen am 27.06.2021].

Sharma, Rakesh (2021): Cryptocurrency Insurance Could Be a Big Industry in the Future, investopedia, [online] https://www.investopedia.com/news/cryptocurrency-insurance-could-be-big-industry-future/ [aufgerufen am 15.08.2021].

Szabo, Nick (2001): Trusted Third Parties are Security Holes, nakamotoinstitute, [online] https://nakamotoinstitute.org/trusted-third-parties/ [aufgerufen am 24.08.2021].

Twitter -Elon Musk (2021), twitter, [online] https://twitter.com/elon-musk?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor [aufgerufen am 15.08.2021].

Wohlmann, Monika (2020): Kryptowährungen – Top oder Flop?, Düsseldorf, Deutschland: FOM-Edition Springer Gabler.

Abbildungsverzeichnis