Ing. Lukas Weichselbraun, BSc

Eine quantitative Analyse der Bitcoin Blockchain

MASTERARBEIT

zur Erlangung des akademischen Grades

Master of Science

Studium: Masterstudium Informationsmanagement

Alpen-Adria-Universität Klagenfurt

Gutachter
Assoc.Prof.Mag.Dr. Alexander Brauneis
Alpen-Adria-Universität Klagenfurt
Institut für Finanzmanagement

Klagenfurt, Juni 2020

Eidesstattliche Erklärung

Ich versichere an Eides statt, dass ich

- die eingereichte wissenschaftliche Arbeit selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe,
- die während des Arbeitsvorganges von dritter Seite erfahrene Unterstützung, einschließlich signifikanter Betreuungshinweise, vollständig offengelegt habe,
- die Inhalte, die ich aus Werken Dritter oder eigenen Werken wortwörtlich oder sinngemäß übernommen habe, in geeigneter Form gekennzeichnet und den Ursprung der Information durch möglichst exakte Quellenangaben (z.B. in Fußnoten) ersichtlich gemacht habe,
- die eingereichte wissenschaftliche Arbeit bisher weder im Inland noch im Ausland einer Prüfungsbehörde vorgelegt habe und
- bei der Weitergabe jedes Exemplars (z.B. in gebundener, gedruckter oder digitaler Form) der wissenschaftlichen Arbeit sicherstelle, dass diese mit der eingereichten digitalen Version übereinstimmt.

Mir ist bekannt, dass die digitale Version der eingereichten wissenschaftlichen Arbeit zur Plagiatskontrolle herangezogen wird.

Ich bin mir bewusst, dass eine tatsachenwidrige Erklärung rechtliche Folgen haben wird.

Lukas Weichselbraun e. h. *Klagenfurt, 26.06.2020*

Danksagung

Ich möchte mich herzlich bei meinen Eltern bedanken, die mich in meinen Ausbildungsjahren stets unterstützten und so mein Studium in erster Linie überhaupt ermöglichten. Ein großes Danke gilt auch meiner Freundin Kathrin, die mir während meines Studiums stets mit Geduld und Wertschätzung entgegnete. Weiters möchte ich mich auch bei meinem Arbeitgeber Infineon Technologies AG bedanken und insbesondere bei Herrn Mag. Michael Grafenauer, ohne welchem mein berufsbegleitendes Studium und der Abschluss dieser Arbeit nicht so nahtlos funktioniert hätte. Ein großer Dank gebührt auch meinem Betreuer Herrn Assoc.Prof.Mag.Dr. Alexander Brauneis, welcher mir den nötigen Freiraum für diese Arbeit gab und mit außerordentlicher Kompetenz zur Seite stand.

Kurzfassung

Seit Anbeginn der Menschheit gibt es den Handel von Gütern und Dienstleistungen. Zur Vereinfachung dessen wurden verschiedenste Währungen genutzt, welche sich über Salz und Gold bis zum heutigen Geldsystem entwickelt haben. Doch die nächste Evolution steht womöglich kurz bevor: Kryptowährungen. Bitcoin, als die Mutter dieser, führte das Konzept der Blockchain ein. Nach einem Jahrzehnt schaut Bitcoin bereits auf viele Höhen und Tiefen zurück und es lohnt sich ein detaillierterer Blick hinter die Fassaden. Mittels quantitativer Analysen stellt diese Arbeit ausgewählte Aspekte der Bitcoin-Blockchain auf den Prüfstand. Zunächst wird in die Thematik Bitcoin als digitales Geld eingeführt, bevor die Blockchain-Technologie erläutert wird. Die empirische Forschung analysiert tatsächliche Funktionsweisen inhärenter Eigenschaften von Bitcoin, welche in der Implementierung des Systems fest verankert wurden. Damit diese quantitative Analyse bewerkstelligt werden kann, werden Datenmengen direkt aus der Blockchain extrahiert und mit Preisinformationen einer Kryptobörse aggregiert. Eine deskriptive Analyse dient dem Erhalt einer umfassenderen Sicht auf die ermittelte Datenbasis. Basierend darauf werden Hypothesen verfasst, die ausgewählte historische Entwicklungen mittels Regressionsanalysen testen. Die Ergebnisse werden interpretiert und eine mögliche Kausalität hergestellt.

Abstract

The trade in goods and services exists since the beginning of mankind. To simplify the trade, various currencies were used, which have developed through salt and gold to the present monetary system. But the next evolution may be just around the corner: cryptocurrencies. Bitcoin, as the mother of them, introduced the concept of the blockchain. After a decade, Bitcoin is already looking back at many ups and downs and it is worth taking a more detailed look behind the facades. With quantitative analyses this work tests the Bitcoin blockchain. Bitcoin is first presented by the foundations of digital money before the blockchain technology is explained. The empirical study analyzes the actual functionality of inherent properties of Bitcoin, which are firmly anchored in the implementation of the system. In order for this quantitative analysis to be carried out, amounts of data are extracted directly from the blockchain and aggregated with price information from a crypto exchange. The descriptive analysis is used to get a more complete overview of the data set. Based on this, hypotheses are defined that test selected historical developments using regression analyses. The results are interpreted and a possible causality is established.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Altcoin	Alternative Coin
API	Application Progamming Interface
BIS	Bank of International Settlement
BIZ	Bank für Internationalen Zahlungsausgleich
BTC	Bitcoin Währungskürzel
CPU	Central Processing Unit
DLT	Distributed Ledger Technology
EUR	Euro Währungskürzel
FX	Foreign Exchange
GB	Gigabyte
H	Hash
ID	Identifikation
Mt.	Mount
N/A	Nicht anwendbar
Nonce	Number only used once
OHLC	Open, High, Low, Close
OTC	Over the Counter
ÖBA	Österreichisches BankArchiv
P2P	Peer-to-Peer
P2PK	Pay-To-Public-Key
P2PKH	Pay-To-Public-Key-Hash
P2SH	Pay-To-Script-Hash
PIN	Persönliche Identifikationsnummer
PoS	Proof of Stake
PoW	Proof of Work
RAM	Random Access Memory
SPV	Simplified Payment Verification
SSD	Solid State Drive
TX	Transaktion
URL	Uniform Resource Locator
US-Dollar	United States Dollar
USD	US-Dollar Währungskürzel
UTC	Coordinated Universal Time
UTXO	Unspent Transaction Output

1 Einleitung

Bevor in das Ziel und in den Gang der Arbeit eingegangen wird, gibt es im ersten Kapitel „1.1 Was ist Bitcoin?“ eine grundlegende Einführung in die Thematik.

1.1 Was ist Bitcoin?

Bitcoin ist eine Form digitaler Währung, eine sogenannte Kryptowährung, und wurde erstmals im Whitepaper von Satoshi Nakamoto mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“ im Jahr 2008 erwähnt. Satoshi Nakamoto ist ein Name oder Pseudonym für einen bis heute unbekannten Autor oder eine unbekannte Gruppe von Autoren und beschrieb in dem Papier, wie ein elektronisches Peer-to-Peer-Geldsystem funktionieren kann. Dabei handelt es sich um ein System, in welchem eine Person einer anderen Person elektronisch Geld überweisen kann, ohne dabei einem zentralen Finanzinstitut vertrauen zu müssen.[1] Die erste Transaktion wurde 2009 im Bitcoin-Netzwerk getätigt, welches sich als Open-Source-Entwicklung stets weiterentwickelt.[2] Die Entstehung von Bitcoin fällt nicht zufällig mit der globalen Finanzkrise 2008/2009 zusammen, welche wohl im zentralisierten Finanzsystem ihren Ursprung fand. Anfangs wurde Bitcoin nur von technischen Experten verwendet, verschaffte sich jedoch zügig durch seine rasanten Preisanstiege in der breiten Masse einen Namen.[3] Spätestens mit dem Hype Ende 2017 war Bitcoin in aller Munde. Mittlerweile darf davon ausgegangen werden, dass neben technikaffinen Personen auch viele Spekulanten und Investoren Bitcoins heute handeln.

Neben der finanzwirtschaftlichen Betrachtung revolutionierte Bitcoin vor allem die elektronische Datenverwaltung mit dem Konzept der Blockchain, welche eine neue technologische Errungenschaft darstellt. Diese bildet die Grundlage für die dezentrale Funktionsweise von Bitcoin. Daher kann Bitcoin auch als eine konkrete Anwendung der Blockchain angesehen werden. Durch kryptografische Mechanismen erschafft die Blockchain das notwendige Vertrauen, um Daten zuverlässig auf verteilten Systemen zu verarbeiten, ohne dabei eine zentrale Instanz involvieren zu müssen.[4] Abbildung Abb. *1* veranschaulicht die Interdisziplinarität der drei Fachgebiete von Bitcoin: Informatik, Kryptografie und Ökonomie.

[1] Vgl. Nakamoto, 2008, S. 1.
[2] Vgl. Lee & Low, 2018, S. 40f.
[3] Vgl. Brauneis & Mestel, 2018, S. 711f.
[4] Vgl. Rosenberger, 2018, S. 2f.

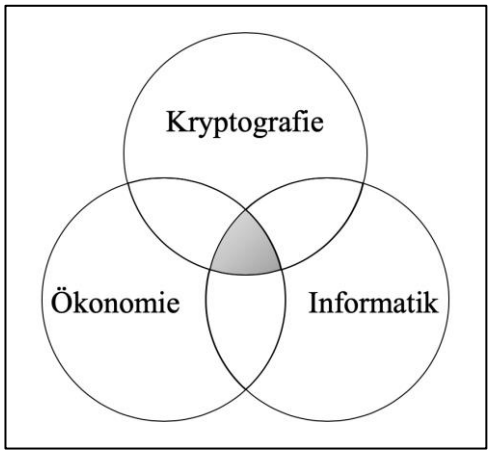

Abb. 1: Interdisziplinarität von Bitcoin[5]

Neben der ursprünglich intendierten Möglichkeit, Bitcoin als elektronisches Zahlungsmittel einzusetzen, bildet das Bitcoin-Netzwerk zusätzlich ein valides Grundgerüst für eine Vielzahl an verschiedenartigen Applikationen. Durch weitere Eigenschaften können Bitcoin-Transaktionen mit beliebigen Versprechen verknüpft sein, wie beispielsweise Ansprüche auf Edelmetalle, Unternehmensanteile, Schuldscheine oder Forderungen. So lassen sich beliebige Formen von Kryptoassets innerhalb der Bitcoin-Blockchain erstellen und transferieren.[6]

1.2 Ziel der Arbeit

Bitcoin besteht nun seit über 10 Jahren und hat sich in Bezug auf die Funktionalität und den Bekanntheitsgrad kontinuierlich weiterentwickelt. Wiederkehrende Hypes sorgen regelmäßig für Haussen und Baissen[7]. Hackerangriffe fanden in den letzten Jahren immer wieder statt, diese haben jedoch nie die Bitcoin-Technologie selbst betroffen, sondern ausschließlich Intermediäre, die meist das Handeln mit Bitcoin vereinfachen. Der wohl bekannteste Vorfall war der Angriff auf die Kryptobörse Mt. Gox im Jahr 2014, die damals für etwa 70 Prozent der gesamten Bitcoin-Transaktionen zuständig war.[8] Das Bitcoin-Protokoll selbst konnte bis heute noch nie gehackt werden. Dem Fortbestand von Bitcoin kann daher Glauben geschenkt werden und ein tieferer Einblick aus wirtschaftlicher Perspektive könnte auch langfristig von Interesse sein.

[5] Quelle: Berentsen & Schär, 2017, S. 1.
[6] Vgl. Berentsen & Schär, 2017, S. 83.
[7] Die Webseite https://coinmarketcap.com zeigt neben der historischen Preisentwicklung von Bitcoin auch die Entwicklung vieler anderer Kryptowährungen an.
[8] Vgl. Lee & Low, 2018, S. 41.

Ziel dieser Arbeit ist nach der Erarbeitung eines theoretischen Verständnisses für die Technologie eine quantitative Analyse der Blockchain-Daten von Bitcoin. Eine einführende und deskriptive Analyse dient dem allgemeinen Überblick über die ermittelte Datenbasis, welche für weiterführende Berechnungsmodelle herangezogen wird. Mittels Regressionsmodellen werden Variablen, wie beispielsweise die Transaktionsgebühren oder Handelsvolumina, in Zusammenhang gebracht, um aufgestellte Hypothesen zu belegen oder widerlegen. Dadurch soll ein grundlegendes Wissen über Zusammenhänge im Bitcoin-System aufgebaut werden und überprüft werden, ob die zugrundeliegende Technologie den inhärenten Eigenschaften folgt.

1.3 Gang der Arbeit

Um eine ausführliche Bearbeitung des Themas dieser Arbeit zu gewährleisten, werden notwendige Grundlagen in Kapitel 2 erarbeitet. Dabei handelt es sich um allgemeine Themen, wie die Eigenschaften von Geld und Märkten. Dies dient einer generellen Einführung in Bezug auf Währungen und deren Handel und ist in theoretischer und praktischer Form auch auf Bitcoin anwendbar. Der Hauptteil des Grundlagenkapitels widmet sich der Bitcoin-Technologie. Das Ziel ist ein solides Verständnis zur Technologie und dessen Handhabung aufzubauen, ohne detaillierte Vorkenntnisse in der Informationstechnologie oder im Finanzwesen selbst bereits besitzen zu müssen.

Nach dem Erarbeiten der Grundlagen folgt das Kapitel 3 „Daten“. In diesem Kapitel wird beschrieben, wie die notwendige Datenbasis für diese Arbeit erhoben und adaptiert wird. Die deskriptive Datenbeschreibung soll zu einem besseren Verständnis über die erhobenen Daten führen und ist in diesem Kapitel ebenso enthalten, wie ein Ansatz für die Aggregation von On-Chain-Daten mit Off-Chain-Daten. Wie bereits erwähnt, werden im Kapitel 4 „Empirie“ Hypothesen mit der in diesem Kapitel vorgestellten Methodik analysiert und interpretiert.

Das Fazit wird im Kapitel 5 „Zusammenfassung und Ausblick“ gezogen, fasst die Arbeit nochmals zusammen und gibt einen Ausblick auf etwaige weitere Forschungsmöglichkeiten.

2 Grundlagen

In diesem Kapitel werden wesentliche Grundlagen erarbeitet, die für die folgende empirische Aufarbeitung der Bitcoin Transaktionen von Bedeutung sind. Ziel ist, die wirtschaftlichen und technologischen Aspekte hinter Bitcoin näherzubringen.

2.1 Monetäre Grundlagen

In den monetären Grundlagen wird erklärt, warum es ein generelles Bedürfnis nach Geld gibt und welche wesentlichen Eigenschaften Geld besitzen sollte. Die monetären Grundlagen sind für die empirische Analyse nicht von großer Relevanz. Sie tragen aber zum Verstehen bei, warum Bitcoin in erster Linie überhaupt entwickelt worden ist und warum Bitcoin eine mögliche Daseinsberechtigung hat.

2.1.1 Begriff des Geldes

Als Menschen setzen wir uns schon früh unterbewusst mit der Geschenkwirtschaft auseinander. Bereits in jungen Jahren bekommen wir unzählige Leistungen von der eigenen Familie geschenkt. Als Gegenleistung entgegnen wir mit Liebe, Dankbarkeit und Vertrauen.[9] Wenn wir älter werden, können auch wir selbst (Gegen-)Leistungen anderer Form erbringen. In unserem engeren Bekanntenkreis werden Gefälligkeiten oft nicht direkt bezahlt. Im Gegensatz wird jedoch unterbewusst eine ebenbürtige Gegenleistung erwartet. Finden in einer Beziehung Gefälligkeiten nur einseitig statt, so kommt es unwiderruflich zu Konflikten.[10] Innerhalb des engeren Bekanntenkreises besteht somit kein unmittelbarer Bedarf nach Geld oder allgemein formuliert, nach einem Tauschmittel. Wollen wir jedoch mit weniger vertrauten Personen Handel betreiben, so möchten wir oft eine sofortige Gegenleistung bekommen. Diese kann nur in Form eines Tauschmittels erfolgen. Bestenfalls erfüllt das Tauschmittel alle in Kapitel 2.1.2 genannten Funktionen des Geldes.

In einer Welt ohne Geld, die ausschließlich auf Gütern und Dienstleistungen basiert, kann ein Tausch nur dann stattfinden, wenn die berühmte Formulierung von Jevons, die „Doppelkoinzidenz von Bedürfnissen“, englisch „Double coincidence of wants“[11], eintritt. Diese besagt, dass in einer Welt vieler Tauschwünsche zwei Wünsche in Bezug auf Raum, Zeit

[9] Vgl. Ametrano, 2016, S. 2.
[10] Vgl. Berentsen & Schär, 2017, S. 7f.
[11] Vgl. Jevons, 1876, S. 2.

und Menge genau zueinander passen müssen. Ansonsten findet der Tausch nicht statt.[12] Um Tauschgeschäfte zu erleichtern, wurden in der Geschichte verschiedenste Medien als Geld verwendet. Darunter zählen Salz, Muscheln, Edelmetalle und Papiergeld, um nur einige wenige zu nennen. Das Kapitel „2.1.3 Geldarten“ gibt eine weiterführende Auskunft über diese verschiedenen Formen. Eine weitere kuriose Form von Geld wurde von den Bewohnern der Insel Yap angewandt. Dabei wurden riesige Mühlsteine, welche von Seefahrern auf die Insel gebracht wurden, als Geld verwendet. Da diese Mühlsteine aufgrund ihrer Größe und ihres Gewichts nur mit äußerst großem Aufwand übergeben werden konnten, blieben diese auf ihren ursprünglich abgesetzten Ort bestehen. Lediglich die Inselbewohner wussten, welcher Bewohner über welche Anteile verfügte. Dieser Anspruch wurde bei einem Tausch als Tauschmittel, also einer Form von Geld, verwendet.[13] Eine geeignete Definition für den Begriff Geld, nach Helmedag, lautet:

„Geld ist in einer modernen, vom ökonomischen Tausch dominierten Gesellschaft ein metrisch skalierter Wertausdruck, dessen Autorität sich darauf gründet, von jedem Verkäufer als Gegenleistung des Käufers im ökonomischen Tausch anerkannt zu werden.“[14]

Geld kann auch als eine Form von Gedächtnis angesehen werden. Leistet eine Person Gefälligkeiten, so bekommt diese im Austausch heutzutage Geld. Fiktiv könnte auch die Bilanz dieser Person im Gedächtnis erhöht werden. Konsumiert diese Person Gefälligkeiten, so bezahlt die Person die Leistung mit Geld oder verringert die eigene Bilanz im Gedächtnis. Geld könnte daher als ein saldiertes Gedächtnis der geleisteten und konsumierten Dienste angesehen werden.[15]

2.1.2 Funktionen des Geldes

Obst/Hintner (2000)[16] nennen drei wesentliche Funktionen, die Geld erfüllen muss: die Zahlungsmittelfunktion, die Funktion als Recheneinheit und die Wertaufbewahrungsfunktion. Die Zahlungsmittelfunktion, auch Tauschmittelfunktion genannt, besagt, dass Handelspartner bereit sind Waren gegen Geld auszutauschen. In den meisten Volkswirtschaften ist gesetzlich geregelt, welche Waren und Dienstleistungen mit welchen Schuldverschreibungen zu bezahlen

[12] Vgl. Kaiser, 2011, S. 15.
[13] Vgl. Furness, 1910, S. 92ff.
[14] Helmedag, 1994, S. 92.
[15] Vgl. Kocherlakota, 1996, S. 233.
[16] Vgl. Obst & Hintner, 2000, S. 94.

sind. Hierbei ist jedoch wichtig festzuhalten, dass dies keine Voraussetzung darstellt. Handelspartner können sich folglich auch auf ein beliebig anderes Tauschmittel einigen. Die Wertaufbewahrungsfunktion besagt, dass Geld über einen Zeitraum Kaufkraft speichern muss. Diese Funktion ist mit der Zahlungsmittelfunktion eng verbunden, da die Eignung von Geld als Zahlungsmittel abnimmt, wenn die Funktion des Geldes als Wertspeicher sich verschlechtert. Die Funktion als Recheneinheit bezieht sich darauf, dass alle Güterpreise in Form von Geld angegeben werden können. Nachfolgende Abbildung veranschaulicht die genannten Funktionen von Geldeinheiten.

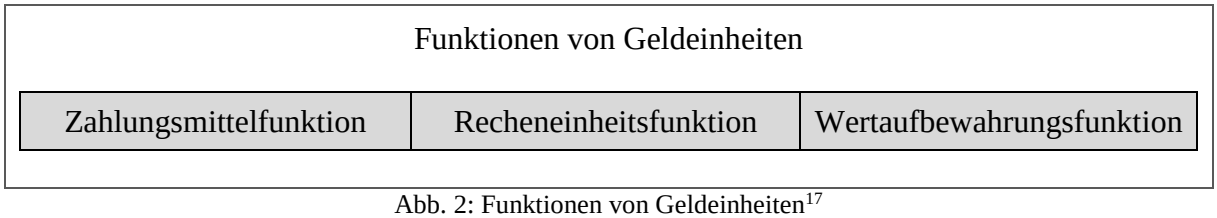

Abb. 2: Funktionen von Geldeinheiten[17]

2.1.3 Geldarten und ihre Entstehung

Dieses Kapitel beschreibt verschiedene Geldarten, die in der Geschichte der Menschheit verwendet wurden und werden. Es wird auch ein Augenmerk auf die Entstehung der Geldarten gelegt.

2.1.3.1 Warengeld

Die Geschichte des Geldes begann mit dem Warengeld. Gewürze, seltene Steine, Muscheln, Zähne, Felle und noch viele andere Waren wurden in der Frühzeit des Wirtschaftens als Zahlungsmittel verwendet. Über die Jahre setzten sich vor allem Metalle als Geld durch. Durch seltene Vorkommen, aufwendiger Herstellung, Unverwüstlichkeit und des damit hohen verbundenen Wertes eignete sich Gold am besten und findet heute noch großen Zuspruch.[18]

2.1.3.2 Papiergeld

Den Ausgangspunkt für das Papiergeld bildete ebenso Gold. Die erste Form von Banknoten waren Quittungen über das eingelagerte Gold bei englischen Goldschmieden. Diese erkannten, dass mehr Quittungen ausgegeben werden konnten als Einlagen verfügbar waren, da nie alle Forderungen zugleich eingelöst werden. Die Möglichkeit zur Geldschöpfung war geboren. In weiterer Folge beauftragten Staaten Banken, gesetzliche Banknoten auszugeben und dafür

[17] Quelle: Verfasser.
[18] Vgl. Thiel, 2011, S. 30f.

einen gewissen Betrag an Gold zu hinterlegen. Diese Hinterlegung wird auch als Goldstandard bezeichnet.[19]

2.1.3.3 Virtuelles Geld

Wie mehrere geschichtliche Ereignisse zeigten, wurde der Goldstandard des Öfteren ad hoc aufgelöst. Staaten hoben den Goldstandard auf, um größere Finanzierungen, beispielsweise für Rüstung, durchführen zu können. Dies führte in den meisten Fällen zu einer Geldentwertung. Am Ende des zweiten Weltkrieges wurde das Bretton-Woods-Abkommen im Jahr 1944 getroffen, welches den US-Dollar als gold-hinterlegte Weltleitwährung vorsieht. Dies sollte zu einem besseren Ablauf der zunehmend globalisierten Weltwirtschaft beitragen. 1971 wurde der Goldstandard wegen des hohen US-Außenhandelsdefizits und der steigenden Kosten des Vietnam- und Koreakriegs wieder aufgehoben und der US-Dollar wurde, wie viele andere Währungen, zu einer Fiat-Währung[20]. Fiat-Währungen beruhen ausschließlich auf dem Vertrauen in die herausgebende Institution der Währung. Durch die zunehmende Digitalisierung im Bankenbereich konnten Finanztransaktionen ab dem Beginn der 70er Jahre zunehmend elektronisch verarbeitet werden.[21] Giralgeld ist der Name für das elektronisch geführte Buchgeld von Banken für ihre Kunden.[22] Im Zuge der fortschreitenden Digitalisierung im Finanzbereich entstanden in weiterer Folge unterschiedlichste Finanzderivate, die unter anderem zur Finanzkrise 2008 beigetragen haben.[23] Die Regierungen mussten im Zuge der Finanzkrise einige Banken retten, um das Finanzsystem aufrechtzuerhalten. Daher wurde im ersten Bitcoin-Block von Satoshi Nakamoto nicht ohne Grund die Notiz „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks“ mit der Anspielung auf den damaligen Titel der britischen *Times*-Zeitung verewigt.[24] Kryptowährungen, wie beispielsweise Bitcoin, sind neben dem Giralgeld eine neue Form von virtuellem Geld.

2.1.4 Kontrollstrukturen

Kontrollstrukturen geben Auskunft auf welche Art und Weise über Geld verfügt werden kann. Berentsen/Schär (2017)[25] gruppieren diese Strukturen grob in drei Kategorien: (1) Die Geldschöpfung dient der Geldmengensteuerung und beschränkt somit die verfügbaren

[19] Vgl. Thiel, 2011, S. 34f.
[20] Fiat ist der lateinische Ausdruck für „es werde“.
[21] Vgl. Thiel, 2011, S. 35ff.
[22] Vgl. Zwahr, 2006, S. 368f.
[23] Vgl. Thiel, 2011, S. 37ff.
[24] Die Webseite https://blockchain.com bietet die Möglichkeit alle Blöcke und Transaktionen der Bitcoin-Blockchain und anderer Kryptowährungen zu durchsuchen.
[25] Vgl. Berentsen & Schär, 2017, S. 23ff.

Geldeinheiten mengenmäßig, um die Zahlungsmittelfunktion zu gewährleisten; (2) Die Repräsentation unterscheidet zwischen physischer und virtueller Form der Wertbindung einer Geldeinheit. Diese Formen können unterschiedliche Vor- und Nachteile aufweisen, wie beispielsweise die Ortsgebundenheit, die Verwahrung und die Teilbarkeit; und (3) die Transaktionsabwicklung bezieht sich auf die Übertragungsformen von Geldeinheiten. Also darauf, ob Transaktionen von Geldeinheiten autonom, zentral (beglaubigt durch Dritten) oder dezentral (ohne Mitwirken eines Dritten) erfolgen können.

2.2 Marktplätze Grundlagen

Nach einer generellen Einführung in Märkte, Marktplätze und dessen Merkmale steigt dieses Kapitel konkret in die Besonderheiten der Finanzmärkte ein. Finanzmärkte sind ebenfalls für Bitcoin relevant, da der Handel mit Bitcoin im weitesten Sinne auch als Devisenhandel eingestuft werden kann. Bitcoins können auf Kryptobörsen gegen andere Kryptowährungen aber auch gegen herkömmliche Fiat-Währungen, wie den Euro oder den US-Dollar, getauscht werden. Dieser Handel bleibt der Bitcoin-Blockchain verborgen, ist jedoch für die Preisfindung unerlässlich.

2.2.1 Was ist ein Markt?

Nach Sissors (1966)[26] gibt es verschiedene Arten einen Markt zu klassifizieren. Der traditionelle Weg ist die Marktklassifizierung nach Produkten. Diese Märkte referenzieren Individuen, die in der Vergangenheit diese Produkte gekauft haben und vermutlich auch in Zukunft diese Produkte kaufen werden. Es kann auch sinnvoll sein, Märkte ausschließlich aufgrund einzelner Eigenschaften, wie zum Beispiel des Alters oder der Herkunft der Kunden, einzuteilen.

Laut Levitt (1960)[27] setzt sich ein Markt aus Personen zusammen, die ähnliche Bedürfnisse aufweisen. Idealerweise erkennt ein Unternehmer diese Bedürfnisse und entwickelt ein Produkt, um diese zu stillen. Um Wettbewerber eines Unternehmens ausfindig zu machen, kann es irreführend sein, wenn ausschließlich auf Basis des Produkts konkurrierende Unternehmen ermittelt werden. In Wahrheit müssen alle Unternehmen einbezogen werden, die dieselben oder ähnliche Bedürfnisse der Kunden abdecken. Ein Unternehmen hat daher mehr Aussicht auf Erfolg, wenn es sich auf den Prozess der Steigerung der Kundenzufriedenheit konzentriert,

[26] Vgl. Sissors, 1966, S. 17ff.
[27] Vgl. Levitt, 1960, S. 55.

anstatt auf den Prozess der Produkterzeugung. Ein Beispiel wäre, dass ein Bahnunternehmen nicht nur andere Bahnunternehmen als Wettbewerber ansieht, sondern alle Transportunternehmen.

Ein Markt bezieht sich im Allgemeinen auf das Verkaufen von Produkten, um Kundenbedürfnisse decken zu können. Daher ist ein Markt eine Gruppe von potentiellen Käufern eines bestimmten Produkts. Ein Markt kann je nach Notwendigkeit weiter unterteilt und segmentiert werden.[28]

2.2.2 Finanzmärkte

Die vorherige und allgemeine Einführung in Märkte besagt, dass auch Finanzmärkte in unterschiedliche Kategorien gruppiert werden können. Eine Gruppierung nach Produkten, Phasen, Lokationen, Fristigkeiten, Regulierungen, Handelskanälen und anderen Eigenschaften ist denkbar. Nach Franzetti (2018)[29] ist die große Gemeinsamkeit von Finanzmärkten, dass Käufer und Verkäufer für Transaktionen direkt oder indirekt (vermittelt) miteinander in Kontakt treten können. Die ausschlaggebende Größe einer (Asset-)Transaktion ist der Kurs, also der Preis zu gegebener Menge. Franzetti (2018) ist eine gute weiterführende Literatur für die verschiedenen Möglichkeiten, Finanzmärkte einzuteilen. Das Kapitel „2.2.4 Die Börse als (Finanz-)Marktplatz“ geht auf die Einteilung des Finanzmarktes nach Phase ein und wie diese Unterteilung mit der Börse in Verbindung steht. Zunächst wird im Folgekapitel jedoch auf die verschiedenen Arten von Finanzmarktplätzen eingegangen.

2.2.3 Arten von Finanz-Marktplätzen

Die folgende Abbildung zeigt, wie Transaktionen mit strukturierten oder derivativen Titeln am Finanzmarkt verschiedenen Marktplätzen zugeteilt werden können. Grundlegend wird der Handel in börslichen und nicht-börslichen Handel unterschieden. Ferner findet der Börsenhandel von Optionen und anderen Terminkontrakten an sogenannten Terminbörsen und der Handel von Wertpapieren, wie Aktien und Anleihen, an Wertpapierbörsen statt. Börsenhandel ist standardisiert und automatisiert, um Transaktionen zeitnah und kostensparend durchzuführen. Nicht-börslicher Handel wird als Over-the-Counter-Handel, kurz OTC,

[28] Vgl. Sissors, 1966, S. 21.
[29] Vgl. Franzetti, 2018, S. 79.

bezeichnet und ist hingegen oft nicht standardisiert und wird auch meist manuell abgewickelt, um besser auf individuelle Kundenwünsche eingehen zu können.[30]

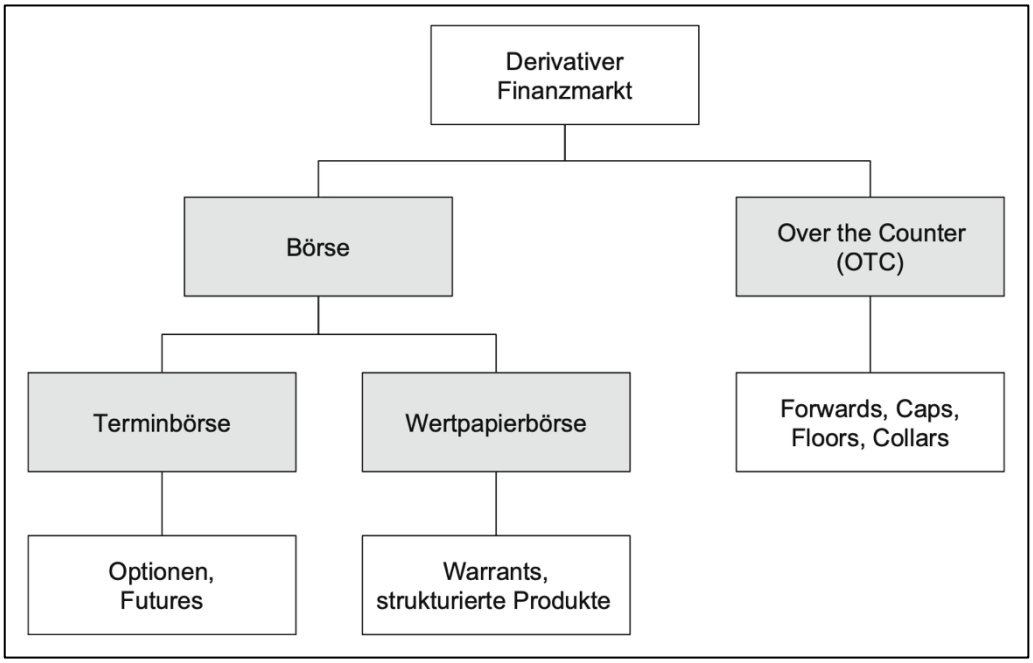

Abb. 3: Übersicht der Marktplätze[31]

2.2.4 Die Börse als (Finanz-)Marktplatz

In Bezug auf Finanzmärkte unterteilen Nabben/Rudolph (1994)[32] Börsen in zwei verschiedene Märkte nach Phase: (1) Der Primärmarkt dient der Emission von erstmalig herausgegebenen Finanztiteln. Finanztitel können Wertpapiere, Terminkontrakte oder Derivate aller Art sein, wie zum Beispiel Aktien, Anleihen, Optionen oder Swaps. Der Primärmarkt erfüllt die Kapitalbeschaffungsfunktion für Unternehmen. Über die Emission von Finanztiteln können Unternehmen sich zusätzliches Kapital von Anlegern beschaffen. (2) Der Sekundärmarkt bezeichnet jeglichen weiteren Handel von emittierten Finanztiteln und steht in enger Verbindung mit dem Primärmarkt. Der Sekundärmarkt erfüllt wichtige Funktionen wie beispielsweise die Liquiditätsfunktion, die Informationsfunktion, die Fristen- und Risikotransformation sowie die Bewertungsfunktion. Die Liquiditätsfunktion besagt, dass Finanztitel jederzeit und in großen Mengen handelbar sind, ohne größeren Einfluss auf die Preisbildung zu nehmen. Da Verkäufe und Käufe meist nicht simultan stattfinden, muss die Börse eine Art Überbrückungsfunktion einnehmen, um die verkauften Titel an den Käufer transferieren zu können. Die Informationsfunktion gibt Auskunft über den Kursverlauf von

[30] Vgl. Franzetti, 2018, S. 83f.
[31] Quelle: Franzetti, 2018, S. 84.
[32] Vgl. Nabben & Rudolph, 1994, S. 167f.

Finanztiteln und offenbart das aggregierte Wissen aller teilnehmenden Wirtschaftssubjekten über das zugrundeliegende Asset. Die Fristen- und Risikotransformationen besagen, dass Renditen und Risiken über die Zeit hinweg transformiert werden und ebenfalls an andere Personen übergeben werden können. Die Bewertungsfunktion bezieht sich auf die Zusammenführung von Angebot und Nachfrage und die damit zusammenhängende Preisbildung. Ohne die genannten Funktionen des Sekundärmarktes wären Anleger oder Investoren unter Umständen nicht oder nur sehr eingeschränkt bereit, die Emissionen am Primärmarkt zu kaufen.

Meist gibt es eine Vielzahl an unterschiedlichen Börsen eines Marktes, beispielsweise des Wertpapiermarktes, die im Wettbewerb zueinanderstehen. Börsen sind aufgrund der Qualität und Kosten ihrer Transaktionsausführung und Depotführung von Konsumenten leicht zu vergleichen. Mittels Standardisierung und Automatisierung sind Börsen daher bedacht, die Qualität für ihre Dienstleistungen hoch und dessen Kosten gering zu halten.[33] Diese Eigenschaften sowie die Funktionen des Sekundärmarktes treffen im weitesten Sinne auch auf Kryptobörsen zu.

2.2.5 Der Devisenmarkt als Spezialform

Der Devisenmarkt ist nach täglichem Umsatzvolumen der größte und liquideste Markt. Devisen werden am Interbankenmarkt gehandelt. Dieser Interbankenmarkt ist kein zentraler Marktplatz und wird daher „over the counter“ durchgeführt. Vierzig Prozent aller Transaktionen finden am Kassamarkt zwischen den Banken statt. Die restlichen sechzig Prozent werden derivativ gehandelt. Devisentransaktionen werden in Währungspaaren angegeben, wie beispielsweise EUR/USD. Die erste angeführte Währung wird als Basiswährung und die zweite als Gegenwährung bezeichnet. Eine Devisentransaktion gibt an, wie viele Einheiten der Gegenwährung notwendig sind, um eine Einheit der Basiswährung zu kaufen. Der Kauf eines Währungspaares beschreibt also den zeitgleichen Kauf der Basiswährung und den Verkauf der Gegenwährung. Ein Verkauf eines Währungspaares besagt folglich das Gegensätzliche.[34] Um den weltweiten Handel der vielen Währungen zu erleichtern, sorgt die Bank für internationalen Zahlungsausgleich (BIZ) für eine bessere Zusammenarbeit zwischen den Zentralbanken. Neben diversen Forschungsarbeiten berät die BIZ Zentralbanken zur Stärkung der weltweiten Währungs- und Finanzstabilität.[35]

[33] Vgl. Nabben & Rudolph, 1994, S. 172.
[34] Vgl. Franzetti, 2018, S. 84f.
[35] Vgl. About BIS - Overview, 2020.

2.3 Bitcoin Grundlagen

Wie im Einleitungskapitel „1.1 Was ist Bitcoin?“ beschrieben, war nicht Bitcoin als Kryptowährung selbst die technologische Erfindung, sondern vielmehr das Konzept der Blockchain. Daher wird in diesem Grundlagenkapitel zuerst die allgemeine Technologie der Blockchain erklärt und nachfolgend die spezifischen Eigenschaften von Bitcoin als eine Anwendung der Blockchain.

2.3.1 Allgemeines

Das Konzept der Blockchain wurde mit dem Bitcoin-Whitepaper von Satoshi Nakamoto[36] eingeführt, wobei im Paper von „chain of blocks“ gesprochen wurde und sich der Term „Blockchain“ erst später etablierte. Die Blockchain-Technologie selbst kann für verschiedenste Anwendungszwecke verwendet werden, ist jedoch mit Bitcoin als Anwendung eines elektronischen Peer-to-Peer-Geldsystems entstanden. Daher gehen die Anforderungen von Bitcoin mit jenen einer Blockchain grundsätzlich einher. Die folgende Abbildung zeigt, wie wichtige Begriffe rund um die Blockchain einzuordnen sind. Eine Top-Down-Betrachtung in Bezug auf ein elektronisches Geldsystem kann wie folgt beschrieben werden: (1) Konsensus besagt, dass jede teilnehmende Person am Geldsystem übereinstimmt, wer wie viel Geld besitzt und welche Transaktionen ausgeführt wurden. (2) Dezentralisierung in diesem Kontext bedeutet, dass alle Personen im Netzwerk gleichberechtigt sind und Transaktionen tätigen und validieren können. Es gibt keine Instanz, die eine Überweisung verbieten kann, es sei denn, die Person handelt nicht nach den vereinbarten Regeln. Beispielsweise kann die Person nur so viel Geld überweisen, wie diese auch besitzt. (3) Blockchain stellt die Technologie dar, wie ein dezentraler Konsens implementiert werden kann. (4) Eine Kryptowährung ist die beschriebene Anwendung eines elektronischen Geldsystems als Blockchain und (5) Bitcoin eine konkrete Implementierung davon.[37]

Konsensus → *Dezentralisierung* → *Blockchain* → *Kryptowährung* → *Bitcoin*

Abb. 4: Route von Bitcoin[38]

[36] Vgl. Nakamoto, 2008.
[37] Vgl. Hosp, 2018, S. 39f.
[38] Quelle: Hosp, 2018, S. 40.

2.3.2 Blockchain

Vereinfacht gesagt ermöglicht eine Blockchain zentralisierten Plattformen dezentral zu werden. Dezentralisierung ist das Gegenteil von Zentralisierung und bedeutet, dass Abläufe von einer beliebigen Anzahl von gleichberechtigten Instanzen, *Peer-to-Peer* (kurz: P2P), durchgeführt werden können. Bei einer Blockchain geht die Dezentralisierung mit einer verteilten Architektur einher. Das bedeutet, dass es eine beliebige und verteilte Anzahl an Knoten gibt, die Prozesse ausführen und direkt miteinander kommunizieren.[39] Nachfolgende Grafik veranschaulicht die Kommunikationswege in dezentralen und zentralen Netzwerken sowie die unterschiedlichen Berechtigungen der Knoten bzw. der Teilnehmer. Die dunkel-eingefärbten Knoten sind höher privilegiert und besitzen die Kontrolle über das Netzwerk.

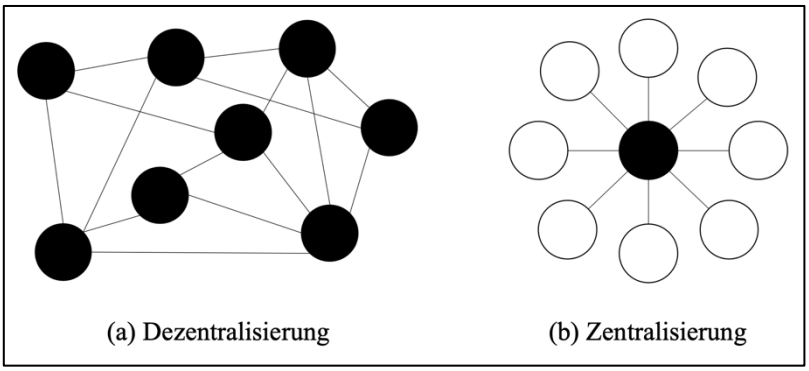

Abb. 5: Unterschiedliche Netzwerktypen[40]

2.3.2.1 Distributed Ledger Technologien

Eine Blockchain kann dem Begriff *Distributed Ledger Technologie* (DLT) untergeordnet werden und war de facto die erste Implementierung einer kompetitiven DLT[41]. Jedoch ist nicht jede DLT eine Blockchain. Eine DLT ist eine über mehrere Computer verteilte und dezentrale Datenbank, in welcher Transaktionen zwischen verschiedenen Parteien sicher verwahrt werden können. Die Blockchain ist eine Möglichkeit, wie diese Datenbank implementiert werden kann, nämlich als unveränderbare Kette von Blöcken. Distributed Ledger Technologien können jedoch auch anders umgesetzt werden. Weitere prominente Beispiele für DLT-Typen sind block- und transaktionsbasierte gerichtete azyklische Graphen.[42] Da diese DLT-Typen nicht im Zusammenhang mit Bitcoin stehen, wird darauf nicht näher eingegangen. Kannengiesser et al. ermitteln sechs Eigenschaften von Distributed Ledger Technologien, welche folglich auch auf Blockchains anwendbar sind:

[39] Vgl. Lee & Low, 2018, S. 175ff.
[40] Quelle: Berentsen & Schär, 2017, S. 96, (leicht modifiziert).
[41] Vgl. Lee & Low, 2018, S. 207.
[42] Vgl. Kannengiesser, Dehling, Lins, & Sunyaev, 2019, S. 1 und 2.

- **Sicherheit**
  Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.
- **Leistung**
  Die Erfüllung einer bestimmten Aufgabe, gemessen an den Standards für Genauigkeit, Vollständigkeit, Kosten und Geschwindigkeit.
- **Benutzerfreundlichkeit**
  Inwieweit ein DLT-Design von bestimmten Benutzern verwendet werden kann, um bestimmte Ziele in Bezug auf Wirksamkeit, Effizienz und Zufriedenheit in einem Nutzungskontext zu erreichen.
- **Entwicklungsflexibilität**
  Die Wartungs- und Weiterentwicklungsmöglichkeiten eines DLT-Designs.
- **Grad der Anonymität**
  Zu welchem Ausmaß Personen innerhalb des Systems identifizierbar sind.
- **Institutionalisierung**
  Die aufkommende Einbettung von Konzepten und Artefakten in soziale Strukturen.[43]

2.3.2.2 Das Double-Spending-Problem und byzantinische Generäle

Die Blockchain löst ein wichtiges Problem des Computerzeitalters, nämlich digitale Daten beliebig oft zu kopieren. In Bezug auf elektronisches Geld, bedeutet es Geld beliebig zu vervielfältigen, oder doppelt auszugeben. Bis dato war die Lösung für dieses Double-Spending-Problem eine zentrale Instanz zu bevollmächtigen, Kontoverrechnungen durchzuführen. Somit wurde ebenso die Geldverwahrung dieser Instanz, zum Beispiel einer Bank, anvertraut. Die Blockchain kombiniert P2P-Datenaustausch mit kryptografischen Mechanismen, um Double-Spending zu vermeiden. Ein Benutzer muss keinem anderen vertrauen, außer dem System selbst. Mittels asymmetrischer Verschlüsselung, Hashing-Algorithmen und einem Konsensus-System wird das Konto eines Benutzers in einer unveränderbaren Kette von Blöcken geführt.[44]

Was haben aber nun die byzantinischen Generäle mit dem Double-Spending-Problem zu tun? Das Double-Spending-Problem ist ähnlich einem spieltheoretischen Problem, welches vor der Blockchain in der Informatik nicht gelöst werden konnte. Die Blockchain kann dieses Problem auch nicht zu 100 Prozent lösen, bietet jedoch eine solide Lösung. Bei diesem Problem geht es um den Angriff von zwei oder mehr byzantinischen Truppen auf eine Stadt. Bekannt ist, dass

[43] Vgl. Kannengiesser, Dehling, Lins, & Sunyaev, 2019, S. 4.
[44] Vgl. Swan, 2015, S. 2.

die Stadt eingenommen werden kann, wenn zumindest die Hälfte der Truppen angreifen. Die Truppen sind in verschiedenen Lagern stationiert und das Problem liegt in der vertraulichen Kommunikation zwischen den Generälen der Truppen untereinander, um den Angriffsplan abzustimmen. Die Information „Angriff“ oder „Kein Angriff“ muss also manipulationssicher zwischen den Lagern ausgetauscht werden können. Dabei stehen die Generäle jedoch vor drei Problemen: Sie müssten 1) wissen, dass die Nachricht ankommt; 2) den Angriffsplan bestätigt bekommen und 3) überprüfen können, ob die ausgetauschten Nachrichten echt und nicht manipuliert worden sind. Da eine Blockchain ein Peer-to-Peer-Netzwerk ist, indem die Nachrichten schnell verbreitet werden, ist 1) erfüllt. Sobald alle Teilnehmer die Nachricht validiert haben ist ebenfalls Nummer 2) gelöst. Voraussetzung für die Validierung in 2) ist jedoch die Echtheit der Nachricht aus 3). Durch die Offenlegung und Verknüpfung aller Informationen kombiniert mit kryptografischen Mechanismen, um die Authentizität von Nachrichten zu gewährleisten, ist dies möglich. Jedoch kann die Weitergabe von falschen Informationen nicht mit absoluter Sicherheit ausgeschlossen werden, aber die damit verbundenen Kosten sind abschreckend hoch, sodass sich eine Manipulation nicht lohnt. Nähere Informationen dazu können in Kapitel „2.3.2.4 Technische Funktionsweise“ nachgelesen werden.[45]

2.3.2.3 Arten von Blockchains

Blockchains können für verschiedene Personen zugänglich sein und unterschiedliche Berechtigungskonzepte vorsehen. Unterschiedliche Anwendungsformen können verschiedene Voraussetzungen an die Blockchain haben. Da eine Blockchain höhere Kosten und andere negative technische Implikationen mit sich bringt, sollte die Blockchain als Technologie nur dann gewählt werden, wenn eine dezentrale Lösung benötigt wird[46]. Morkunas et al. (2019) unterscheiden zwischen öffentlichen und privaten Blockchains. Öffentliche Blockchains kennzeichnen, dass jeder die Daten einsehen und verändern kann. Somit können Personen anonym miteinander interagieren und Daten austauschen. Der Datenfluss ist vollkommen transparent und kann von jedem eingesehen werden. Jedoch werden im Vergleich zu privaten Blockchains energieintensive Konsensus-Algorithmen benötigt. Bei privaten Blockchains müssen Personen vorab überprüft und berechtigt werden, sodass sie die Blockchain lesen und verändern können. Im Gegensatz zu einer öffentlichen Blockchain kann eine private Blockchain mehr Privatsphäre bieten und somit Anwendungen sensible Datenverarbeitung

[45] Vgl. Dixon, 2017, S. 220f.
[46] Vgl. Hosp, 2018, S. 63f.

ermöglichen. Weiters sind private Blockchains leichter zu skalieren sowie kostengünstiger und performanter zu gestalten als öffentliche Blockchains.[47]

2.3.2.4 Technische Funktionsweise

Die Blockchain ist eine geordnete und rückwärts verlinkte Liste von Blöcken, die miteinander verknüpft sind. Dabei beinhaltet ein jeder Block die ID des Vorgängerblocks und weist so auf diesen zurück. Eine Block-ID ist ein sogenannter Hash[48], welcher sich aus allen Daten des jeweiligen Blocks berechnet. Sollte eine Änderung in einem Block im Nachhinein passieren, so ändert sich auch der Hash-Wert dieses Blocks und der Folgeblock müsste ebenfalls die vorherige ID des veränderten Blocks durch die Neue ersetzen. Dadurch verändert sich ebenfalls die ID des nächsten Folgeblocks und folglich müssen auch alle weitere Folgeblöcke neu berechnet werden. Alle Blöcke sind dadurch quasi aneinander gekettet, daher der Name „Blockchain". Der allererste Block besitzt keine Vorgängerblock-ID und wird als Genesis-Block bezeichnet. Da jeder andere Block den Hash des Vorgängerblocks aufweist, ist es unter Umständen möglich, dass ein Block mehrere Folgeblöcke hat. Dies ist meist nur temporär der Fall und wird als „Fork", zu Deutsch Gabelung, bezeichnet. Mehr dazu im Kapitel „2.3.2.6 Forks".[49] Folgende Abbildung veranschaulicht die Verkettung der Blöcke in einer Blockchain. Die ID oder der Hash des Vorgängerblocks befindet sich in den „Block Header"-Daten und wird hier als „Parent Block Hash" bezeichnet. Neben den Header-Daten besitzt ein Block auch die Daten der stattgefundenen Transaktionen. Der betrachtete Block in der Mitte wird hier „Block i" genannt, der Vorgängerblock „Block i-1" und der Folgeblock „Block i+1".

[47] Vgl. Morkunas, Paschen, & Boon, 2019, S. 297.
[48] Ein Hash ist ein digitaler Fingerabdruck von Daten. Durch ein kryptografisches Einwegverfahren kann aus Daten beliebiger Länge eine Zeichenfolge definierter Länge berechnet werden. Wichtig hierbei ist, dass die berechnete Zeichenfolge, die als Hash bezeichnet wird, nicht zu den Ausgangsdaten umkehrbar ist und dass eine winzige Änderung in den Ausgangsdaten zu einem komplett veränderten Hash-Wert führt.
[49] Vgl. Antonopoulos, 2014, S. 163f.

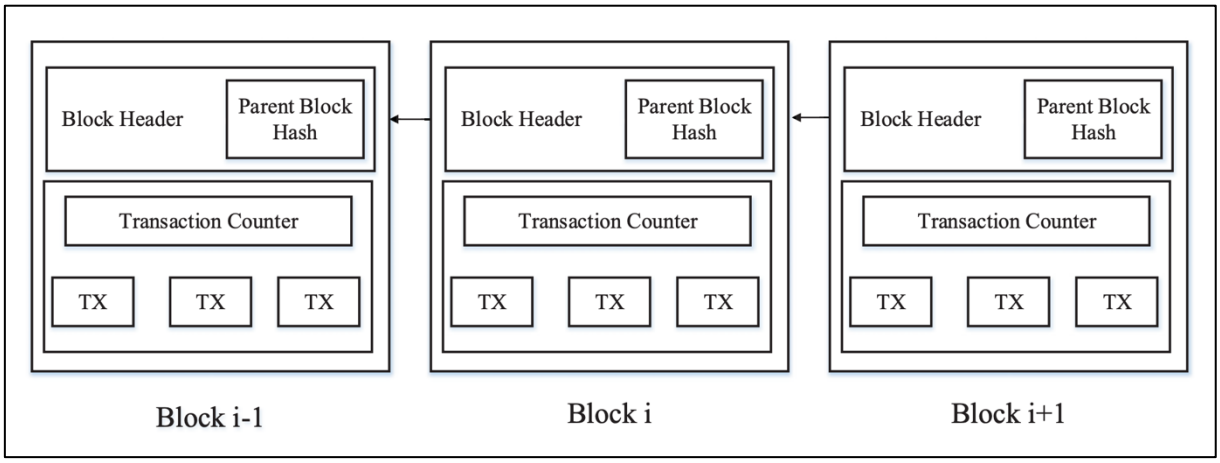

Abb. 6: Blockchain Architektur[50]

2.3.2.4.1 Struktur eines Blocks

Ein Block ist eine Datenstruktur und setzt sich aus den Metadaten, die im „Block Header" zu finden sind, und den Transaktionsdaten, welche im Hauptteil des Blocks im sogenannten „Block Body" enthalten sind, zusammen. Nachfolgende Abbildung Abb. 7 veranschaulicht die Struktur eines Blocks. Der Block Header beinhaltet: (a) Block Version: Bestimmt die vorgegebenen Validierungsregeln. (b) Merkle Tree Root Hash: Der Hash-Wert aller Transaktionsdaten dieses Blocks. (c) Timestamp: Der (Unix-)Zeitstempel, wann der Block hinzugefügt wurde. (d) nBits: Zielschwelle unter welcher ein gültiger Block Hash liegen muss. (e) Nonce: Eine Zahl, die für den Proof-of-Work-Algorithmus benötigt wird[51]. (f) Parent Block Hash: der Hash-Wert des Vorgängerblocks zur Verkettung. Mehr zu (d) und (e) im Kapitel „2.3.2.5 Mining, Konsensus und Proof-of-Work**Mining, Konsensus**". Der Block Body setzt sich aus dem Transaktionszähler und den einzelnen Transaktionen zusammen. Die maximale Anzahl an Transaktionen pro Block variiert je nach Gesamtgröße des Blocks. Wenn es eine hohe Anzahl an Transaktionen gibt, die wenig Datenbedarf benötigen, können mehr Transaktionen in den Block mitaufgenommen werden.[52] Im Bitcoin-System hat ein Block eine Größe von rund 1 Megabyte[53] und beinhaltet durchschnittlich laut der Webseite https://www.blockchain.com rund 2000 Transaktionen. Transaktionsdaten werden hier nicht näher beschrieben, da diese je nach Blockchain-Anwendung voneinander abweichen können und die technische Funktionsweise der Blockchain nicht wesentlich beeinflussen.

[50] Quelle: Zheng, Xie, Dai, Chen, & Wang, 2017, S. 558.
[51] Vgl. Antonopoulos, 2014, S. 165.
[52] Vgl. Zheng, Xie, Dai, Chen, & Wang, 2017, S. 558,
[53] Vgl. Antonopoulos, 2014, S. 172.

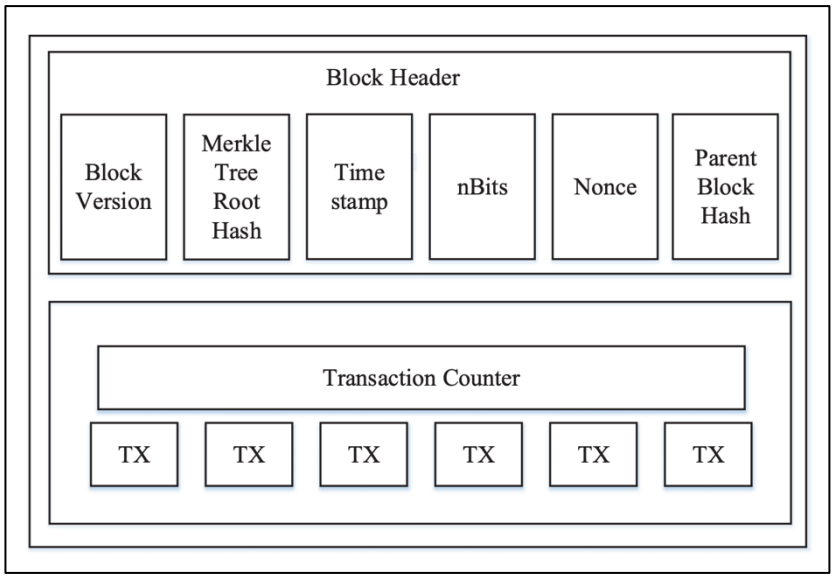

Abb. 7: Block Struktur[54]

2.3.2.4.2 Vertraulichkeit und Signaturen

Ein asymmetrischer Verschlüsselungsmechanismus stellt sicher, dass nur berechtige Personen Transaktionen tätigen können. Eine Transaktion transferiert ein Asset von einer Person zur anderen. Folglich muss die Sender-Person das Asset vorher besitzen, welches an die Empfänger-Person übertragen werden soll. Um dies zu bewerkstelligen, benötigt jeder Benutzer einen öffentlichen und privaten Schlüssel. Den privaten Schlüssel darf nur der Benutzer selbst kennen, der öffentliche Schlüssel ist hingegen für alle anderen Blockchain-Benutzer sichtbar. Beispielsweise kann ein Sender mit seinem privaten Schlüssel seine Nachricht verschlüsseln und diese dem Empfänger schicken. Der Empfänger kann die verschlüsselte Nachricht mit dem öffentlichen Schlüssel des Senders wieder entschlüsseln. Auf eine ähnliche Art und Weise erfolgen die Signaturen bei Blockchain-Transaktionen, sodass mit Sicherheit gesagt werden kann, ob eine gewisse Person die Transaktion getätigt hat oder nicht.[55]

2.3.2.4.3 Merkle Trees

Merkle Trees werden verwendet, um auf effiziente Weise überprüfen zu können, ob eine Transaktion in einem Block enthalten ist oder nicht. Der Merkle Tree ist ein binärer Hash-Baum, welcher als Blätter alle Transaktionen des jeweiligen Blocks besitzt. Aufeinanderfolgende Transaktions-Hashes werden in 2er-Paaren zu einem kombinierten Hash-Wert gebildet. Dieser Vorgang wird so lange wiederholt bis nur mehr ein Hash-Wert als Wurzel übrigbleibt. Diese Wurzel wird als „Merkle Tree Root Hash“ bezeichnet und ist im Block

[54] Quelle: Zheng, Xie, Dai, Chen, & Wang, 2017, S. 558
[55] Vgl. Zheng, Xie, Dai, Chen, & Wang, 2017, S. 558

Header hinterlegt. Sollte es eine ungerade Anzahl an Transaktionen geben, so wird die letzte Transaktion dupliziert, um die Voraussetzung eines binären Baumes zu erfüllen. Folgende Abbildung veranschaulicht die Berechnung der Merkle Root mittels den Transaktionen A, B, C und D.[56]

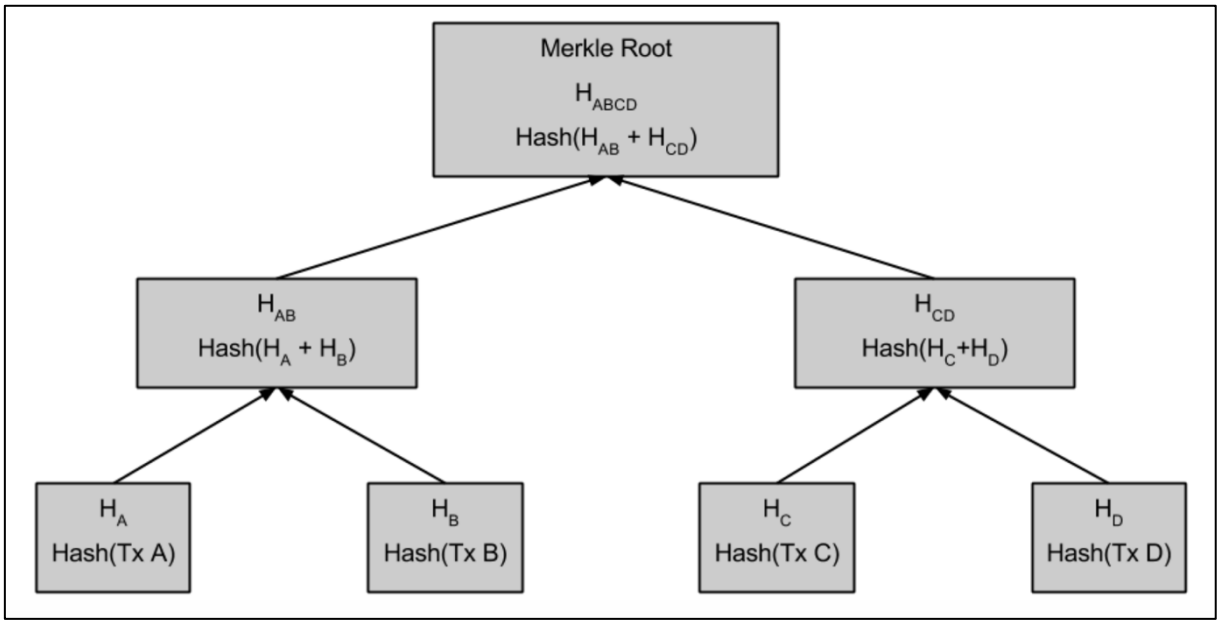

Abb. 8: Merkle Tree Beispiel[57]

Der Vorteil, den ein Merkle Tree neben der Berechnungseffizienz bietet, ist, dass ein Node, ein Teilnehmer im Bitcoin-System, nicht den vollkommenen Block respektive die vollkommene Blockchain lokal gespeichert haben muss, um Transaktionsüberprüfungen durchführen zu können. Es wird lediglich der Block Header sowie ein kurzer Merkle Path benötigt. Diese Daten können von einem Full Node[58] ad hoc angefragt werden. Die nachfolgende Abbildung zeigt die beispielhafte Überprüfung, ob die Transaktion K im Block vorkommt. Dafür werden ausschließlich die dunkelgrau eingefärbten Hashes, der Merkle Path, benötigt. Der Merkle Path wird neben dem Block Header zusätzlich dem ausführenden Node übermittelt, welcher ebenfalls die Transaktion K kennt. Nun müssen ausschließlich die strichlierten Hash-Werte berechnet werden, um zur Root zu gelangen. Diese wird mit der Merkle Tree Root im Block Header verglichen. Stimmt der berechnete Root-Hash mit dem Merkle Tree Root Hash vom Block Header überein, so befindet sich die Transaktion im Block.[59]

[56] Vgl. Antonopoulos, 2014, S. 170ff.
[57] Quelle: Antonopoulos, 2014, S. 171.
[58] Ein Full Node ist ein teilnehmender Computer im Blockchain-Netzwerk, welcher die gesamte Blockchain heruntergeladen hat und am Netzwerk teilnimmt.
[59] Vgl. Antonopoulos, 2014, S. 172 und 175.

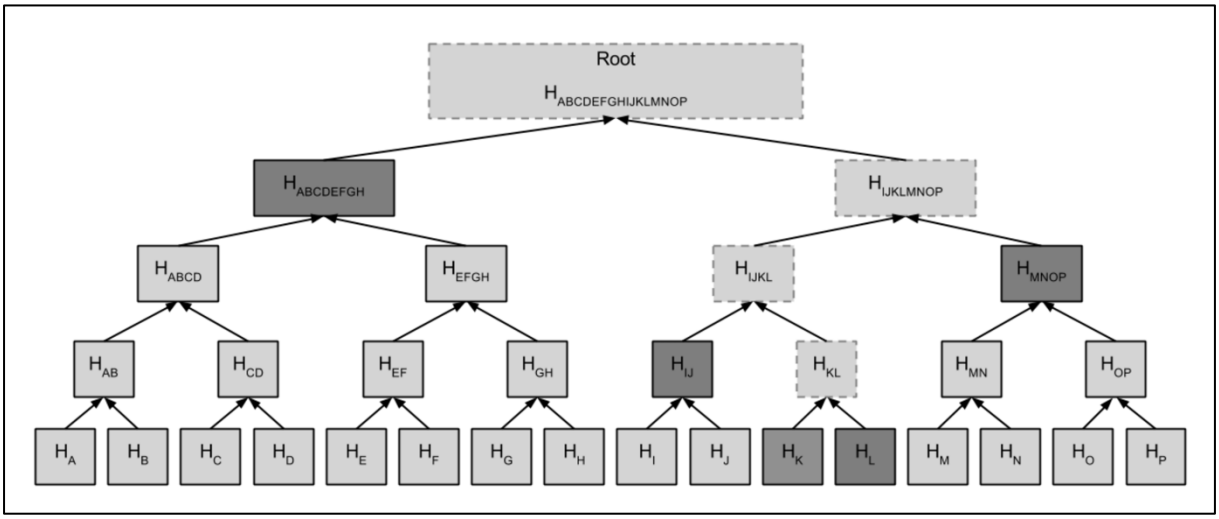

Abb. 9: Merkle Path zur Transaktionsüberprüfung[60]

2.3.2.5 Mining, Konsensus und Proof-of-Work

Die Blockchain löst das wichtige Problem des vertraulichen Datenaustausches in einem Netzwerk bestehend aus unbekannten Teilnehmern.[61] Beispielhaft wurde dies bereits im Kapitel „2.3.2.2 Das Double-Spending-Problem und byzantinische Generäle“ beschrieben. Mining bezeichnet den Prozess zur Bereitstellung der Rechenleistung für die Validierung und Konsensfindung in einer Blockchain. Diverse Kryptowährungen, wie beispielsweise Bitcoin, belohnen den Mining-Aufwand mit neu geschafften Assets innerhalb des jeweiligen Blockchain-Systems. Zudem können Transaktionsgebühren ebenfalls an die Miner ausbezahlt werden.[62] Der Konsens-Algorithmus schafft daher Anreize, dass die Teilnehmer aus reinem Eigeninteresse bereits den Regeln folgen und das System nicht betrügen versuchen.[63]

Proof-of-Work (PoW) ist der von Bitcoin verwendete Konsensus-Algorithmus. Theoretisch könnte ein neuer Block in Millisekunden berechnet werden und der Blockchain hinzugefügt werden. Das Blockchain-Netzwerk benötigt jedoch Zeit sich auf einen neuen Zustand zu einigen und neue Transaktionen anzunehmen. Der PoW-Algorithmus ermöglicht dies, indem er einer schnellen Berechnung Schwierigkeit hinzufügt, welche die Berechnung bei zunehmender (abnehmender) Rechenleistung schwieriger (leichter) macht. Diese Schwierigkeit wird im Block-Header im Wert „nBits“, auch oft als „Schwellenwert“ oder „Zielschwelle“ bezeichnet, mitgeführt und passt sich dynamisch an die Rechenleistung des Blockchain-Netzwerks an. Die Schwierigkeit wird konkret verwendet, um das Ergebnis der

[60] Quelle: Antonopoulos, 2014, S. 173.
[61] Vgl. Zheng, Xie, Dai, Chen, & Wang, 2017, S. 559.
[62] Vgl. Antonopoulos, 2014, S. 177.
[63] Vgl. Berentsen & Schär, 2017, S. 206.

Berechnung zu validieren. Hierzu muss das Ergebnis eines Hash-Verfahrens unter dem Schwellenwert liegen. Da ein Hash-Verfahren ein Einwegverfahren ist, kann nicht von einem Output auf einen Input geschlossen werden. Nur mittels der Trial-and-Error-Methode, also stetigem Probieren, kann somit ein gültiges Ergebnis errechnet werden[64]. Im Bitcoin-Netzwerk ist diese Schwierigkeit so konfiguriert, dass in etwa alle 10 Minuten ein neuer Block gefunden wird.[65] Die aufzubringende Rechenleistung verursacht den Minern kosten und besichert so die Blockchain. Da diese Art der Buchführung mit Kosten verbunden ist, wird ein ehrliches Verhalten im Blockchain-Netzwerk gestärkt, um nicht die investierte Rechenleistung zu verlieren.[66] Folglich wäre auch ein Angriff auf die Blockchain extrem teuer, denn der Angriff benötigt 51 % der gesamten Rechenleistung im Netzwerk und ebenfalls viel Zeit, um nachträglich Blöcke manipulieren zu können.[67] Theoretisch sind solche Angriffe denkbar, aufgrund des Anreizsystems sind diese jedoch praktisch von der Hand zu weisen. Denn angenommen solch ein Angriff wäre erfolgreich, so würde unmittelbar das Vertrauen in das System verloren gehen und somit auch dessen Wert.[68] Neben Proof-of-Work gibt es noch andere Konsensus-Mechanismen, wie zum Beispiel *Proof-of-Stake* (PoS). Diese werden aber nicht näher beleuchtet, da sie in keinem Zusammenhang mit Bitcoin stehen.

2.3.2.6 Forks

Ein Fork, zu Deutsch Gabelung, bezeichnet verschiedene Versionen einer Blockchain. Neue Blöcke können zu unterschiedlichen Zeiten zu unterschiedlichen Teilnehmern oder Minern gelangen. So kann im Blockchain-Netzwerk eine Inkonsistenz auftreten und Miner können daher unterschiedliche Perspektiven auf die Blockchain besitzen. Eine wichtige Regel besagt, dass neu gefundene Blöcke nur der längsten Blockchain angehängt werden dürfen, da nur die längste Kette als gültig angesehen wird. Dies schließt jedoch nicht aus, dass zu einer gegebenen Zeit mehrere gleich lange Blockchains existieren können. Dennoch wird erwartet, dass bei aufkommenden Forks die Blockchain auf diese Art und Weise wieder zu einer gültigen und eindeutigen Blockchain konvergiert. Normalerweise werden solche Forks mit dem nächsten Block bereinigt. Theoretisch ist es möglich, dass die Blockchain nach einem Fork erst nach zwei Blocken konvergiert. Dies ist aber aufgrund des PoW-Konsensus-Protokolls äußerst unwahrscheinlich.[69]

[64] Vgl. Antonopoulos, 2014, S. 193.
[65] Vgl. Berentsen & Schär, 2017, S. 211.
[66] Vgl. Berentsen & Schär, 2017, S. 207f.
[67] Vgl. Lee & Low, 2018, S. 214.
[68] Vgl. Antonopoulos, 2014, S. 217.
[69] Vgl. Antonopoulos, 2014, S. 204ff.

2.3.3 Die Bitcoin Technologie

Nachdem im vorhergehenden Kapitel „2.3.2 Blockchain“ die Blockchain-Technologie im Allgemeinen beschrieben wurde, geht dieses Kapitel auf spezifische Merkmale von Bitcoin ein. Wichtig hierbei ist, dass ausschließlich auf die wichtigsten und für diese Arbeit notwendigen Besonderheiten eingegangen wird.

2.3.3.1 Bitcoin Adresse

Um Bitcoins empfangen oder versenden zu können, wird eine Bitcoin Adresse benötigt. Eine solche Adresse setzt sich aus einem öffentlichen und einem privaten Schlüssel zusammen. Die Adresse ist der Fingerabdruck, ein Hash-Wert, des öffentlichen Schlüssels und wird als Empfänger oder Sender in einer Bitcoin-Transaktion verwendet. Somit kann in einer Analogie der öffentliche Schlüssel als Kontonummer und der private Schlüssel als PIN angesehen werden. Eine Bitcoin-Wallet oder digitale Bitcoin-Brieftasche kümmert sich im Regelfall ums Erzeugen und Verwalten der Schlüssel. Somit sieht der Benutzer der Wallet die Schlüssel oft gar nicht. Wichtig ist, dass der Besitz des privaten Schlüssels jede Person ermächtigt, Bitcoins einer Person transferieren zu können. Daher ist der private Schlüssel unbedingt geheim zu halten.[70]

Die Schlüsselgenerierung basiert auf einem mathematischen Einwegverfahren, wie es ebenfalls im Internet beim Online-Banking zur Anwendung kommt. Zuerst wird der private Schlüssel mittels einer Zufallszahl generiert. Durch Elliptische-Kurven-Kryptografie wird vom privaten Schlüssel der zugehörige öffentliche Schlüssel berechnet. Abschließend wird die sichtbare Bitcoin Adresse über ein Hash-Verfahren vom öffentlichen Schlüssel generiert. So ist es unmöglich von der Bitcoin Adresse auf den öffentlichen Schlüssel und vom öffentlichen Schlüssel auf den privaten Schlüssel rückschließen zu können.[71]

2.3.3.2 Transaktionen

Eine Transaktion sagt dem Netzwerk, dass eine definierte Menge an Bitcoins den Besitzer wechseln soll. Der neue Besitzer kann, sobald die Transaktion bestätigt ist, frei über diese Menge verfügen. Eine Transaktion kann wie ein Eintrag in einer doppelten Buchführung angesehen werden. Jede Transaktion besteht aus einen oder mehreren Eingängen (Inputs) und einen oder mehreren Ausgängen (Outputs). Ein Input oder Output steht unmittelbar für eine

[70] Vgl. Antonopoulos, 2014, S. 61.
[71] Vgl. Bistarelli, Mercanti, & Santini, 2018, S. 93.

Bitcoin-Adresse. Um Bitcoins in einem Input ausgeben zu können, müssen diese vorher in einer getätigten Transaktion im Output erhalten worden sein. Das Bitcoin-Netzwerk führt jedoch keinen expliziten Kontostand einer jeden Bitcoin Adresse. Der verfügbare Kontostand ist implizit durch die noch nicht ausgegebenen Bitcoins gegeben. Nicht ausgegebenen Bitcoins sind nicht ausgegebene Transaktions-Outputs (engl. unspent transaction output) und werden mit UTXO abgekürzt. Die Summe aller UTXOs ergibt somit den Kontostand einer Adresse. Wollen nun Bitcoins ausgegeben werden, so müssen diese im Input verlinkt mit ihrer Herkunft zum Output angegeben werden. Somit ist es für alle Teilnehmer im Bitcoin-Netzwerk möglich, eine Validierung der Transaktion durchführen zu können. Ferner ist hier wichtig, dass immer der komplette Betrag eines UTXO im Input ausgegeben werden muss. Daher ist es in der Regel üblich, dass der zu bezahlende Betrag nicht exakt einem UTXO entspricht. Um dennoch eine genaue Bezahlung tätigen zu können, werden zwei Outputs benötigt. Der erste Output bezahlt den Empfänger auf den Satoshi[72] genau und der Restbetrag wird als Wechselgeld (engl. Change) wieder an sich selbst zurücküberwiesen, welches erneut in einem Input wieder ausgegeben werden kann. Ebenfalls ist es üblich, dass eine Transaktion eine Transaktionsgebühr aufweist. Diese wird analog zum Kontostand implizit geführt, indem die Summe von ausgegebenen Bitcoins (Inputs) etwas größer ist, als die in derselben Transaktion erhaltenen Bitcoins (Outputs). Die Differenz ist die Transaktionsgebühr (engl. Fee), die der Miner erhält, sobald dieser die Transaktion in einem neuen Block aufnimmt. Eine Ausnahme stellt die Coinbase-Transaktion dar, welche keinen Input und nur einen Output aufweist. Die Coinbase-Transaktion ist die Belohnung in Form von neu geschaffenen Bitcoins an jenen Miner, der den nächsten Block findet und der Blockchain hinzufügt.[73]

Nachfolgende Abbildung zeigt den Aufbau einer Bitcoin-Transaktion. Die Version gibt Auskunft welche Validierungsregeln auf die Transaktion anzuwenden sind. Mittels der Sperrzeit kann festgelegt werden, wann die Transaktion frühestens in die Blockchain aufgenommen wird. Ein Wert von „0“ bedeutet, dass die Transaktion ehest möglich einem Block hinzugefügt werden kann. Weiters kann aber ein beliebiger Zeitpunkt in der Zukunft oder die Blockhöhe mit diesem Parameter definiert werden. Die Anzahl an Inputs und Outputs gibt an, wie viele Inputs und Outputs in der Transaktion vorkommen. Wie bereits erwähnt, müssen mindestens ein Input und ein Output vorkommen. Abgesehen von dieser Mindestanzahl kann die Anzahl der Inputs und Outputs eine beliebige Menge annehmen. Inputs weisen eine

[72] Als Satoshi wird die kleinste Einheit eines Bitcoins bezeichnet, ähnlich wie ein Cent eines Euros.
[73] Vgl. Antonopoulos, 2014, S. 114ff.

Referenztransaktion (Transaktions-Hash) auf, welche auf jene Transaktion mit den UTXOs verweist. Der Output-Index gibt an, auf welchen Output die UTXO-Menge konkret anzuwenden ist. Freigabebedingung ist das Entsperrsskript (engl. unlock script), welches die Auszahlungsbedingung, die in den UTXO vorgegeben ist, erfüllt und somit die Bitcoins freigibt. Im Regelfall ist diese Freigabebedingung die Signatur, also der Nachweis auf den Besitz des privaten Schlüssels, jener Adresse, die als Empfänger in der Auszahlungsbedingung in der referenzierten UTXO-Transaktion hinterlegt ist.[74]

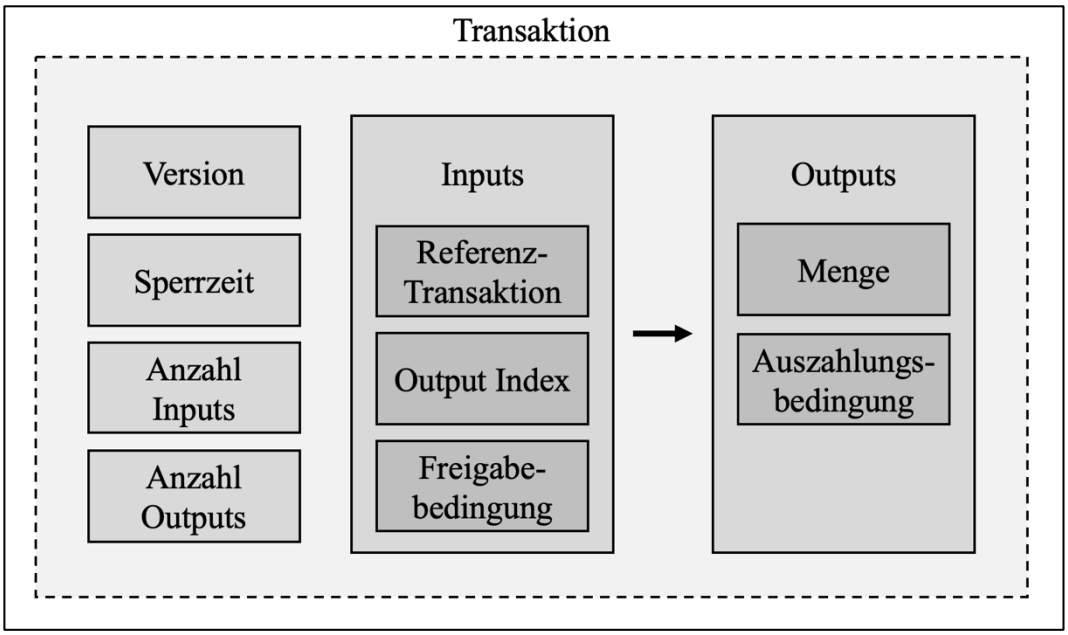

Abb. 10: Aufbau einer Bitcoin-Transaktion[75]

Wie bereits angeschnitten, gibt die Auszahlungsbedingung vor, wer über den entsprechenden Output verfügen darf. Es sperrt somit den Output. Daher wird dieser Parameter üblicherweise als *locking script* benannt. Um einen konkreten UTXO ausgeben zu können, wird folglich eine Freigabebedingung, das *unlocking script*, benötigt. Üblicherweise wird in der Auszahlungsbedingung der Nachweis des Besitzes des privaten Schlüssels mittels Signatur gefordert. Dies geschieht durch ein internes Standardskript von Bitcoin, welches als Pay-to-Public-Key-Hash (P2PKH) bezeichnet wird. Es gibt noch andere standardmäßig hinterlegte Skripte, wie beispielsweise Pay-to-Public-Key (P2PK) und Pay-to-Script-Hash (P2SH). Es müssen jedoch nicht zwingend Standardskripte in der Auszahlungsbedingung verwendet werden. Vereinfacht zur Anschauung könnte beispielsweise jemand „X + 2 = 8“ als

[74] Vgl. Antonopoulos, 2014, S. 113ff.
[75] Quelle: Eigene Darstellung, angelehnt an: Berentsen & Schär, 2017, S. 171, Antonopoulos, 2014, S. 116 und 119.

Auszahlungsbedingung hinterlegen. Jene Person, die als Erstes diesen UTXO mit der Freigabebedingung „X = 6“ in einer neuen Transaktion referenziert, kann über die gesperrten Bitcoins verfügen.[76]

2.3.4 Handel mit Bitcoin

Der Handel von Kryptowährungen erfolgt gewöhnlich an Kryptobörsen. Kryptobörsen sind Online-Plattformen, über welche verschiedenste Währungspaare, wie BTC/EUR, gehandelt werden können. Börsen unterscheiden sich in ihrem Angebot an Währungspaaren und ihrer Kostenstruktur. Letztere ist im Vergleich zu herkömmlichen Online-Brokern im Aktienbereich jedoch vernachlässigbar gering. Neben Börsen findet der Handel von Bitcoin auch direkt von Person zu Person statt. Im Folgenden wird auf den Unterschied zwischen On- und Off-Chain-Transaktionen eingegangen.

2.3.4.1 On-Chain Transaktionen

Wenn Transaktionen ins Blockchain-Netzwerk gesendet werden und ein Miner diese erfolgreich validiert und in einen Block aufnimmt, verändern sie den Blockchain-Datenbestand und sind somit irreversibel. Dabei werden je nach aktueller Last und Anzahl von offenen Transaktionen geringere oder höhere Transaktionsgebühren bezahlt. Da diese Transaktionen direkt in der Blockchain stattfinden, werden sie als On-Chain-Transaktionen bezeichnet. Damit eine solche On-Chain-Transaktion durchgeführt werden kann, wird eine Bitcoin-Adresse benötigt. On-Chain-Transaktionen finden bei Kryptobörsen im Wesentlichen nur dann statt, wenn ein Kunde sein Guthaben auf eine persönliche Blockchain-Adresse transferieren möchte. Bei allen anderen Transaktionen ist die Kryptobörse bemüht, so wenig Blockchain-Transaktionen wie möglich auszulösen, um die Kosten gering zu halten. On-Chain-Transaktionen finden Anwendung, wenn beispielsweise eine Person direkt einer anderen Person einen Betrag über eine Wallet überweist.[77]

2.3.4.2 Off-Chain Transaktionen

Von Off-Chain-Transaktionen wird gesprochen, wenn Transaktionen nicht über die Blockchain abgebildet werden. Hierbei übernimmt ein vertrauenswürdiger Dritter den Transfer der Werte von einer Person zur anderen. Da solche Transaktionen die Blockchain nicht verändern, müssen auch keine Transaktionsgebühren an das Bitcoin-Netzwerk bezahlt werden. Gewöhnlich hebt

[76] Vgl. Bistarelli, Mercanti, & Santini, 2018, S. 93f.
[77] Vgl. Frankenfield, On Chain Transactions (Cryptocurrency), 2018.

jedoch die durchführende Instanz der Off-Chain-Transaktionen eine kleine Gebühr ein. Off-Chain-Transaktionen werden vor allem von Kryptobörsen eingesetzt, um den Handel günstiger und wesentlich schneller durchführen zu können. Hierbei besteht jedoch das Risiko des Ausfalls der Kryptobörse. Da der private Schlüssel dem Kunden der Börse vorenthalten wird, kann der Besitzer aus der Blockchain-Perspektive nicht über seine Einlagen direkt verfügen.[78]

[78] Vgl. Frankenfield, Off-Chain Transactions (Cryptocurrency), 2019.

3 Daten

Bevor eine empirische Analyse durchgeführt werden kann, müssen die Daten zunächst beschafft werden. Dieses Kapitel gibt Auskunft, wie die Daten beschafft werden. Die empirische Analyse dieser Arbeit beschäftigt sich neben den internen Blockchain-Transaktionsdaten ebenfalls mit den historischen Preisen für Bitcoin. Preisdaten müssen von einem Drittsystem beschafft werden, da Preise nicht in der Blockchain abgebildet sind. Damit diese Verknüpfung zweier verschiedener Datenquellen hergestellt werden kann, ist es notwendig eine Datenaggregation durchzuführen. Wie eine solche Aggregation durchgeführt werden kann, wird ebenfalls in diesem Kapitel beschrieben.

3.1 Datenbeschaffung

Wie bereits eingehend erläutert, befasst sich die empirische Analyse hauptsächlich mit den internen Daten der Bitcoin Blockchain. Diese Daten sind öffentlich für jeden einsehbar ohne spezielle Authentifizierungs- oder Autorisierungsverfahren. Diese Daten werden auch als „On-Chain-Daten“ bezeichnet, da sie sich direkt in der Blockchain befinden. Da sich der Bitcoin-Preis basierend auf Angebot und Nachfrage bildet und dieser je nach Handelsplatz variieren kann, kann der Preis nicht in der Blockchain gespeichert sein. Die Bitcoin-Blockchain ermöglicht den Handel von Bitcoins und bildet intern die Ansprüche ab, welche Adresse über welche Menge von Bitcoins verfügen darf und kann. Folglich müssen die Preisdaten von einem Dritten, beispielsweise einer Kryptobörse, zur Verfügung gestellt werden. Da sich diese Daten nicht in der Blockchain befinden, wird hier von „Off-Chain-Daten“ gesprochen.

3.1.1 On-Chain-Daten

Bitcoin interne Blockchain-Daten können grundsätzlich auf zwei verschiedene Wege ermittelt werden: Entweder (1) mittels dediziertem Full-Node, oder (2) mittels API-Zugriff[79] auf ein Drittsystem, welches die Daten zur Verfügung stellt.

3.1.1.1 Datenbeschaffung mittels Full-Node und BlockSci

Bitcoin ist eine Open-Source-Software und kann daher auf jedem beliebigen Computer lizenzfrei installiert werden. Dafür benötigt der Computer die notwendigen Software- und Hardwareanforderungen sowie eine aktive Internetverbindung. Wenn das Bitcoin-Programm erfolgreich installiert ist, muss es zunächst die gesamte Blockchain herunterladen und sich

[79] API steht für *Application Programming Interface* und bezeichnet eine Schnittstelle an ein Computerprogramm.

kontinuierlich synchronisieren. Laut der Webseite blockchain.com beträgt der gesamte Speicherbedarf am 17.06.2020 rund 283 Gigabyte.[80] Sobald die Blockchain erfolgreich heruntergeladen ist, können die Daten auf verschiedenste Wege analysiert werden. Eine Eigenentwicklung erfordert großes Know-How in der Blockchain-Technologie selbst sowie außerordentliche Programmierfähigkeiten. Alternativ gibt es frei verfügbare Analysetools, wie beispielsweise BlockSci, welches von Forschenden der Princeton University entwickelt worden ist. Dieses Kapitel beschäftigt sich etwas näher mit BlockSci, da diese Software für die On-Chain-Datenbeschaffung dieser Arbeit verwendet wurde.

BlockSci ist eine frei verfügbare Software zur Blockchain-Analyse. BlockSci unterstützt mehrere Blockchain-Technologien und Analyse-Möglichkeiten. Die Software komprimiert die Blockchain bestmöglich und hält diese im Arbeitsspeicher des Computers, um Abfragen performant durchführen zu können. Neben Bitcoin werden noch andere Altcoins[81], wie Litecoin, unterstützt. Für Smart-Contract-Plattformen, wie Ethereum, ist BlockSci nicht verwendbar. Bei der aktuellen Größe der Bitcoin Blockchain wird ein Speicher von 64 GB RAM, eine SSD-Festplatte von 600 GB und 8 CPUs empfohlen.[82] Wie in der nachfolgenden Abbildung zur Architektur-Übersicht entnommen werden kann, werden als Basis die rohen Blockchain-Daten benötigt. Diese werden mit einem Parser in das BlockSci-Kerndatenformat gebracht und stetig aktualisiert. Die Kerndaten werden für die Analyse in einer Datenbank, welche im Arbeitspeicher des Computers gehalten wird, dem Benutzer zur Verfügung gestellt. Der Anwender hat die Möglichkeit Abfragen direkt oder über ein Jupyter-Notebook in der BlockSci-Datenbank abzusetzen. Python kann als Programmiersprache im Jupyter-Notebook verwendet werden.[83]

[80] Die aktuelle Größe der Bitcoin Blockchain kann unter https://www.blockchain.com/charts/blocks-size nachgeschlagen werden. Da Blöcke in regelmäßigen Abständen hinzukommen, hat der Speicherzuwachs in den letzten Jahren einen linearen Verlauf.
[81] Als Altcoin wird jede Kryptowährung außer Bitcoin bezeichnet.
[82] Vgl. Kalodner, BlockSci 0.5.0 documentation, 2020.
[83] Vgl. Kalodner, Goldfeder, Chator, Möser, & Narayanan, 2017, S. 2ff.

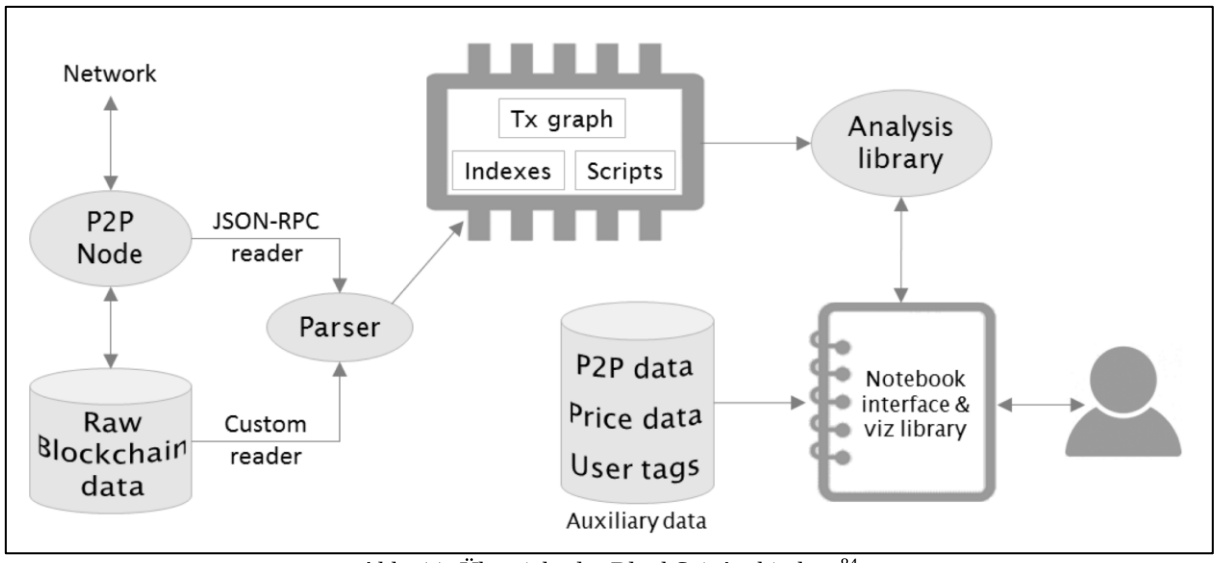

Abb. 11: Übersicht der BlockSci-Architektur[84]

3.1.1.2 Datenbeschaffung mittels API

Die Aufwendungen, die im Zusammenhang mit dem Betreiben eines Full-Nodes und BlockSci stehen, können auch umgangen werden, indem eine Web-API für die Datenabfragen konsumiert wird. Ein großer Vorteil gegenüber eines Full-Nodes ist, dass die Hardwareanforderungen des eigenen Computers beim Konsumieren einer API geringgehalten werden können. Auf einem Full-Node ist immer die ganze Blockchain gespeichert, welche höchstwahrscheinlich auch einige Daten beinhaltet, die nicht abgefragt werden. Ein Nachteil einer Online-API kann die Komplexität bei Datenanalysen sein, da viele Abfragen unter Umständen separat abgesetzt werden müssen. Datenaggregation kann sich zudem als schwierig erweisen, wenn der API-Anbieter dies nicht im Vorhinein vorsieht. Ferner kommt hinzu, dass die meisten API-Anbieter ihre Dienste kostenpflichtig zur Verfügung stellen oder nur eine limitierte Anzahl an Zugriffen innerhalb einer gewissen Zeitspanne kostenlos erlauben. Hierbei darf nicht außer Acht gelassen werden, dass die returnierten Datenstrukturen, wie beispielsweise jene von Blöcken oder Transaktionen, in der Hand des API-Anbieters liegen und nicht die Blockchain-Daten spiegelbildlich übernehmen müssen. Letzteres ist kein Nachteil, da die Anbieter die Daten für die Kunden zur weiteren Verarbeitung meist sehr gut aufbereiten. Jedoch kann der Anbieter das Format der aufbereiteten Datenstruktur frei bestimmen und somit können auch die Formate zwischen verschiedenen Anbietern unterschiedlich ausfallen, was zu einem Mehraufwand bei einer weiteren Datenverarbeitung führen kann.

[84] Quelle: Kalodner, Goldfeder, Chator, Möser, & Narayanan, 2017, S. 2.

3.1.1.3 Beschaffte Datenstrukturen

Die On-Chain-Daten wurden mittels BlockSci, wie in Kapitel 3.1.1.1 beschrieben, beschafft. Um möglichst viel Spielraum für die Empirie zu bekommen, wurden alle vorhandenen Block- und Transaktionsdaten innerhalb der Bitcoin-Blockchain erhoben. Nachfolgende Tabellen zeigen die gewonnenen Datenstrukturen als Basis für die weitere Verarbeitung. Tabelle 1 zeigt die Blockdaten und Tabelle 2 die Transaktionsdaten mit der zugehörigen Einheit jeweils in eckiger Klammer.

On-Chain-Blockdaten
Zeitstempel [Unix-Zeitstempel]
Block Höhe [Zahl]
Version [Zahl]
Nbits [Zahl]
Größe [Byte]
Miner Name [String]
Miner Gewinn [Satoshi]

Tabelle 1: Datenstruktur der beschafften Blockdaten[85]

On-Chain-Transaktionsdaten
Zeitstempel [Unix-Zeitstempel]
Ist Coinbase Transaktion [Boolean]
Block Höhe [Zahl]
Größe [Byte]
Gebühr [Satoshi]
Anzahl Inputs [Zahl]
Menge Input [Satoshi]
Anzahl Outputs [Zahl]
Menge Output [Satoshi]
Wechselgeld/Change [Satoshi]

Tabelle 2: Datenstruktur der beschafften Transaktionsdaten[86]

[85] Quelle: Verfasser.
[86] Quelle: Verfasser.

3.1.2 Off-Chain-Daten

Im Gegensatz zu den On-Chain-Daten können die Off-Chain-Daten ausschließlich mithilfe von Dritten ermittelt werden. Diese Dritte sind hauptsächlich Kryptobörsen, können jedoch auch andere Unternehmen oder Personen sein. In der Regel werden die Daten ebenfalls über (kostenpflichtige) APIs oder Dateidownloads bereitgestellt. Kryptobörsen bieten Preisdaten an, um das Angebot und die Reichweite ihrer Börse zu erhöhen. Jedoch werden meist nur aktuelle Daten in der für diese Arbeit erforderlichen Granularität angeboten. Stündliche oder noch genauere Daten der vergangenen Jahre sind schwer zu erhalten. Die Website kaggle.com bietet unter der URL https://www.kaggle.com/mczielinski/bitcoin-historical-data minütliche USD-Preisdaten von Bitcoin der Kryptobörse Bitstamp seit 01.01.2012 an, welche für die Datenaggregation und Analyse dieser Arbeit herangezogen wurden. Die erhaltene Datenstruktur wird in Tabelle 3 veranschaulicht.

Off-Chain-Preisdaten
Zeitstempel [Unix-Zeitstempel] Preis [USD]

Tabelle 3: Datenstruktur der beschafften Preisdaten[87]

3.2 Datenaggregation

Durch die Datenbeschaffung wurden insgesamt Daten für rund 574 Tsd. Blöcke mit 408 Mio. Transaktionen und 4 Mio. zugehörigen Preisdaten ermittelt. Die Preisdaten stammen von einer anderen Datenquelle als die Blockchaindaten. Daher ist es abgesehen vom Bedürfnis der Komprimierung der Datenmengen umso mehr notwendig die Daten zu aggregieren. Für die Aggregation bedarf es einer beidseitig vorkommenden Eigenschaft, mit welcher die On-Chain-Daten mit den Off-Chain-Preisdaten in Verbindung gebracht werden können. Dafür eignet sich ausschließlich der Zeitstempel. Zu beachten ist hierbei eine Limitierung des On-Chain-Zeitstempels, welche im Kapitel „3.2.1.1 Zeitraum“ näher erläutert wird. Die Preise sind insbesondere wichtig im Zusammenhang mit den Transaktionen. Daher können die Blockdaten in Bezug auf die Preisdaten für die Aggregation außer Acht gelassen werden. Die beschafften Datenstrukturen wurden im Vorkapitel bereits tabellarisch visualisiert. Bei der Datenaggregation ist es wichtig, dass der Informationsgehalt der Einzeldaten nicht zu stark verwässert wird und möglichst viel Aussagekraft weiterhin behalten bleibt. Nachfolgende

[87] Quelle: Verfasser.

Tabelle zeigt das aggregierte Datenformat mit den Einheiten in eckiger Klammer. Die Tabelle kategorisiert die aggregierten Werte nach ihrer Herkunft in Gesamt-, On-Chain- und Off-Chain-Daten. In den folgenden Unterkapiteln wird genauer auf die einzelnen Aggregationswerte eingegangen, um deren Wahl und Eigenschaften zu diskutieren.

	Aggregierte Daten
Gesamt	Zeitraum [Startzeit und Endzeit in UTC: 30-Minuten-Intervall]
On-Chain	Kumulierte Menge mit Coinbase [Bitcoin] Kumulierte Menge ohne Coinbase [Bitcoin] Anzahl an Blöcken [Zahl] Anzahl Transaktionen [Zahl] Anzahl Transaktionen je Block [Zahl] Durchschnittliche Transaktionsgröße [Byte] Durchschnittliche Gebühr [Bitcoin] Durchschnittliche Anzahl an Inputs [Zahl] Durchschnittliche Anzahl an Outputs [Zahl] Durchschnittliche Menge an Inputs [Bitcoin] Durchschnittliche Menge an Outputs [Bitcoin]
Off-Chain	OHLC Preise [USD] Rendite zum vorherigen Zeitraum [%] Volatilität zum vorherigen Zeitraum [%]

Tabelle 4: Aggregierte Datenstruktur[88]

3.2.1 Aggregationswerte

Dieses Kapitel beschreibt die einzelnen Aggregationswerte der ermittelten und aggregierten Datenstruktur von der obigen Tabelle.

3.2.1.1 Zeitraum

Um 408 Millionen Transaktionsdaten besser analysieren zu können, ist es notwendig Transaktionen innerhalb eines bestimmten Zeitfensters oder Zeitraums zusammenzufassen.

[88] Quelle: Verfasser.

Nachdem der UTC-Zeitstempel der Transaktionsdaten und der Preisdaten in Millisekunden angegeben ist, und nur die wenigsten Daten daher zusammenfallen, ist eine Aggregation die beste Lösung.

Eine wichtige Einschränkung gibt es beim Zeitstempel der Bitcoin Transaktionen. Wie im Kapitel „2.3.3.2 Transaktionen“ hervorgeht, besitzt die Transaktion selbst in der Blockchain keinen Zeitstempel. Daher muss der Zeitstempel des Blocks, für alle ihm zugeordneten Transaktionen, verwendet werden. Dieser kann jedoch selbst eine inhärente Ungenauigkeit mit sich bringen. Ein Zeitstempel eines neuen Blocks wird als gültig angesehen, wenn (1) der Zeitstempel größer ist als der Median der Zeitstempel der vorherigen 11 Blöcke und (2) der Zeitstempel abzüglich 2 Stunden kleiner ist als die Netzwerkzeit der Bitcoin Blockchain. Die Netzwerkzeit eines Bitcoin-Nodes ist definiert als der Median aller zurückgegebenen Zeitstempel der verbundenen Nodes. Jeder Node führt seine eigene Bitcoin-Zeit abhängig von seiner eigenen lokalen Systemzeit. Die Bitcoin-Zeit darf dabei nicht mehr als 70 Minuten von der lokalen Systemzeit des Nodes abweichen. Weiters beschreibt Szalachowski, dass aufgrund des genannten Algorithmus die Genauigkeit des Block-Zeitstempels nur auf Stunden genau geschätzt werden kann.[89]

Aufgrund dieser Umstände ist es möglich, dass ein später hinzugefügter Block in der Blockchain einen früheren Zeitstempel hat, als sein Vorgängerblock. Ein konkretes Beispiel dafür sind die Blöcke mit der Höhe 217.310 und 217.311. Der Block 217.310 wurde laut Bitcoin-Blockchain am 20.01.2013 um 18:34 hinzugefügt und der Folgeblock der Höhe 217.311 zwei Minuten vorher um 18:32.[90] Auch wenn in der Regel die Zeitstempel der Blöcke auch der hinzugefügten Reihe entsprechen, sollte diese Ungenauigkeit im Hinterkopf behalten werden. Da sich nur der Zeitstempel als einzig möglicher Aggregationswert für On- und Off-Chain-Daten eignet, muss dieser auch trotz dieser Ungenauigkeit beibehalten werden.

Ein Aggregationszeitraum von 30 Minuten wurde gewählt, um eine möglichst geringe Zeitspanne für die Datenmengen zu haben. Größere Zeiträume könnten die Daten verwässern und kürzere Zeiträume wären aufgrund der angesprochenen Ungenauigkeit sowie Blockschürfzeit von jeweils rund 10 Minuten zu granular. Ein Aggregationszeitraum bis zu einer Stunde wäre aber ebenso zu vertreten.

[89] Vgl. Szalachowski, 2018, S. 1f.
[90] Dies kann im Block-Explorer der Website https://www.blockchain.com verifiziert werden.

3.2.1.2 Kumulierte Menge mit und ohne Coinbase

Die kumulierte Menge an transferierten Bitcoins innerhalb eines Zeitraums wird in zwei verschiedenen Formen angegeben, nämlich mit und ohne Coinbase-Transaktionen. Als Coinbase-Transaktion wird jene Transaktion mit neu geschaffenen Bitcoins bezeichnet, die den Miner eines neuen Blocks zugutekommt. Da es sich hierbei nicht um eine herkömmliche Überweisung zwischen zwei Personen handelt, berücksichtigt der Wert „Kumulierte Menge ohne Coinbase" diese Transaktionen nicht. Weiters sind die kumulierten Transaktionsmengen um das Wechselgeld bereinigt, welches die meisten Transaktionen mit sich führen. Wie in der Theorie erläutert, überweist eine jede Transaktion als Input immer den vollen Betrag, der in der Vergangenheit als Output empfangen wurde. Da diese noch nicht ausgegebenen Outputs (UTXOs) vollständig ausgegeben werden müssen, wird der Differenzbetrag als Wechselgeld (Change) in einer neuen Transaktion an sich selbst zurücküberwiesen. BlockSci verwendet für diese Wechselgeld-Erkennung zwei wesentliche Adressen-Verlinkung-Heuristiken, wie (1) Adressen, die als Inputs in derselben Transaktion verwendet werden, derselben Entität zugehören und (2) Wechselgeld-Adressen nicht weiterverwendet werden[91].

3.2.1.3 Anzahl an Blöcken, Transaktionen und Transaktionen je Block

Die Anzahl an Blöcken gibt an, wie viele Blöcke innerhalb eines Zeitraums gefunden wurden. Respektive gibt die Anzahl an Transaktionen an, wie viele Transaktionen in den Blöcken eines Zeitraums stattgefunden haben. Die Anzahl an Transaktionen je Block gibt die durchschnittliche Anzahl an stattgefundenen Transaktionen eines jeden Blocks innerhalb eines Zeitraumes an.

3.2.1.4 Durchschnittliche Transaktionsgröße

Jede Information, die in der Blockchain abgespeichert wird, erfordert einen bestimmten Speicherbedarf, so auch die Transaktion. Die durchschnittliche Transaktionsgröße gibt Auskunft, wie groß im Schnitt eine jede Transaktion innerhalb eines Zeitraums ist.

3.2.1.5 Durchschnittliche Gebühr

Die durchschnittliche Transaktionsgebühr bezeichnet das arithmetische Mittel der bezahlten Gebühren aller Transaktionen im jeweiligen Zeitraum.

[91] Vgl. Kalodner, Goldfeder, Chator, Möser, & Narayanan, 2017, S. 4.

3.2.1.6 Durchschnittliche Anzahl an Inputs und Outputs

Die zwei Durchschnittswerte, Anzahl an Inputs und Anzahl an Outputs, geben an, wie viele Inputs und Outputs im Mittel je Transaktion eines Zeitraums verwendet wurden. Bis auf die Coinbase-Transaktion besitzt eine jede Transaktionen mindestens eine oder mehrere Input-Adressen und eine oder mehrere Output-Adressen. Da die Coinbase-Transaktion ausschließlich neu geschaffene Bitcoins enthält, besitzt diese Art von Transaktion keinen Input und nur einen Output. Weiters ist zu beachten, dass es meistens mindestens zwei oder mehrere Output-Adressen in normalen Transaktionen gibt. Grund ist das Wechselgeld, denn in der Regel wird nicht der gesamte UTXO an eine andere Adresse überwiesen. Der Rest- oder Differenzbetrag wird daher grundsätzlich an sich selbst zurücküberwiesen.

3.2.1.7 Durchschnittliche Menge an Inputs und Outputs

Die durchschnittliche Menge an Inputs und Outputs ist jene Menge an Bitcoins, die im Schnitt in den Inputs und Outputs je Transaktion im jeweiligen Zeitraum transferiert werden. Diese Mengen sind nicht um das Wechselgeld oder die Coinbase-Transaktion bereinigt, sondern sind die absoluten Mengen, die überwiesen und zurücküberwiesen werden. Die durchschnittliche Menge an Outputs muss daher stets größer sein als die zugehörige Menge an Inputs.

3.2.1.8 OHLC Preise

Die OHLC-Preise sind die ermittelten Eröffnungs-, Höchst-, Kleinst- und Schlusskurse eines jeden Zeitraums.

3.2.1.9 Rendite

Die Rendite wird als Preisänderung des Schlusspreises (engl. Close Price) zum vorherigen Vergleichszeitraum berechnet. Die Berechnung der Rendite erfolgt auf Basis der Formel für die logarithmierte Rendite. Nähere Details dazu können im Kapitel „3.5.13 Logarithmierte Rendite“ nachgelesen werden.

3.2.2 Technische Umsetzung

Die technische Umsetzung der Datenaggregation erfolgte mittels einer C#-Eigenentwicklung im .NET-Core-Framework. Der Programmcode ist auf der Plattform GitHub hinterlegt und kann unter folgender URL abgerufen werden: https://github.com/lukasw93/mt-bitcoin-code.

3.3 Dateneingrenzung

Die Bitcoin-Blockchain startete mit dem Genesisblock am 3. Januar 2009. Seit jeher wird etwa alle 10 Minuten ein neuer Block mit den dazugehörigen Transaktionen der Blockchain hinzugefügt. Zur Startzeit war Bitcoin jedoch weitgehend unbekannt und die Verwendung von Bitcoin stieg erst im Laufe der Jahre an. Um aussagekräftige Analysen zu erhalten, kann folglich nicht mit dem Startzeitpunkt des Bitcoin-Netzwerks begonnen werden und es muss ein passender Startzeitpunkt ermittelt werden. Folgende Abbildung zeigt die durchschnittliche Anzahl an Transaktionen pro Sekunde im jeweiligen Jahr. Zu beachten ist, dass es keine kompletten Jahreswerte für die erhobenen Daten von 2009 und 2019 gibt. Die Transaktionen pro Sekunde für diese zwei Jahre wurde daher hochgerechnet, um vergleichbare Jahreswerte zu erhalten. Der Endzeitpunkt für die Analyse wurde für diese Arbeit mit 01.05.2019 0 Uhr festgelegt.

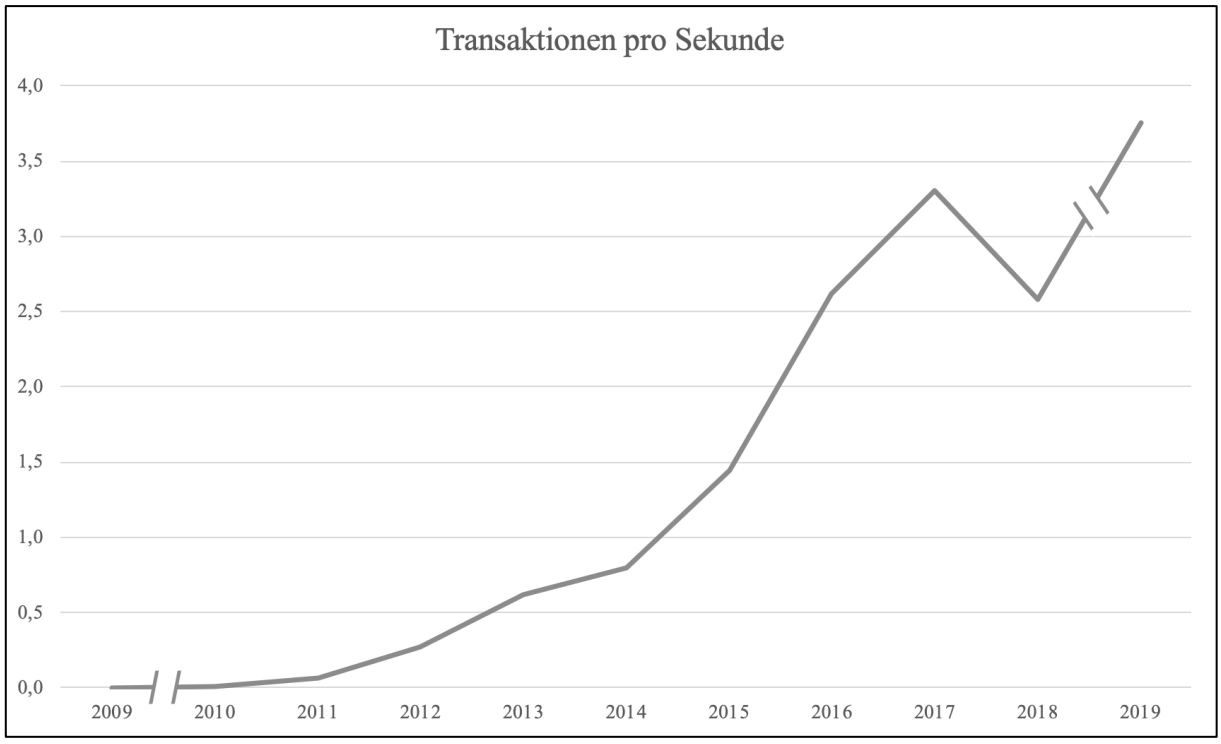

Abb. 12: Bitcoin-Transaktionen pro Sekunde[92]

Die Grafik zeigt, dass kaum Transaktionen in den Jahren 2009 bis 2011 durchgeführt wurden. Jedes Jahr, bis auf 2018, wurden mehr Transaktionen durchgeführt als im Vorjahr. Nachfolgende Tabelle zeigt die konkreten Werte sowie die Steigerungsraten in Prozent für die obige Abbildung. Die Steigerungen von über 100 % der Jahre 2010 bis 2013 können als die

[92] Quelle: Verfasser.

Startjahre des Blockchain-Netzwerks interpretiert werden. Das Minimum an Transaktionen pro Sekunde beträgt 0,00167 Transaktionen pro Sekunde, was eine Transaktion alle 10 Minuten oder je Block bedeutet. Das ist die Coinbase-Transaktion, welche im Jahr 2009 fast ausschließlich stattgefunden hat. Ab 2013 gab es im Schnitt mehr als eine Transaktion alle 2 Sekunden, was rund 310 Transaktionen pro Block entspricht. 2015 gab es im Schnitt erstmals mehr als eine Transaktion pro Sekunde. Im Jahr 2019 sind bis Anfang Mai 3,76 Transaktionen pro Sekunde durchgeführt worden. Hochgerechnet auf das Jahr 2019 entspricht das dem Höhepunkt. 2018 ist das einzige Jahr in der Liste, das einen Rückgang der Transaktionen pro Sekunde zu verzeichnen hat. Dies kann auf den Bitcoin-Hype im Jahr 2017 und das anschließende Platzen der Preisblase zurückzuführen sein.

JAHR	TRANSAKTIONEN PRO SEKUNDE	STEIGERUNG IN PROZENT ZUM VORJAHR
2009[93]	0,001	n/a
2010	0,006	462%
2011	0,060	926%
2012	0,268	344%
2013	0,623	132%
2014	0,801	29%
2015	1,448	81%
2016	2,620	81%
2017	3,300	26%
2018	2,581	-22%
2019[94]	3,757	46%

Tabelle 5: Transaktionen pro Sekunde und jährliche Steigerungsraten[95]

Nach dieser Verwendungsanalyse werden die Startjahre von 2009 bis einschließlich 2012 für die weitergehenden Analysen nicht berücksichtigt, da diese signifikant weniger Transaktionen aufweisen als die Folgejahre. Der Zeitraum von 01.01.2013 0 Uhr bis 01.05.2019 0 Uhr wird daher für die weiteren Analysen definiert. Die aggregierten Daten beinhalten somit 359.428 Blöcke und 397.582.622 Transaktionen (inklusive Coinbase-Transaktionen). Diese Daten sind auf 110.928 30-Minuten-Zeiträume aggregiert.

[93] Ab 03.01.2009 19:15 Uhr. Das entspricht dem Genesisblock, siehe https://www.blockchain.com.
[94] Bis 01.05.2019 00:00 Uhr. Dieser Zeitpunkt entspricht dem Ende der Datenerhebung der vorliegenden Arbeit.
[95] Quelle: Verfasser.

3.4 Datenadaption

Von den ermittelten Zeiträumen des Vorkapitels „3.3 Dateneingrenzung“ sind 4.446 Zeiträume ohne gefundenen Block. Weitere 836 Zeiträume sind ohne Preisinformation. Von diesen 836 Zeiträumen sind 45 ohne Blockinformation. Nachfolgende Tabelle veranschaulicht die jährlichen Zahlen der fehlenden Daten. Der Median für Zeiträume ohne Block liegt bei 718 und der Median für Zeiträume ohne Preisinformation liegt bei 7. Das Jahr 2019 wurde für diese Median-Berechnung nicht berücksichtigt, da es sich um kein volles Jahr handelt. Es ist gut zu sehen, dass Zeiträume ohne Block jedes Jahr in etwa gleich oft vorkommen, Zeiträume ohne Preisinformation hingegen haben mit den Jahren 2013 und 2015 starke Ausreißer. Die nächsten zwei Unterkapitel gehen näher darauf ein, wie mit den unvollständigen Daten umgegangen wird.

Jahr	***Zeiträume ohne Block***	***Zeiträume ohne Preisinformation***
2013	518	603
2014	613	11
2015	715	216
2016	807	3
2017	721	1
2018	786	1
2019[96]	286	1
Summe	**4446**	**836**

Tabelle 6: Unvollständige Zeitraumdaten[97]

3.4.1 Zeiträume ohne Preisinformation

Wenn ein Zeitraum ohne Preisinformation auftritt, kann das auf eine unvollständige Datenbasis hindeuten oder darauf, dass in diesem Zeitraum auf der hier untersuchten Kryptobörse Bitstamp kein Handel stattgefunden hat. Die Preisdaten der Jahre 2016 bis 2019 sind beinahe vollständig, hingegen weisen die Jahre 2013 und 2015 mehrere Lücken auf. Daher beziehen sich etwaige Preisanalysen auf das Zeitfenster von 01.01.2016 bis 01.05.2019. In dieser Zeitspanne fehlen aggregiert sechs einzelne Preisinformationen. Diese fehlenden Preise werden mit dem Preis des Vorgängerzeitraums fortgeschrieben. Da es sich hierbei um einige wenige Fortschreibungen handelt, kann diese Adaption ohne Bedenken durchgeführt werden und es bleibt keine Datenlücke für die empirische Untersuchung ausständig.

[96] Daten von 01.01.2019 bis 01.05.2019 0 Uhr.
[97] Quelle: Verfasser.

3.4.2 Zeiträume ohne Block

Bei einem Zeitraum ohne Block wurde im jeweils untersuchten Zeitraum kein Block der Blockchain hinzugefügt. 4,01 Prozent der Zeiträume von Januar 2013 bis Mai 2019 besitzen keine Blockinformation. Normalerweise sollten solche Datenlücken bei 30-Minuten-Zeiträumen nicht existieren, da im Schnitt laut Bitcoin-Algorithmus alle 10 Minuten ein neuer Block gefunden werden soll. Ein Beispiel hierfür wäre der Zeitraum am 01.01.2019 von 09:33 bis 10:03. In diesem Zeitraum wurde kein Block der Blockchain hinzugefügt. Der Block mit der Höhe 556.509 wurde an diesem Tag um 09:25 hinzugefügt und sein Folgeblock der Höhe 556.510 um 10:12.[98] Solche Datenlücken können auftreten, weil entweder Miner tatsächlich länger benötigen, um einen neuen Block zu finden, oder die Zeiteinstellungen der Miner, wie im Kapitel „3.2.1.1 Zeitraum“ beschrieben, so voneinander abweichen, dass die UTC-Zeitstempel aufeinanderfolgender Blöcke mehr als 30 Minuten auseinanderfallen. Im Worst-Case-Szenario gehen diese Blockinformationen zwar nicht verloren, werden aber einem vorhergehenden oder nachfolgenden Zeitraum zugerechnet. Dieser Unschärfe könnte nur entgegengewirkt werden, indem die Blöcke unabhängig vom Zeitstempel der Reihe nach gruppiert werden. Somit wäre es jedoch unmöglich weitere Daten, wie beispielsweise Preisinformationen einer anderen Datenquelle, in die Untersuchung miteinzubeziehen. Für die vorliegende Arbeit werden folglich die Zeiträume ohne Block von den Grunddaten entfernt. Somit gibt es zwar Datenlücken in Betracht auf die Zeiträume, nichtsdestotrotz werden weiterhin alle Transaktionsdaten der Blockchain berücksichtigt. Nach dieser Datenbereinigung bleiben Daten in Summe von 106.482 Zeiträumen für die Empirie erhalten.

3.5 Datenbeschreibung

Dieses Kapitel dient der deskriptiven Datenbeschreibung der ermittelten Blockchain- und Preisdaten. Die Blockchain-Daten wurden direkt aus der Bitcoin-Blockchain mittels BlockSci, einer Analysesoftware für Blockchains, extrahiert. Historische Preisdaten der Bitstamp-Kryptobörse wurden von der Website www.kaggle.com bezogen. Die Vorkapitel Datenaggregation, Dateneingrenzung und Datenadaption beschreiben die vorgenommene Datenaufbereitung der beschafften Daten und erklären zeitliche Eingrenzungen. Somit kann festgehalten werden, dass die aggregierten Daten im Zeitraum vom 01.01.2013 0 Uhr bis 01.05.2019 0 Uhr analysiert werden und Preisdaten im Subzeitraum vom 01.01.2016 0 Uhr bis 01.05.2019 0 Uhr betrachtet werden. Alle stattgefundenen Transaktionen in den genannten Zeitspannen werden in jeweils 30-Minuten-Zeiträumen unterteilt. Zeiträume, in denen keine

[98] Blockdetails können im Bitcoin-Explorer unter https://www.blockchain.com nachgeschlagen werden.

Transaktionen stattgefunden haben, werden nicht in die Analyse miteinbezogen und können daher die Empirie nicht verfälschen. Schlussendlich wurden Daten für 106.482 Zeiträume für die empirische Analyse beschafft. Nachdem die Preisdaten ab 2016 verwendet werden, beziehen diese sich auf 55.768 30-Minuten-Zeiträume. Dieses Kapitel beschreibt die einzelnen aggregierten Daten aus dem Kapitel „3.2.1 Aggregationswerte“ mithilfe der deskriptiven Statistik zur besseren Veranschaulichung.

3.5.1 Kumulierte Menge mit Coinbase

Die kumulierte Menge mit Coinbase bezieht sich auf die gesamte Anzahl an transferierten Bitcoins von einer Adresse zur anderen. Dieser Betrag ist bereits um das Wechselgeld bereinigt, sodass, wie bei einer herkömmlichen Banküberweisung, nur jene Menge gezählt wird, die wirklich den Besitzer wechselt. Der Mittelwert je Zeitraum beläuft sich auf rund 24.000 Bitcoins und ist vom Median mit rund 17.000 etwas entfernt. Der Minimum-Wert beläuft sich auf 12,5 Bitcoins und entspricht exakt der Block-Belohnung (Coinbase-Transaktion) für den Miner. Somit gab es unter allen untersuchten Zeiträumen zumindest einen Zeitraum, indem keine Transaktion von einer Adresse zur anderen stattgefunden hat. Die höchste Menge an Bitcoins in Höhe von über 1,95 Mio. Bitcoins ist im Vergleich zum Mittel exorbitant hoch. 50 Prozent der Mengen befinden sich zwischen 9.463 und 29.888 Bitcoins je Zeitraum.

Kumulierte Menge mit Coinbase	
Mittelwert	24.047,06
Standardabweichung	29.065,05
Min	12,50
Max	1.951.558,32
Median	17.047,82
25%-Quantil	9.463,16
75%-Quantil	29.888,28

Tabelle 7: Kumulierte Menge mit Coinbase[99]

3.5.2 Kumulierte Menge ohne Coinbase

Wie auch die kumulierte Menge mit Coinbase, bezieht sich die kumulierte Menge ohne Coinbase auf die transferierten Bitcoins wechselgeldbereinigt von einer Adresse zur anderen. Nachdem sich die Werte nur um die Coinbase-Transaktionen unterscheiden, also jene Menge

[99] Quelle: Verfasser.

an neu geschaffenen Bitcoins pro Block und somit auch je Zeitraum, liefert die deskriptive Auswertung ähnliche Ergebnisse. Der Minimalwert wird mit 0 angegeben. Das bedeutet, dass es zumindest einen Zeitraum gegeben hat, in dem keine einzige Transaktion stattgefunden hat. Die deskriptiven Werte sind zwar nahezu identisch, dennoch liefert die kumulierte Menge ohne Coinbase aussagekräftigere Daten, da wirklich nur Transaktionen berücksichtigt werden, in denen Bitcoins den Besitzer wechseln. Es kann jedoch davon ausgegangen werden, dass sich die Mengen mit und ohne Coinbase in der Zukunft noch weiter annähern, da die Block-Belohnung für Miner alle 4 Jahre durch das im Bitcoin-Protokoll vorgesehene *Halving* halbiert werden[100].

Kumulierte Menge ohne Coinbase	
Mittelwert	23.979,07
Standardabweichung	29.063,63
Min	0,00
Max	1.951.432,37
Median	16.980,76
25%-Quantil	9.394,34
75%-Quantil	29.821,50

Tabelle 8: Kumulierte Menge ohne Coinbase[101]

3.5.3 Anzahl an Blöcken

Die Anzahl an Blöcken gibt an, wie viele Blöcke je Zeitraum gefunden wurden. Im Mittel beläuft sich das auf 3,38 Blöcke je Zeitraum. Der Median zeigt exakt die zu erwartende Anzahl laut Protokoll an: 1 Block alle 10 Minuten. 50 % aller Daten befinden sich zwischen 2 und 4 Blöcken je Zeitraum. Die Datenbasis wirkt somit solide. Der Maximalwert an 15 Blöcken je 30-Minuten-Zeitraum ist ein extrem hoher Ausreißer für das Bitcoin-Protokoll. Wichtig zu erwähnen ist, dass Zeiträume ohne Block aus der Datenbasis entfernt wurden (siehe Kapitel „3.4 Datenadaption“), ansonsten läge der Minimalwert bei 0. Dasselbe gilt für die Anzahl an Transaktionen.

[100] Vgl. Bariviera, Basgall, Hasperué, & Naiouf, 2017, S. 84.
[101] Quelle: Verfasser.

Anzahl an Blöcken	
Mittelwert	3,38
Standardabweichung	1,72
Min	1,00
Max	15,00
Median	3,00
25%-Quantil	2,00
75%-Quantil	4,00

Tabelle 9: Anzahl an Blöcken[102]

3.5.4 Anzahl an Transaktionen

Die Anzahl an Transaktionen gibt die stattgefundenen Transaktionen je Zeitraum an. Der Mittelwert beläuft sich im Schnitt auf rund 3.700 Transaktionen alle 30 Minuten. Am Minimalwert ist zu sehen, dass diese Werte inklusive Coinbase-Transaktion sind. Die Spannweite der Daten ist sehr groß. 50 % der abgesetzten Transaktionen sind zwischen 1.500 und 5.215 Transaktionen je Zeitraum.

Anzahl an Transaktionen	
Mittelwert	3.733,80
Standardabweichung	2.897,91
Min	1,00
Max	26.228,00
Median	2.840,00
25%-Quantil	1.500,00
75%-Quantil	5.215,00

Tabelle 10: Anzahl an Transaktionen[103]

3.5.5 Anzahl an Transaktionen je Block

Die Anzahl an Transaktionen je Block bringt die Anzahl an Transaktionen im untersuchten Zeitraum in Verbindung mit der Anzahl an Blöcken je Zeitraum. Durch die Coinbase-Transaktion muss mindestens eine Transaktion je Block stattfinden. Im Mittel finden 1.254 Transaktionen je Block statt. Der Maximalwert ist hier ebenfalls ein starker Ausreißer.

[102] Quelle: Verfasser.
[103] Quelle: Verfasser.

Anzahl an Transaktionen je Block	
Mittelwert	1.254,49
Standardabweichung	835,19
Min	1,00
Max	5.257,00
Median	1.095,80
25%-Quantil	486,67
75%-Quantil	1.973,00

Tabelle 11: Anzahl an Transaktionen je Block[104]

3.5.6 Durchschnittliche Transaktionsgröße

Die durchschnittliche Transaktionsgröße bezieht sich auf die Größe in Bytes der Transaktions-Datenstruktur innerhalb der Blockchain. Der Mittelwert beläuft sich auf rund 550 Bytes und der Median ist mit 506 Bytes ebenfalls nahe. Der Minimalwert beträgt 107 Bytes. Hingegen ist der Maximalwert mit fast 500.000 Bytes im Vergleich extrem weit entfernt und bezieht sich auf eine Transaktion im Block mit der Höhe 364.292. Dieser Block hat neben der Coinbase-Transaktion eine weitere Transaktion welche 5.569 Inputs verwendet und somit riesengroß ist. Diese Transaktion selbst ist bereits 999.657 Bytes groß und kommt zusammen mit der Coinbase-Transaktion im genannten und einzigen Block in diesem Zeitraum auf 999.842 Bytes. Dividiert durch die Anzahl von 2 Transaktionen in diesem Zeitraum kommt der Maximalwert von 499.921 Bytes zustande. In der Regel ist jedoch eine Transaktion laut dem Interquartilsabstand zwischen 447 und 590 Bytes groß.

Durchschnittliche Transaktionsgröße in Bytes	
Mittelwert	551,96
Standardabweichung	1.543,26
Min	107,00
Max	499.921,00
Median	506,93
25%-Quantil	447,59
75%-Quantil	589,37

Tabelle 12: Durchschnittliche Transaktionsgröße in Bytes[105]

[104] Quelle: Verfasser.
[105] Quelle: Verfasser.

3.5.7 Durchschnittliche Gebühr

Die durchschnittliche Gebühr einer Transaktion beläuft sich im Mittel auf 0,00044404 Bitcoin beziehungsweise 44.404 Satoshi. Der Median von 22.122 Satoshi ist in etwa die Hälfte des Mittelwerts. Die geringste Gebühr war 0 Satoshi und die Höchste lag bei rund 0,34 Bitcoin.

Durchschnittliche Gebühr in Bitcoin	
Mittelwert	0,00044404
Standardabweichung	0,00137184
Min	0,00
Max	0,34285274
Median	0,00022122
25%-Quantil	0,00015426
75%-Quantil	0,00053479

Tabelle 13: Durchschnittliche Gebühr in Bitcoins[106]

3.5.8 Durchschnittliche Anzahl an Inputs

Der Mittelwert und der Median sind bei der durchschnittlichen Anzahl an Inputs sehr ähnlich. Rund 2,5 Inputs werden in einer jeden Transaktion verwendet. Der Maximalwert mit 2.784 Inputs bezieht sich auf dieselbe Transaktion, die ebenfalls für das Maximum für die durchschnittliche Transaktionsgröße verantwortlich ist. Der Minimalwert von 0 kommt bei Blöcken zustande, die ausschließlich die Coinbase-Transaktion beinhalten.

Durchschnittliche Anzahl an Inputs	
Mittelwert	2,64
Standardabweichung	8,60
Min	0,00
Max	2.784,50
Median	2,41
25%-Quantil	2,07
75%-Quantil	2,85

Tabelle 14: Durchschnittliche Anzahl an Inputs[107]

[106] Quelle: Verfasser.
[107] Quelle: Verfasser.

3.5.9 Durchschnittliche Anzahl an Outputs

Eine jede Transaktion hat zumindest einen Output. Daher liegt der Minimalwert bei 1. Im Schnitt werden rund 2,5 Outputs in einer Transaktion verwendet. Die Wechselgeldadresse ist hierbei inkludiert. Folglich besitzen die meisten Transaktionen zumindest 2 Outputs. Der Maximalwert von 130 Outputs wurde im Block der Höhe 407.355 erzielt. Hierbei handelt es sich um eine Coinbase-Transaktion, welche die neu geschaffenen Bitcoins an 130 Adressen ausbezahlte. Dies war die einzige Transaktion dieses Blocks.

Durchschnittliche Anzahl an Outputs	
Mittelwert	2,80
Standardabweichung	1,46
Min	1,00
Max	130,00
Median	2,49
25%-Quantil	2,29
75%-Quantil	2,83

Tabelle 15: Durchschnittliche Anzahl an Outputs[108]

3.5.10 Durchschnittliche Menge an Inputs

Die durchschnittliche Menge an Inputs zeigt an, wie viele Bitcoins im Schnitt je Transaktion übertragen werden. Das Wechselgeld wird in den Inputs nicht näher berücksichtigt und ist somit nicht herausgerechnet. Der Mittelwert beträgt rund 12 Bitcoins je Transaktion, der Median 8,5 Bitcoins. 50 % aller Transaktionen liegen im Rahmen von 5,48 und 13,22 Bitcoins. Das Maximum an übertragenen Bitcoins im Schnitt je Transaktion beläuft sich auf 2.365 Bitcoins. Dieser Höchstwert wurde im Block der Höhe 394.745 erzielt. Hierbei wurden rund 5,7 Mio. Bitcoins in 2.406 Transaktionen übertragen.

[108] Quelle: Verfasser.

Durchschnittliche Menge an Inputs	
Mittelwert	11,90
Standardabweichung	22,09
Min	0,00
Max	2.365,35
Median	8,53
25%-Quantil	5,48
75%-Quantil	13,22

Tabelle 16: Durchschnittliche Menge an Inputs[109]

3.5.11 Durchschnittliche Menge an Outputs

Die durchschnittliche Menge an Outputs gibt an, wie viele Bitcoins im Schnitt je Transaktion übertragen werden inklusive der Menge an neugeschaffenen Bitcoins als Belohnung für die Miner. Folglich müssen die ermittelten Durchschnittsdaten gering höher ausfallen, als die durchschnittliche Inputmenge. Würden die Coinbase-Transaktionen nicht berücksichtigt werden, so müssten die durchschnittlichen Output-Mengen gering kleiner ausfallen als die Input-Mengen, denn in der Regel fällt eine Gebühr je Transaktion für den Miner ab. Diese Gebühr berechnet sich durch die Differenz der Input- und Output-Menge.

Durchschnittliche Menge an Outputs	
Mittelwert	11,94
Standardabweichung	22,10
Min	0,17
Max	2.365,36
Median	8,57
25%-Quantil	5,51
75%-Quantil	13,27

Tabelle 17: Durchschnittliche Menge an Outputs[110]

[109] Quelle: Verfasser.
[110] Quelle: Verfasser.

3.5.12 OHLC Preise

Nachfolgende vier Tabellen zeigen die OHLC-Preise in US-Dollar an. Im Gegensatz zu den bisherigen beschriebenen Daten beziehen sich die OHLC-Preisdaten auf den Zeitraum von 01.01.2016 0 Uhr bis 01.05.2019 0 Uhr. Da die dargestellten OHLC-Daten sehr ähnlich zueinander sind, wird nur der Schlusskurs textuell beschrieben. Die hohe Preisschwankung von Bitcoin kann hier sehr gut abgelesen werden. Im Mittel beläuft sich der Preis für einen Bitcoin auf rund 4 Tsd. US-Dollar. Die Standardabweichung mit 3.714 USD ist hingegen hoch. Der Minimalpreis lag Anfang 2016 bei 352 USD, der Höchstpreis dotierte Ende 2017 hingegen bei 19.600 USD. Die untere Grenze des Interquartilsabstands beläuft sich auf 704 USD und die obere Grenze auf 6.448 USD.

Eröffnungskurs (Open)	
Mittelwert	$ 4.026,17
Standardabweichung	$ 3.714,71
Min	$ 354,50
Max	$ 19.616,67
Median	$ 3.435,24
25%-Quantil	$ 704,98
75%-Quantil	$ 6.449,20

Tabelle 18: Eröffnungskurs (Open)[111]

Höchstkurs (High)	
Mittelwert	$ 4.041,75
Standardabweichung	$ 3.734,90
Min	$ 360,62
Max	$ 19.665,76
Median	$ 3.442,37
25%-Quantil	$ 705,82
75%-Quantil	$ 6.462,90

Tabelle 19: Höchstkurs (High)[112]

Niedrigstkurs (Low)	
Mittelwert	$ 4.009,12
Standardabweichung	$ 3.692,36
Min	$ 352,56
Max	$ 19.560,44
Median	$ 3.429,12
25%-Quantil	$ 703,23
75%-Quantil	$ 6.436,62

Tabelle 20: Niedrigstkurs (Low)[113]

Schlusskurs (Close)	
Mittelwert	$ 4.026,10
Standardabweichung	$ 3.714,60
Min	$ 352,56
Max	$ 19.600,01
Median	$ 3.435,05
25%-Quantil	$ 704,94
75%-Quantil	$ 6.448,14

Tabelle 21: Schlusskurs (Close)[114]

[111] Quelle: Verfasser.
[112] Quelle: Verfasser.
[113] Quelle: Verfasser.
[114] Quelle: Verfasser.

3.5.13 Logarithmierte Rendite

Die stetige (logarithmierte) Rendite wird basierend auf den Schlusskurs berechnet. Die Formel der stetigen Rendite r_t setzt sich für einen Zeitraum t aus dem natürlichen Logarithmus des Verhältnisses des Schlusskurses k_t des Zeitraumes t und des Schlusskurses des Vorgängerzeitraumes k_{t-1} zusammen.[115]

$$r_t = \ln (k_t / k_{t-1})$$

Analog zum Schlusskurs je Zeitraum bezieht sich die deskriptive Datenanalyse der stetigen Rendite ebenfalls auf den Zeitraum von 01.01.2016 0 Uhr bis 01.05.2019 0 Uhr. Hierbei handelt es sich um die durchschnittliche Rendite zweier aufeinanderfolgender 30-Minuten-Zeiträume. Der Mittelwert von 0,0045 % und der Median von 0,0053 % zeigen eine kleine positive Rendite je Zeitraum an. Die schlechtesten und besten Renditen sind massive Ausreißer. Der Minimalwert von -16,76 % wurde am 10.03.2017 erreicht und der Höchstwert von 10,65 % am 02.04.2019.

Logarithmierte Rendite	
Mittelwert	0,0045%
Standardabweichung	0,6355%
Min	-16,7641%
Max	10,6478%
Median	0,0053%
25%-Quantil	-0,1772%
75%-Quantil	0,1965%

Tabelle 22: Logarithmierte Rendite[116]

3.6 Rohe Blockdaten

Neben den beschafften und aggregierten Transaktionsdaten liegen der Arbeit noch die rohen Metadaten aller Blöcke zur Verfügung. Beispielhaft zeigt nachfolgende Abbildung die Daten des Blocks der Höhe 214.554. Diese Daten liegen für jeden Block seit Beginn der Bitcoin-Blockchain und bis zum Stichtag dieser Arbeit, den 01.05.2019, vor. Da diese Daten allgemein zugänglich sind und ohne größeren Aufwand extrahiert werden können, werden diese im

[115] Vgl. Eckstein, 2012, S. 370.
[116] Quelle: Verfasser.

Weiteren nicht näher deskriptiv analysiert. Für die vorliegende Arbeit ist vor allem die kumulierte Gebühr aller Transaktionen eines Blocks interessant, welche als „Fee Reward“ in der Abbildung bezeichnet wird. Die Belohnung für den Miner zum Finden eines neuen Blocks wird als „Block Reward“ angeführt und beträgt für dieses Beispiel 25 Bitcoin.

Hash	00000000000000c5939573777a5305b2135b4a4594787ab0772700d1032a4fc0
Confirmations	419,612
Timestamp	2013-01-01 00:00
Height	214554
Miner	Unknown
Number of Transactions	240
Difficulty	2,979,636.62
Merkle root	a36896bc3b9cd2dde66d6f7a646162708884636846781 32edd529f504b7d7c30
Version	0×1
Bits	436,576,619
Weight	485,116 WU
Size	121,279 bytes
Nonce	1,735,147,243
Transaction Volume	4961.67996805 BTC
Block Reward	25.00000000 BTC
Fee Reward	0.19960000 BTC

Abb. 13: Metadaten des Blocks der Höhe 214.554[117]

Das Datenformat der Blockdaten kann in Tabelle 1 im Kapitel „3.1.1.3 Beschaffte Datenstrukturen“ nachgeschlagen werden.

[117] Quelle: https://www.blockchain.com (Abrufdatum: 11.06.2020).

4 Empirie

Ziel der Arbeit ist es ein grundlegendes Verständnis über die Bitcoin-Transaktionen und deren Zusammenhänge mittels quantitativer Analysen zu erarbeiten. Zudem soll geklärt werden, ob inhärente Annahmen und Gesetzmäßigkeiten der Bitcoin-Technologie Gültigkeit besitzen. Dafür werden Hypothesen aufgestellt und mit den ermittelten Daten aus dem Vorkapitel „3 Daten“ belegt oder widerlegt. Die Hypothesen wurden so gewählt, sodass inhärente Eigenschaften, die auch von Interesse für die Zukunft von Bitcoin sind, geprüft werden.

4.1 Hypothesen

Es werden fünf Hypothesen aufgestellt, die die historische Verwendung der Bitcoin-Technologie auf den Prüfstand stellen. Sollten einige dieser Hypothesen abgelehnt werden müssen, so würde Bitcoin nicht nach inhärenten Vorgaben funktionieren und das System müsste stark hinterfragt werden.

- *H1: Die Anzahl der Transaktionen steigt.*

Die erste Hypothese klingt banal und die Transaktionen pro Sekunde konnten bereits grafisch veranschaulicht werden, doch *H1* bildet die Basis für jede weitere Untersuchung. Würde die Steigerung der Anzahl an Transaktionen nicht statistisch signifikant nachweisbar sein, so fände Bitcoin offenbar keine Verwendung in der Öffentlichkeit.

- *H2: Die Transaktionsgebühren ersetzen nach und nach die Block-Belohnung (Coinbase-Transaktion) für den Miner.*

Die Coinbase-Transaktion als Belohnung in Form von neu geschaffenen Bitcoins zum Finden eines neuen Blocks stellt in der Anfangszeit den größten Anreiz für einen Miner dar, um am System teilzunehmen. Diese Belohnung halbiert sich jedoch im Schnitt alle 4 Jahre. Details können im Kapitel „2.3.3.2 Transaktionen“ nachgelesen werden. Die Kosten zum Finden eines neuen Blocks bleiben hingegen annähernd gleich. Die Halbierung der Block-Belohnung bedeutet somit eine dauerhafte Ertragsreduktion für den Miner. Um den Anreiz für das Mining bei gegebener Miner-Anzahl zu erhalten, sollte folglich der Preis für Bitcoin steigen oder der reduzierte Ertrag durch die Transaktionsgebühren ausgeglichen werden. Dies wird im Bitcoin-Whitepaper ebenfalls explizit genannt.[118] Die Historie zeigte, dass Bitcoin kurz- und mittelfristig im Preis extrem schwankt, doch langfristig gesehen müssen die Gebühren die Kosten für den Miner decken, da die Belohnung an neuen Bitcoins gegen 0 strebt. Würde die

[118] Vgl. Nakamoto, 2008, S. 4.

Hypothese *H2* abgelehnt werden, so müsste das gesamte Bitcoin-System infrage gestellt werden.

- *H3: Es werden immer weniger Bitcoins in einer Transaktion verwendet.*

Die regelmäßige Halbierung von neu geschaffenen Bitcoins bedeutet im weiteren Sinne eine Reduktion der inhärenten Inflation. Die maximale Menge an Bitcoins wurde somit durch den Algorithmus bereits zu Beginn festgelegt und wird sich im Jahr 2140 auf 21 Millionen belaufen.[119] Da die meisten Bitcoins zu Anfangszeiten erschafft werden und im Laufe der Zeit mehr Personen das System nutzen sollten, kann von deflatorischen Eigenschaften ausgegangen werden. Folglich sollte der Preis steigen und reale Güter und Dienstleistungen mit immer weniger Bitcoins bezahlt werden können. Sollte *H3* belegt werden können, so sollte das im Sinne des Erschaffers Satoshi Nakamoto sein, der das Belohnungssystem von Bitcoin selbst mit Gold vergleicht[120].

- *H4: Die Transaktionsgebühren sind höher, wenn mehr Transaktionen stattfinden.*

Frei nach Angebot und Nachfrage soll mit dieser Hypothese überprüft werden, ob sich die Bitcoin-Blockchain mit Knappheit ähnlich verhält, wie es eine normale Marktwirtschaft täte. Als knappes Angebotsgut wird hier die maximale Kapazität an Transaktionen pro Block angesehen. Die aufgegebenen Transaktionen stellen die Nachfrage dar. Da die Blockgröße limitiert ist, kann nur eine begrenzte Anzahl an Transaktionen in einen Block aufgenommen werden. So müssten Miner in Zeiten hoher Nachfrage, also vieler gleichzeitig aufgegebenen Transaktionen, jene in einen Block aufnehmen, die eine höhere Gebühr bezahlen.

- *H5: Preisänderungen gehen mit einem höheren Handelsvolumen einher.*

Karpoff (1987) verweist auf einige empirische Studien, die eine positive Korrelation zwischen absoluter Preisänderung und Handelsvolumen bei Aktien und Anleihen nachweisen.[121] Wenn Bitcoin heutzutage als Investitions- oder Spekulationsgut Anwendung finden sollte, so müsste ebenfalls eine positive Korrelation zwischen Preisänderung und Volumen statistisch nachweisbar sein.

4.2 Methode

Die vorgestellten Hypothesen werden basierend auf den ermittelten Daten und der Regressionsanalyse untersucht. Aufgabe der Regressionsanalyse ist es zwei oder mehr

[119] Vgl. Antonopoulos, 2014, S. 2.
[120] Vgl. Nakamoto, 2008, S. 4.
[121] Vgl. Karpoff , 1987, S. 113.

Merkmale auf ihre Abhängigkeit zueinander zu überprüfen und diese durch eine mathematische Funktion, die Regressionsfunktion, auszudrücken. Dabei greift die Regressionsanalyse auf die Methode der kleinsten Quadrate zurück. Ziel ist, eine Form oder Tendenz des abhängigen Merkmals Y (Regressand) durch das unabhängige Merkmal X (Regressor) herleiten zu können. Sollte eine Wechselseitige Abhängigkeit der Merkmale bestehen, so ist die Regressionsanalyse für X und Y durchzuführen.[122]

Wichtig zu erwähnen ist, dass eine Regressionsanalyse ausschließlich den Zusammenhang der Merkmale überprüft, nicht jedoch Auskunft über eine mögliche Kausalität (Ursache-Wirkung-Beziehung) gibt. Wird von einer linearen Regressionsanalyse ausgegangen, die zwei Merkmale untersucht, so kann die Regressionsfunktion wie folgt definiert werden:[123]

$$Y = b_0 + b_1 * X + U$$

Der Regressand Y wird als eine Zufallsgröße betrachtet und versucht durch das erklärende Merkmal X auszudrücken. Dabei ist der Parameter b_0 die Ausgleichskonstante und der Parameter b_1 der Regressionskoeffizient, der die Steigung des Merkmals angibt. Wenn b_0 weggelassen wird, handelt es sich um eine homogene Regression, andernfalls, wie hier dargestellt, um eine inhomogene Regressionsgleichung. Die Variable U ist eine nicht direkt beobachtete Restvariable. Die Variablen b_0 und b_1 sind durch die Regressionsanalyse ermittelte Schätzwerte und sollten möglichst nah am „wahren“ Wert liegen.[124]

Um den Zufall ausschließen zu können, wird ein Hypothesentest auf die Regressoren durchgeführt. Der Hypothesentest gibt Auskunft darüber, ob die Nullhypothese abgelehnt oder angenommen werden kann. Dabei wird das Signifikanzniveau α meist mit 10, 5 oder 1 Prozent festgelegt. Mittels einem t-Test wird die Zufallswahrscheinlichkeit (p-Wert) eines Regressionskoeffizienten ermittelt. Diese Zufallswahrscheinlichkeit ist jene Wahrscheinlichkeit, mit welcher der Koeffizient auch durch Zufall ermittelt werden könnte. Sollte diese Wahrscheinlichkeit über dem festgelegten Signifikanzniveau liegen, so muss die Nullhypothese abgelehnt werden. Beispielsweise bedeutet ein Signifikanzniveau von 5 %, dass bei mehrmaligen durchführen der Analyse mit verschiedenen Stichproben eine Wahrscheinlichkeit von 5 % besteht, die Nullhypothese abzulehnen, obwohl sie richtig wäre.[125]

[122] Vgl. Bourier, 2018, S. 199f.
[123] Vgl. Eckstein, 2012, S. 315.
[124] Vgl. Eckstein, 2012, S. 316.
[125] Vgl. Winkler, 2017, S. 152f.

4.3 Ergebnisse und Interpretationen

Die Hypothesen H1 bis H5 wurden mithilfe der vorgestellten Methode analysiert. Die Trendgeradenanalyse mit statistischer Signifikanzprüfung wurde bewusst als statistisches Instrument gewählt, um die Ergebnisse leichter nachvollziehen zu können. Tabelle 23 auf der nachfolgenden Seite veranschaulicht die empirischen Ergebnisse. Für jede Hypothese wurde die Regressionsanalyse einzeln durchgeführt. Der Regressand, der Regressor und die Untersuchungsmenge sowie das Bestimmtheitsmaß (R2) werden in der Tabelle für jede Hypothese angeführt. Zudem wird der berechnete Koeffizient und der p-Wert für den Regressor genannt. Der konkrete Wert des Koeffizienten kann vernachlässigt werden, da dieser Abhängig von den Variablen ist. Zeitpunkte gehen als Unix-Zeitstempel in die Berechnung mit ein und sind von Natur aus vergleichsweise zu der Anzahl an Transaktionen oder bezahlten Gebühren stark verschieden. Wichtig ist jedoch das Vorzeichen des Koeffizienten, denn dies gibt die Richtung des Zusammenhangs an, was für die Deutung des Ergebnisses essentiell ist. Der p-Wert gibt die Irrtumswahrscheinlichkeit an. Wenn diese unter dem festgelegten Signifikanzniveau von 5 Prozent ist, so ist das Ergebnis statistisch signifikant. In der nachfolgenden Tabelle sind alle p-Werte 0 Prozent. Das liegt vor allem an der großen Untersuchungsmenge und geht damit einher, dass beinahe die gesamte Grundgesamtheit analysiert wurde. In der Spalte der Untersuchungsmenge ist zusätzlich das Bestimmtheitsmaß gelistet, welches die Güte des Modells angibt. Da jedoch eine homogene lineare Regression durchgeführt wurde, kann das Bestimmtheitsmaß vernachlässigt werden[126]. Generell gilt jedoch, dass das berechnete Regressionsmodell umso besser zu den Daten passt, je näher das Bestimmtheitsmaß bei 100 Prozent liegt. Die Untersuchungsmengen der Hypothesen beziehen sich auf die aggregierten Zeitraumdaten, welche die Daten aller Transaktionen in 30-Minuten-Zeiträume zusammenfasst. Nur die Hypothese *H2* bezieht sich auf Daten, die genauer durch die rohen Metadaten der Blöcke gewonnen werden können. Details dazu können im Kapitel „3.6 Rohe Blockdaten“ nachgelesen werden. Die Datenbasis sowie die deskriptive Datenanalyse für alle anderen Regressanden und Regressoren kann im Kapitel „3.5 Datenbeschreibung“ nachgeschlagen werden.

[126] Vgl. Eckstein, 2012, S. 316 und 320.

Nr.	(Null-)Hypothese	Regressand	Regressor (Koeffizient; p-Wert)	Untersuchungsmenge; Bestimmtheitsmaß
H1	Die Anzahl der Transaktionen steigt.	Anzahl an Transaktionen eines Zeitraumes	Endzeitpunkt eines Zeitraumes (2,783; 0,000)	106.482 Zeiträume; 41,08 %
H2	Die Transaktionsgebühren ersetzen nach und nach die Block-Belohnung (Coinbase-Transaktion) für den Miner.	Anteil der Gebühr am Miner-Erlös eines Blocks[128]	Zeitstempel eines Blocks (0,0000305; 0,000)	359.428 Blöcke; 13,51 %
H3	Es werden immer weniger Bitcoins in einer Transaktion verwendet.	Durchschnittliche Anzahl an Bitcoins pro Transaktion eines Zeitraumes	Endzeitpunkt eines Zeitraumes (-0,00337; 0,000)	106.482 Zeiträume; 5,09 %
H4	Die Transaktionsgebühren sind höher, wenn mehr Transaktionen stattfinden.	Durchschnittliche Gebühr in Satoshis eines Zeitraumes	Anzahl an Transaktionen eines Zeitraumes (0,587; 0,000)	106.482 Zeiträume; 0,02 %
H5	Preisänderungen gehen mit einem höheren Handelsvolumen einher.	Absolute logarithmierte Rendite eines Zeitraumes	Kumulierte Menge ohne Coinbase eines Zeitraumes (1,22E-08; 0,000)	55.768 Zeiträume[127]; 0,52 %

Tabelle 23: Ergebnisse der Hypothesen[129]

[127] Diese Zeiträume enthalten die Preisdaten von 01.01.2016 bis 01.05.2019.
[128] Der Miner-Erlös ist die Summe aus der Block-Belohnung und der Transaktionsgebühren.
[129] Quelle: Verfasser.

Da die p-Werte aller Hypothesen unter dem Signifikanzniveau von 5 Prozent liegen, werden alle Nullhypothesen behalten und keine wird verworfen. Es lohnt sich, die Hypothesen im Einzelnen näher zu beleuchten und mögliche Kausalitäten aufzustellen.

- *H1: Die Anzahl der Transaktionen steigt.*

Um diese Hypothese zu analysieren, wird als Regressand die Anzahl an Transaktionen je Zeitraum (Kapitel 3.5.4) definiert. Als unabhängiges Merkmal wird der Endzeitpunkt als Zeitstempel eines Zeitraumes verwendet. Folglich sollten, je fortgeschrittener die Zeit oder je größer der Zeitstempel wird, mehr Transaktionen stattfinden. Das Ergebnis mit einem p-Wert von 0 Prozent ist äußerst statistisch signifikant. Da der Koeffizient des Regressors positiv ist, stimmt auch die Richtung des Zusammenhangs und die Hypothese kann angenommen werden. Zur Veranschaulichung werden die Zeitraumdaten monatlich gemittelt und unten grafisch dargestellt. Die gemittelten Daten passen besser zum Regressionsmodell (punktierte Trendlinie; Gleichung in Grafik), als die einzelnen Zeitraumdaten. Die Hypothese H1 kann demnach ohne Bedenken angenommen werden und der vermehrten Verwendung von Bitcoin kann zugestimmt werden.

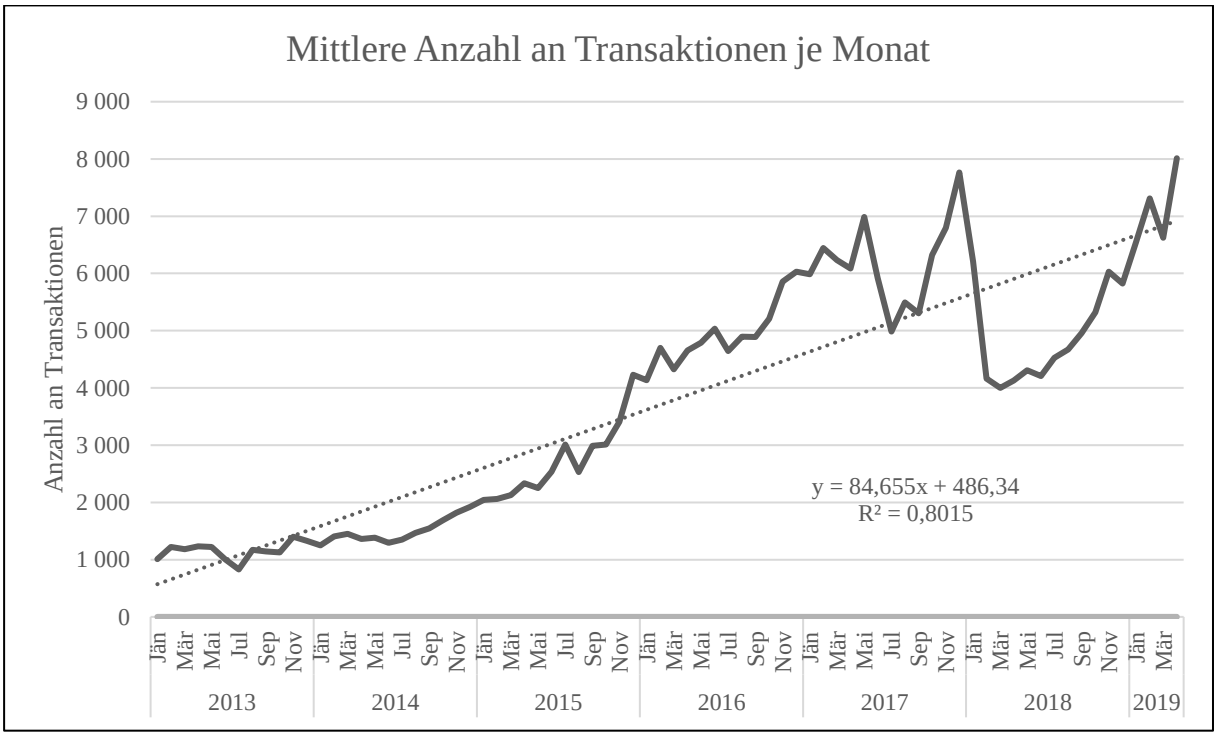

Abb. 14: Mittlere Anzahl an Transaktionen je Monat[130]

[130] Quelle: Verfasser.

- *H2: Die Transaktionsgebühren ersetzen nach und nach die Block-Belohnung (Coinbase-Transaktion) für den Miner.*

Auch diese Hypothese weist einen p-Wert von 0 Prozent auf und das Ergebnis ist folglich statistisch signifikant. Der Koeffizient ist ein sehr kleiner Wert, was daran liegt, dass die Werte des Zeitstempels und der Gebühr weit auseinanderfallen. Wichtig ist jedoch, dass der Wert positiv ist. Das bedeutet, das umso mehr Zeit (Regressor) vergeht, der Anteil der Gebühr am gesamten Miner-Erlös (Regressand, siehe Kapitel 3.6) steigt. Das kann jedoch auch auf die Halving-Events zurückzuführen sein, welches die Block-Belohnung in etwa alle vier Jahre halbiert und somit die Gebühren prozentual mehr am gesamten Miner-Erlös ausmachen. Folgende Abbildung macht das zweite Halving-Event im Juli 2016 mit dem Block der Höhe 420.000 ersichtlich und zeigt, dass der gesamte Miner-Erlös weiterhin stark von der Block-Belohnung abhängig ist. Diese Abhängigkeit soll von Zeit zu Zeit geringer werden und die Gebühren sollten immer mehr zum Miner-Erlös beitragen. Eine leichte und positive Tendenz ist zu erkennen und ist wie bereits beschrieben statistisch signifikant, jedoch bleibt abzuwarten, ob sich dieser Trend in Zukunft (stärker) durchsetzen wird.

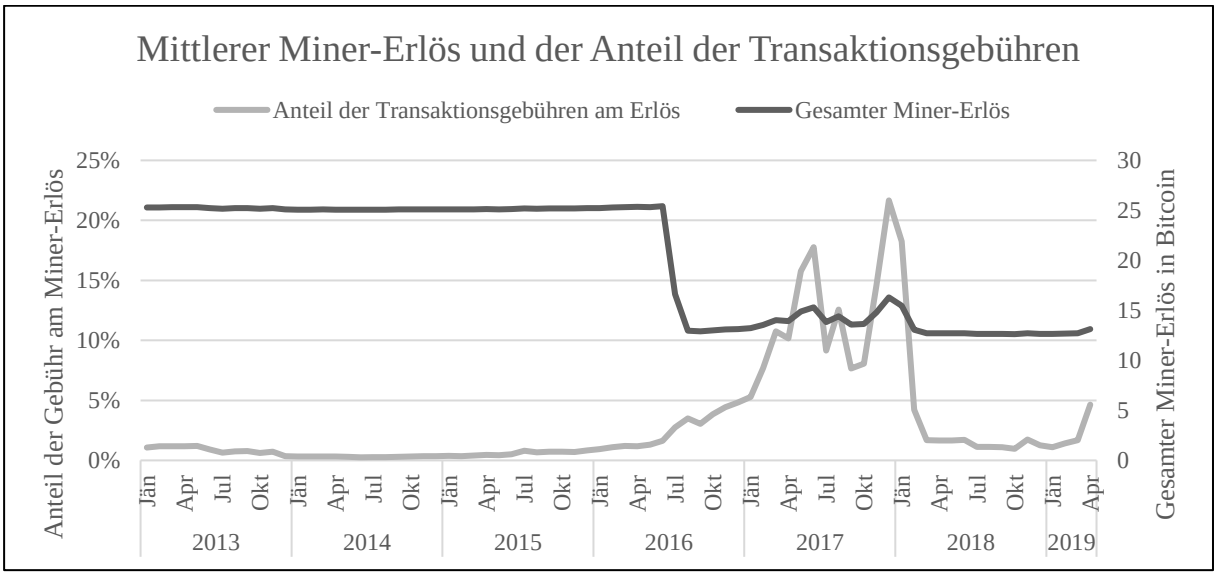

Abb. 15: Mittlerer Miner-Erlös und der Anteil der Transaktionsgebühren[131]

Wird der starke Einfluss des Halving-Events nicht berücksichtigt und es wird nur die Gebühr betrachtet, wie es in der nachfolgenden Abbildung der Fall ist, so wird ebenfalls eine leicht positive Tendenz der kumulierten, monatlich gemittelten Transaktionsgebühr sichtbar. Auch falls diese in Zukunft etwa gleichbleiben sollte und der Bitcoin im Verhältnis zu anderen

[131] Quelle: Verfasser.

Währungen wie den US-Dollar steigt, könnte der Anreiz am System teilzunehmen für die Miner weiterhin bestehen bleiben.

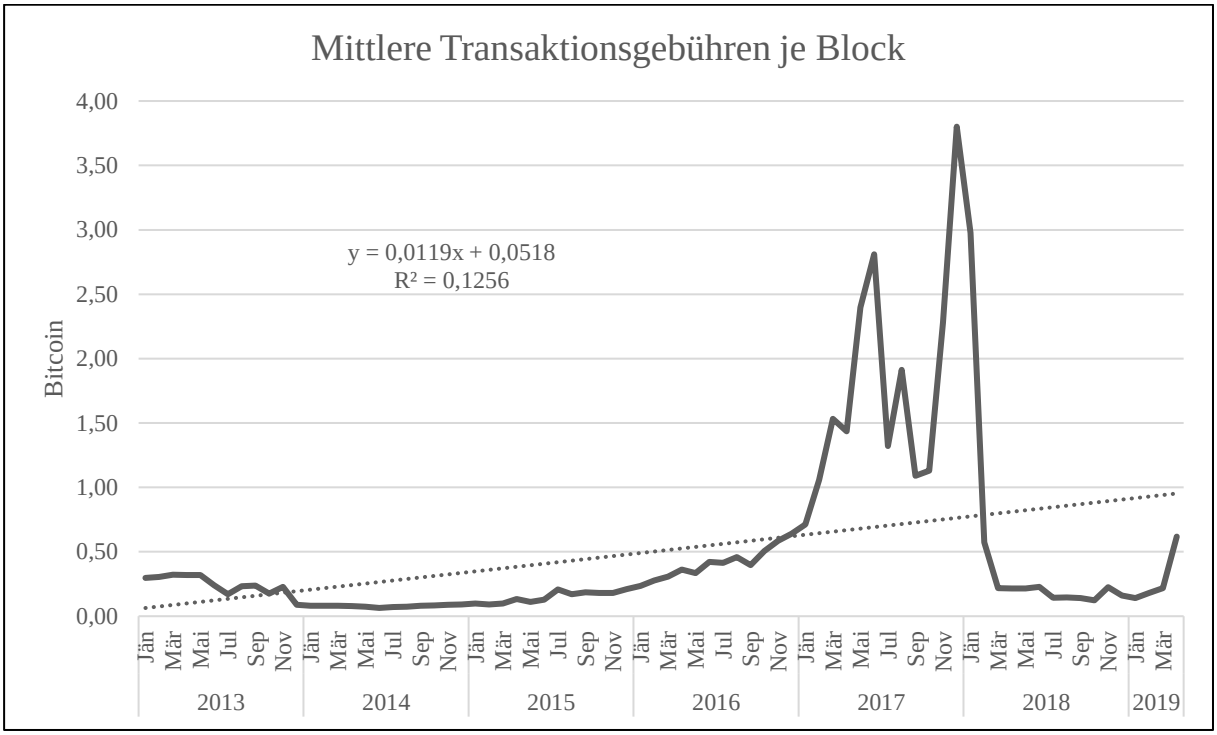

Abb. 16: Mittlere Transaktionsgebühren je Block[132]

- *H3: Es werden immer weniger Bitcoins in einer Transaktion verwendet.*

Um diese Hypothese und somit die deflatorischen Eigenschaften von Bitcoin zu überprüfen wurde als Regressand die durchschnittliche Anzahl an Bitcoins pro Transaktion und je Zeitraum verwendet. Dieser berechnet sich aus der kumulierten Menge ohne Coinbase (Kapitel 3.5.2) dividiert durch die Anzahl an Transaktionen (Kapitel 3.5.4). Als Regressor wurde wieder der Zeitstempel des Endzeitpunktes gewählt. Der p-Wert ist ebenfalls wieder statistisch äußerst signifikant mit 0 Prozent. Da der Koeffizient negativ ist, gibt es einen inversen Zusammenhang. Je mehr Zeit vergeht, je größer folglich der Zeitstempel ist, desto kleiner ist die Anzahl an transferierten Bitcoins je Transaktion. Wie auch bei allen anderen Hypothesen zeigt die Regression keine Kausalität an. Daher lohnt es sich einen Blick auf die nächste Grafik zu werfen. Die Grafik verwendet eine logarithmierte Darstellung und zeigt eine annähernd gegenläufige Tendenz zwischen den transferierten Bitcoins je Transaktion und des Preises an. Über die Zeit hinweg werden weniger Bitcoins in einer jeden Transaktion verwendet und zugleich ist der Bitcoin-Preis in USD stark angestiegen. In der Abbildung wurden gemittelte Monatsdaten für den Untersuchungszeitraum ermittelt.

[132] Quelle: Verfasser.

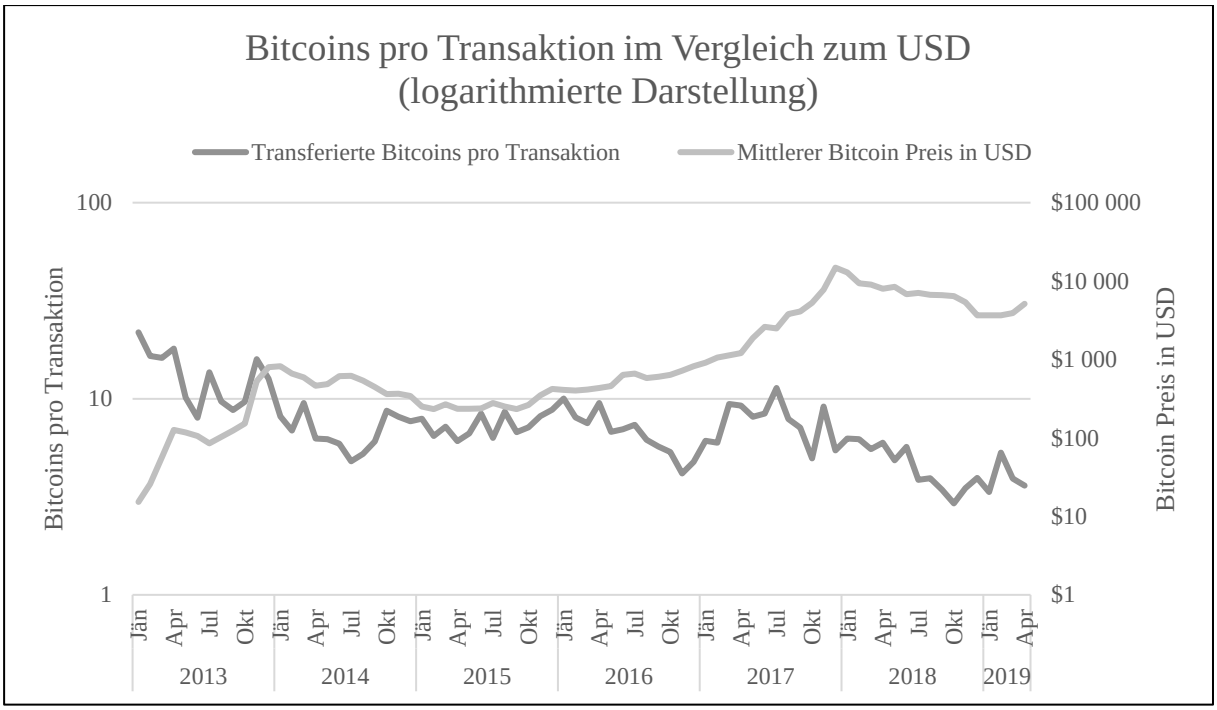

Abb. 17: Mittlere Bitcoins pro Transaktion im Vergleich zum USD[133]

- *H4: Die Transaktionsgebühren sind höher, wenn mehr Transaktionen stattfinden.*

Um diese Hypothese zu belegen oder widerlegen wurde als Regressand die durchschnittliche Gebühr (Kapitel 3.5.7) und als Regressor die Anzahl an Transaktionen (Kapitel 3.5.4) je Zeitraum gewählt. Der berechnete Koeffizient ist positiv und der p-Wert liegt bei 0,0052 Prozent. Somit ist das Ergebnis wiederum statistisch signifikant. Die Hypothese, dass die Transaktionsgebühren höher sind, wenn mehr Transaktionen stattfinden, stimmt demnach. Abbildung Abb. 18 veranschaulicht die konkreten und gemittelten Monatsdaten. Auffällig ist vor allem das Jahr 2013, in welchem vergleichsweise zu den Folgejahren hohe Gebühren bezahlt worden sind. Im Dezember 2013 gibt es einen starken Rücksetzer bei den Gebühren. Dieser ist vermutlich auf den extremen Preisanstieg in diesem Monat zurückzuführen. Der Preis hat sich im Dezember 2013 fast verzehnfacht und die Auslastung gemessen an den Transaktionen blieb hingegen in etwa gleich. Die Anzahl an Transaktionen stieg ab 2015 kontinuierlich an, doch die Gebühren blieben gleich. Erst im Hype im Jahr 2017 gab es einen rasanten Anstieg der Gebühren je Transaktion. Die Anzahl an Transaktionen fiel 2018 stark ab und holte ebenso stark wieder auf. Die Gebühren fielen ebenso stark, doch blieben auf diesem neuen Level und stiegen erst 2019 wieder an, als mehr als 6.000 Transaktionen je Monat durchgeführt wurden. Die Punktewolke in Abbildung Abb. 19 zeigt die mittleren Gebühren in Bezug auf die Anzahl an Transaktionen ohne das erwähnte Jahr 2013. Die Grafik beinhaltet

[133] Quelle: Verfasser.

weitere Ausreißerwerte, welche meist auf das Jahr 2017 zurückzuführen sind, in welchem ein globaler Bitcoin-Hype herrschte. Interessant zu sehen ist, dass bei Betrachtung der eng aneinander liegenden Punkte die Gebühr nicht groß schwankt, die Anzahl der Transaktionen hingegen sehr wohl.

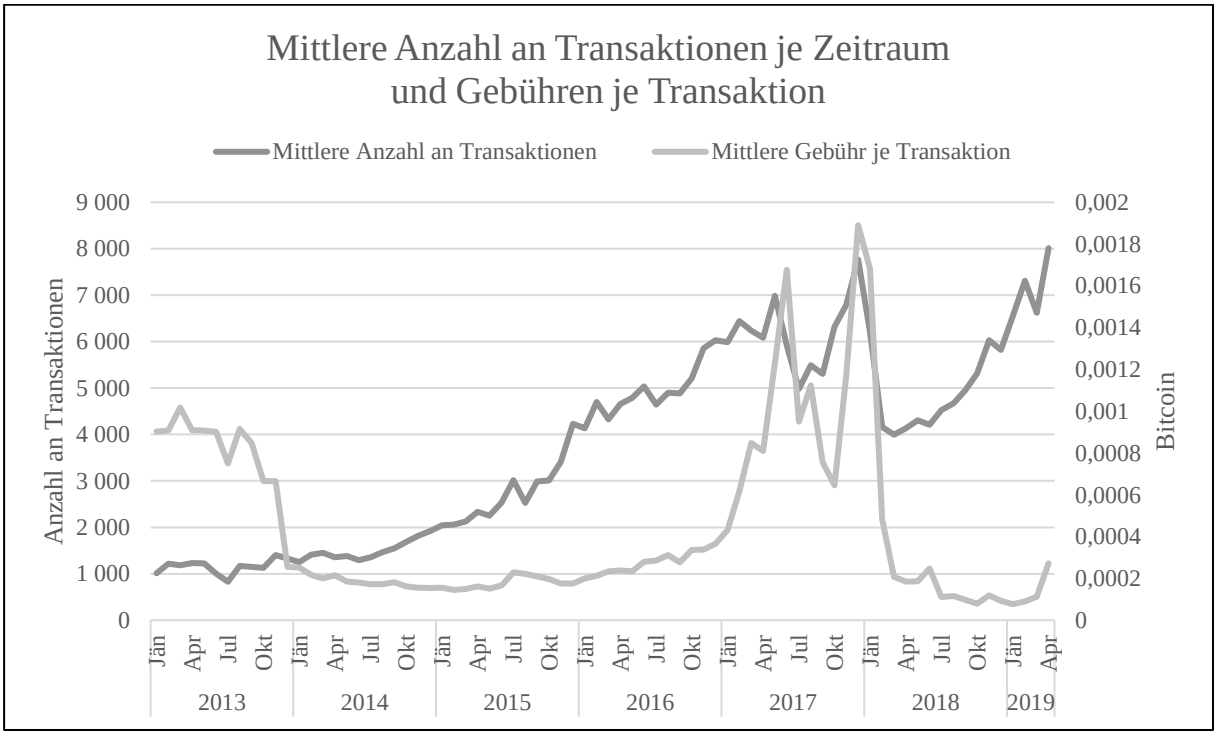

Abb. 18: Mittlere Anzahl an Transaktionen und Gebühren je Transaktion[134]

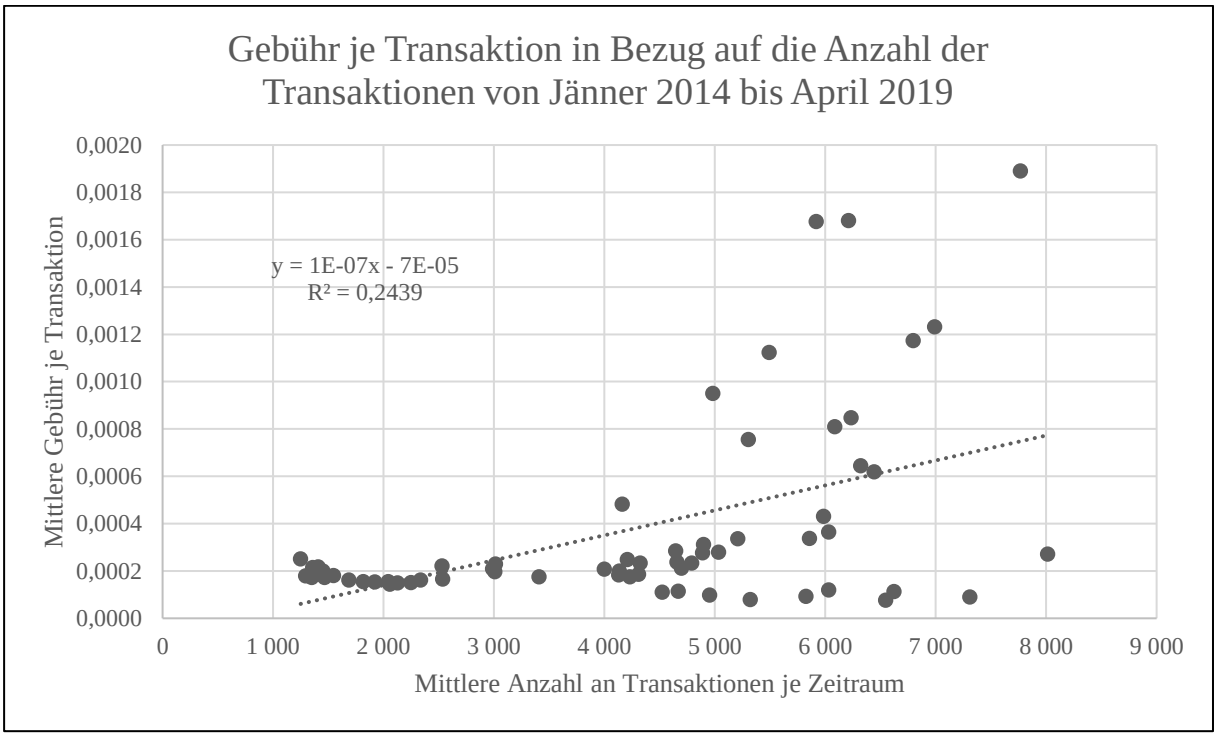

Abb. 19: Gebühr in Bezug auf die Anzahl der Transaktionen[135]

[134] Quelle: Verfasser.
[135] Quelle: Verfasser.

- *H5: Preisänderungen gehen mit einem höheren Handelsvolumen einher.*

Zur Überprüfung dieser Hypothese wird als Regressand die absolute logarithmierte Rendite (Kapitel 3.5.13) als Preisänderung eines Zeitraumes verwendet. Die absolute Rendite wird genutzt, da es für die Analyse keinen Unterschied machen soll, ob Preise gestiegen oder gefallen sind. Denn es wird angenommen, dass das Handelsvolumen erhöht ist, wenn Preise sich (stark) ändern. Das Handelsvolumen wird hier definiert als die kumulierte Menge ohne Coinbase (siehe Kapitel 3.5.2) und gibt somit die totale Menge an transferierten Bitcoins je Zeitraum an. Es wird bewusst der Preis in USD außer Acht gelassen, um etwaige Preiseinflüsse auf den Regressor zu umgehen. Folglich wird erwartet, dass bei großen Preisänderungen vermehrt Bitcoins den Besitzer wechseln. Die Untersuchungsmenge beinhaltet alle beschafften Zeiträume ab 2016 und bezieht sich somit auf ungefähr die Hälfte der Zeitspanne als alle anderen Hypothesen. Der p-Wert ist wiederum 0 und das Ergebnis statistisch signifikant. Der Koeffizient ist äußerst klein, jedoch positiv und zeigt somit die richtige Richtung des Zusammenhangs an. Folgende Abbildung zeigt die monatlich gemittelten Zeitraumdaten an. Der leicht positive Trend ist kaum erkennbar, verläuft beinahe waagrecht und die Streuung der Punkte ist hoch. Aufgrund der statistischen Signifikanz kann die Hypothese zwar angenommen werden, doch die Aussagekraft bleibt gering.

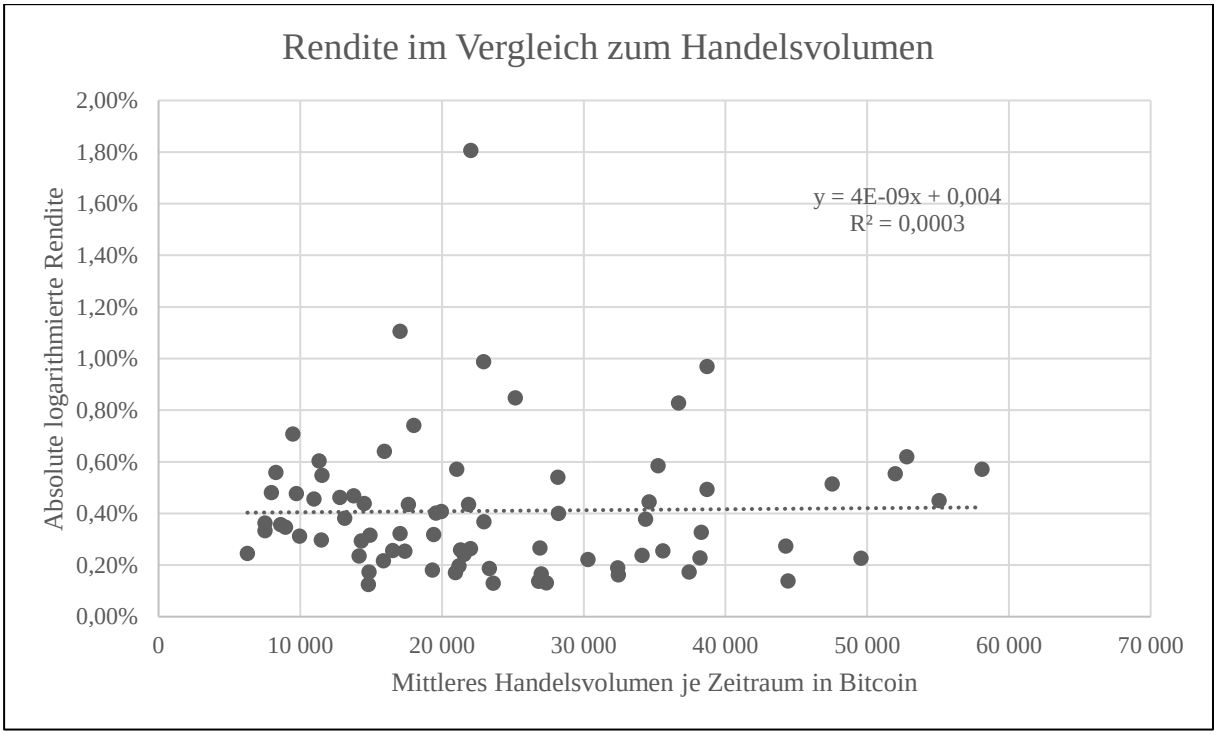

Abb. 20: Rendite im Vergleich zum Handelsvolumen[136]

[136] Quelle: Verfasser.

5 Zusammenfassung und Ausblick

Die vorliegende Arbeit führte zunächst in den Grundlagen in die Thematik Bitcoin als digitales Geld ein. Es wurden verschiedenste Aspekte, wie die Funktionen von Geld und Marktplätzen, behandelt, bevor in die Blockchain-Technologie eingegangen wurde. In den Grundlagen zu Bitcoin wurde die Innovation der neuen Technologie näher erläutert. Die Empirie setzte sich zum Ziel ausgewählte und inhärente Eigenschaften von Bitcoin quantitativ zu analysieren. Um dies zu bewerkstelligen, mussten zunächst Daten für die Analyse beschafft werden. Diese Daten beinhalteten zum Großteil interne Blockchain-Daten. Da jedoch Preisinformationen nicht in der Blockchain zur Verfügung stehen, mussten diese aus einer externen Datenquelle besorgt und aggregiert werden. Um einen besseren Überblick über die zusammengestellte Datenbasis zu bekommen, wurde zunächst eine deskriptive Datenanalyse durchgeführt. In der Empirie wurden Hypothesen aufgestellt, die auch von Interesse für die zukünftige Entwicklung Bitcoins sind. Die Ergebnisse wurden interpretiert und eine mögliche Kausalität durch tiefergehende Analysen hergestellt.

Die Empirie untersuchte mit den Hypothesen Teile der Entwicklung Bitcoins von Januar 2013 bis einschließlich April 2019. Die verfassten Hypothesen behandeln eine Auswahl von Eigenschaften, die als wichtig und zukunftsweisend für Bitcoin empfunden werden und geben keine Rückschlüsse auf andere verwandte Untersuchungsgegenstände. Alle aufgestellten Hypothesen wurden mit statistischer Signifikanz belegt und deuten somit in eine für Bitcoin positive Richtung. Wichtige Erkenntnisse dieser Arbeit sind, dass Bitcoin zunehmend mehr verwendet wird, deflatorische Eigenschaften sich wie angenommen entfalten und Miner weiterhin den Anreiz haben am System teilzunehmen. Gebühren scheinen sich grundsätzlich der Transaktionsauslastung im Bitcoin-Netzwerk anzupassen, jedoch ist die ermittelte Ausprägung schwach und es bleibt abzuwarten, wie sich die Sachlage verhält, wenn die Block-Belohnung zunehmend geringer wird. Ferner wurde gezeigt, dass es einen statistisch signifikanten Zusammenhang zwischen Preisänderungen an Kryptobörsen und den gehandelten Mengen in der Blockchain gibt. Diese Ausprägung ist jedoch auch als schwach anzusehen. Die Ergebnisse dieser quantitativen Analyse deuten zwar auf eine positive Entwicklung Bitcoins hin, jedoch handelt es sich hierbei nicht um eine vollständige Untersuchung aller möglichen Eigenschaften. Ebenso wie das aktuelle Geldsystem lebt Bitcoin vom Vertrauen und ist vor regulatorischen Eingriffen nicht geschützt. Auch wenn die dezentrale Infrastruktur nicht abgeschaltet werden kann, so kann die Nutzung erschwert oder das Vertrauen verloren gehen.

Diese Arbeit trägt zu einem allumfassenden Blick auf Bitcoin bei und analysiert dessen Funktionsweise in Bezug auf inhärente Eigenschaften der Technologie. Es gibt bereits viel Literatur und Analysen zu Bitcoin, die jedoch oft entweder rein auf das Technische oder auf das Wirtschaftliche abzielen. In dieser Arbeit wurden beide Komponenten einbezogen, indem gezielt Hypothesen verfasst und analysiert wurden. Abseits der vorliegenden Untersuchung gibt es viele weitere Forschungsmöglichkeiten, die aufgegriffen werden können. Beispielsweise wäre es interessant, weitere Hypothesen zu erforschen sowie Kryptobörsen noch stärker miteinzubeziehen. Viel Handel findet ausschließlich auf Börsen statt und bleibt somit der Blockchain verborgen. Weiters könnte versucht werden Adressencluster in der Blockchain zu finden, Geldflüsse zu analysieren und mögliche Arbitragegeschäfte ausfindig zu machen. Zudem wären etwaige Zusammenhänge zwischen verschiedenen Blockchains interessant sowie der Einfluss der Lightning-Technologie auf Bitcoin.

Literaturverzeichnis

About BIS - Overview, 2020

About BIS - Overview. (2020). Abgerufen am 19.06.2020 von BIS.org: https://www.bis.org/about/

Ametrano, 2016

Ametrano, F. M. (2016). *Hayek Money: the Cryptocurrency Price Stability Solution.* http://ssrn.com/abstract=2425270.

Antonopoulos, 2014

Antonopoulos, A. M. (2014). *Mastering Bitcoin.* Sebastopol: O'Reilly Media.

Bariviera, Basgall, Hasperué, & Naiouf, 2017

Bariviera, A. F., Basgall, M., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. *Physica A: Statistical Mechanics and its Applications*, 82-90.

Berentsen & Schär, 2017

Berentsen, A., & Schär, F. (2017). *Bitcoin, Blockchain und Kryptoassets.* Basel: Norderstedt.

Bistarelli, Mercanti, & Santini, 2018

Bistarelli, S., Mercanti, I., & Santini, F. (2018). Short Paper: An Analysis of Non-standard Bitcoin Transactions. *Crypto Valley Conference on Blockchain Technology* (S. 93-96). IEEE Computer Society.

Bourier, 2018

Bourier, G. (2018). *Beschreibende Statistik.* Regensburg: Springer Gabler.

Brauneis & Mestel, 2018

Brauneis, A., & Mestel, R. (2018). *Finanzwissen – allgemein verständlich: Kryptowährungen.* Wien: ÖBA.

Dixon, 2017

Dixon, P. (2017). *Innovationen und Innovationsmanagement in der Finanzbranche.* (R. Smolinski, M. Gerdes, M. Siejka, & M. C. Bodek, Hrsg.) Wiesbaden: Springer Gabler.

Eckstein, 2012

Eckstein, P. P. (2012). *Statistik für Wirtschaftswissenschaftler.* Berlin: Springer Gabler.

Frankenfield, On Chain Transactions (Cryptocurrency), 2018
Frankenfield, J. (5. April 2018). *On Chain Transactions (Cryptocurrency)*. Abgerufen am 23.03.2020 von https://www.investopedia.com/terms/c/chain-transactions-cryptocurrency.asp

Frankenfield, Off-Chain Transactions (Cryptocurrency), 2019
Frankenfield, J. (31. Oktober 2019). *Off-Chain Transactions (Cryptocurrency)*. Abgerufen am 23.03.2020 von https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp

Franzetti, 2018
Franzetti, C. (2018). *Investmentbanken.* Meilen: Springer Gabler.

Furness, 1910
Furness, W. H. (1910). *The Island of Stone Money: Uap of the Carolines.* Philadelphia: J. B. Lippincott.

Helmedag, 1994
Helmedag, F. (1994). *Warenproduktion mittels Arbeit. Zur Rehabilitation des Wertgesetzes.* Marburg: Metropolis.

Hosp, 2018
Hosp, J. (2018). *Blockchain 2.0.* München: FinanzBuch Verlag.

Jevons, 1876
Jevons, W. S. (1876). *Money and the Mechanism of Exchange.* New York: D. Appleton and Co.

Kaiser, 2011
Kaiser, D. (2011). *Treasury Management.* Wiesbaden: Gabler.

Kalodner, BlockSci 0.5.0 documentation, 2020
Kalodner, H. (2018). *BlockSci 0.5.0 documentation*. Abgerufen am 19.06.2020 von https://citp.github.io/BlockSci/readme.html

Kalodner, Goldfeder, Chator, Möser, & Narayanan, 2017
Kalodner, H., Goldfeder, S., Chator, A., Möser, M., & Narayanan, A. (8. September 2017). *BlockSci: Design and applications of a blockchain analysis platform.* https://arxiv.org/pdf/1709.02489.pdf

Kannengiesser, Dehling, Lins, & Sunyaev, 2019
Kannengiesser, N., Dehling, T., Lins, S., & Sunyaev, A. (2019). What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs. *SSRN Electronic Journal. 10.24251/HICSS.2019.848.*

Karpoff , 1987
Karpoff , J. M. (1987). The Relation Between Price Changes and Trading Volume: A Survey. *The Journal of Financial and Quantitative Analysis, 22*(1), 109-126.

Kocherlakota, 1996
Kocherlakota, N. R. (1996). Money is memory. *Federal Reserve Bank of Minneapolis Research Department Staff Report*, (S. 218).

Krugman & Obstfeld, 2006
Krugman, P., & Obstfeld, M. (2006). *Internationale Wirtschaft.* Hallbergmoos: Pearson Studium.

Lee & Low, 2018
Lee, D. K., & Low, L. (2018). *Inclusive fintech.* Singapur: World Scientific.

Levitt, 1960
Levitt, T. (1960). Marketing Myopia. *Harvard Business Review* (S. 55). Juli-August: Vol. 38.

Morkunas, Paschen, & Boon, 2019
Morkunas, V., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons 62*, 295—306.

Nabben & Rudolph, 1994
Nabben, S., & Rudolph, B. (1994). Die Börse als Marktplatz und Dienstleister. *Marketing: ZFP – Journal of Research and Management* (S. 167-180). C.H.Beck.

Nakamoto, 2008
Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Obst & Hintner, 2000
Obst, G., & Hintner, O. (2000). *Geld-, Bank- und Börsenwesen.* (J. Hagen, & J. Stein, Hrsg.) Stuttgart: Schäffer-Poeschel.

Rosenberger, 2018
Rosenberger, P. (2018). *Bitcoin und Blockchain.* Münster: Springer Vieweg.

Sissors, 1966
Sissors, J. Z. (1966). What Is a Market? *Journal of Marketing* (S. 17-21). Vol.30(3).

Swan, 2015
Swan, M. (2015). *Blockchain: Blueprint for a new economy.* O'Reilly Media.

Szalachowski, 2018
Szalachowski, P. (2018). *Towards More Reliable Bitcoin Timestamps.* Singapore: https://arxiv.org/pdf/1803.09028.pdf.

Thiel, 2011
Thiel, C. (2011). *Das „bessere“ Geld.* Augsburg: VS.

Winkler, 2017
Winkler, P. (2017). *Empirische Wirtschaftsforschung und Ökonometrie.* Gießen: Springer Gabler.

Zheng, Xie, Dai, Chen, & Wang, 2017
Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *6th International Congress on Big Data* (S. 557-564). IEEE.

Zwahr, 2006
Zwahr, A. (Hrsg.). (2006). *Brockhaus-Enzyklopädie in 30 Bänden* (Bd. 10). Leipzig/Mannheim: F.A. Brockhaus.