Die approbierte Originalversion dieser Diplom-/Masterarbeit ist in der Hauptbibliothek der Technischen Universität Wien aufgestellt und zugänglich.
http://www.ub.tuwien.ac.at

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology.
http://www.ub.tuwien.ac.at/eng

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Bitcoin

Eine Analyse von Kryptowährungen und deren Anwendung im Onlinehandel

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Medieninformatik

eingereicht von

Ing. Manfred Linzner BSc
Matrikelnummer 0825180

an der Fakultät für Informatik
der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 28. Juni 2016

Manfred Linzner | Markus Haslinger

FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

Bitcoin

An In-Depth Analysis of Cryptocurrencies

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Media Informatics

by

Ing. Manfred Linzner BSc
Registration Number 0825180

to the Faculty of Informatics
at the Vienna University of Technology

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, 28th June, 2016

Manfred Linzner | Markus Haslinger

Erklärung zur Verfassung der Arbeit

Ing. Manfred Linzner BSc
Stiegengasse 7/31, 1060 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 28. Juni 2016

Manfred Linzner

Danksagung

Mein Dank gebührt meinen Eltern Petra & Manfred, die mich nicht nur bei dieser Arbeit, sondern während der gesamten Studienzeit mit allen Mitteln unterstützt haben und stets mit Rat und Tat zur Seite gestanden sind.

Danke Philipp für die regelmäßigen Gespräche und langen Autofahrten, die voll und ganz dem Thema Bitcoin gewidmet waren. #usa2015

Danke Marlene für die tatkräftige mentale Unterstützung und das Lektorat.

Zuletzt darf die ausgezeichnete Betreuung durch Prof. Dr. Markus Haslinger nicht unerwähnt bleiben. Vielen Dank für den Einsatz, die Inspiration und das kontinuierliche Feedback.

Einleitende Anmerkungen

Aus Gründen der Ästhetik und Lesbarkeit der vorliegenden Arbeit wurde sowohl auf das Binnen-I als auch auf die Beidnennung bei Personenbezeichnungen verzichtet. Sämtliche Ausführungen in dieser Arbeit beziehen sich gleichermaßen auf das weibliche und männliche Geschlecht.

Bitcoin in Singularform wird in der vorliegenden Arbeit verwendet, um auf die Technologie und das technische Grundgerüst zu verweisen. Um auf die Währung und deren monetären Wert zu verweisen findet die Pluralform („Bitcoins“) oder die abgekürzte Form („XBT“) Verwendung. Die Entscheidung für die Abkürzung XBT anstelle der geläufigeren Variante BTC liegt im internationalen Standard für Währungs-Abkürzungen[1] begründet. Dieser sieht vor, dass die ersten beiden Stellen dem Landeskürzel entsprechen zu haben. Als solches ist BT bereits dem Königreich Bhutan zugewiesen. Des Weiteren sieht ISO-4217 vor, dass supranationale Währungen mit einem X zu beginnen haben. Im Gegensatz zum Kürzel BTC spricht bei XBT also nichts gegen eine offizielle Aufnahme in den Internationalen Standard.

Sämtliche Quellen (Literatur, Rechts- sowie Onlinequellen) dieser Arbeit wurden mit BibTeX verwaltet und sind im gemeinsamen Kapitel *Quellen* zusammengefasst.

[1] ISO-4217:2015

Kurzfassung

Historisch bedingt lassen sich Währungen stets auf eine herausgebende, regulierende Stelle staatlicher Provenienz zurückführen. Diese zentrale Stelle übernimmt die Aufsichtsfunktion und bürgt für den Wert der Währung. Kryptowährungen setzen einen gezielten Schritt in Richtung Dezentralisierung. Bitcoin und Alternativen verfügen über keine derartige zentrale Stelle. Währungskurse werden durch den freien Markt geregelt, die Verifikation von Transaktionen geschieht durch ein Kollektiv von Nutzern und jede Transaktion ist öffentlich einsehbar.

Diese Diplomarbeit legt zunächst die Entwicklung von Währungssystemen, ausgehend vom Goldstandard im 19. Jahrhundert über das Bretton-Woods-System bis hin zu Fiat-Geld und Kryptowährungen, dar. Der Fokus der Arbeit liegt auf der Kryptowährung Bitcoin. Deren Entwicklung sowie die technisch komplexen Abläufe rund um die Anwendung von Bitcoin werden allgemeinverständlich dargelegt. Des Weiteren wird die bestehende Rechtslage in Österreich, den USA und Russland näher betrachtet und der Versuch unternommen, Problematiken und offene Fragen rund um Bitcoin in Relation zu bestehendem Recht zu setzen.

Der zweite Abschnitt der Arbeit beleuchtet mögliche Einsatzgebiete für Kryptowährungen. Dazu wird die Einführung von Bitcoins als Zahlungsmittel in einem Online-Shopsystem beschrieben und in weiterer Folge deren Akzeptanz analysiert.

Abschließend erfolgt der Versuch, die zukünftige Entwicklung der Technologie Bitcoin zum einen und von Bitcoins – der Währung – zum anderen einzuschätzen.

Stichwörter: Kryptowährungen, Digitales Geld, Bitcoin, Elektronischer Handel

Abstract

Throughout history, currencies are always attributable to a central governmental authority which is not only issuing money and regulating the supply but also acting as a guarantor for the value of a currency. Cryptocurrencies aim for a decentralized system. Bitcoins and other cryptocurrencies lack a centralized authority. The exchange rates are based on a free enterprise economy. Transactions are verified collectively and each transaction is publicly accessible.

This master thesis starts in the 19th century and investigates the evolution of monetary systems covering gold standard, Bretton Woods system, fiat money up to the latest developments concerning cryptocurrencies. This work's focus lies on the historical development of Bitcoin as well as on Bitcoin's technically complex processes and how to express them in a way which everyone can understand. In addition, this work covers the current legal point of view on Bitcoin in Austria, the United States of America and Russia.

The second part of this thesis focuses on how Bitcoins can be applied. The implementation of Bitcoins as an additional payment method in an online shop will be explained. In a second step this work analyses to which degree customers of this online shop accept this new method of payment.

Lastly an outlook for the Bitcoin framework on the one hand and Bitcoins – the currency — on the other hand will be given.

Keywords: cryptocurrencies, digital money, bitcoin, e-commerce

Inhaltsverzeichnis

Kurzfassung **xi**

Abstract **xiii**

Inhaltsverzeichnis **xv**

Abbildungsverzeichnis **xvii**

Tabellenverzeichnis **xix**

1 Währungen **1**

1.1 Goldstandard 1

1.2 Bretton-Woods-Konferenz 3

1.3 Fiatgeld 5

1.4 Virtuelle Währungen 7

2 Rechtliche Abgrenzung **15**

2.1 Regulierung durch die Finanzmarktaufsicht 15

2.2 Steuerrecht 19

2.3 Strafrecht 20

2.4 Internationale Entwicklung 23

3 Bitcoin **31**

3.1 Historische Entwicklung 32

3.2 Technische Grundlagen 35

3.3 Transaktionen 43
3.4 Blockchain 57
3.5 Mining 59
3.6 Dezentraler Konsens 66

4 Bitcoin im E-Commerce **71**
4.1 Gegenüberstellung Zahlungsabwickler 71
4.2 Integration 75

5 Bitcoin Akzeptanz **87**
5.1 Hypothese 1: Bitcoin Verwendung 87
5.2 Hypothese 2: Länderverteilung 88
5.3 Hypothese 3: Anonymität 89

6 Conclusio und Ausblick **93**

A Satoshi Nakamoto Essay **95**

B Bitcoin-Transaktion **97**

C Bitcoin-Block **99**

D Berechnung von Bitcoin-Adressen **101**

E Mining Anreiz **103**

F Coinbase Server Antwort **105**

G Coinbase Order Callback **107**

H Wegwerf-E-Mail Adressen **109**

Quellen **111**

Abbildungsverzeichnis

3.1 Verschlüsselung mit asymmetrischer Kryptographie 36
3.2 Digitales Signieren mit asymmetrischer Kryptographie 37
3.3 Elliptische Kurve – secp256k1 im reellen Zahlenbereich –10 bis +10 38
3.4 Merkle-Baum mit 4 Blättern 41
3.5 Merkle-Baum mit 16 Blättern 42
3.6 Bitcoin-Transaktion 45
3.7 Bitcoin-Transaktion verkettet 47
3.8 Statistik Bitcoin-Transaktionstypen 50
3.9 Zusammensetzung einer Bitcoin-P2PKH-Adresse 53
3.10 Entwicklung Bitcoin-Geldmenge 64
3.11 Blockchain mit Forks 68
3.12 Blockchain mit neuer aktive Kette 69

4.1 Coinbase – API Schlüsselerstellung 76
4.2 Coinbase – Bezahlseite 81
4.3 Coinbase – Callback URL konfigurieren 83

5.1 XBT Anteil an allen Bestellungen 87
5.2 Länderanteil der Bestellungen mit Bitcoins 88
5.3 Länderanteil der Bestellungen mit anderen Bezahlmethoden 89
5.4 Anteil anonymen Bestellungen mit Bitcoins 90
5.5 Anteil anonymen Bestellungen mit anderen Bezahlmethoden 91

Tabellenverzeichnis

1.1 Money-Matrix 9

3.1 Script-Beispiel 49
3.2 Script Pay to Public Key Hash 51

4.1 Vergleich Zahlungsabwickler 73

B.1 Transaktionsobjekt 97

C.1 Blockobjekt 99

E.1 Entwicklung Mining-Anreiz 104

1 Währungen

1.1 Goldstandard

Der Goldstandard an sich und dessen regulierende Wirkungsfähigkeit wurde bereits 1752 vom schottischen Ökonomen und Philosophen David Hume in abstrakter Form beschrieben.[2] In Ländern, die den Goldstandard umsetzten, ist die Geldmenge, die sich im Umlauf befindet, demnach stets an die Goldvorräte des Landes gebunden. Papiergeld kann damit auch als Optionsschein für Gold angesehen werden und jederzeit beim Staat in seinen Goldgegenwert getauscht werden.[3] David Hume beschreibt nun, dass der Import von Waren oder Dienstleistungen einen Abfluss von Gold zu bedeuten hat, während der Export von Waren gegenteiliges bewirkt und neues Gold in ein Land bringt. Wenn nun das Gleichgewicht aus Import und Export gestört ist, beschreibt Hume des Weiteren die Mechanismen, die zur Regulierung in Kraft gesetzt werden. Für den Fall, dass Importe stets die Exporte übersteigen, muss ein Land mit permanentem Abfluss von Gold kämpfen. Nach Definition des Goldstandards ist dies gleichbedeutend mit einer Verringerung der in Umlauf befindlichen Geldmenge. Die Verringerung der Geldmenge führt zu einer Preisreduktion bei nationalen Produkten, die dadurch wiederum einen Vorteil im Vergleich zu internationalen Produkten erfahren und vermehrt gekauft werden. Regulierende Kräfte setzen somit automatisch ein.[4]

Bis zur breiten Anwendung des Goldstandards sollte jedoch noch einige Zeit vergehen. Großbritanniens Bank Charter Act 1844 setzte nicht nur die Bank of England als alleinige Ausgabestelle für Geld ein, sondern setzte auch voraus, dass Geld zu 100% an

[2] [Hum77, Essay V: Of the Balance of Trade]
[3] [All09, Seite 180 Gold-Specie-Flow Mechanism]
[4] [All09, Seite 180ff Gold-Specie-Flow Mechanism]

die Goldreserven gebunden sein musste.[5] Großbritannien war damit das erste Land, dass den klassischen Goldstandard einsetzte.[6] Bis zum Beginn der 1870er Jahr setzte sich der Goldstandard international durch und verdrängte damit zunehmend den zuvor existierenden Bimetallstandard und die Abkommen der Lateinischen Münzunion, die Silber- und Goldmünzen vorsahen.[7]

Ein jähes Ende fand der Goldstandard mit dem bevorstehenden Ersten Weltkrieg in den Jahren 1913 und 1914.[8] Für Länder, die im Kriegsgeschehen involviert waren, wurde es zunehmend interessant, die Freiheit zu besitzen, zusätzliches Papiergeld zu drucken und damit Kriegsinteressen zu finanzieren.[9]

Nach den Kriegsjahren gab es abermals Bestrebungen, einen Goldstandard zu schaffen und erneut war Großbritannien unter den ersten Ländern, die 1925 einen Standard einführten.[10] Im Jahr 1926 fand der Goldstandard in 39 Ländern Anwendung[11]. Die unterschiedliche wirtschaftliche Ausgangslage der Länder nach dem Ersten Weltkrieg sowie deren unterschiedliche konjunkturelle Entwicklung führte jedoch zu Problemen beim Goldstandard, der nicht mehr wie in den Vorkriegsjahren funktionieren konnte. So stiegen die Goldreserven in Frankreich und Deutschland in kurzer Zeit massiv an, während Länder wie Großbritannien mit einem permanenten Abfluss an Goldreserven zu kämpfen hatten. Frankreich erlebte im Zeitraum von 1926 bis 1931 eine Vervierfachung der nationalen Goldreserven.[12]

Die Probleme des Goldstandards in den Zwischenkriegsjahren führten schließlich dazu, dass ein Großteil der Staaten 1929 die Bindung an Gold beendete.[13] Dieser Schritt wird auch als einer der Auslöser für die Weltwirtschaftskrise der 1930er Jahre gesehen.[14]

In den Vereinigten Staaten von Amerika verbot der Gold Reserve Act 1934 jeglichen privaten Besitz von Währungsgold. Des Weiteren legte Theodore Roosevelt mit dem Gold Reserve Act einen fixen Goldkurs von 35 US-Dollar pro Feinunze Gold fest, der bis

---

5 [BCA44]
6 [Eic98, Seite 15ff The advent of the Gold Standard]
7 [All09, Seite 182 Gold Standard]
8 [All09, Seite 42 The Stability of the System]
9 [All09, Seite 182 Gold Standard]
10 [Eic98, Seite 57]
11 [Eic98, Seite 60]
12 [Eic98, Seite 63ff Problems of the new Gold Standard]
13 [Eic98, Seite 66]
14 [Eic98, Seite 72]

1971 bestehen bleiben sollte.[15]

1.2 Bretton-Woods-Konferenz

Nach den Jahren des Zweiten Weltkriegs wurde es zunehmend wichtiger, eine neue Weltwirtschaftsordnung zu finden. Zu diesem Zweck gab es bereits während des Kriegs Vorbereitungen. Vor allem die USA und Großbritannien waren seit Beginn der 1940er Jahre auf der Suche nach neuen Systemen.[16]

1944 wurde schließlich die „United Nations Monetary and Financial Conference“ in Bretton Woods (New Hampshire, USA) ausgetragen, die später vor allem als Bretton Woods-Konferenz bekannt wurde. Geladen waren Repräsentanten von 44 Nationen[17], denen zwei mögliche Pläne vorgestellt wurden: Einerseits ein Plan des britischen Ökonomen John Maynard Keynes und andererseits ein Vorschlag des US-Amerikanischen Ökonomen Harry Dexter White.[18]

John Maynard Keynes Plan sah die Gründung einer internationalen Bank, genannt International Clearing Unit (ICU) sowie eine supranationale Währung, genannt Bancor, vor. Alle nationalen Währungen sollten an den Bancor mit einem fixen Währungskurs gebunden sein. Internationaler Handel sollte Bancor als Rechnungseinheit verwenden. Bancor könnte in diesem Fall dazu verwendet werden, um Überschüsse oder Defizite in der Handelsbilanz von Ländern zu vergleichen. Für jede Nation hätte die ICU ein Konto mit Überziehungsfunktion vorgesehen, aber sowohl starke Defizite als auch hohe Überschüsse mit Zinsen belegt. Länder mit Überschüssen hätten also ein Interesse deren Überschüsse einzudämmen. Mittel, die dies in Gang setzten, zum Beispiel eine Aufwertung der nationalen Währung, würden automatisch dazu beitragen, das Defizit in anderen Ländern auszugleichen. Für Länder mit konstanten Bilanzüberschüssen ist es naheliegend, dass dieses System Nachteile beziehungsweise höhere Kosten mit sich bringen würde.[19]

---

15 [All09, Seite 175 Gold Reserve Act of 1934 (United States)]
16 [Eic98, Seite 96]
17 [Ste13, Seite 1 Introduction]
18 [Eic98, Seiten 93ff]
19 [Mon08]

Der Plan von Harry Dexter White wiederum sah den US Dollar als zentrale Währung vor, zu dem nationale Währungen mit festem Kurs gebunden waren. Der US-Dollar sollte damit zur einer weltweiten, zentralen Währung werden und war in diesem Vorschlag mit einem fixem Wechselkurs an Gold gebunden. Nationen waren verpflichtet, durch An- oder Verkäufe von Fremdwährungen die eigenen Währungen in einem Bereich innerhalb von Plus/Minus 1% des fixierten Wechselkurses zu halten. White sah des Weiteren die Gründung eines Fonds, genannt International Monetary Fund (Internationaler Währungsfonds) vor, in den Staaten Beträge einzuzahlen hatten und der im Zweifelsfall Kredite an Staaten vergeben konnte. Des Weiteren sah der Plan die Gründung der International Bank for Reconstruction and Development (IBRD) vor, die die Einhaltung der Regeln überwachen sollte.[20]

Die Vormachtstellung der USA in den Verhandlungen führte schließlich dazu, dass das Bretton-Woods-Abkommen und damit das neu geschaffene Bretton-Woods-System zu großen Teilen jenem Vorschlag von Harry Dexter White entsprach.[21]

> „(a) The par value of the currency of each member shall be expressed in terms of gold as a common denominator or in terms of the United States dollar of the weight and fineness in effect on July 1, 1944.“[22]

Der US-Dollar wurde zu einer internationalen Leitwährung, an die alle anderen Währungen mit einem fixen Wechselkurs gebunden waren. Staaten waren verpflichtet, Schwankungen innerhalb einer Bandbreite von 1% auszugleichen[23]. Die USA andererseits verpflichteten sich zu einem festen Wechselkurs von 35 USD pro Feinunze Gold[24], zu welchem jede teilnehmende Nation unbegrenzt US-Dollar zu Gold und umgekehrt tauschen konnte.

Das Bretton Woods System funktionierte, solange sich die USA einer guten Konjunktur erfreuen konnten und sich das Dollarangebot international annähernd gleichzeitig zum Welthandel entwickelte. Mit Ende der 1950er Jahre mussten die USA aus

[20] [Eic98, Seite 96], [All09, Seite 50–51], [BWA44]
[21] [Eic98, Seite 97]
[22] [BWA44, Art IV Section 1: Expression of Par Values]
[23] [BWA44, Art IV Section 3: Foreign Exchange Dealings Based On Parity]
[24] Vergleiche Gold Reserve Act 1934 in *Goldstandard (Abschnitt 1.1).*

unterschiedlichen Gründen, darunter auch wegen des Vietnam-Kriegs, mit Leistungsbilanzdefiziten kämpfen. Der belgische Ökonom Robert Triffin warnte bereits 1959 vor Konstruktionsfehlern im Bretton-Woods-Systems[25]. Den USA blieb nur eine von zwei möglichen Reaktionen, die jedoch beide die Weltwirtschaft in Gefahr bringen würden[26]:

- Defizit stoppen und damit der Weltwirtschaft den Zustrom von Liquidität in US-Dollar entziehen;
- Defizit beibehalten und Weltwirtschaft mit US-Dollar versorgen, jedoch langfristig der Goldkonvertibilität die Glaubwürdigkeit entziehen.

Dieser Konstruktionsfehler sollte später als „Triffin-Dilemma“ bekannt werden.[27] Der Vorschlag Triffins war die Einführung eines neuen Reservemediums und damit eine teilweise Rückbesinnung auf John Maynard Keynes Vorschläge. Dieses neue Reservemedium wurde vom Internationale Währungsfond 1967 beschlossen und 1970 eingeführt. Allerdings zu spät, um einen Zusammenbruch zu vermeiden.[28]

1.3 Fiatgeld

Durch den Vietnam-Krieg und dessen Finanzierung sowie durch andere Ereignisse in den 1960er Jahren kam es also von Seiten der USA zu einer massiven Ausgabe von US-Dollar Noten (Dollarschwemme). Bretton-Woods-Mitgliedsstaaten mussten USD kaufen, um den nationalen Währungskurs innerhalb der vereinbarten Bandbreiten zu halten. Dieses Ungleichgewicht führte dazu, dass die USA 1971 lediglich 291.6 Millionen Feinunzen Gold besaßen, die 7 Europäischen Mitgliedsstaaten hingegen 481.7 Millionen Feinunzen. Im Vergleich dazu lag der Goldbesitz im Jahr 1950 bei 652 Millionen Feinunzen (USA) und 95 Millionen Feinunzen durch die 7 Europäischen Mitglieder.[29]

Die US-Regierung unter Präsident Richard Nixon setze schließlich die Goldkonvertabilität mit dem Wochenende zum 13. August 1971 aus.[30] Richard Nixon wandte sich mit einer Fernsehansprache am Sonntag, den 15. August an das amerikanische Volk:

[25] [Han08, Seiten 11–12]
[26] [Han08, Seiten 11–12]
[27] [Eic98, Seite 116]
[28] [Han08, Seiten 11–12]
[29] [Han08, Seite 12]
[30] [Eic98, Seite 133]

„The third indispensable element in building the new prosperity is closely related to creating new jobs and halting inflation. We must protect the position of the American dollar as a pillar of monetary stability around the world.
In the past 7 years, there has been an average of one international monetary crisis every year…
I have directed Secretary Connally to suspend temporarily the convertibility of the dollar into gold or other reserve assets, except in amounts and conditions determined to be in the interest of monetary stability and in the best interests of the United States.
Now, what is this action — which is very technical — what does it mean for you?
Let me lay to rest the bugaboo of what is called devaluation.
If you want to buy a foreign car or take a trip abroad, market conditions may cause your dollar to buy slightly less. But if you are among the overwhelming majority of Americans who buy American-made products in America, your dollar will be worth just as much tomorrow as it is today.
The effect of this action, in other words, will be to stabilize the dollar.“[31]

Wenn die Konvertibilität auch vorerst nur temporär ausgesetzt wurde, sollte dieses Ereignis das Ende des Bretton-Woods-Systems einläuten. Versuche, das Bretton-Woods-System zu retten, scheiterten und so hatten ab 1973 die wichtigsten Weltwährungen frei schwankende Wechselkurse.[32]

Moderne Währungen haben keinen Wert per se, es liegt ihnen kein wertbehafteter Rohstoff oder Vergleichbares zu Grunde. Der Wert moderner Währung kommt dadurch zustande, dass ein Staat seine Macht nützt: Einerseits als ausgebende Stelle, um das Angebot an Geld zu limitieren und andererseits als Normsetzer durch Festlegung eines gesetzlichen Zahlungsmittels und damit Erzeugung einer entsprechenden Nachfrage.[33] Dieses System wird deshalb auch als inkonvertibler Papierstandard und dessen Wäh-

[31] [Nix71]
[32] [Han08, Seite 12]
[33] [All09, Seite XIV]

rung als Fiatgeld (vom Lateinischen fiat – „es entstehe“) bezeichnet.[34]

1.4 Virtuelle Währungen

Fiat-Währungen mit flexiblen Wechselkursen sind zum Zeitpunkt dieser Arbeit nach wie vor gültig und in nahezu allen Ländern weltweit in Verwendung. Flexible Wechselkurse ungeachtet existieren jedoch auch zwischenstaatliche Vereinbarungen, die die Wechselkurse in gewissen fixierten Bandbreiten halten. Ein Beispiel dafür ist das 1979 gegründete Europäische Währungssystem.

Mit Einführung des Europäischen Währungsraums und des Euro im Jahr 2002[35] als supranationaler Währung wurde von den Mitgliedstaaten die Zuständigkeit der Währungspolitik an die Europäische Union abgetreten.[36]

Bedingt durch die Entwicklung des Internets und dessen großflächige Verbreitung in 1990er Jahren gab es zunehmend Bestrebungen, Währungen für das digitale Zeitalter zu schaffen. Als Teil dieser Entwicklung haben sich neue Begriffe[37] etabliert, die oftmals in widersprüchlicher Weise verwendet werden. Es erscheint demnach notwendig, vorerst eine Differenzierung von Begriffen wie Kryptowährungen, digitalen Währungen, virtuellen Währungen und E-Geld vorzunehmen.

Die einfachste Definition kann möglicherweise für **Kryptowährung** („cryptocurrency“) gefunden werden. Wie der Name bereits andeutet, nutzen Kryptowährungen Methoden der Kryptographie, um Eigenschaften von Transaktionen wie Integrität, Authentizität und mehr sicherzustellen.[38]

E-Geld (als Abkürzung für elektronisches Geld) wiederum stellt eine herkömmliche Fiat-Währung dar, die in einer digitalen Geldbörse gespeichert ist und von dort verwendet werden kann. Als E-Geld klassifiziert werden kann zum Beispiel die Quick-Funktion auf Bankkomatkarten. Diese erlauben das Aufladen des Chips mit einem bestimmten Betrag, der jederzeit an Quick-Akzeptanzstellen ausgegeben werden kann. Die

[34] [All09, Seite XIV]
[35] Der Euro wurde bereits am 1. Januar 1999, jedoch ausschließlich als Buchgeld eingeführt.
[36] Vertrag über die Arbeitsweise der Europäischen Union 2012/C 326/01.
[37] [Bra14]
[38] [Sch95, Seiten 15–16 Kapitel 1 Foundations]

Online-Anbieter wie PayPal[39] oder ClickandBuy[40] können ebenfalls als E-Geld-Börsen qualifiziert werden. In der Europäischen Union legt die E-Geld-Richtlinie beziehungsweise deren Umsetzung in nationales Recht die Rahmenbedingungen der Anwendung vom E-Geld fest.[41]

Digitale Währung stellt einen weiteren, häufig verwendeten Begriff dar. Der Begriff „digital“ lässt darauf schließen, dass die Verarbeitung der Währung rechnergestützt geschieht. Hier muss jedoch bedacht werden, dass auch bei herkömmlichen Fiat-Währungen ein großer Anteil mittlerweile ausschließlich digital verarbeitet wird. Beispiele sind unter anderem Kartenzahlungen, aber auch bankeninterne Transaktionen. So werden 75% aller Transaktionen im britischen Einzelhandel bereits per Kredit- oder Bankomatkarten abgewickelt.[42]

Virtuelle Währungen sind jene Währungen die eine physische Existenz ausschließen und demnach nur virtuell existieren. In abweichenden Begriffsdefinitionen werden virtuelle Währungen teilweise auf einen bestimmten Bereich (zum Beispiel Währung in Online-Spielen) beschränkt. Diese Währungen zeichnet aus, dass es üblicherweise keine Möglichkeit der Umwechslung zurück zu Fiat-Währungen gibt und die Akzeptanz auf den Kontext des Spieles beschränkt ist.

Allerdings schließen sich virtuelle und digitale Währungen als Begrifflichkeit nicht aus. Virtuelle Währungen sind in der Regel auch digitale Währungen, umgekehrt ist dies nicht unbedingt gegeben. Wie *Rechtliche Abgrenzung (Kapitel 2)* zeigen wird, ist E-Geld digital, jedoch kann es nach geltendem Recht nicht virtuell sein. Kryptowährungen sind digitale Währungen und nach allgemeiner Auffassung auch virtuelle Währungen.

1.4.1 Klassifikation

Die **Europäische Zentralbank** (EZB) hat im Jahr 2012 als eine der ersten internationalen Einrichtungen eine Einschätzung zu virtuellen Währungen publiziert. Der 55-seitige Bericht mit dem Titel „Virtual Currency Schemes“ analysiert verschiedene Ausprägungen von virtuellen Währungen, gibt eine Einordnung in bestehende Finanzsysteme, führt

[39] https://paypal.com
[40] http://clickandbuy.com
[41] [E-G15], [EG209]
[42] [Dod15]

Tabelle 1.1: Money-Matrix[46]

Rechtsstatus	**Unreguliert**	Bestimmte Arten von regionalen Währungen	Virtuelle Währungen
	Reguliert	Banknoten und Münzen	E-Geld Geschäftsbankgeld
		Physisch	**Digital**
		Geldformat	

Definitionen ein und gibt in Folge Risikoabschätzungen aus Sicht einer Zentralbank mit weltweiter Bedeutung.[43]

> „A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.“[44]

Wie sowohl der Titel des publizierten Dokuments als auch dieses Zitat – entnommen aus der einleitenden Kurzfassung – augenscheinlich machen, verwendet die Europäische Zentralbank als Überbegriff jenen der virtuellen Währung, definiert den Begriff selbst jedoch nicht so offen, wie es die allgemeine Auffassung vermuten lassen würde.[45]

Zur Position von virtuellen Währungen und deren Einordnung in herkömmliche Systeme definiert die EZB eine so genannte *Money Matrix (Tabelle B.1)* und positioniert virtuelle Währungen damit als digitales, unreguliertes Geld.

Nach Einschätzung der Europäischen Zentralbank sind virtuelle Währungen unterschiedlichster Natur und sind deshalb in 3 Typen zu klassifizieren. Die Typen unterscheiden sich im Detail vor allem durch die Möglichkeit inwiefern die virtuelle Währung in herkömmliche Fiat-Währung getauscht werden kann oder nicht.[47]

Virtuelle Währungen vom Typ 1 werden als „closed virtual currency schemes“ definiert und besitzen wenig bis keine Bindung zur realen Wirtschaft. Typ 1 findet zum Beispiel in Spielen Anwendung, ein konkretes Beispiel ist WoW Gold im Onlinespiel World of Warcraft. Die Geschäftsbedingungen von World of Warcraft verbieten den

[43] [Eur12]
[44] [Eur12, Seite 5 Executive Summary]
[45] Vergleiche *Virtuelle Währungen (Abschnitt 1.4)*.
[46] Nach [Eur12, Table 1 A money matrix]
[47] [Eur12, Seite 13 Kapitel 2.1 Definition and Categorisation]

Erwerb oder Verkauf von WoW Gold mit Gegenwert in Fiat-Geld. Für Spieler gibt es unterschiedliche Abonnements die das Spielen ermöglichen. Im Laufe des Spielens wird regelmäßig WoW Gold an die Spieler ausgeschüttet und ermöglicht so innerhalb des Spiels den Kauf von Ausrüstung, Waren, et cetera, um in höhere Level aufzusteigen.[48]

Als „Virtual currency schemes with unidirectional flow" werden virtuelle Währungen vom Typ 2 bezeichnet. Sie sind mit herkömmlichem Fiat-Geld zu erwerben (umtauschbar), können jedoch nicht zurückgetauscht (verkauft) werden. Ihre Verwendung ist ausschließlich auf einer dafür vorgesehen Plattform, bei einem speziellen Händler oder dergleichem vorgesehen. Als Beispiele dafür werden unter anderem Facebook Credits[49] und Nintendo Points erwähnt. Beide sind zu einem vom Anbieter festgelegten Kurs zu erwerben. Die Verwendung ist jedoch auf die jeweilige Plattform und die dort angebotenen Waren beschränkt.[50] Auch das Meilenkonto bei Vielfliegerprogrammen von Fluglinien wird als **Typ 2** klassifiziert.[51]

Typ 3 ist als „Virtual currency schemes with bidirectional flow" bezeichnet. Es ist also ein Erwerb und auch Verkauf der virtuellen Währung möglich. Als Beispiel genannt werden Linden Dollars (jene Währung, die in der Onlinewelt Second Life verwendet wird). Zweifelsohne muss auch Bitcoin in die dritte Kategorie eingeordnet werden.[52] Nichtsdestotrotz merkt die Europäische Zentralbank jedoch an, dass Bitcoin signifikante Unterschiede zu anderen virtuellen Währungen vom selben Typ aufweist.[53]

Das **Financial Crime Enforcement Network** (FinCEN), welches dem United States Department of the Treasure (US-Finanzministerium) untersteht, hat im Jahr 2013 eine Einschätzung zur Regulierung[54] von modernen Währungen vorgelegt.

Auch das FinCEN verwendet als übergeordneten Begriff „virtuelle Währungen" („Virtual Currencies") und im Zuge dieses Leitfadens wird eine Unterteilung von virtuellen Währungen in Kategorien vorgenommen. Die Kategorisierung weicht von jener der Europäischen Zentralbank ab und richtet den Fokus vor allem auf den Rechtsstatus

---

48 [Eur12, Seiten 13–14 Kapitel 2.1 Definition and Categorisation]

49 Die Akzeptanz von Facebook Credits wurde September 2013 zugunsten von lokalen Währungen eingestellt.[Coh13]

50 [Eur12, Seiten 13–14 Kapitel 2.1 Definition and Categorisation]

51 [Eur12, Seite 15 Box 1 Frequent-Flyer Programmes]

52 [Eur12, Seite 13–14 Kapitel 2.1 Definition and Categorisation]

53 [Eur12, Seite 21 Kapitel 3.1 The Bitcoin Scheme]

54 Vergleiche *USA (Unterabschnitt 2.4.1).*

der Währung.[55]

FinCEN unterscheidet demnach lediglich zwei Arten von virtuellen Währungen. Jene, die sich durch eine zentrale regulierende Stelle auszeichnen („Centralized Virtual Currencies“) und jene, die dezentral ausgerichtet sind („De-Centralized Virtual Currencies“). FinCEN listet des Weiteren noch eine dritte Kategorie: E-Geld und E-Edelmetalle („E-Currencies and E-Precious Metals“), die von der Europäischen Zentralbank explizit von den virtuellen Währungen ausgenommen wurden.[56]

1.4.2 Historie

Das erste Zahlungsmittel der Internet-Ära war DigiCash. David Chaum hat das Konzept zu DigiCash 1990 in einem Arbeitspapier, betitelt als „Untraceable Electronic Cash“[57], vorgestellt. DigiCash war bis 1998 aktiv, musste jedoch im November 1998 Konkurs anmelden.[58]

Weitere frühe Vertreter waren E-Gold (1996), B-Money (1998) sowie Bit Gold (1998) und Gold Money (2001). Besonders das von Wei Dai entworfene B-Money war Satoshi Nakamoto, dem Erfinder von Bitcoin, bekannt und wird im Bitcoin Arbeitspapier als Quelle zitiert.[59]

Alle frühen Versuche hatten zum Ziel, eine Währung für das digitale Zeitalter zu schaffen. Als Problem stellte sich jedoch heraus, dass stets eine zentrale Stelle notwendig war. Dieser zentralen Stelle musste von jedem Nutzer vertraut werden und sie war des Weiteren ein möglicher Angriffspunkt, sei es für Staaten, die ein gewisses Interesse durchsetzen wollen, oder auch für dritte Angreifer.

Das Konzept von Bitcoin verwendet ein Peer-to-Peer Netzwerk und benötigt keine zentrale Stelle. Es ist niemandem möglich, den Erfinder zur Abschaltung des Netzwerks zu zwingen – selbst wenn dessen Identität bekannt wäre[60]. Noch kann ein Währungskurs von einer zentralen Stelle angepasst werden. Bitcoin ist eine entnationalisierte

[55] [Fin13]
[56] [Fin13]
[57] [CFN90]
[58] [Pit99]
[59] [Nak09a]
[60] Vergleiche *Historische Entwicklung (Abschnitt 3.1)*.

Währung. Der Währungskurs ergibt sich – wie in der freien Marktwirtschaft – ausschließlich durch Angebot und Nachfrage.

Als solches stellt Bitcoin in vielen Bereichen eine Währung dar, die von Ökonomen der österreichischen Schule und allen voran Friedrich Hayek nach dem Scheitern des Bretton-Woods-Systems theoretisch konzipiert wurde. Hayek führt Krisen wie die Weltwirtschaftskrise 1929 unter anderem auf Eingriffe in den Geldzinssatz und dessen Abweichung vom natürlichen Zinssatz zurück. In seinen Publikationen „Denationalisation of Money“[61] und „Choice in Currency: A Way to Stop Inflation“[62] wird deshalb die Entnationalisierung und die Einführung von Wettbewerb bei Währungen vorgeschlagen.

Der frei verfügbare Quellcode von Bitcoin legt nahe, dass es eine Vielzahl von Abwandlungen zu Bitcoin geben wird. Mit 15. Januar 2016 listet coinmarketcap.com 652 Kryptowährungen, darunter das Bitcoin Derivat Litecoin und einige Währungen, die auf ähnlichen Konzepten, aber unterschiedlichem Code basieren wie zum Beispiel Ripple oder Ethereum. Die Marktkapitalisierung von Kryptowährungen beträgt derzeit 6,5 Milliarden US-Dollar, wobei zirka 90% davon auf Bitcoin entfallen.[63]

1.4.3 Zusammenfassung

Auch wenn die Anfänge von virtuellen Währungen bereits 25 Jahre zurückliegen[64], fällt die Einordnung von Bitcoins und anderen Kryptowährungen schwer. Eine eindeutige Einordnung in die bestehenden Lehren der Ökonomie scheinen nicht ohne Weiteres möglich zu sein. Diese Erkenntnis teilt auch die Europäische Zentralbank in einer – 2015 publizierten – erweiterten Analyse von virtuellen Währungen:

> „Although the term “virtual currency” is commonly used – indeed, it often appears in this report – the ECB does not regard virtual currencies, such as Bitcoin, as full forms of money as defined in economic literature. Virtual currency is also not money or currency from a legal perspective. For the

[61] [Hay76a]
[62] [Hay76b]
[63] [coia]
[64] Vergleiche *Historie (Unterabschnitt 1.4.2)*.

> purpose of this report, it is defined as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money. The term "virtual currency scheme(s)" is used throughout this report to describe both the aspect of value and that of the inherent or in-built mechanisms ensuring that value can be transferred."[65]

In dieser Arbeit wird in Folge sowohl der Begriff „virtuelle Währungen" als auch „Kryptowährungen" verwendet.

[65] [Eur15]

2 Rechtliche Abgrenzung

Dieses Kapitel unternimmt den Versuch einer Einschätzung, inwiefern – als neu einzustufende Technologie – Bitcoin von der bestehenden Gesetzgebung abgedeckt ist. Der Fokus liegt hierbei auf dem österreichischen Recht. Nachdem Österreich ein Teil der Euro-Zone ist und durch dem Vertrag von Lissabon[66] die ausschließliche Zuständigkeit für Währungspolitik an die Europäische Union übertragen hat, wird Europarecht in den Einschätzungen nicht auszublenden sein.

Abschließend erfolgt eine Gegenüberstellung der Einschätzung mit der internationalen Entwicklung. International wird der Fokus auf zwei konträre Positionen gelegt: Einerseits jene der USA, in der es bereits erste dedizierte Gesetze für virtuelle Währungen gibt und andererseits jene Russlands, gemäß welcher anzunehmen ist, dass Bitcoin aufgrund von bestehendem Recht als gesetzwidrig einzustufen ist.

Wie sich zeigen wird, erschweren vor allem zwei spezielle Aspekte von Bitcoin die Einordnung: Zum einen die dezentrale, nicht staatlich anerkannte Provenienz der Währung und zum anderen die schwer definierbare Position des Emittenten.

2.1 Regulierung durch die Finanzmarktaufsicht

Um zu klären, ob der Handel mit Bitcoin einer Konzessionspflicht und damit einer Regulierung durch die Finanzmarktaufsicht unterliegt, müssen vor allem Definitionen aus dem Bankenwesengesetz, Wertpapieraufsichtsgesetz und Zahlungsdienstegesetz betrachtet und muss deren Anwendbarkeit auf Bitcoin untersucht werden.

Eine einheitliche und allgemein gültige Definition des Geldbegriffes existiert nicht[67].

[66] Art 3 Abs 1 lit c – Vertrag über die Arbeitsweise der Europäischen Union 2012/C 326/01.
[67] [SKG12, Seite 484, 4.2 Geld]

Nach allgemeiner juristischer Auffassung aber entsteht **Geld** durch einen „hoheitlichen Akt"; so definieren Falschlehner und Klausberger Geld als „das vom Staat anerkannte und mit Annahmezwang ausgestattete Zahlungsmittel".[68] Im österreichischen Recht erfolgt die Definition des staatlich anerkannten Zahlungsmittels in § 1 Eurogesetz. Nachdem der Bitcoin Mining Prozess[69] weder einen hoheitlichen Akt darstellt, noch ein Annahmezwang für Bitcoin besteht, kann eine Einordnung als Geld ausgeschlossen werden. Aufgrund der Tatsache, dass Bitcoin nicht als Geld einzustufen ist, ergibt sich des Weiteren, dass Bitcoin Tauschbörsen nicht dem Devisen- und Valutengeschäft im Sinne des §1 BWG[70] unterliegen[71].

§ 1 Abs 1 Z 7 BWG definiert neben Devisen- und Valutengeschäft noch weitere Punkte, die ein konzessionspflichtiges Bankgeschäft erfordern würden. Im Besonderen ist zu klären, ob Bitcoin als **Geldmarktinstrumente** nach § 1 Abs 1 Z 7 lit b BWG beziehungsweise **Wertpapiere** nach § 1 Abs 1 Z 7 lit e BWG definiert werden können.[72] Falschlehner und Klausberger kommen zum Schluss, dass beides zu verneinen ist. Geldmarktinstrumente liegen einerseits nicht vor, weil das vordergründige Ziel von Bitcoins nicht die kurzfristige Liquiditätsversorgung sei[73]. Wertpapiere andererseits liegen nicht vor, weil die vordergründige Anwendung von Bitcoins nicht der Kapitalanlage dient und ein laufender Ertrag fehlt. Aufgrund des fehlenden Ertrags, sind sie auch nicht als Effekte einzustufen[74].

E-Geld ist in Österreich durch § 1 Abs 1 E-Geldgesetz definiert:

> „E-Geld bezeichnet jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten [...] der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird."

und folgt damit bis auf kleine Abweichungen jener Definition in Art 2 Z 2 EU Richtlinie 2009/110/EG. E-Geld lässt sich grob in zwei Bereiche trennen: Zum einen die

[68] [FK14, Seiten 38ff, II. Bitcoin als Geld?]
[69] Vergleiche *Mining (Abschnitt 3.5).*
[70] Bankwesengesetz
[71] [FK14, Seiten 38ff, II. Bitcoin als Geld?]
[72] [FK14, Seiten 42ff, II. Bitcoin als Finanzinstrumente?]
[73] [FK14, Seite 44, A. Finanzinstrumente iSd § 1 Abs 1 Z 7 bzw. 7a BWG]
[74] [FK14, Seite 45, A. Finanzinstrumente iSd § 1 Abs 1 Z 7 bzw. 7a BWG]

elektronische Geldbörse wie zum Beispiel die Quickfunktion auf österreichischen Bankomatkarten und zum anderen das Service von Onlineanbietern wie PayPal[75], ClickandBuy[76] und anderen. Für Bitcoin sind zwei Probleme vordergründig: Einerseits wird kein monetärer Wert gespeichert, sondern lediglich der private Schlüssel, der das Einlösen erlaubt[77]. Dies könnte allerdings äquivalent zu einer Speicherung des monetären Wertes gesehen werden[78]. Andererseits stellt die Formulierung „Forderung gegenüber dem E-Geld-Emittenten" ein Problem dar. Weder begründen Bitcoins eine Forderung gegenüber dem Emittenten[79], noch kann der Emittent bei Bitcoin genau festgemacht werden[80]. Der Europäische Gerichtshof teilt diese Ansicht, argumentiert jedoch mit der Tatsache, dass Forderungen nicht in „konventionellen Rechnungseinheiten" ausgedrückt werden[81].

Betreffend Geld und E-Geld kommt Ohler zu folgendem Schluss:

> „Vor allem macht der Gestaltwandel des Geldes eine einheitliche Beschreibung unmöglich. Das heutige Buchgeld bzw. das elektronische Geld ist mit den früheren Erscheinungsformen eben nur funktionell, aber nicht inhaltlich vergleichbar."[82]

Neben Finanzmarkinstrumenten, die im Bankwesengesetz definiert sind und deren Anwendbarkeit bereits verneint wurde, führt das Wertpapieraufsichtsgesetz eine weitere Definition von **Finanzinstrumenten**, die nicht vollständig der Definition des BWG entspricht. Würde die Definition von Finanzinstrumenten nach § 1 Z 6 WAG auf Bitcoin passen, so würden Tätigkeiten wie Anlagenberatung, Portfolioverwaltung und mehr[83] eine Konzessionspflicht bei der Finanzmarktaufsicht erfordern. Wie Falschlehner und Klausberger zeigen, ist jedoch auch diese Definition für Bitcoin nicht zutreffend. Argu-

---

75 https://paypal.com
76 http://clickandbuy.com
77 Vergleiche *Transaktionen (Abschnitt 3.3)*.
78 [SKG12, Seite 483, 4.1 E-Geld]
79 [SKG12, Seite 483, 4.1 E-Geld]
80 [FK14, Seite 40, III. Bitcoin als E-Geld?]
81 [EuG15b, Absatz 12]
82 [Ohl08, Seite 318, II. Das Wesen des Geldes]
83 Vergleiche § 3 Abs 2 WAG.

mentiert wird damit, dass Bitcoin nicht dem Kapitalmarkt zuzurechnen sind, weil sie in erster Linie für die Zahlungsabwicklung vorgesehen sind.[84]

Das Zahlungsdienstegesetz definiert den Begriff **Zahlungsinstrument** in § 3 Z 21 ZaDiG folgendermaßen:

> "Zahlungsinstrument: jedes personalisierte Instrument oder jeder personalisierte Verfahrensablauf, das oder der zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde und das oder der vom Zahlungsdienstnutzer eingesetzt werden kann, um einen Zahlungsauftrag zu erteilen;"

Nach Falschlehner und Klausberger ist auch diese Definition für Bitcoin nicht zutreffend. Einerseits fehlt die erwähnte Personalisierung und andererseits wird bei der Ausgabe von Bitcoins kein Vertragsverhältnis abgeschlossen.[85]

Falschlehner und Klausberger kommen schlussendlich zur Auffassung, dass Bitcoins unter den Begriff **Zahlungsmittel** nach BWG subsumiert werden können. Dadurch ergibt sich wegen § 1 Abs 1 Z 6 BWG die Notwendigkeit einer Konzessionsverleihung durch die Finanzmarktaufsicht, wenn eine Bitcoin-Tauschbörse betrieben wird.[86] Diese Ansicht entspricht jedoch nicht jener der Finanzmarktaufsicht[87] und auch nicht jener des Bundesministeriums für Finanzen[88]. FMA und BMF gehen im Gegensatz zu Falschlehner und Klausberger davon aus, dass eine grundsätzliche Konzessionspflicht nicht gegeben ist:

> „Nach Auffassung des Bundesministeriums für Finanzen stellen Bitcoins keine Finanzinstrumente dar. Grundsätzlich wird daher die Auffassung der Finanzmarktaufsicht (FMA) geteilt. Ebenso hält es das Bundesministerium für Finanzen für nicht ausgeschlossen, dass es Geschäftsmodelle geben kann, die eine Konzessionspflicht auslösen."[89]

---

[84] [FK14, Seiten 46ff, B. Finanzinstrumente iSd § 1 Z 6 WAG]
[85] [FK14, Seite 52, B. Anwendung auf Bitcoins]
[86] [FK14, Seiten 52ff, B. Anwendung auf Bitcoins]
[87] [Ö15]
[88] [Spi14, Zu 1., 2., 7. bis 13. und 15. bis 17.]
[89] [Spi14, Zu 1., 2., 7. bis 13. und 15. bis 17.]

2.2 Steuerrecht

Auch für die Klärung der Frage, ob der Tausch von Bitcoins steuerrechtliche Relevanz hat, muss geklärt werden, inwiefern Bitcoins unter bestehende Gesetze subsumiert werden können. Auf österreichisches Recht bezogen, gilt hier vor allem, die Frage zu klären, ob Bitcoins nach § 6 Abs 1 UStG steuerbefreit sind.

§ 6 Abs 1 Z 8 lit b UStG befreit „Umsätze und die Vermittlung der Umsätze von gesetzlichen Zahlungsmitteln“ von der Umsatzsteuerpflicht, § 6 Abs 1 Z 8 lit c UStG wiederum „Umsätze im Geschäft mit Geldforderungen und die Vermittlung dieser Umsätze“. Wie bereits in *Regulierung durch die Finanzmarktaufsicht (Abschnitt 2.1)* gezeigt wurde, beurteilen Juristen Bitcoins als Zahlungsmittel nach § 1 Abs 1 Z 6 BWG, staatliche Institutionen widersprechen dieser Ansicht jedoch. § 6 Abs 1 Z 8 lit c UStG ist auszuschließen, nachdem bei Bitcoin keine Forderungen anzunehmen sind, wie ebenfalls bereits in *Regulierung durch die Finanzmarktaufsicht (Abschnitt 2.1)* gezeigt werden konnte.[90][91]

Dieser Ansicht hat jedoch der Europäische Gerichtshof im Oktober 2015 widersprochen. David Hedqvist, Betreiber einer schwedischen Bitcoin Webseite[92], hat beim schwedischen Steuerrechtsausschuss (Skatterättsnämnden) einen Vorbescheid bezüglich Mehrwertsteuerrechtlicher Handhabung des Bitcoin An- sowie Verkaufs angefordert. Skatterättsnämnden kam 2013 zu dem Schluss, dass Bitcoins gesetzlichen Zahlungsmitteln gleichzusetzen seien und deshalb eine Steuerbefreiung anzuwenden sei[93]. Auf diesen Bescheid hinauf wurde durch die schwedische Steuerbehörde (Skatteverk) Klage beim obersten Verwaltungsgericht (Högsta förvaltningsdomstol) erhoben, der diese Frage wiederum dem Europäischen Gerichtshof vorgelegt hat.[94] Der Europäische Gerichtshof kommt in seiner Entscheidung zum Schluss, dass Richtlinie 2006/112/EG[95] Art. 2 Abs. 1 lit c derart auszulegen sei, dass der Betrieb einer Bitcoin-Börse als

[90] [Spi14, Zu 3.]
[91] [LW14, Seiten 87ff IV. Umsatzsteuer und Gebühren]
[92] https://bitcoin.se
[93] [SRN13]
[94] [EuG15a]
[95] Richtlinie 2006/112/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem.

eine gegen „Entgelt erbrachte Dienstleistung“ zu betrachten sei[96]. Zum anderen sieht der Europäische Gerichtshof die Steuerbefreiung beim An- und Verkauf von Bitcoins durch Art. 135 Abs. 1 lit e Richtlinie 2006/112/EG als gegeben an[97].

2.3 Strafrecht

Eine Sachbeschädigung ist nach § 125 StGB[98] folgendermaßen definiert:

> “Wer eine fremde Sache zerstört, beschädigt, verunstaltet oder unbrauchbar macht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.”

Wie zu sehen, bedient sich der Gesetzgeber zur Definition der Sachbeschädigung des Begriffs der **Sache**. Dies trifft auch auf eine Vielzahl von weiteren – und potenziell auf Bitcoins anwendbaren – Vermögensdelikten zu.[99] Die Sache als Grundlage haben Delikte wie:

- Diebstahl nach §§ 127–131 StGB
- Dauernde Sachentziehung § 135 StGB
- Entwendung § 141 StGB
- Raub nach § 142 StGB und schwerer Raub nach § 143 StGB
- Hehlerei § 164 StGB

Die Sache als Grundlage von Vermögensdelikten im Strafgesetzbuch baut hier auf dem Sachbegriff im Sinne des § 292 ABGB auf und man versteht darunter etwas körperliches, eine wahrnehmbare „abgrenzbare Materie“. Zweifelsohne ist dadurch eine Anwendbarkeit auf Bitcoins ausgeschlossen.[100] Die fehlende Körperlichkeit schließt im Weiteren Bitcoins auch von Delikten gegen unbare Zahlungsmittel aus, da sich die Definition von unbaren Zahlungsmitteln in § 74 Abs 1 Z 10 StGB ebenso auf den Begriff der Körperlichkeit bezieht:

[96] [EuG15b, Entscheidung 1]
[97] [EuG15b, Entscheidung 2]
[98] Strafgesetzbuch
[99] [Gla14, Seite 128 A. Gut, Sache und unbares Zahlungsmittel]
[100] [Gla14, Seite 128 A. Gut, Sache und unbares Zahlungsmittel]

„unbares Zahlungsmittel: jedes personengebundene oder übertragbare körperliche Zahlungsmittel, das den Aussteller erkennen lässt, durch Codierung, Ausgestaltung oder Unterschrift gegen Fälschung oder missbräuchliche Verwendung geschützt ist und im Rechtsverkehr bargeldvertretende Funktion hat oder der Ausgabe von Bargeld dient."

Neben dem Begriff der Sache sowie dem Begriff der unbaren Zahlungsmitteln sieht das StGB des Weiteren Delikte vor, die auf Begriff des **Guts** aufbauen. Darunter fallen vor allem die Delikte nach § 133 StGB (Veruntreuung) sowie § 134 StGB (Unterschlagung). In der Literatur besteht keine eindeutige Ansicht, wie der Begriff des Guts auszulegen ist. So wird er einerseits als ausschließlich auf körperliche Sachen anwendbar, interpretiert[101]. Andererseits gibt es jedoch auch Stimmen, die den Begriff weiter fassen und darunter „alles, was einen wirtschaftlichen Wert hat"[102] verstehen.[103]

Wenn auch Vermögensdelikte, basierend auf dem Begriff der Sache, keine Anwendung auf Bitcoins finden können und die Frage, ob Bitcoins unter den Begriff Gut eingeordnet werden können, nicht eindeutig geklärt ist, ist der Begriff der **Daten** im Sinne des § 74 Abs 2 StGB sehr allgemein auszulegen. Darunter zu verstehen sind im Gegensatz zum Datenbegriff im DSG[104] auch nicht personenbezogene Daten und damit kommen Delikte wie Datenbeschädigung (§ 126a StGB), Widerrechtlicher Zugriff auf ein Computersystem (§ 118a), Betrügerischer Datenverarbeitungsmißbrauch (§ 148a) und weitere für Bitcoin in Frage.[105]

So kann die Unterdrückung von Daten – zum Beispiel durch Entwendung eines Speichermediums, auf welchem sich Schlüssel[106] für den Zugriff auf Bitcoins befinden – den Tatbestand der Datenbeschädigung nach § 126a StGB erfüllen. In diesem Zusammenhang denkbar ist des Weiteren § 118a StGB, der ein widerrechtlichen Zugriff auf ein Computersystem unter Strafe setzt, sowie § 126c StGB, der einen Vorbereitungsdelikt zu den zwei genannten Paragraphen darstellt.[107] Glaser definiert die Strafbarkeit nach

[101] *Leukauf/Steininger,* Kommentar zum Strafgesetzbuch (§ 133 Rn 1a) 3. Auflage; zitiert nach [Gla14, Seite 129].
[102] *Bertel* in *Höpfel/Ratz*, WK2 StGB § 133 (Stand: 1.12.2008, rdb.at); zitiert nach [Gla14, Seite 129].
[103] [Gla14, Seiten 129ff A. Gut, Sache und unbares Zahlungsmittel]
[104] § 4 Z 1 Datenschutzgesetz (DSG 2000)
[105] [Gla14, Seiten 130ff B. Computerstrafrecht]
[106] Vergleiche *Asymmetrische Kryptographie (Unterabschnitt 3.2.1).*
[107] [Gla14, Seiten 130ff B. Computerstrafrecht]

§ 126c StGB folgendermaßen:

> „… bereits die Herstellung, Einführung, Bereitstellung, Verschaffung etc von Tatmitteln (Computerprogrammen, Passwörtern, Daten etc) zur Begehung eines Delikts nach §§ 118a, 126a StGB mit dem entsprechenden erweiterten Vorsatz.“[108]

Wie *Mining (Abschnitt 3.5)* und *Dezentraler Konsens (Abschnitt 3.6)* zeigen werden, ist es die Aufgabe eines Netzwerkknotens, publizierte Transaktionen auf deren Korrektheit zu überprüfen und nur bei erfolgreicher Prüfung an seine bekannten Knoten weiterzuleiten. Ein Miner[109] wiederum hat ausstehende Transaktionen ebenfalls auf deren Korrektheit zu überprüfen und in Blöcke zu sammeln. Wenn nun bewusst Transaktionen – auch im Fall von nicht erfolgreicher Prüfung – weitergeleitet werden, könnte dies ein Betrugsdelikt nach § 146 StGB darstellen. Nachdem die Entscheidung der zur Weiterleitung jedoch nicht von einer Person, sondern vielmehr von einem automatisierten Computersystem ausgeht, schließt Glaser die Anwendbarkeit von § 146 StGB in diesem Falle aus. Sehr wohl aber ist das Delikt des Betrügerische Datenverarbeitungsmissbrauchs erfüllt, das in § 148a Abs 1 StGB folgendermaßen definiert ist:[110]

> „(1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, daß er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflußt, …“

Aufgrund der pseudonymen Eigenschaft[111] von Bitcoin und üblicherweise fehlender Regulierung[112] erscheint Bitcoin als ein geeignetes Mittel zur Geldwäsche. Die

[108] [Gla14, Seite 132 B. Computerstrafrecht]
[109] Spezieller Bitcoin Netzwerkknoten, der versucht neue Blöcke zu finden und damit neuen monetären Wert zu erzeugen. Vergleiche *Mining (Abschnitt 3.5)*.
[110] [Seiten 132ff C. Datenfälschung, Betrug und Betrügerischer Datenverarbeitungsmissbrauch]
[111] Vergleiche *Bitcoin-Adressen (Unterabschnitt 3.3.3)*.
[112] Vergleiche *Regulierung durch die Finanzmarktaufsicht (Abschnitt 2.1)*.

Existenz von Dienstleistern[113], die Hilfe beim Verschleiern der Transaktionskette anbieten, scheint die These zu unterstützen. Das österreichische Strafgesetzbuch regelt das Delikt der Geldwäscherei in § 165 StGB und verwendet hierfür den Begriff der **Vermögensbestandteile**. Dieser Begriff wird in der Literatur ebenfalls weitläufig ausgelegt. Von Relevanz ist die Übertragbarkeit, die bei Bitcoin zweifelsohne gegeben ist. Eine Handlung im Sinne von § 165 StGB kann also auch mit Bitcoin begangen werden. § 278d StGB Abs 1 und Abs 1a definieren das Delikt der Terrorismusfinanzierung und verwenden hierfür ebenfalls den Terminus Vermögenswerte. Die Bereitstellung von Vermögenswerten, auch in Bitcoins, mit dem Vorsatz eine erpresserische Entführung auszuführen (§ 278d Abs 1 Z 2 StGB) oder alternative Delikte nach § 278d StGB, finden demnach auch Anwendung wenn dafür Bitcoins eingesetzt werden.[114]

Bitcoins können des Weiteren auch unter den Begriff **Vorteil** subsumiert werden. Damit können für die Verwendung von Bitcoins auch Wirtschaftdelikte in Betracht gezogen werden, die auf diesem Begriff aufbauen. Im Speziellen sind dies die Korruptionsdelikte nach §§ 304–309 StGB, demnach Delikte wie Bestechlichkeit, Vorteilsannahme, Beeinflussung, Vorteilszuwendung und Geschenkannahme.

2.4 Internationale Entwicklung

2.4.1 USA

Das Financial Crimes Enforcement Network (FinCEN), eine Institution, die dem US-Finanzministerium unterstellt ist, war im März 2013 die erste staatliche Einrichtung, die sich zur Regulierung von virtuellen Währungen geäußert hat. Im März 2013 wurde dazu von FinCEN ein Leitfaden[115] publiziert. Auch wenn Bitcoin in diesem Leitfaden keine Erwähnung findet, wird festgelegt, dass jede „decentralized convertible virtual currency“ (dezentrale umtauschbare virtuelle Währung) dem Bank Secrecy Act unterliegt. Die Verwendung von Bitcoins kann dadurch die Definition eines „Money Services Business“ (MSB) erfüllen und eine Lizenzierung und Regulierung als „Money Transmit-

[113] Üblicherweise als Bitcoin Mixer oder Bitcoin Tumbler bezeichnet. Beispiele sind https://bitmixer.io, http://joinmarket.io, https://bitlaunder.com, et cetera.
[114] [Gla14, Seiten 135ff D. Geldwäscherei]
[115] [Fin13]

ter“ nach 31 CFR[116] § 1010.100(ff)(5) erfordern.[117] Die Einordnung des Leitfades sieht vor:[118]

- Privatpersonen, die Bitcoins hauptsächlich in Waren und Dienstleistungen tauschen (und umgekehrt), sind als Nutzer der Währung und nicht als MSB einzustufen.
- Unternehmen, die Bitcoins von Personen akzeptieren und diese an andere Personen weitergeben, sind als MSB einzustufen, auch wenn keine Transaktionen in Fiat-Währungen getätigt werden.
- Miner sind als MSB einzustufen, auch wenn diese nicht als Unternehmer agieren.
- Unternehmen, die Fiat-Währungen zu virtuellen Währungen oder virtuelle Währungen zu virtuellen Währungen tauschen, sind als MSB einzustufen.

Dabei wurde auch der Begriff Miner nicht explizit genannt, sondern mit folgendem Satz umschrieben:

> „A person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent [...]“[119]

Einmal mehr gilt hier, die Frage des Emittenten von neuen Bitcoins zu klären und ob ein Miner, der für den Arbeitsaufwand mit monetärem Gegenwert belohnt wird[120], tatsächlich als „Person that creates units of convertible virtual currency“ bezeichnet werden kann. Im Gegensatz zum europäischen Recht[121] dürfte dies im US-Recht jedoch der Fall sein:

> „The (albeit anecdotal) consensus among legal professionals is that despite the terminological confusion, FinCEN did, in fact, mean to specifically call out miners.“[122]

[116] Code of Federal Regulations
[117] [San13b, Money transmission on the federal level]
[118] [San13b, Money transmission on the federal level]
[119] [Fin13, c. De-Centralized Virtual Currencies]
[120] Vergleiche *Anreiz (Unterabschnitt 3.5.2)*.
[121] Vergleiche *Regulierung durch die Finanzmarktaufsicht (Abschnitt 2.1)*.
[122] [San13b]

Die Subsumierung unter den Bank Secrecy Act bedeutet auf Bundesebene (federal law), dass Unternehmen Regelungen nach der „Anti Money Laundering Policy“, festgelegt in 31 CFR § 1023.210, sowie „Know Your Customer Policy“, definiert in 31 CFR § 1023.220, umzusetzen haben und Teilen des Patriot Acts unterliegen.[123]

Die tatsächliche Lizenzierung unterliegt jedoch den Bundesstaaten (state law) und deren Gesetzgebung legt fest, ob eine Lizenzierung notwendig ist. So verleihen South Carolina und Montana keine Money Transmission Lizenz.[124] Der Commissioner of Banks in North Carolina andererseits hat im Dezember 2015 angekündigt, bestimmte Bitcoin Unternehmen („digital currency miners; non-financial blockchain services; and multi-signature and non-custodial wallet providers“) von der Lizenzpflicht auszunehmen.[125][126] Sofern ein Bundesstaat eine Lizenzierung voraussetzt, ist es des Weiteren vom Bundesstaat abhängig – eine Frage der extraterritorialen Zuständigkeit – wann diese Lizenzierung greift. So kann das Anbieten eines Dienstes in einem Bundesstaat bereits die Lizenzpflicht auslösen, während in anderen Bundesstaaten ein Firmensitz notwendig ist, um diese Pflicht auszulösen.[127] So hat das Unternehmen Coinbase[128] zum Zeitpunkt des Verfassens dieser Arbeit Lizenzen in 25 Bundesstaaten sowie eine weitere Lizenz im District of Columbia, der nach US-Recht keinen eigenständigen Bundesstaat darstellt.[129]

BitLicense

New York hat im Juni 2015 als erster Bundesstaat ein Gesetz speziell zur Regulierung von virtuellen Währungen – auch BitLicense genannt – verabschiedet.[130] BitLicense (23 CRR-NY I 200) definiert Virtual Currency Business Activity und damit verbunden die Pflicht einer Lizenzierung in Section 200.2 (q) folgendermaßen:

> „(q) Virtual Currency Business Activity means the conduct of any one of the

[123] [San13b]
[124] [San13a]
[125] [Nor]
[126] [Riz15a]
[127] [San13a]
[128] Vergleiche *Bitcoin im E-Commerce (Kapitel 4)*.
[129] [Coib]
[130] [New15b]

> following types of activities involving New York or a New York Resident: (1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;
> (2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
> (3) buying and selling Virtual Currency as a customer business;
> (4) performing Exchange Services as a customer business; or
> (5) controlling, administering, or issuing a Virtual Currency.
> The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity."

Der Tätigkeitsbereich ist demnach sehr weit gefächert und umfasst jede Aktivität, die New York oder Bewohner des Bundesstaates New York involviert. Kritik an BitLicense betrifft vor allem zwei essentielle Bereiche des Gesetzes: Einerseits die Kosten, die durch Bewerbung, aber in Folge auch durch die Umsetzung von geforderten Maßnahme entstehen. Andererseits Bedenken hinsichtlich der Privatsphäre, die jeden Nutzer von BitLicense-regulierten Unternehmen betreffen.

Die Lizenzierung als MSB ist „kein Recht, sondern vielmehr ein Privileg".[131] Auch bei Erfüllung der formalen Anforderungen besteht kein Rechtsanspruch, die Bundesstaaten können eine Bewerbung demnach ablehnen.[132] Section 200.5 sieht eine Anmeldegebühr von 5,000 USD für jedes Unternehmen vor, die auch im Fall einer Ablehnung nicht retourniert wird („If the application is denied or withdrawn, such fee shall not be refunded."). Neben der Anmeldegebühr sind des Weiteren Kapitalreserven Voraussetzung, die Section 200.8 definiert. Die Höhe der notwendigen Kapitalreserven wird von Fall von Fall festgelegt.

Zu diesen Kosten müssen des Weiteren laufende Kosten für die Aufzeichnung sämtlicher Transaktionen und Speicherung der Daten beachtet werden. Die Aufzeichnungspflicht ist in Section 200.12 festgelegt und umfasst folgende Daten für jede Transaktion:

[131] [San13a]
[132] [San13a]

- Transaktionsumfang und Umfang an Gebühren
- Datum und präzise Zeitangabe
- Name, Kontonummer und physische Adresse jeder involvierten Personen

Sowie ausführliche weitere Aufzeichnungen (in Section 200.12 (a)(2) bis (a)(9) definiert) über einen Großteil der Firmenaktivitäten. Diese Daten sind für 7 Jahre zu speichern und müssen nach Section 200.12 Absatz (b) jederzeit auf Anfrage Behörden zur Verfügung gestellt werden.[133]

2.4.2 Russland

Artikel 75 Abs 1 der Verfassung der russischen Föderation definiert den Rubel als Währung folgendermaßen:

> „1. Die Geldeinheit in der Rußländischen Föderation ist der Rubel. Die Geldemission erfolgt ausschließlich durch die Zentralbank der Rußländischen Föderation. Die Einführung und die Emission anderen Geldes in der Rußländischen Föderation ist unzulässig."[134]

Das Russische Bundesgesetz zur Zentralbank der russischen Föderation (Bank of Russia) in Artikel 27 des Weiteren:

> „The rouble shall be the official monetary unit (currency) of the Russian Federation. It shall be equal to 100 kopecks. The issue of any other monetary units or quasi-money shall be prohibited in the Russian Federation."[135]

Bezugnehmend auf Artikel 27 des russischen Zentralbankgesetzes hat die Bank of Russia im Januar 2014 in einer Aussendung die Verwendung von Bitcoin als illegal bezeichnet und Unternehmen, die Bitcoin verwenden, pauschal eine Verwicklung in Aktivitäten wie Geldwäsche und Terrorismusfinanzierung unterstellt.[136]

---

[133] [Rei14]
[134] [CRF93]
[135] [RCB08]
[136] [Ban14]

Diese Position, und dabei vor allem die Subsumierung von Bitcoins unter den Begriff der „Money Surrogates“, wurde kurz darauf vom Büro des Generalstaatsanwaltes untermauert.[137]

Die Ansicht, dass Bitcoins in Russland als verboten einzustufen seien, hat auch das Europäische Parlament in einer Analyse der internationalen Entwicklung im April 2014 als Fakt erachtet.[138]

Im August 2014 wurde in Folge durch den russischen Finanzminister Aleksey Moiseev ein Gesetz angekündigt, zumal die russische Gesetzgebung keine Formaldefinition des Begriffes „Money Surrogate“ vorsehe:

> „According to Article 27 of the Federal Law ‘On the Central Bank of the Russian Federation’ (Bank of Russia) the official Russian currency is ruble. The issuance of monetary surrogates in Russia is forbidden as well as the introduction of other monetary units. However, monetary surrogate has no standard definition in the Russian legislation.“[139]

Trotz gegenteiliger Ansichten des Ministeriums für Wirtschaftsentwicklung[140] wurde der ablehnende Kurs von Russland fortgesetzt. Ein Gesetzesentwurf vom Oktober 2014, der die Nutzung von Bitcoin mit bis zu 500,000 RUB unter Strafe stellt, wurde jedoch nicht umgesetzt.[141] Im Januar 2015 wurde durch die staatliche Medienaufsicht Roskomnadzor damit begonnen, den Zugriff auf Webseiten[142] mit Bitcoin-relevanten Inhalten und Diensten in Russland zu sperren.[143] Diese Blockaden wurden im Mai 2015 wiederum aufgelöst, nachdem die Unternehmen BTCsec.com und Event Smile rechtliche Schritte eingeleitet hatten und das Landesgericht in Sverdlovsk die Sperren für unzulässig erklärt hat.[144]

Wladimir Putin, Russlands Präsident, hat sich 2015 ebenfalls gegen eine Kriminalisierung von Bitcoin ausgesprochen:

---

137 [Rus14a]
138 [Eur14]
139 [Kos14]
140 [Rus14b]
141 [Riz14]
142 bitcoin.org, btcsec.com, bitcoin.it, coinspot.ru, indacoin.com, hasbitcoin.ru sowie bitcoinconf.ru
143 [Rus15]
144 [Bit15d]

„[Bitcoins] are backed by nothing. This money [is backed by nothing], that's the point, this is the major problem. They are not really linked to anything and backed by nothing, [...] However as an accounting unit, these ‚coins' or whatever are they called, they can be used, and their adoption becomes wider and wider. As some kind of unit in some account, probably, it's possible. [...] We do not reject anything, but there are serious, really fundamental issues related to its wider usage, at least, today."[145]

Das Finanzministerium dürfte, davon unbeeindruckt, einen neuen Gesetzesentwurf vorbereitet haben und so wurde im October 2015 erneut ein Entwurf für ein Gesetz, das die Nutzung von Bitcoin unter Strafe stellt, vorgelegt. In diesem Entwurf sind Haftstrafen bis zu einem Ausmaß von 4 Jahren vorgesehen.[146]

Zusammenfassend ist zu sagen, dass der rechtliche Status in Russland als äußert unklar einzustufen ist. Für den Fall, dass Bitcoin im russischen Recht unter den Begriff des Geldersatzes (Money Surrogate) subsumiert werden kann, ist dennoch nicht geklärt, ob Artikel 27 des Zentralbankgesetzes Anwendung finden kann. Es wird vordergründig das Emittieren von neuem Wert verboten, doch wie bereits in *Regulierung durch die Finanzmarktaufsicht (Abschnitt 2.1)* thematisiert wurde, ist es fragwürdig ob das neuartige Konzept des Minings überhaupt als Geldausgabe angesehen werden kann.

Die russische Bevölkerung scheint von der unklaren rechtlichen Situation derzeit unbeeindruckt. So lag das Umtauschvolumen der zwei größten Bitcoin-Tauschbörsen, die auch den Russischen Rubel unterstützen, im Zeitraum von 11.Dezember 2014 bis 11. Dezember 2015 bei 95,733.50 XBT[147] sowie 150,784.66 XBT[149].

[145] [Riz15b]
[146] [Sor15]
[147] [BTC15b] Handelsvolumen der Plattform https://localbitcoins.com[148] von 11.12.2014 bis 11.12.2015.
[149] [BTC15a] Handelsvolumen der Plattform https://btc-e.com[150] von 11.12.2014 bis 11.12.2015.

3 Bitcoin

Der Begriff Bitcoin hat mehrere Bedeutungen und kann demnach auf unterschiedlichste Arten verwendet werden. „Bitcoin ist eine dezentrale, virtuelle Währung“ könnte eine allgemeine Beschreibung lauten. Tatsächlich umfasst Bitcoin aber ein deutlich weiteres Spektrum: vom Bitcoin-Netzwerk angefangen über die Architektur eines E-Commerce Systems und die geschickte Kombination aus unzähligen bestehenden Technologien bis hin zu einem öffentlich einsehbaren, digitalen Kassabuch, das auch Potential für viele weitere Anwendungsfälle hat, kann alles zum Teil mehr, zum Teil weniger als Bitcoin bezeichnet werden. Ein System, bei dem die Währung an sich noch lange keine Grenzen des Systems aufzeigt.

Internetnutzer, die sich dazu entscheiden, Bitcoins als Währung zu verwenden, können wie auch bei herkömmlichen Währungen beliebige Beträge in die virtuelle Währung umtauschen oder aber sich am sogenannten Mining beteiligen und neue Bitcoin-Münzen abbauen, also neuen Wert erzeugen. Unabhängig davon auf welche Art und Weise Nutzer in Besitz von Bitcoins kommen, können diese wiederum – ebenso wie bei konventionellen Währungen – in Güter und Dienstleistungen umgesetzt werden. Vom neuen Computer[151] über Kaffee im Coffeeshop[152] bis hin zu rechtswidrigen Angeboten wie Drogen[153] ist die Bandbreite an Angeboten groß und wächst stetig.

Während die Verwendung von Bitcoin oftmals den Eindruck hinterlässt, dass digitale Münzen von einem Nutzer zum nächsten übertragen werden, ist es tatsächlich jedoch so, dass lediglich Transaktionen mit einander verkettet werden. Bitcoin verwendet Methoden der asymmetrischen Kryptographie und ermöglicht es damit einem

[151] Siehe http://dell.com/bitcoin.
[152] Siehe http://www.paralelnipolis.cz/bitcoin-coffee-en/.
[153] Siehe http://www.onlinemba.com/blog/bitcoins/.

Nutzer, sich als Besitzer von monetärem Wert auszuweisen und diesen in Transaktionen zu verwenden. Transaktionen wiederum werden in Blocks zusammengefasst und nach eingehender Prüfung der Teilnehmer des Bitcoin-Netzwerks an die Blockkette (Blockchain) angehängt. Die Blockchain ist im Bitcoin-Netzwerk das öffentlich einsehbare, chronologische Kassabuch. Jede – seit Anbeginn der Währung – durchgeführte Transaktion ist darin in einem Block vermerkt. Durch die starke Nutzung von asymmetrischer Kryptographie wird Bitcoin auch oftmals als Kryptowährung bezeichnet.

Bitcoin ist ein verteiltes, dezentrales System, das bewusst auf eine zentrale vertrauenswürdige Stelle verzichtet. Jedem Teilnehmer des Peer-to-Peer Netzwerks wird misstraut, dadurch gibt es auch keine Abstimmungen oder ähnliches und keinen fixen Zeitpunkt, an dem eine Übereinstimmung (zum Beispiel über die Richtigkeit von Transaktionen) zustande kommt. Übereinstimmung entsteht implizit dadurch, dass alle Teilnehmer am Bitcoin-Netzwerk einfachen Regeln folgen. Diese im englischen als emergent consensus bezeichnete Eigenschaft ist mitunter eine der größten Innovationen von Bitcoin und führt, wie eingangs erwähnt, dazu dass das von Bitcoin eingeführte Netzwerk für viele weitere Anwendungsfälle adaptiert werden kann.[154]

Die folgenden Kapitel bieten zunächst einen Überblick über die historische Entwicklung von Bitcoin. In weiterer Folge werden technische Grundlagen erläutert und im Anschluss wird auf die Komponenten von Bitcoin und deren Zusammenspiel im Detail eingegangen.

3.1 Historische Entwicklung

Bitcoin ist die erste konkrete Implementierung einer Kryptowährung, die breite Bekanntheit erlangt hat. Das Arbeitspapier zu Bitcoin wurde am 1. November 2008 von Satoshi Nakamoto in einer Mailinglist für Kryptographie – genannt „The Cryptography Mailing List“ – als Artikel veröffentlicht.[155] Die Software, aufbauend auf Nakamotos Arbeitspapier („Bitcoin: A Peer-to-Peer Electronic Cash System“), war ab Januar 2009 frei zugänglich und einsetzbar.[156]

[154] [Ant14, Seite 177 Decentralized Consensus]
[155] [Nak09b]
[156] [Nak09c]

Satoshi Nakamoto hat sich 2010 aus dem Bitcoin-Projekt zurückgezogen und Gavin Andresen mit der Funktion des Core Maintainers betraut. Des Weiteren wurde der so genannte Alert Key[157] ebenfalls an Gavin Andresen weitergeben.[158]

Nakamoto hat im Zeitraum von November 2008 bis einschließlich April 2011 in etwa 100.000 Wörter publiziert.[159] Er hat sich selbst im Jahr 2009 als 36-jähriger Japaner beschrieben. Journalisten sind jedoch seit seinem „Verschwinden" an der Aufklärung des vermutlichen Pseudonyms Satoshi Nakamoto interessiert. Analysen der verwendeten Worte, deren Schreibweise sowie der üblichen Interaktionszeiten von Nakamoto führen dabei unweigerlich nach Großbritannien.

Spekulationen über die Person Nakamoto gehen in unterschiedlichste Richtungen: Zum einen könnte es sich bei Satoshi Nakamoto um einen Teilnehmer der Kryptographie-Konferenz Crypto 2011 handeln und hier im speziellen um Michael Clear, einem Abgänger des Trinity Colleges in Dublin. Mutmaßungen gibt es allerdings auch, dass es sich um Neal J. King, einen in München lebenden Consultant, handeln könnte. Dan Kaminsky, ein Spezialist für Computersicherheit, kommt nach 4-monatiger Analyse des Bitcoin-Core-Quellcodes zu der Erkenntnis, dass es sich mitunter um ein Team handelt, dass hinter dem Pseudonym steht:[160]

> „Either there's a team of people who worked on this [...] or this guy is a genius."[161]

Nakamotos Kommunikation war fast ausschließlich auf Unterhaltungen mit anderen Entwicklern und Interessenten in Mailinglisten und Foren beschränkt. In einem kurzen Essay hat er allerdings seine Beweggründe für Bitcoin dargelegt.[162]

> „The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the

[157] Das Bitcoin-Netzwerk sieht vor, dass im Fall von Notfällen Nachrichten an jeden Teilnehmer des Netzwerks gesendet werden können. Diese Nachrichten müssen in geeignetem Format signiert sein, wofür der Alert Key notwendig ist.
[158] [Bos13]
[159] [Smi14]
[160] [Smi14], [Dav11]
[161] [Smi14]
[162] Siehe *Satoshi Nakamoto Essay (Anhang A)*.

> currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible [...] With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless."[163]

Aus diesem Essay geht ebenfalls hervor, dass politische Motive Satoshi Nakamoto bei der Entwicklung von Bitcoin begleitet haben. Zum Zeitpunkt der Verfassung dieser Arbeit im September 2015 war die Identität von Satoshi Nakamoto – trotz regem Interesse an der Aufklärung – nicht geklärt. Aus der öffentlich einsehbaren Blockchain kann geschlossen werden, dass Satoshi Nakamoto mit September 2015 im Besitz von etwa 1 Million Bitcoins[164] ist,[165] diese jedoch nicht tauschen kann, ohne einen massiven Kursverfall und damit eine Gefahr für das gesamte Netzwerk herauszufordern.

Die kleinstmögliche Bitcoin-Einheit (0.00000001 XBT), jene Einheit, die auch der Bitcoin-Quellcode für alle Berechnungen verwendet, wird seit 2011 als „satoshi" bezeichnet. Der Vorschlag dazu wurde – ebenso wie der Gegenvorschlag („austrian") – vom Benutzer ribuck im Bitcoin Talk Forum eingebracht.[166]

> „[...] on 10 February 2011 I proposed naming the smallest base unit (0.00000001 XBT) either an "austrian" or a "satoshi". In retrospect it's obvious that "satoshi" was the better name."[167]

[163] [Nak09b]
[164] Entsprach zeitweise mehr als 1 Milliarde Euro.
[165] [Liu13]
[166] [Rib11]
[167] [Rib14]

3.2 Technische Grundlagen

3.2.1 Asymmetrische Kryptographie

Grundlegende Überlegungen und Konzeptionen in Bitcoin basieren auf asymmetrischer Kryptographie. Der wichtige Bestandteil Kryptographie zeigt sich zum Beispiel in der alternativen Bezeichnung („Kryptowährung“), aber auch in der Tatsache, dass Satoshi Nakamoto seine Konzeption einer digitalen Währung zunächst in einer Mailing List für Kryptographie-Interessierte[168] publiziert hat.

Asymmetrische Kryptographie zeichnet im Gegensatz zu symmetrischen Methoden dadurch aus, dass jeder Teilnehmer ein zusammengehöriges Schlüsselpaar – bestehend aus einem öffentlichen Schlüssel (genannt public key) und einem privaten Schlüssel (genannt private key) – besitzt. Während der private Schlüssel unter allen Umständen geheimgehalten werden soll, soll der öffentliche Schlüssel durchaus Verbreitung finden. Für den Anwendungsfall von asymmetrischer Kryptographie bei E-Mails, existieren zum Beispiel eigene Keyserver, auf welche der öffentliche Schlüssel geladen werden kann. Kommunikationsteilnehmer können diese Keyserver ähnlich wie ein Telefonbuch verwenden und öffentliche Schlüssel für eine bestimmte Person darin suchen.

Das Zusammenspiel dieser beiden Schlüssel eignet sich nun für unterschiedlichste Anwendungsfälle, wie zum Beispiel für die Authentifizierung auf Servern[169], die Verschlüsselung von Inhalt oder aber zur digitalen Signatur von Inhalt und damit für den Nachweis, dass eine Nachricht von einer bestimmten Person kommt.

Angenommen, Alice will Bob eine Nachricht übermitteln. Die Nachricht hat wichtigen Inhalt und soll demnach **verschlüsselt** übermittelt werden. Dazu muss Alice zunächst in Besitz des öffentlichen Schlüssels von Bob sein. Mit Bobs öffentlichem Schlüssel kann Alice ihre Nachricht nun in einer Art und Weise verschlüsseln, die es ausschließlich Bob – unter Zuhilfenahme seines privaten Schlüssels – ermöglicht, die Nachricht zu entschlüsseln. Die vereinfachte Abfolge einer Verschlüsselung mittels asymmetrischer Kryptographie ist in *Abbildung 3.1* dargestellt.

[168] [Nako8a]
[169] Wird optional im SSH Protokoll unterstützt.

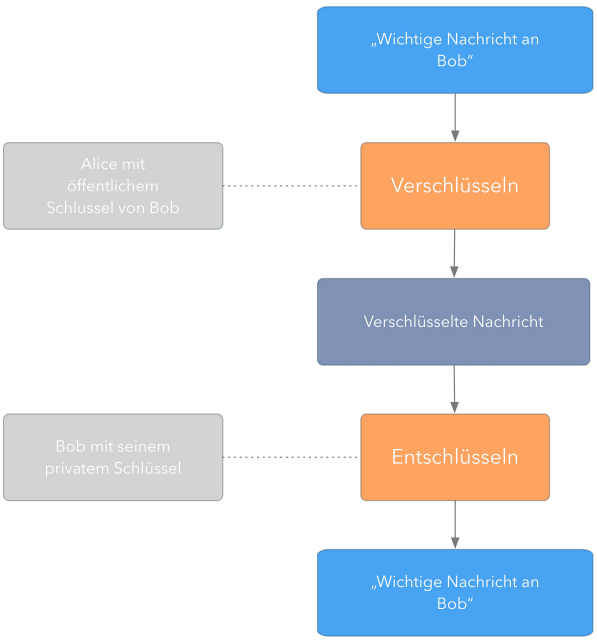

Abbildung 3.1: Verschlüsselung mit asymmetrischer Kryptographie

Während Verschlüsselung in Bitcoin nicht zur Anwendung kommt, hat eine weitere Anwendung der asymmetrischen Kryptographie einen großen Stellenwert. Wesentliche Teile der Bitcoin-Architektur beruhen auf digitalen Signaturen. Mittels **digitaler Signatur** kann sichergestellt werden, dass ein Inhalt tatsächlich von einer bestimmten Person stammt. In *Abbildung 3.2* ist ersichtlich, wie sich Alice gegenüber Bob als Absenderin der Nachricht ausweisen kann. Alice erstellt eine Nachricht, die sie gerne Bob übermitteln würde. Unter Verwendung ihres privaten Schlüssels kann sie diese Nachricht signieren (oder auch anders ausgedrückt, digital unterzeichnen) und damit sich selbst als Absenderin ausweisen. Wenn Bob die Nachricht erhält, kann er den öffentlichen Schlüssel von Alice verwenden, um die Signatur zu überprüfen. Bei erfolgreicher Prüfung kann Bob davon ausgehen, dass diese Nachricht am Weg von Alice zu Bob von keiner anderen Person modifiziert werden konnte.

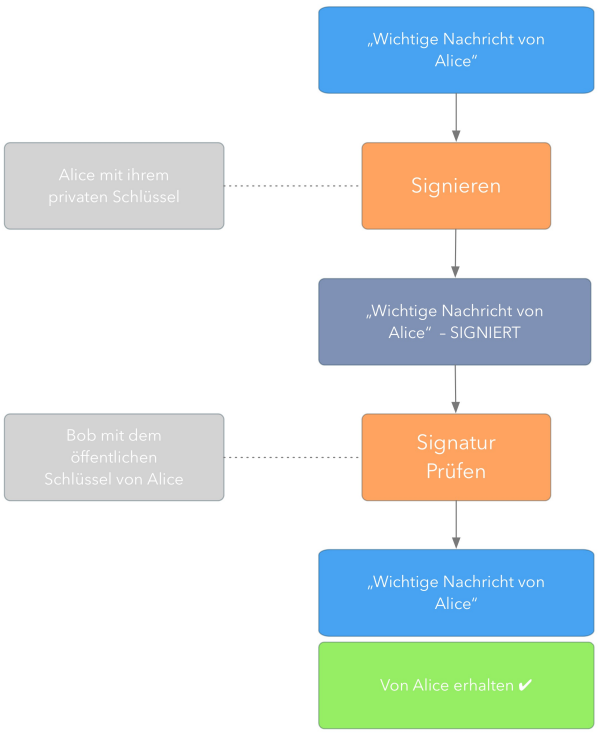

Abbildung 3.2: Digitales Signieren mit asymmetrischer Kryptographie

Wichtig ist die Tatsache, dass digitale Signaturen und Verschlüsselungen sich gegenseitig nicht ausschließen. Vielmehr kommen sie oftmals in Kombination zum Einsatz.

Elliptic Curve Cryptography

Im konkreten verwendet Bitcoin Elliptic Curve Cryptography (ECC) als kryptographisches Verfahren.[170] ECC beruht dabei auf einem diskreten logarithmischen Problem, das mittels Additionen und Multiplikationen auf Punkte einer elliptischen Kurve ausgedrückt wird.[171]

ECC Verfahren finden seit 2004 vermehrt Anwendung und können damit als junges Verfahren unter den Kryptographie-Methoden bezeichnet werden. Im Vergleich

[170] [Bit15h, Cryptography]
[171] [Ant14, Seite 65ff Elliptic Curve Cryptography Explained]

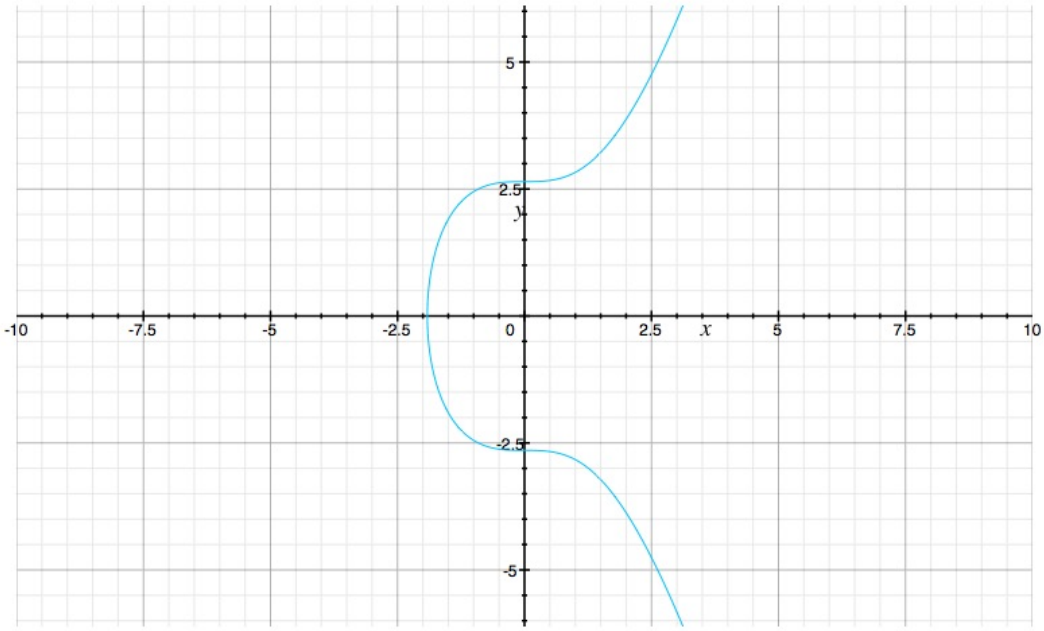

Abbildung 3.3: Elliptische Kurve – secp256k1 im reellen Zahlenbereich –10 bis +10

zu Vorgängern wie RSA bestehen die Vorteile vor allem in vergleichbaren Sicherheitsstandards bei deutlich kleineren Schlüssellängen.

So bietet ein ECC Schlüssel mit 256 bis 383-bit vergleichbare Sicherheit wie ein 3072-bit RSA Schlüssel.[172] Bitcoin verwendet als elliptische Kurve secp256k1, spezifiziert vom U.S. National Institute of Standards and Technology (NIST). Die Kurve wird dabei folgendermaßen ausgedrückt[173]:

$$y^2 = (x^3 + 7) \ \texttt{über} \ \mathbb{F}_p$$

Abbildung 3.3 zeigt die elliptische Kurve – zur vereinfachten Darstellung – im reellen Zahlenbereich visualisiert. Tatsächlich ist die Kurve jedoch im endlichen Raum mit der Primzahl $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ definiert („über $\mathbb{F}_p$“). Kurven dieser Art haben keine stetige Eigenschaft und erscheinen deshalb visualisiert nicht wie eine

[172] [BBB+12, Seite 64 Kapitel 5.6.1 Comparable Algorithm Strengths]
[173] [Ant14, Seite 65ff Elliptic Curve Cryptography Explained]

fortlaufende Kurve.[174][175]

3.2.2 Hash Funktionen

Eine Hashfunktion ist eine mathematische Funktion, die aus Inhalt beliebiger Länge mittels einer einfachen Berechnung reproduzierbar ein identisches Ergebnis mit fixer Länge liefert[176]. Es gibt unzählige Entwicklungen und Abwandlungen von Hashfunktionen. Bei Bitcoin finden kollisionsresistente Einweg-Hashfunktionen Anwendungen. Hashfunktionen dieser Art werden häufig auch als kryptographische Hashfunktionen bezeichnet. Unter der Annahme, dass die Hashfunktion mit dem Großbuchstaben H (für „Hash“), der Eingangswert mit dem Großbuchstaben M (für „message“) und das Resultat mit klein d (für „digest“) bezeichnet wird, ergibt sich die Formel der Hashfunktion als H(M) = d. Die Eigenschaften oder Anforderungen an die Hashfunktion lassen sich damit folgendermaßen ausdrücken[177]:

- Bei bekanntem M ist es leicht, d zu berechnen.
- Bei bekanntem d ist es praktisch unmöglich, ein M zu finden, sodass H(M) = d erfüllt ist.
- Bei bekanntem M ist es praktisch unmöglich eine andere Nachricht M’ zu finden, sodass H(M) = H(M’).
- Es ist praktisch unmöglich, zwei unterschiedliche Eingabewerte M und M’ zu finden, sodass H(M) = H(M’).

Die Bitcoin-Spezifikation setzt an mehreren Stellen auf Hashfunktionen. Dazu zählen Bitcoin-Adressen, Transaktionsreferenzen in Blocks oder Blockreferenzen in der Blockchain. Die vermutlich wichtigste Anwendung innerhalb von Bitcoin, der Arbeitsnachweis (Proof-of-Work) beim Mining, baut auf einem Entwurf von Adam Back – publiziert im Dokument „Hashcash - A Denial of Service Counter-Measure[178]“ – auf und setzt ebenfalls Hashfunktionen ein. Konkret kommen die Hashfunktionen SHA256 und

[174] [Lam14]
[175] [Ant14, Seite 65ff Elliptic Curve Cryptography Explained]
[176] [MvOV96, Seite 322 Kapitel 9.2.1]
[177] [Sch95, Seite 359 Kapitel 18.1]
[178] [Bac02]

RIPEMD160 zum Einsatz. In beinahe allen Bereichen wird die Hashfunktion doppelt aufgerufen, also zum Beispiel SHA256(SHA256(Nachricht)).

SHA256 gehört zur Familie der „Secure Hash Algorithms“ und wurde als Teil von DSA – einem Standard für digitale Signaturen – vom U.S. National Institute for Standards and Technology (NIST) vermutlich in Zusammenarbeit mit der „U.S. National Security Agency“ (NSA)[179] entworfen. Die SHA2-Funktionen (zu denen auch SHA256 gezählt wird) stellen dabei eine Weiterentwicklung von SHA1-Funktionen dar, die seit 2005 als unsicher eingestuft werden[180]. Das Resultat der SHA256-Funktion umfasst immer exakt 64 Zeichen. *RIPEMD160* im Gegenzug hat ein Resultat mit 40 Zeichen Länge und wird in Bitcoin eingesetzt an Stellen, an welchen kürzere Ergebnisse wünschenswert sind. RIPEMD160 wurde 1996 an der Universität Leuven (Belgien) entwickelt[181].

Beispielhafte Resultate bei Anwendung der angeführten Hashfunktionen:

```
SHA256(Franz)=
bae10942b11649e784f7e4c2728203612368ff3f871fe0a6c0c706eb52318223
SHA256(Franz jagt im komplett verwahrlosten Taxi)=
2379f93fb4d77495a17db3142a682480fcd288549c4b61486b52521ac9c1ec7a
SHA256(Frank jagt im komplett verwahrlosten Taxi)=
14c0315f1e1e403f9a4d6c7af36caba712864c7d06923641133dccc5cfc767a3
RIPEMD160(Franz)=
a963518d3ce41be8eb68bb6cb1750685c6b028a4
RIPEMD160(Franz jagt im komplett verwahrlosten Taxi)=
eb35320f733d97e68c3b7d39a9fd6121b016cf4f
RIPEMD160(Frank jagt im komplett verwahrlosten Taxi)=
f5ba982546c7e59d731b28edc7051ec7dd2c9572
```

Wie die Beispiele 2 und 3 sowie 5 und 6 zeigen, sollen bereits minimale Änderungen an der Nachricht M dafür sorgen, dass sich der resultierende digest d möglichst stark verändert. Dieser Tatsache wird auch als *Lawineneffekt* beziehungsweise *Avalanche*

[179] U.S. Patent 5,231,668 wurde David W. Kravitz, einem ehemaligen NSA-Mitarbeiter zugesprochen.
[180] [PvW08, Seite 3 Kapitel 1.2.1]
[181] [DBP96]

effect bezeichnet[182]. Die Erstellung eines SHA256 Hashes unter OS X ist mit folgendem Kommando möglich: `perl -e "print qw(Franz)"| shasum -a 256`. Für RIPEMD160 wiederum kann folgende Eingabe verwendet werden: `perl -e "print qw(Franz)"| openssl rmd160`.

3.2.3 Merkle Tree

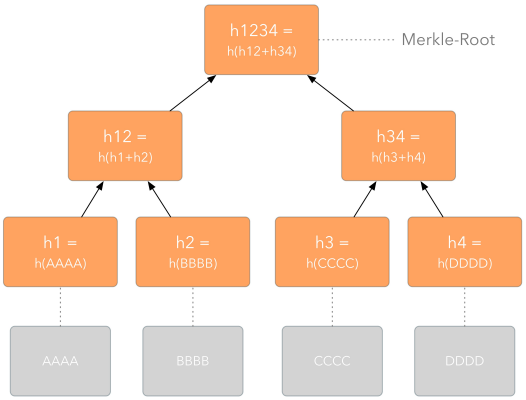

Abbildung 3.4: Merkle-Baum mit 4 Blättern

Ein Merkle Tree (oder in Deutsch Merkle-Baum) ist eine Datenstruktur, die eine effiziente und sichere Verifikation von großen Datenstrukturen ermöglicht. Der Merkle-Baum ist nach seinem Erfinder Ralph C. Merkle benannt, wird allerdings aufgrund seiner technischen Umsetzung auch als binärer Hash-Baum bezeichnet[183]. Binär einerseits bedeutet, dass jeder Knoten im Baum wiederum zwei Kindknoten besitzt. Hash-Baum andererseits weist darauf hin, dass nicht die Daten selbst, sondern Hashwerte[184] davon gespeichert werden – Doppel SHA256 im Fall von Bitcoin[185]. Wie in *Abbildung 3.4* zu sehen ist, erfolgt ausgehend von den Datenelementen, die Teil des Baums werden sollen, die Berechnung der Hashwerte. Für jedes Datenelement im Baum existiert ein Hashwert in Form eines Blattes. Um die binären Eigenschaften des Baumes sicher-

[182] [Sch95, Seite 273 Kapitel 12.1]
[183] [Mer82]
[184] Vergleiche *Hash Funktionen (Unterabschnitt 3.2.2)*
[185] [Ant14, Seite 163 Merkle Trees]

stellen zu können, sind damit 2^n Objekte nötigt. Die Bitcoin-Implementation umgeht dieses Problem, indem bei ungerader Anzahl die letzten Elemente dupliziert werden, also ein weiteres Mal in den Baum aufgenommen wird[186]. Dieses Vorgehen führt jedoch zu einem ernsthaften Sicherheitsproblem, weil durch Duplizieren von Elementen aus unterschiedlichen Eingangswerten die identische Merkle-Root entstehen könnte[187]. Dieses Problem wurde mit Bitcoin-Version 0.6.2 behoben, indem bereits vor Erstellung der Merkle-Root auf Duplikate geprüft wird[188]. Wenn nun die Hashwerte der Blätter berechnet sind, erfolgt die Berechnung der Knoten der nächsten Ebene dadurch, dass jeweils zwei Blätter zusammengefasst werden und davon wiederum der Hashwert berechnet wird. Wie *Abbildung 3.4* zeigt, wird h_1 (der Hashwert von AAAA) sowie h_2 (der Hashwert von BBBB) verwendet, miteinander verknüpft und davon abermals der Hashwert berechnet. Das Resultat wird in diesem Fall als h_{12} bezeichnet. Dieses Vorgehen wird solange wiederholt, bis der Wurzelknoten (auch als Merkle Root bezeichnet) berechnet ist[189].

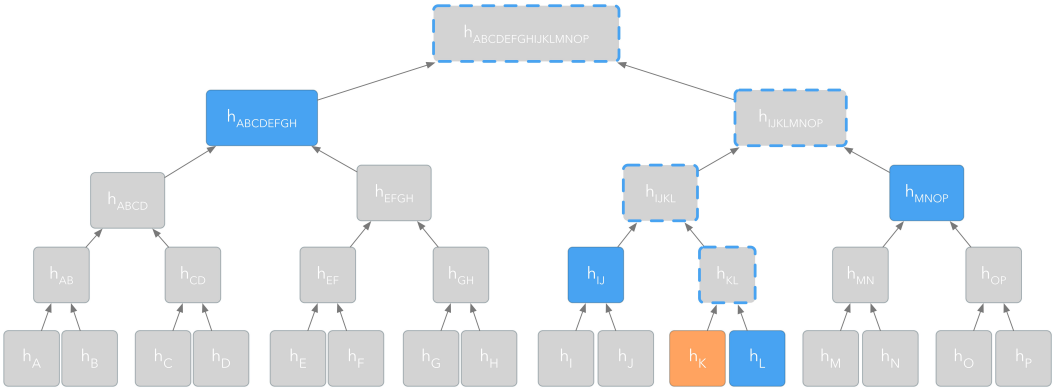

Abbildung 3.5: Merkle-Baum mit 16 Blättern[190]

Bitcoin berechnet aus allen Transaktionen, die in einem Block zusammengefasst sind, einen Merkle-Baum und speichert dessen Wurzel (die Merkle-Root) im Header

[186] [Krz14, Seite 3 Merkle Tree > Other cases]
[187] Siehe CVE–2012–2459 (http://www.cvedetails.com/cve/CVE-2012-2459).
[188] [For12]
[189] [Mer82]
[190] [Blo15a]

des Blocks[191]. Wie bereits angeführt, kann durch Nutzung von Merkle-Bäumen effizient überprüft werden, ob ein bestimmtes Element Teil des Baumes ist. *Abbildung 3.5* zeigt einen Baum mit 16 Blättern, die wiederum Transaktionen in einem Bitcoin-Block darstellen könnten. Um nun zu überprüfen, ob eine bestimmte Transaktion – in diesem Fall h_K – Teil eines Blocks ist, müssen nicht alle Transaktionen geladen werden, sondern lediglich die 4 blauen Knoten (h_L, h_{IJ}, h_{MNOP} sowie $h_{ABCDEFGH}$). Durch Berechnung von 4 Hashes (h_{KL}, h_{IJKL}, $h_{IJKLMNOP}$, $h_{ABCDEFGHIJKLMNOP}$) und Vergleich des resultierenden Merkle-Roots kann damit jederzeit nachgewiesen werden, dass h_K Teil des Baumes ist.

In einem Merkle-Baum mit N Elementen benötigt die Überprüfung, ob ein bestimmtes Element enthalten ist höchstens

$$2 * ln(N)$$

Berechnungen[192]. Ein Bitcoin-Block beinhaltet üblicherweise mehrere hundert Transaktionen (Oktober 2015 enthielt der kleinste Block 667 Transaktionen, der größte Block 1138 Transaktionen)[193]. Für den größten Block mit 1138 Transaktionen sind demnach höchstens

$$2 * ln(1138) = 14.07405523$$

Vergleiche notwendig.

3.3 Transaktionen

Satoshi Nakamoto definierte eine elektronische Münze folgendermaßen:

> „We define a electronic coin as a chain of digital signatures.“[194]

Auch wenn es für den Nutzer oft anders erscheint, bewegen sich elektronische Münzen nicht von Besitzer zu Besitzer, wie es bei klassischen Währungen der Fall ist. Vielmehr werden Transaktionen miteinander verkettet. Um grundlegende Anforderungen an eine Transaktion (Identifikation, Authentizität und Integrität)[195] zu erfüllen, wird

[191] Siehe *Block Chain (Abschnitt 3.4)* für eine detaillierte Beschreibung.
[192] [Ant14, Seite 163 Merkle Trees]
[193] [Blo15a]
[194] [Nak09a, Seite 2 Transactions]
[195] [Krz14, Seite 16 Bitcoin ownership]

asymmetrische Kryptographie verwendet. Transaktionen beruhen zu einem wesentlichen Teil auf digitalen Signaturen, wie in *Asymmetrische Kryptographie (Unterabschnitt 3.2.1)* beschrieben[196]. Angenommen Alice besitzt monetären Wert in Form von Bitcoins aus vorhergehenden Transaktionen und will diesen Wert an Bob übertragen. Alice kennt also die vorhergehenden Transaktionen, benötigt damit nur noch den öffentlichen Schlüssel des Empfängers, in diesem Fall von Bob. Alice fügt nun vorherige Transaktionen sowie öffentlichen Schlüssel von Bob zusammen und signiert Selbiges unter Zuhilfenahme ihres privaten Schlüssels. Nachdem nur Alice in Besitz dieses privaten Schlüssels sein darf, kann diese Signatur von keiner anderen Person erzeugt worden sein. Wenn Bob nun diese Transaktion erhält, kann er den öffentlichen Schlüssel von Alice verwenden und prüfen, ob die Signatur tatsächlich von Alice stammt[197]. Es ist also ersichtlich, dass die Identifikation des Empfängers durch Hinzufügen seines öffentlichen Schlüssels sichergestellt ist. Authentifikation und Integrität der Transaktion stellt wiederum die Signatur sicher[198]. Bob kann nun die Kette der vorhergehenden Transaktionen weiter zurückverfolgen und damit sicherstellen, dass Alice tatsächlich in Besitz der angegebenen Münzen war. Was Bob jedoch nicht feststellen kann ist, ob Alice diesen Betrag gleichzeitig auch ihrer Freundin Carol versprochen hat und dafür ebenfalls eine passende Signatur (unter Verwendung des öffentlichen Schlüssels von Carol) erzeugt hat. Alice würde damit die Münzen in ihrem Besitz zweimal ausgeben. Dieses Problem wird deshalb als Double-Spending Problem bezeichnet. Gelöst wird dieses Problem durch Einführung einer Blockchain (*Blockchain (Abschnitt 3.4)*), in welcher alle Transaktionen – zu Blöcken zusammengefasst – gespeichert werden.

Die Bitcoin-Spezifikation kennt zwei Arten von Transaktionen: reguläre Transaktionen zum einen und Coinbase-Transaktionen – nicht zu verwechseln mit dem gleichnamigen Zahlungsabwickler, der in *Bitcoin im E-Commerce (Kapitel 4)* Erwähnung findet – zum anderen. Nachdem Coinbase-Transaktionen als eine spezielle Form von regulären Transaktionen angesehen werden können, werden in den folgenden Abschnitten reguläre Transaktionen beschrieben. In *Coinbase-Transaktionen (Unterabschnitt 3.3.5)* wird näher auf die Unterschiede der beiden Transaktionstypen eingegangen. Transaktio-

[196] [Nak09a, Seite 2 Transactions]
[197] [Nak09a, Seite 2 Transactions]
[198] [Krz14, Seite 16 Bitcoin ownership]

nen müssen des Weiteren Eigenschaften erfüllen, um von Knoten im Bitcoin-Netzwerk akzeptiert zu werden. Die Eigenschaften sind in *Standard-Transaktionen (Unterabschnitt 3.3.4)* thematisiert.

3.3.1 Transaktionsstruktur

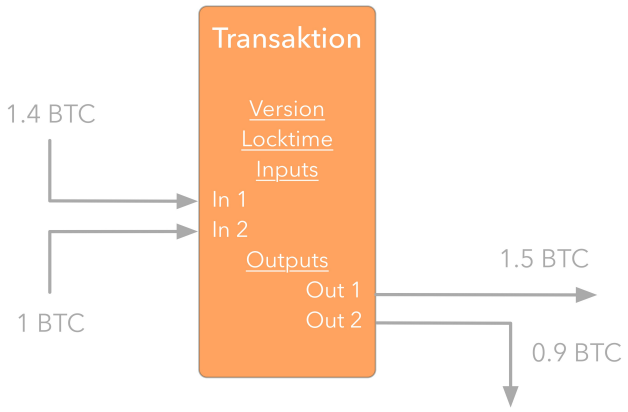

Abbildung 3.6: Bitcoin-Transaktion

Ein Transaktionsobjekt, wie in *Abbildung 3.6* dargestellt, stellt den Übertrag eines gewissen monetären Wertes von einer Person zur nächsten dar. Alle dazu notwendigen Informationen sind in einem Transaktionsobjekt gespeichert. Auf die Struktur dieses Objekts wird im folgenden eingegangen.

Version bezeichnet die Transaktionsversionsnummer und ist derzeit 1 [199]. Die Versionsnummer wird von Netzwerkknoten herangezogen und gibt Hinweis darauf, mit welchen Regeln verifiziert wird, ob eine Transaktion gültig ist.

Mittels *Locktime* ist es möglich, den erhaltenen Betrag für eine gewisse Zeit zu sperren. Bitcoin unterscheidet zwischen einer zeitlichen Sperre (ein Wert größer oder gleich $5 * 10^8$ wird als Zeitangabe im UNIX Zeitformat[200] interpretiert) oder aber eine Sperre für eine gewisse Anzahl an Blöcken (ein Wert kleiner $5 * 10^8$ bezeichnet die Blocknummer, auch Blockhöhe genannt, an der die Sperre aufgehoben wird)[201]. Unab-

[199] [Bit15a, Zeile 184 /primitives/transaction.h:CURRENT_VERSION]
[200] [Ope15, 4.15 Seconds Since the Epoch]
[201] [Krz14, Seite 11 nLockTime]

hängig davon, auf welche Art die *LockTime* definiert ist, beschreibt sie demnach den frühestmöglichen Zeitpunkt, an dem die Transaktion in die Blockchain aufgenommen werden kann. Jede Transaktion hat des weiteren einen oder mehrere Eingänge (*Inputs*) und einen oder mehrere Ausgänge (*Outputs*). Jeder Eingang verweist dabei auf einen Ausgang einer vorherigen Transaktion, der bisher noch nicht anderwertig ausgegeben wurde (deshalb auch im Englischen als Unspent Transaction Output oder abgekürzt UTXO bezeichnet). Alle Ausgänge, die von dieser Transaktion generiert werden, sind vorläufig ebenfalls UTXOs, bis sie als Eingang einer anderen Transaktion verwendet werden. Ein vollständiges Transaktionsobjekt ist in *Tabelle B.1* abgebildet.

Angenommen, Alice möchte sich einen – zugegebenermaßen überteuerten – Kaffee kaufen. Die Coffeeshop-Besitzerin bietet diesen um 1.5 XBT an. Alice hat bereits zuvor Bitcoin verwendet und besitzt aus einer älteren Transaktion 1.4 XBT sowie 1 XBT aus einer weiteren, vergangenen Transaktion. Erhaltene Bitcoinwerte können nicht aufgeteilt werden und nachdem keiner der beiden älteren Werte den Kaffeepreis abdecken kann, muss sie beide Werte als Eingang der neuen Transaktion verwenden. Nun hat diese Transaktion also 2.4 XBT an Eingängen. Nachdem aber auch mehrere Ausgänge möglich sind, legt Alice einerseits einen Ausgang für die Coffeeshop-Besitzerin in Höhe von 1.5 XBT an, andererseits einen weiteren Ausgang über die verbleibenden 0.9 XBT, die sie sich jedoch selbst überträgt. Die 0.9 XBT könnten also auch als Retourgeld bezeichnet werden. Dieses bewusst vereinfachte Beispiel ignoriert das Konzept von Transaktionsgebühren (vergleichbar mit Trinkgeld), die per Definition die Differenz zwischen Ein- und Ausgangswerten betragen. Transaktionsgebühren werden im Detail in *Abschnitt 3.5.2* behandelt.

3.3.2 Transaktionskette

Wie im vorhergehenden Kapitel bereits angemerkt, hat jeder Eingang einer Transaktion einen dazu passenden Ausgang einer älteren Transaktion, woraus sich implizit eine Verkettung von Transaktionen ergibt. Jeder Ausgang einer Transaktion besitzt einerseits den Wert dieses Ausgangs in der Einheit Satoshi[202] und andererseits ein Feld *scriptPubKey*, welches beschreibt, wie sich eine Person als rechtmäßige Besitze-

[202] 1 XBT = 100,000,000 Satoshi

rin dieses Ausgangs ausweisen kann. Jeder Eingang besitzt einen Verweis auf einen vorherigen Ausgang. Der Ausgang lässt sich über 2 Felder eindeutig identifizieren:

- *Hash* – Ein Doppel-SHA256 Hash über das vorhergehende Transaktionsobjekt
- *Index* – Ein numerischer Index des Ausgangs im vorherigen Transaktionsobjekt

Es fehlt nun noch die Möglichkeit, sich als rechtmäßige Besitzerin des Wertes auszuweisen. Dafür besitzt der Eingang das Feld *scriptSig* und damit das Gegenstück zum *scriptPubKey* Feld des referenzierte Ausgangs.

Die Namensgebung dieser beiden Felder ist historisch bedingt und erscheint aus heutiger Sicht etwas verwirrend sowie nicht mehr zeitgemäß. *scriptPubKey* wurde derart benannt, weil üblicherweise der öffentliche Schlüssel (Public Key) darin gespeichert wurde. In *scriptSig* wiederum wurde die digitale Signatur gespeichert, was deren Referenz im Namen erklärt.[203] Unter Zuhilfenahme einer Metapher in Form einer verschließbaren Türe kann *scriptPubKey* mit dem Schloss verglichen werden. Das Schloss ermöglicht es, die Tür zu versperren und regelt die Rahmenbedingungen, die notwendig sind, um Zutritt zu erlangen. *scriptSig* andererseits ist mit dem Schlüssel vergleichbar, der zum Schloss passt und die Entriegelung der Türe ermöglicht.

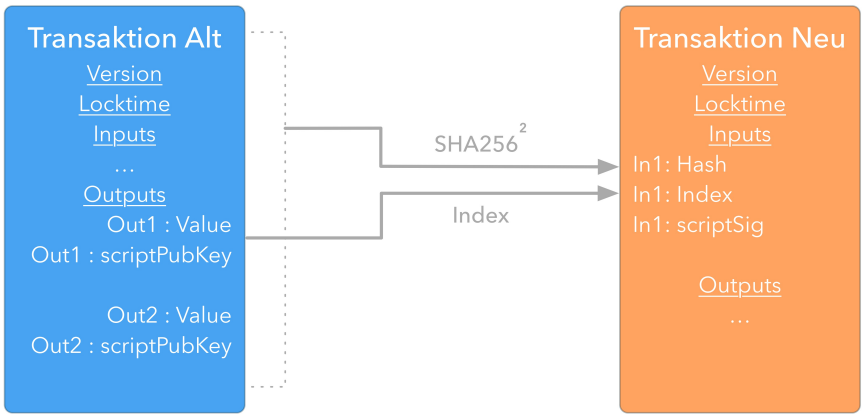

Abbildung 3.7: Bitcoin-Transaktion verkettet[204]

[203] [Krz14, Seite 122 Script Construction (Lock + Unlock)]
[204] [Krz14, Seite 9, Bild 3.2]

Tatsächlich besitzt Bitcoin eine eigens dafür entwickelte Programmiersprache, genannt *Script* (Abschnitt 3.3.2), die es theoretisch ermöglicht, beliebig komplexe Aufgaben zu formulieren, um sich als Besitzer ausweisen zu können. In der Praxis müssen jedoch Netzwerkknoten gefunden werden, die diese komplexen Transaktionen überprüfen und dann an andere Knoten weiterleiten. Aus diesem Grund gibt es eine festgelegte Menge an sogenannten Standard-Transaktionstypen (Unterabschnitt 3.3.4), die jeder Netzwerkknoten akzeptiert.

Script Sprache

Bitcoin verwendet also Script, um Besitz von Bitcoins zu validieren. Daher rührt auch die englische Bezeichnung „programmable money“ (zu deutsch programmierbares Geld).[205] Script ist eine einfach gehaltene Scriptsprache, die Anleihe an der 1970 erfundenen Sprache Forth nimmt. Script basiert auf einem Stack, von welchem Daten gelesen und geschrieben werden können, und verzichtet bewusst auf Schleifenkonstrukte, wodurch sie nicht Turing-kompatibel ist. Ein Script ist, einfach ausgedrückt, eine Liste von Anweisungen, die von links nach rechts abgearbeitet werden.[206]

Anweisungen in Script beginnen stets mit den Buchstaben *OP_* und werden deshalb auch als OP-Codes bezeichnet. Verfügbare Anweisungen können in unterschiedliche Bereiche gruppiert werden und umfassen zum Beispiel[207]:

- Stackoperationen wie OP_DROP um das oberste Element from Stack zu entfernen
- Vergleiche wie OP_EQUAL
- Arithmetische Operationen wie OP_ADD für Addition der zwei obersten Elemente am Stack
- Kryptofunktionen wie OP_SHA256, das den Hashwert vom obersten Element am Stack berechnet

und weitere.

[205] [Ant14, Seite 121 Transaction Scripts and Script Language]
[206] [Bit15j]
[207] [Ant14, Seite 126 Script Language]

Tabelle 3.1: Script-Beispiel

Stack	Script	Beschreibung
leer	**5** 8 3 <OD_SUB> <OD_ABS> <OP_NUMEQUAL>	Werte werden auf den Stack gelegt (gepushed).
5	**8** 3 <OD_SUB> <OD_ABS> <OP_NUMEQUAL>	
8 5	**3** <OD_SUB> <OD_ABS> <OP_NUMEQUAL>	
3 8 5	**<OD_SUB>** <OD_ABS> <OP_NUMEQUAL>	<OD_SUB> Subtrahiert die obersten 2 Werte und legt das Ergebnis auf den Stack.
-5 5	**<OD_ABS>** <OP_NUMEQUAL>	<OD_ABS> ist die Betragsfunktion, nimmt den obersten Wert vom Stack und legt dessen absoluten Wert auf den Stack.
5 5	**<OP_NUMEQUAL>**	<OP_NUMEQUAL> vergleicht die obersten 2 Werte am Stack und legt 1 (gleich) oder 0 (ungleich) zurück.
1	leer	

Sofern keine Anweisung einen Fehler erzeugt hat, gilt ein Script als erfolgreich, wenn der Stack leer ist oder sich darauf ein Wert ungleich 0 (FALSE) befindet[208]. Das einfache arithmetische Script-Beispiele in Tabelle 3.1 zu sehen, wurde also erfolgreich beendet.

Der Verzicht auf gewisse Programmiersprachenkonstrukte wie Schleifen ist bewusst und soll vor allem einen möglichen Angriffspunkt auf das Netzwerk ausschließen. *scriptSig* und *scriptPubKey* werden von jedem Netzwerknoten im Bitcoin-Netzwerk ausgeführt. Ein Konstrukt wie beispielsweise eine Endlosschleife könnte Probleme im gesamten Netzwerk verursachen.[209]

Standard-Transaktionsausgänge

Wie die vorangehenden Kapitel gezeigt haben, könnten in Transaktionen unter Verwendung von Script theoretisch beliebig komplexe Aufgaben formuliert werden. Die Bitcoin-Referenzimplementation und in Folge ein Großteil der Netzwerkknoten erlauben und verarbeiten jedoch nur eine bestimmte vordefinierte Anzahl von Transaktionstypen. Es besteht dafür eine spezielle Methode `isStandard`[210], die überprüft, ob

[208] [Ant14, Seite 126 Script Language]
[209] [Ant14, Seite 126 Turing Incompleteness]
[210] [Bit15a, Zeile 183 /script/standard.cpp:`IsStandard()`]

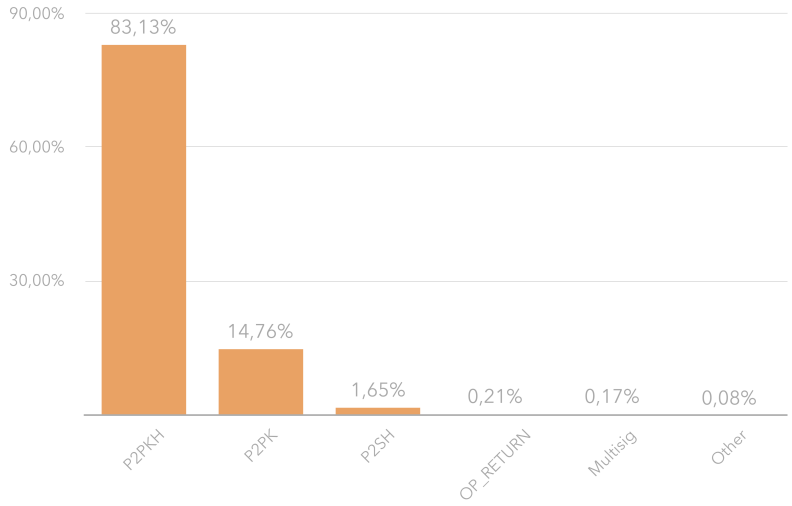

Abbildung 3.8: Statistik Bitcoin-Transaktionstypen bis 6.11.2015

es sich um eine von 5 vordefinierten Standard-Transaktionen handelt. Die 5 Standard-Transaktionen sind im `enum txnouttype` definiert und könnten jederzeit auch erweitert werden[211]. Die Prüfung auf Standard-Transaktion war nicht von Beginn an Teil der Bitcoin-Referenzimplementierung, sondern wurde vielmehr nachgereicht, nachdem einige schwerwiegende Angriffspunkte über Transaktionen entdeckt wurden.[212] Die 5 derzeit akzeptierten Standard-Transaktionen sind[213]:

- Pay to Public Key (P2PK)
- Pay to Public Key Hash (P2PKH)
- Pay to Script Hash (P2SH)
- Multisignature (Multisig)
- Data Output (OP_RETURN)

Wie *Abbildung 3.8*[214] zeigt, ist ein großer Anteil aller Transaktionen vom Typ **Pay to Public Key Hash**[215]. Deshalb wird auf diesen Typen im folgenden im Detail eingegangen.

[211] [Bit15a, Zeile 59 /script/standard.h:`txnouttype`]
[212] [Bit15b, Standard Transactions]
[213] [Bit15a, Zeile 59 /script/standard.h:`txnouttype`]
[214] [Web15]
[215] Beispiel für P2PKH: Transaktion b8fe51942de3cdf00ffe29c8edc8ce1966b1b11e099736c27c71dbeef52770c2

Tabelle 3.2: Script Pay to Public Key Hash

Stack	Script	Beschreibung
leer	**sigCoffeeshop** pubKeyCoffeeshop <OP_DUP> <OP_HASH160> pubKeyHashCoffeeshop <OP_EQUALVERIFY> <OP_CHECKSIG>	Element wird auf den Stack gelegt
sigCoffeeshop	**pubKeyCoffeeshop** <OP_DUP> <OP_HASH160> pubKeyHashCoffeeshop <OP_EQUALVERIFY> <OP_CHECKSIG>	Element wird auf den Stack gelegt
pubKeyCoffeeshop sigCoffeeshop	**<OP_DUP>** <OP_HASH160> pubKeyHashCoffeeshop <OP_EQUALVERIFY> <OP_CHECKSIG>	Der oberste Eintrag am Stack wird dupliziert
pubKeyCoffeeshop pubKeyCoffeeshop sigCoffeeshop	**<OP_HASH160>** pubKeyHashCoffeeshop <OP_EQUALVERIFY> <OP_CHECKSIG>	HASH160(SHA256 gefolgt von RIPEMD160) vom obersten Eintrag am Stack wird berechnet
pubKeyHashCoffeeshop pubKeyCoffeeshop sigCoffeeshop	**pubKeyHashCoffeeshop** <OP_EQUALVERIFY> <OP_CHECKSIG>	Element wird auf den Stack gelegt
pubKeyHashCoffeeshop pubKeyHashCoffeeshop pubKeyCoffeeshop sigCoffeeshop	**<OP_EQUALVERIFY>** <OP_CHECKSIG>	Die beiden obersten Einträge werden auf Übereinstimmung geprüft
pubKeyCoffeeshop sigCoffeeshop	**<OP_CHECKSIG>**	Signatur wird über die beiden obersten Einträge am Stack validiert
TRUE	leer	

Um auf das Beispiel aus *Transaktionsstruktur (Unterabschnitt 3.3.1)* zurückzukommen: Alice hat im Coffeeshop ihres Vertrauens einen Kaffee erworben und als Transaktiontyp *Pay to Public Key Hash* verwendet. Im *scriptPubKey* Feld der ausgehenden Transaktion hat Alice deshalb folgendes Script hinterlegt[216]:

```
OP_DUP OP_HASH160 <pubKeyHashCoffeeshop> OP_EQUALVERIFY OP_CHECKSIG
```

pubKeyHashCoffeeshop ist in diesem Fall einen Hash über den öffentlichen Schlüssel der Coffeeshop-Besitzerin, also eine Referenz auf den Empfänger. Dieser Hash wird auch als Bitcoin-Adresse bezeichnet. In *Bitcoin-Adressen (Unterabschnitt 3.3.3)* wird näher auf deren Zusammensetzung eingegangen. Einfach ausgedrückt, kann also gesagt werden: Alice überträgt die Transaktion an eine Besitzerin einer Bitcoin-Adresse (in diesem Fall die Besitzerin des Coffeeshops). Alice führt dazu den pubKeyHash an und fordert zwei Kriterien, die nachzuweisen sind: A) Mittels `OP_EQUALVERIFY` wird die Kenntnis des passenden öffentlichen Schlüssels zum pubKeyHash überprüft B) Mit `OP_CHECKSIG` wird die Kenntnis des dazu passenden privaten Schlüssels überprüft.[217]

Um als Coffeeshop-Besitzerin diesen Wert nun ausgeben, also in einer neuen Transaktion verwenden zu dürfen, muss die Besitzerin Kriterium A und B erfüllen. Kriterium B ist leicht nachzuweisen, da der öffentliche Schlüssel ohnehin publiziert werden darf, wird dieser einfach im Script gespeichert. Für Kriterium A darf jedoch keinesfalls

[216] [Bit15m, Pay-to-PubkeyHash]
[217] [Krz14, Seite 19 Kapitel 4.3.2 Pay-to-PubkeyHash]

der private Schlüssel darin gespeichert werden, nachdem dieses Script im gesamten Bitcoin-Netzwerk publiziert wird. Stattdessen signiert die Coffeeshop-Besitzerin das neue Transaktionsobjekt und legt die Signatur ebenfalls im Script ab. Die Bitcoin-Spezifikation sieht unterschiedliche Arten der Signatur vor. Standardmäßig wird das scriptSig Feld mit dem dazugehörigen scriptPubKey Feld getauscht und dann das gesamte Transaktionsobjekt signiert (`SIGHASH_ALL`). Nachdem die Signatur im scriptSig Feld gespeichert wird, ist der Schritt des Austausches notwendig. Andernfalls könnte keine valide Signatur erstellt werden. Die Coffeeshop-Besitzerin führt nun die genannten Schritte aus und legt damit folgendes Script im scriptSig Feld ab[218]:

```
<sigCoffeeshop> <pubKeyCoffeeshop>
```

Jeder Netzwerkknoten, der nun diese Transaktion auf Richtigkeit überprüfen will, kombiniert scriptSig und ScriptPubKey und führt das Script, wie in Tabelle 3.2 zu sehen, aus.

Das **Pay to Public Key**[219] Verfahren kann als vereinfachtes P2PKH Verfahren angesehen werden. Die Person, die die Transaktion verwenden will, muss ausschließlich die Kenntnis des privaten Schlüssels nachweisen.[220] Die Felder sehen demnach folgendermaßen aus:

```
scriptPubkey: <pubkey> OP_CHECKSIG
scriptSig:    <signature>
```

Bei **Pay to Script Hash** wird die Transaktion an die Besitzerin eines ScriptHashes adressiert. Für das Einlösen muss diese Person zusätzlich ein serialisiertes Script im scriptSig Feld ablegen. Diese Methode stellt die einzige Methode dar, bei der die Empfängerin die Kriterien für den Anspruch an der Transaktion – über das serialisierte Script – selbst bestimmen kann.[221]

Bei **Multisig**[222] wiederum muss die Empfängerin nachweisen, in Besitz von m privaten Schlüsseln zu sein, die zu ihrem öffentlichen Schlüssel passen.[223]

---

[218] [Bit15m, Pay-to-PubkeyHash]
[219] Beispiel für P2PK: Transaktion ac3e686574072f5fe09e6c190d5ad365613833bbdf2ad8295e43468631132cd9
[220] [Krz14, Seite 18 Kapitel 4.3.1 Pay-to-Pubkey]
[221] [Krz14, Seite 21 Kapitel 4.3.3 Pay-to-ScriptHash]
[222] Beispiel für Multisig: Transaktion cf0d6a6d751a87f13f04937e95fbac604184d0cc0493ae1d92dc7f21ef61053d
[223] [Krz14, Seite 23 Kapitel 4.3.4 Multisig]

Eine Sonderform bei Transaktionen stellt ein *OP_RETURN* Transaktionsausgang[224] dar. Dieser Ausgang besitzt keinen minimalen Wert, kann deshalb auch mit 0 Satoshi erzeugt werden. Das scriptSig Feld bleibt leer, am scriptPubKey befindet sich die Instruktion OP_RETURN, gefolgt von beliebigen Daten von maximal 40 Byte Größe. Auf diese Weise können beliebige Daten in der Blockchain gespeichert werden. Als Sicherheitsvorkehrung ist jedoch pro Transaktion nur ein OP_RETURN Ausgang erlaubt.[225]

3.3.3 Bitcoin-Adressen

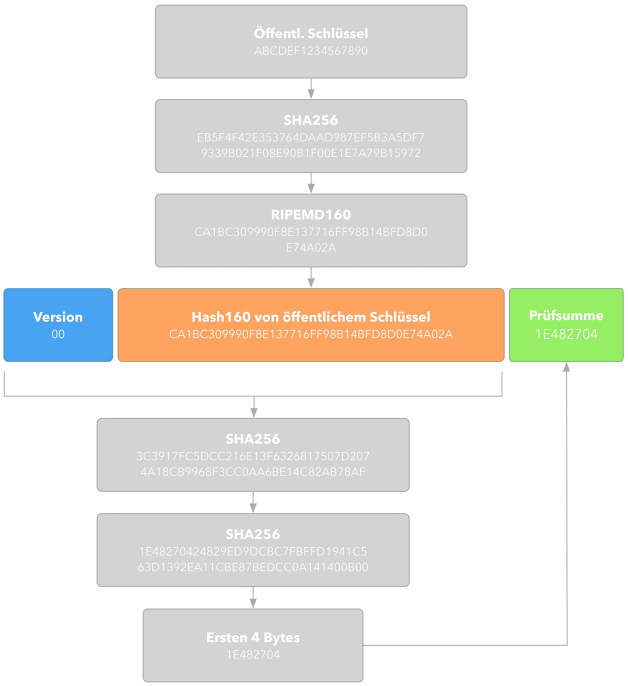

Abbildung 3.9: Zusammensetzung einer Bitcoin-P2PKH-Adresse

Eine Bitcoin-Adresse ist ein eindeutige Kombination von 26–35 alphanumerischen Zeichen[226], die als Adressat einer Bitcoin-Transaktion angeführt werden kann. Derzeit

[224] Beispiel für OP_RETURN: Transaktion 8bae12b5f4c088d940733dcd1455efc6a3a69cf9340e17a981286d3778615684
[225] [Krz14, Seite 25 Kapitel Nulldata]
[226] [Bit15e]

sind 2 Arten von Bitcoin-Adressen vorgesehen. Jene, die auf einem öffentlichen Schlüssel basieren und bei P2PKH Anwendung finden sowie jene, die auf einem serialisierten Einlösescript basieren und für P2SH verwendet werden.[227]

Abbildung 3.9 zeigt die Zusammensetzung und den Weg vom öffentlichen Schlüssel (`ABCDEF1234567890`) hin zur Bitcoin-Adresse. Zunächst wird durch Anwendung von SHA256, gefolgt von RIPEMD160, der HASH160 des öffentlichen Schlüssels berechnet. Diesem Hash wird die Versionsnummer vorangestellt, wobei Version `0x00` für P2PKH Adressen verwendet wird, `0x05` wiederum für P2SH-Adressen. Aus der Kombination von Version und Hash wird ein Doppelt-SHA256-Hash errechnet. Die ersten 4 bytes dessen werden als Prüfsumme hinten angehängt. Das Resultat im Hexadezimalsystem (Basis 16) sieht also folgendermaßen aus:

`00CA1BC309990F8E137716FF98B14BFD8D0E74A02A1E482704`

Üblicherweise werden Bitcoin-Adressen den Nutzerinnen ausschließlich in Base58 (Basis 58) präsentiert. Das Alphabet von Base58 umfasst zunächst die natürlichen Zahlen, gefolgt von allen Großbuchstaben sowie Kleinbuchstaben. Bewusst verzichtet wurde auf die Zahl 0, die Großbuchstaben O und I sowie den Kleinbuchstaben l. Damit kombiniert Base58 einerseits eine kompaktere Schreibweise mit dem Vorteil der Fehlerreduktion, weil leicht zu verwechselnde Zeichen nicht in der Adresse vorkommen können.[228] Die oben angeführte Adresse, in Base58 kodiert, sieht folgendermaßen aus:

`1KRekgKeEag8UTQQ1MMSkRHm1MUyBzr8qq`

Nachdem Bitcoin-Adressen an erster Stelle stets eine Versionsangabe haben, kann auch in Base58-Kodierung die erste Stelle verwendet werden, um den Typ der Adresse einfach zu bestimmen. Übliche Varianten sind[229]:

- `1...` – Bitcoin-P2PKH-Adresse
- `3...` – Bitcoin-P2SH-Adresse
- `m...` oder `n...` – Testnet[230] P2PKH Adresse
- `2...` – Testnet-P2SH-Adresse

[227] [Krz14, Bitcoin-Addresses]
[228] [Ant14, Seite 72ff Base58 and Base58Check Encoding]
[229] [Bit15i]
[230] Testnet ist ein parallel laufendes Bitcoin-Netzwerk, dessen Einheit keinen monetären Gegenwert besitzt und in erster Linie zu Testzwecken verwendet wird.

Die Berechnung einer Bitcoin-P2PKH-Adresse in der Programmiersprache Python ist in *Berechnung von Bitcoin-Adressen (Anhang D)* dargelegt.

3.3.4 Standard-Transaktionen

Transaktionen müssen bestimmte Eigenschaften aufweisen, damit Sie als Standard-Transaktion klassifiziert und von Netzwerkknoten akzeptiert werden[231]:

- **Versionsnummer** muss zwischen 1 und der derzeitigen Versionsnummer liegen (gespeichert in `CTransaction::CURRENT_VERSION`[232]).
- **Transaktionsgröße** darf die maximale Größe von `MAX_STANDARD_TX_SIZE` (derzeit 100,000 Bytes[233]) nicht überschreiten.

Für alle **Transaktionseingänge**:

- Das `scriptSig` Feld darf die Größe von 1,650 bytes nicht überschreiten.
- Das `scriptSig` Feld muss „Push Only“ sein (darf nur einen Teil der verfügbaren OP-Instruktionen[234] beinhalten).

Für alle **Transaktionsausgänge**:

- Jeder Ausgang muss einem der Standardausgänge[235] entsprechen.
- Transaktionsausgänge, die mehr als ein Drittel ihres Gesamtwertes in Transaktionsgebühren investieren, werden als „Dust“ (Staub) bezeichnet und nicht akzeptiert. Aus der minimalen Transaktionsgebühr, die derzeit bei 5000 Satoshi liegt[236], kann der minimale auszugebende Betrag mit folgender Formel[237]

  $$MinValue = 3 * \frac{MinTxFeeRate}{1000} * (TxOutSize + 148)$$

  abgeleitet werden. Eine durchschnittliche P2PKH Transaction hat die Größe von 34 Bytes, damit ergibt sich ein minimaler Betrag von $3 * \frac{5000}{1000} * (34 + 148) = 2730$ Satoshi.

[231] [Bit15a, Zeile 636 main.cpp:`isStandardTx()`]
[232] [Bit15a, Zeile 184 primitives/transaction.h:`CURRENT_VERSION`]
[233] [Bit15a, Zeile 58 main.h:`MAX_STANDARD_TX_SIZE`]
[234] Siehe *Script Sprache (Abschnitt 3.3.2)*.
[235] Siehe *Standard-Transaktionsausgänge (Abschnitt 3.3.2)*.
[236] [Bit15a, Zeile 67 main.cpp:`minRelayTxFee`]
[237] [Krz14, Appendix B: Minimum Spending Amount]

3.3.5 Coinbase-Transaktionen

Wie bereits angeführt, existiert neben regulären Transaktionen des Weiteren noch eine Spezialform, die sogenannten Coinbase-Transaktionen. Diese Art von Transaktion emittiert einen neuen Wert im Bitcoin-Netzwerk und weist als solche einige Unterschiede zu regulären Transaktionen auf. Der offensichtlichste Unterschied liegt in den Eingängen der Transaktion. Eine Coinbase-Transaktion besitzt stets genau einen Eingang, der auf keinen vorhergehenden Ausgang verweist. Er generiert somit neuen Wert im Netzwerk. Die Zusammensetzung dieses Wertes wird in *Anreiz (Unterabschnitt 3.5.2)* im Detail beschrieben. Nachdem der Hashwert dieses Eingangs auf keinen Wert verweisen kann, wird dieser auf den Wert 0 gesetzt. Das zugehörige scriptSig-Feld wird in diesem Fall oftmals auch als coinbase-Feld bezeichnet. Nachdem in diesem Fall keine Notwendigkeit vorherrscht, sich als rechtmäßiger Besitzer auszuweisen, kann dieses Feld bis zu einer Größe von 100 Bytes vom Erzeuger mit beliebigen Daten befüllt werden. Üblicherweise wird ein Teil des Feldes jedoch für Variationen während des Minings verwendet[238]. Außerdem ist seit Bitcoin Improvement Proposal Nummer 34[239] und der damit eingeführten Versionsnummer 2 für Blocks der erste Teil des coinbase-Feldes für einen Verweis auf die Blockhöhe[240] reserviert. Bei Ausgängen bestehen im Format keine Unterschiede zu jenen von regulären Transaktionen. Einzig die Verwendung dieser Ausgänge ist für die nächsten 100 Blocks – was einer zeitlichen Dauer von etwa 16 Stunden entspricht – gesperrt[241]. Gründe für diese Sperre werden in *Wahl der aktiven Blockchain (Unterabschnitt 3.6.4)* erläutert.

Die erste Coinbase-Transaktion[242] wurde durch Satoshi Nakamoto mit dem ersten jemals erzeugten Block, dem sogenannten **Genesis Block**[243] erzeugt. Im Script dieser Coinbase-Transaktion ist ein Verweis auf einen Artikel der britische Tageszeitung „The Times“ gespeichert:

> The Times 03/Jan/2009 Chancellor on brink of second bailout for banks [244]

[238] Siehe extraNonce in *Arbeitsnachweis (Unterabschnitt 3.5.1)*.
[239] [Bit15c, BIP0034]
[240] Siehe Blockhöhe in *Blockchain (Abschnitt 3.4)*.
[241] [Bit15a, Zeile 14 consensus/consensus.h:`COINBASE_MATURITY`]
[242] Siehe Transaktion 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
[243] Siehe Block 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
[244] Siehe The Times – Article 2160028

Die Coinbase-Transaktion sowie der dazugehörige Genesis Block sind üblicherweise, wie in der Referenzimplementierung, fest im Quellcode codiert.[245]

3.4 Blockchain

Wie bereits in *Transaktionen (Abschnitt 3.3)* behandelt, sind Transaktionen miteinander verknüpft und bilden eine Transaktionskette. Eine Transaktion beziehungsweise die daraus resultierende Kette kann verwendet werden, um nachzuweisen, dass ein bestimmter Betrag von einer Person ausgegeben werden darf. Was jedoch nicht überprüft werden kann ist, ob der Betrag nicht auch annähernd zeitgleich einer weiteren Person versprochen wurde. Dafür ist üblicherweise eine vertrauenswürdige, zentrale Stelle von Nöten, die eine zeitliche Aufzeichnung über den Besitz des Wertes führt.

Satoshi Nakamoto hat dafür in seinem Arbeitspapier[246] die Einführung eines verteilten Zeitstempel-Servers[247] vorgesehen. Dieser Vorschlag, der zu weiten Teilen auf den Konzepten von Adam Back und dessen Konzeption Hashcash[248] beruht, sieht vor, dass Netzwerkknoten in regelmäßigen Abständen neue Blocks erzeugen. Die Erzeugung eines neues Blocks erfordert einen gewissen Arbeitsaufwand (Proof-of-Work). Neue Blöcke werden an das Ende angereiht und mit bestehenden Blöcken verkettet. Ausgehend vom Genesis Block mit dem Zeitstempel 03 Jan 2009 18:15:05 GMT[249], entsteht so die Blockchain (Blockkette), die vergleichbar zu einem Kassabuch (public ledger) jegliche Transaktion chronologisch in einem öffentlich einsehbaren Buch aufzeichnet. Jeder vollwertige Netzwerkknoten führt eine Kopie jener Blockchain. Die Blockchain und deren Inhalt kann jedoch auch jederzeit auf Online-Diensten wie blockchain.info eingesehen werden.

Nachdem jeder Block auf einem vorhergehenden Block basiert und die Erzeugung einen Arbeitsaufwand verursacht, kann ein potenzieller Angreifer des Systems nicht einfach einen älteren Block beziehungsweise eine Transaktion darin modifizieren.

[245] Siehe [Bit15a, Zeile 56–84 chainparams.cpp].
[246] [Nak09a]
[247] [Nak09a, Seite 2 – Timestamp Server]
[248] [Bac02]
[249] Siehe Block 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Durch die Verkettung wäre es notwendig, jeden nachfolgenden Block ebenfalls neu zu berechnen.

3.4.1 Blockstruktur

Ein Block ist ein Datenobjekt[250], das eine bestimmte Menge an Transaktionen zusammenfasst. Um einen Block zu erzeugen, ist ein Arbeitsaufwand notwendig, der bei Bitcoin durch wiederholtes Ausführen von Hashfunktionen sichergestellt wird. Erfüllt ein Netzwerkknoten die Aufgabe und kann den *Arbeitsnachweis (Unterabschnitt 3.5.1)* erbringen, wird dieser Block in die Blockchain aufgenommen. Ein Block ist unterteilt in den Header und den Payload. Während vollwertige Netzwerkknoten immer eine Kopie aller Blöcke gespeichert halten, wurden die Header von Nakamoto[251] derart spezifiziert, dass die darin enthaltene Information zur vereinfachten Verifikation von Transaktionen ausreichend sind. Mobile Netzwerkknoten machen zum Beispiel von diesen Eigenschaften Gebrauch. Weiters wurde von Nakamoto[252] das Verwerfen von Payloads in älteren Blocks in Betracht gezogen, um Speicherplatz zu sparen. Diese Spezifikation ist in der Bitcoin-Standardimplementation allerdings bis heute nicht umgesetzt[253].

Der Blockheader einerseits umfasst eine *Versionsnummer* (derzeit werden Blöcke der Version 3 erzeugt[254]), den *Merkle Root* (Wurzelknoten eines Merkle Baumes, erstellt aus allen Transaktionen, die im Block integriert sind) sowie den Hash des vorhergehenden Blocks, des Weiteren einen *Zeitstempel*, eine *Arbeitsaufgabe* und ein Feld genannt *Nonce*. Die 3 letztgenannten Felder sind für das Erledigen der Arbeitsaufgabe vorgesehen und werden in *Arbeitsnachweis (Unterabschnitt 3.5.1)* näher betrachtet. Der Payload andererseits speichert alle Transaktionsobjekte, die Teil des Blocks sind, und hält den Merkle Baum über die Transaktionen im Speicher.

Dadurch, dass jeder Block einen Hash des vorhergehenden Blocks im Header gespeichert hat, besteht immer ein fix definierter Vorgänger in der Kette von Blöcken.

[250] Siehe *Bitcoin-Block (Anhang C)* für die vollständige Zusammensetzung eines Blockelements.
[251] [Nak09a, Seite 5 Kapitel 8 Simplified Payment Verifikation]
[252] [Nak09a, Seite 5 Kapitel 7 Reclaiming Disk Space]
[253] [Bit15l, Full Node Clients]
[254] [Bit15a, Zeile 24 primitives/block.h:`CURRENT_VERSION`] festgelegt in BIP66.

Aufgrund der dezentralen Struktur von Bitcoin kann es jedoch zu Gabelungen in der Kette kommen und so kurzzeitig mehrere Nachfolgerblöcke für einen Block geben. Diese Tatsache wird in *Dezentraler Konsens (Abschnitt 3.6)* im Detail betrachtet.

Jeder Block kann auf zwei unterschiedliche Arten identifiziert werden: Einerseits über seinen Hash, andererseits über die Blockhöhe. Die Blockhöhe bezeichnet die Position des Blocks in der Blockchain. Der Hash des Genesisblocks hat folgenden Wert:

```
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```

Die Blockhöhe wiederum hat den Wert 0, zumal es sich beim Genesisblock um den ersten jemals erzeugten Block handelt. Aufgrund des Konzepts der Gabelungen können Blockhöhen bei jungen Blöcken (weniger als 100 Blocks in der Blockchain) nicht immer eindeutig sein. Aus diesem Grund ist für die eindeutige Identifizierung die Verwendung des Blockhashes zu empfehlen.

3.5 Mining

Mit Mining (Abbauen) verwendet Bitcoin einmal mehr einen Begriff, der ursprünglich für Gold geprägt wurde. Es stellt den Prozess dar, der neuen monetären Wert in Umlauf bringt. Netzwerkknoten, die sich am Mining beteiligen, versuchen ein „mathematisches Rätsel“ so schnell wie möglich zu lösen und so einen neuen Block an die Blockchain anzuhängen. Derjenige Netzwerkknoten, der die geforderte Aufgabe als erstes erledigt, publiziert den neuen Block im gesamten Netzwerk und bekommt dafür einerseits alle Transaktionsgebühren und andererseits einen fixen Wert in Bitcoin, der als Incentive (Anreiz) bezeichnet wird. Die Höhe des Incentives betrug zu Beginn 50 XBT und wird alle 210,000 erzeugten Blöcke halbiert.

3.5.1 Arbeitsnachweis

Um einen neuen Block zu erstellen, ist es demnach notwendig, einen Arbeitsnachweis, auch Proof-of-Work genannt, zu erbringen. Nakamoto hat die Bitcoin-Spezifikation des Proof-of-Work Systems stark an jenes von Adam Back und dessen Hashcash-System

angelehnt. Back bezeichnet die zugrunde liegende Funktion als cost-function (Kostenfunktion) und definiert diese folgendermaßen:

> „A *cost-function* should be efficiently verifiable, but parameterisably expensive to compute.“[255]

Die Kostenfunktion, aus welcher der Proof-of-Work resultiert, soll also in der Schwierigkeit mittels Parameter(n) anzupassen sein und muss des Weiteren leicht überprüfbar sein.

> „The proof-of-work involves scanning for a value that when hashed, [...], the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.“[256]

Ein Miner, der nach einem neuen Block „sucht“, verwendet den Blockheader und versucht die Felder im Header derart anzupassen, dass die geforderte Aufgabe erfüllt werden kann. Für das Hashing des Blockheaders kommt einmal mehr Doppel-SHA256 zur Anwendung[257]. Der Parameter, der die Schwierigkeit der Aufgabe angibt, ist die Anzahl an führenden Nullen im Ergebnis der Hashfunktion.

Durch die Tatsache, dass bereits kleine Änderungen im Eingang einer Hashfunktion ein stark verändertes Ergebnis liefern, also das scheinbar zufällige Verhalten von Hashfunktionen, ist die einzige Möglichkeit, einen geforderten Arbeitsnachweis zu finden, die sogenannte Brute Force Methode.[258] Brute Force im Zusammenhang mit Mining bedeutet vor allem, dass das dafür vorgesehene Nonce-Feld im Block Header für jeden Hashing Versuch um den Wert 1 erhöht wird und damit ein neuer Versuch vorgenommen wird. Folgendes Codebeispiel[259] in Python zeigt vereinfacht den Miningablauf:

```
import hashlib
header = "nVersion||HashPrevBlock||HashMerkleRoot||nTime||nBits||"
for nonce in xrange(15):
```

[255] [Bac02, Seite 1 Kapitel 2 Cost Functions]
[256] [Nak09a, Seite 3 Kapitel 4 Proof-of-Work]
[257] [Krz14, Seite 36 Kapitel 5.2 Mining > Proof of Work]
[258] [Bac02, Seite 3 Kapitel 3 The Hashcash cost-function]
[259] Vergleiche [Ant14, Seite 188 Proof-of-Work Algorithm].

```
    inp = (header + str(nonce))
    print 'Nonce ' + str(nonce) + ' => ' + hashlib.sha256(hashlib.sha256(
        inp).digest()).digest().encode('hex_codec')

## Ausgabe
# Nonce  0 => 84ee0c553525dc...
# Nonce  1 => 8e30a264f1a7a0...
# Nonce  2 => e04f738648a2cc...
# Nonce  3 => 62038fa34c1cd2...
# Nonce  4 => 3fbfc7d301dfea...
# Nonce  5 => 9837ee17180592...
# Nonce  6 => c2cbaae006cc78...
# Nonce  7 => 84001e98fdeb7b...
# Nonce  8 => b54656ae1dcb88...
# Nonce  9 => 6dfdff065e8f20...
# Nonce 10 => daf47d1a0c1305...
# Nonce 11 => ce39f3003cc7c2...
# Nonce 12 => 66299c1f90b4ac...
# Nonce 13 => 9a49af43834053...
# Nonce 14 => 5f423aabeaf2ca...
# Nonce 15 => 7781c86d2eaf53...
# Nonce 16 => 04fa07ffe8d5a9...
```

Wäre im konkreten Fall ein Hash mit zumindest einer führenden Null gefordert, hätte der Miner die Aufgabe bereits mit dem 17. Versuch (`04fa07ffe8d5a9...`) erfüllt. Die Aufgabe hat also einerseits einen parametrisierbaren Schwierigkeitsgrad (Anzahl der führenden Nullen) und kann andererseits leicht verifiziert werden, in dem nur ein Hash (jener vom Blockheader mit Nonce 16) berechnet werden muss, um das Ergebnis zu überprüfen.[260]

Das Nonce-Feld im Blockheader hat als maximalen Wert 4294967295 und erlaubt damit 4.2 Milliarden Hashingversuche. Für Fälle, in denen dies nicht ausreichend ist, wird die extraNonce[261] in der zugehörigen Coinbase-Transaktion modifiziert und erneut mit einem Nonce-Wert von 0 gestartet[262]. Nachdem alle Transaktionen inklusive der

[260] [Ant14, Seite 188 Proof-of-Work Algorithm]
[261] Siehe *Coinbase-Transaktionen (Unterabschnitt 3.3.5)*.
[262] [Bit15f]

Coinbase-Transaktion im Merkle Root – und damit im Header – enthalten sind, wird durch das extraNonce-Feld ebenfalls das Ergebnis der Hashfunktion modifiziert.

Die Definition der Schwierigkeit kann zusätzlich noch auf eine weitere Art erfolgen. Die Aufgabe einen Hash zu finden, der mindestens eine führende Null aufweist, ist gleichbedeutend mit der Anforderung, einen Hashwert zu finden, der kleiner als jene Zahl ist[263]:

$$\texttt{0x1000000000000000000000000000000000000000000000000000000000000000}$$

Diese Zahl wird auch als Target bezeichnet und in komprimierter Form im Blockheader gespeichert, um die Schwierigkeit der aktuellen Aufgabe zu beschreiben[264]. Durch die Verwendung des Target-Wertes ist Bitcoin nicht – wie Hashcash – auf führende Nullen angewiesen, sondern erlaubt über die Definition des Target-Wertes auch Zwischenwerte[265]. So liegt der Zielwert zum Zeitpunkt dieser Arbeit in kompakter Schreibweise bei folgendem Wert: `0x1810B289`[266]. Die kompakte Schreibweise setzt sich aus Exponent (die ersten beiden Stellen) sowie Koeffizient (die verbleibenden Stellen) zusammen. Der eigentliche Zielwert lässt sich damit über jene Formel[267] bestimmen:

$$\texttt{target} = \texttt{coefficient} * 2^{(8*(\texttt{exponent}-3))}$$

Im konkreten Fall ergibt dies einen Target-Wert von:

$$\texttt{target} = \texttt{0x10B2B9} * 2^{(\texttt{0x08}*(\texttt{0x18}-\texttt{0x03}))} =$$

$$\texttt{0x00000000000000010b2890000000000000000000000000000000000000000000}$$

Die durchschnittliche Anzahl an Versuchen, bis ein Wert kleiner dem Zielwert (target) gefunden wird, lässt sich über folgende Formel[268] berechnen:

[263] [Ant14, Seite 190 Proof-of-Work Algorithm]
[264] [Bit15g, How is difficulty stored in blocks?]
[265] [Cla13, Seite 45 Proof of Work]
[266] Siehe Block 0000000000000000003cafbbe523eff065b688f1ea9d72f3b4efda702a38f837b
[267] [Ant14, Seite 194 Difficulty Representation]
[268] [Cla13, Seite 46ff Difficulty Targeting]

$$N(T) = \frac{2^{256}}{T}$$

$$N(T) = \frac{2^{256}}{40941912913922503071612068926197936615222106087944198553 6}$$

$$N(T) = 282,820,417,992,586,062,194$$

Mit dieser Schwierigkeit sind demnach im Durchschnitt 282 Trillionen Hashing-Versuche notwendig, um die Aufgabe zu lösen. Das gesamte Bitcoin-Netzwerk kann zum Zeitpunkt dieser Arbeit etwa 586 Billiarden Hashes pro Sekunde berechnen[269] und benötigt damit durchschnittlich 8 Minuten, um eine neue Arbeitsaufgabe zu lösen.

Anpassungen der Schwierigkeit

Alle Netzwerkknoten streben danach, dass idealerweise nur alle 10 Minuten ein neuer Block erzeugt werden kann. Vor allem aufgrund von steigender Leistungsfähigkeit von Computern sowie von schwankenden Userzahlen im Bitcoin-Netzwerk muss die Schwierigkeit regelmäßig angepasst werden, um die geforderte Zeit von 10 Minuten pro Block möglichst genau einhalten zu können. Jeder Netzwerkknoten berechnet nach jeweils 2016 Blocks die Schwierigkeit für die nächsten 2016 Blocks. Im Idealfall müsste die Erstellung der letzten 2016 Blocks[270] eine Zeit von 1,209,600 Sekunden[271], also 14 Tage, in Anspruch genommen haben. Für den Fall, dass die Erstellung der Blocks länger als 14 Tage in Anspruch genommen hat, wird die Schwierigkeit reduziert. Für den Fall, dass weniger als 1,209,600 Sekunden aufgewendet werden mussten, wird der Schwierigkeitswert für die kommenden 2016 Blocks angehoben. Um zu starke Schwankungen zu verhindern, sind die Anpassungen beschränkt. Maximalwerte sind 75% für die Reduktion sowie 300% für die Anhebung je Evaluierungsdurchgang[272].

[269] [Blo15b, 585,926,879 GH/s am 16.November 2015 12:20]
[270] Durch einen Fehler im Bitcoin Core Quellcode erfolgt die Evaluierung alle 2016 Blocks, verwendet aber für die Zeitberechnung nur 2015 Blocks und daraus resultierend leichte Abweichungen in der Berechnung.[Bit15b, Block Chain > Proof of Work].
[271] [Bit15a, Zeile 39 chainparams.cpp:`consensus.nPowTargetTimespan`]
[272] [Bit15b, Block Chain > Proof of Work]

3.5.2 Anreiz

Ein Netzwerkknoten, der sich am Mining beteiligt, sammelt während des Versuchs, den geforderten Arbeitsnachweis zu erfüllen, ausstehende Transaktionen und fügt diese zu seinem Blockobjekt hinzu. Neben diesen ausstehenden Transaktionen gibt es jedoch noch eine weitere Transaktion. An erster Stelle aller Transaktionen befindet sich eine Coinbase-Transaktion. Die Coinbase-Transaktion umfasst einerseits den Anreiz – und damit jenen Betrag, der neuen Geldwert in Umlauf bringt – andererseits auch alle Transaktionsgebühren der anderen Transaktionen aufsummiert. Die Summe aus Anreiz sowie Transaktionsgebühren darf der Miner an sich selbst adressieren – als Belohnung für die durchgeführte Arbeit.

Maximale Geldmenge

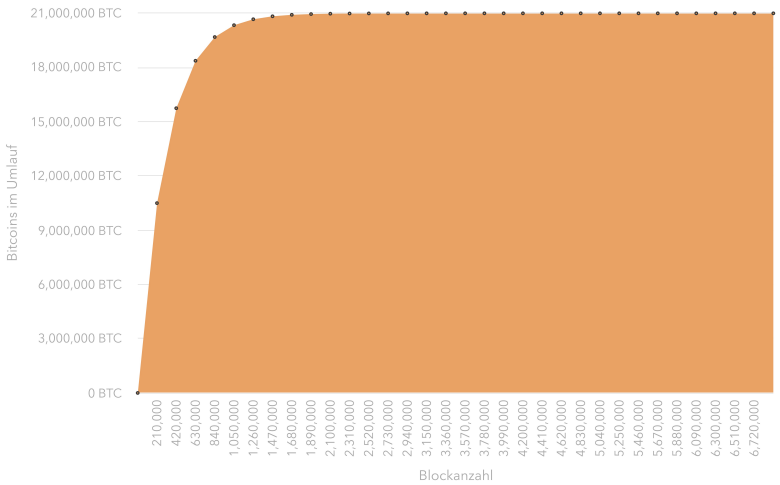

Abbildung 3.10: Entwicklung Bitcoin-Geldmenge

Der Anreiz für das Finden eines neuen Blocks betrugt zu Beginn 50 XBT. Alle 210,000 Blocks – also in etwa alle 4 Jahre – erfolgt eine Halbierung des Wertes. Die erste Halbierung fand am 28.November 2012[273] statt. Unter der Annahme, dass die Blockerstellung möglichst genau dem Zielwert von 10 Minuten entspricht, wird damit die nächste Halbierung auf den Wert 12.5 XBT in der zweiten Jahreshälfte 2016 eintreten.

[273] Siehe Block 000000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e

Durch diesen exponentiellen Abfall des Anreizes kann auch der maximal jemals existierende Bitcoin-Wert abgeleitet werden. Wie *Abbildung 3.10* zeigt, nähert sich die maximalen Anzahl der Bitcoins, die jemals im Umlauf sein werden, dem Wert von 21 Millionen an, erreicht diesen Wert jedoch nicht. Bereits zuvor fällt der Anreiz unter den Wert von 0 Satoshi und kann deshalb nicht mehr ausbezahlt werden. Die Menge an Bitcoins, die jemals verfügbar sein wird, wird 20999999.9769 XBT betragen[274] und in etwa im Jahr 2140 erreicht werden. Eine Entwicklung des Anreizes bis zu diesem Datum ist in *Mining Anreiz (Anhang E)* angeführt.

Transaktionsgebühren

Wie bereits in *Transaktionen (Abschnitt 3.3)* angeführt, sieht Bitcoin das Konzept von Transaktionsgebühren vor. Für Transaktionsgebühren steht kein eigenes Feld im Transaktionsobjekt zur Verfügung. Vielmehr sind die Gebühren durch die Differenz zwischen Eingangs- und Ausgangssumme einer Transaktion[275] bestimmt und sollen als Anreiz dienen eine ausstehende Transaktion in einen Block aufzunehmen. Ein Miner verwendet üblicherweise die Transaktionsgebühr sowie die Transaktionspriorität als Kriterium, welche Transaktionen wie schnell in einen Block aufgenommen werden.

Für Transaktionsgebühren gibt es – mit Ausnahme der Minimalhöhe – keine fixen Vorgaben. Jeder Netzwerkknoten kann selbst über die Höhe entscheiden. Die Standardimplementierung gibt jedoch mit dem Kommando `bitcoin-cli estimateFee` eine Empfehlung ab, welchen Wert die Gebühr betragen soll. Zum Zeitpunkt dieser Arbeit[276] lag die Empfehlung bei 0.00051539 XBT/kB für eine Verarbeitung der Transaktion in bis zu 10 Minuten sowie bei 0.00019760 XBT/kB für eine Verarbeitung in bis zu 20 Minuten. Wie an den Einheiten zu sehen, ist die Transaktionsgebühr in Bitcoin nicht vom monetären Wert der Transaktion abhängig, sondern von der Größe des resultierenden Transaktionsobjekts. Das hat zur Folge, dass einr Transaktion mit wenigen Ein- sowie Ausgängen aber einem hohen monetären Wert mitunter weniger Gebühren hinzufügt werden muss, als einer Transaktion mit unzähligen Ein- und Ausgängen aber insgesamt niedrigem monetären Wert.

[274] [Ant14, Seite 174 Bitcoin Economics and Currency Creation]
[275] [Bit15a, Zeile 273 miner.cpp:nTxFees]
[276] Aufgerufen 17. November 2015 13:29.

Die Priorität einer Transaktion wiederum ist folgendermaßen festgelegt[277]:

$$\frac{\sum \texttt{InputValue} * \texttt{InputAge}}{\texttt{TransactionSize}}$$

Während die Standardimplementation zum Zeitpunkt dieser Arbeit eine minimale Transaktionsgebühr von 5000 Satoshi sowohl für die Weiterleitung im Netzwerk als auch für die Aufnahme von Blocks vorsieht[278], gibt es zumindest für Letzteres eine Ausnahme. Die Standardimplementation sieht vor, dass jeder Miner einen Teil seines Blocks (üblicherweise die ersten 50 Byte) für sogenannte High-Priority Transaktionen freihält[279]. Eine High-Priority Transaktion ist jene, deren Priorität $\texttt{COIN} * 144/255 = 57600$[280] oder höher ist. Der Wert 57,600 beschreibt eine Transaktion mit einem Eingang in Höhe von 1 XBT, der für zumindest einen Tag (144 Blocks) nicht verarbeitet wurde und dessen Größe 255 bytes entspricht. Eine Transaktion, die diese Anforderungen erfüllt, wird von Minern auch ohne Transaktionsgebühr in den Block mit aufgenommen. Wenn die ersten 50 Bytes belegt sind, sortiert die Standardimplementierung alle weiteren ausstehenden Transaktionen nach Gebührenrate, gefolgt von Priorität, und wählt aus dieser Liste die verbleibenden Transaktionen für den Block aus[281].

3.6 Dezentraler Konsens

Eine zentrale und wichtige Eigenschaft von Bitcoin stellt die Findung des Konsenses in einem dezentralen Netz ohne jegliche Vertrauensstelle statt. Im Bitcoin-Netzwerk wird prinzipiell jedem Netzwerkknoten misstraut, es gibt zu keiner Zeit einen expliziten Konsens, der durch Abstimmungen oder Ähnliches herbeigeführt wird. Stattdessen entsteht aufgrund von einfachen Mechanismen im Netzwerk ein emergenter Konsens. Dieses Konzept wird in nahezu allen Bereichen von Bitcoin angewandt und entsteht vor allem aus jenen 4 Teilbereichen[282]:

- Unabhängige Verifikation aller Transaktionen durch jeden Netzwerknoten.

[277] [Bit15a, Zeile 232 coins.cpp:`CCoinsViewCache::GetPriority`]
[278] [Bit15a, Zeile 67 main.cpp:`minRelayTxFee`]
[279] [Bit15a, Zeile 54 main.h:`DEFAULT_BLOCK_PRIORITY_SIZE`]
[280] [Bit15a, Zeile 18 txmempool.h:`AllowFreeThreshold`]
[281] [Bit15a, Zeile 262 miner.cpp]
[282] [Ant14, Seite 177 Decentralized Consensus]

- Unabhängige Aggregation von Transaktionen zu Blöcken durch Mining-Netzwerkknoten, in Verbindung mit der Erfüllung der Arbeitsaufgabe.
- Unabhängige Verifikation aller neugefundenen Blöcke durch alle Netzwerkknoten.
- Unabhängige Wahl der längsten Blockchain durch jeden Netzwerkknoten.

3.6.1 Verifikation von Transaktionen

Jeder Netzwerkknoten, der eine Transaktion erstellt, publiziert diese an seine unmittelbar bekannten Knoten im Netzwerk. Nachdem jeder Knoten jedem anderen Knoten misstraut, führt jeder Knoten im Netzwerk unabhängig von allen anderen Knoten eine Prüfung der Transaktion durch. Jeder Netzwerkknoten prüft grundlegende Dinge wie die korrekte Struktur des Transaktionsobjekts, Einhaltung der maximalen Größe, aber evaluiert in Folge auch das Script und überprüft damit, ob die Berechtigung für die Zahlung vorliegt[283].

Nur für den Fall, dass eine Transaktion diese Prüfung besteht, wird diese wiederum an die bekannten Knoten weitergeleitet und in den eigenen Transaction Pool (Sammlung von Transaktionen, die akzeptiert, aber noch nicht in einen Block aufgenommen wurden) aufgenommen. Dieses Verhalten stellt sicher, dass ungültige Transaktionen nur von einer kleinen Gruppe von Netzwerknoten überprüft werden und sich daraufhin nicht weiter im Netzwerk verbreiten.[284]

3.6.2 Aggregation in Blöcken

Eine valide Transaktion verteilt sich demnach in Kürze im gesamten Netzwerk und befindet sich im Transaction Pool (auch als Memory Pool bezeichnet). Diese Sammlung an ausstehenden Transaktionen verwenden Miner, um ein neues Blockobjekt zu erstellen und damit zu versuchen, die geforderte Arbeitsaufgabe zu lösen. Bevor eine Transaktion in den Block mit aufgenommen wird, erfolgt nochmals eine grundlegende Überprüfung der Transaktion[285]. Schafft es ein Miner, die geforderte Aufgabe zu

[283] [Bit15a, Zeile 4355 main.cpp]
[284] [Bit15a, Zeile 4379 main.cpp:`RelayTransaction( )`]
[285] [Bit15a, Zeile 283 miner.cpp]

erfüllen publiziert er das Ergebnis (das neue Blockobjekt) an seine bekannten Netzwerkknoten[286].

3.6.3 Verifikation von Blöcken

Ähnlich wie bei Transaktionen erhält jeder Netzwerkknoten unabhängig neue Blöcke und beginnt, diese zu evaluieren. Die Evaluation des Blocks beinhaltet[287]:

- Überprüfung des Block Headers;
- Überprüfung des Merkle Roots;
- Einhaltung der Größenlimitierungen;
- Prüfung, ob die erste enthaltene Transaktion eine Coinbase Transaktion ist;
- Prüfung aller weiteren Transaktionen auf Gültigkeit.

Nur wenn ein Netzwerkknoten einen Block für ordnungsgemäß befindet, leitet er diesen wiederum an seine bekannten Netzwerkknoten weiter. Wie schon bei *Verifikation von Transaktionen (Unterabschnitt 3.6.1)* thematisiert, wird dadurch sichergestellt, dass sich ausschließlich valide Blöcke über das Netzwerk verteilen und in die Blockchain aufgenommen werden.[288]

3.6.4 Wahl der aktiven Blockchain

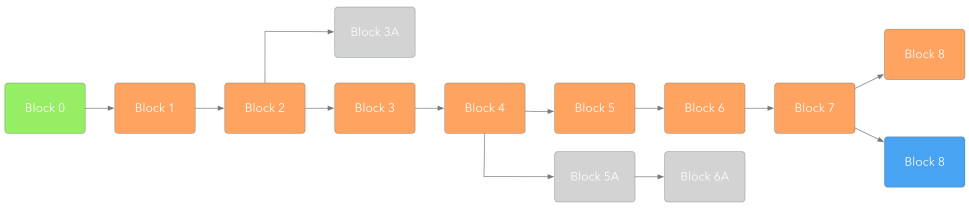

Abbildung 3.11: Blockchain mit Forks

[286] [Bit15a, Zeile 414 miner.cpp:`ProcessBlockFound( )`]
[287] [Bit15a, Zeile 2686 main.cpp:`CheckBlock( )`]
[288] [Bit15a, Zeile 4533 main.cpp]

Akzeptiert ein Netzwerkknoten einen Block als valide, beginnt der Knoten damit, diesen Block in seine Blockchain einzubauen. Nachdem ein neuer Block stets eine Referenz auf seinen vorhergehenden Block hat, kann der Netzwerknoten diese Information nutzen um die korrekte Position in der Blockchain zu finden.[289] Netzwerkknoten haben dafür 3 Arten von Blöcken zu verwalten[290]:

- Blöcke in der Hauptkette (mainchain);
- Blöcke die sich in einer parallelen Kette zur Hauptkette befinden (secondary chains);
- Blöcke, deren Elternknoten nicht bekannt ist (orphan blocks).

Während im Idealfall ein Block an die Hauptkette angehängt werden kann und die Blockkette sich chronologisch aufbaut, kann nicht ausgeschlossen werden, dass Miner annähernd zeitgleich eine Arbeitsaufgabe lösen und unabhängig voneinander 2 valide Ergebnisse im Netzwerk publizieren. In diesem Fall werden in der Blockkette Abzweigungen, so genannte Forks, angelegt. Diese Abzweigungen werden auch als secondary chains (zweitrangige Ketten) bezeichnet. Nachdem in einem dezentralen P2P-System, wie von Bitcoin verwendet, nicht sichergestellt ist, wann ein Block die einzelnen Netzwerkknoten erreicht, besteht weiters die Möglichkeit, einen Block zu erhalten obwohl dessen Elternknoten noch nicht bekannt sind. Diese so genannten orphan transactions (Waisentransaktionen) werden gespeichert und finden ihren Platz in der Blockchain, sobald das Elternelement den Netzwerkknoten erreicht hat.

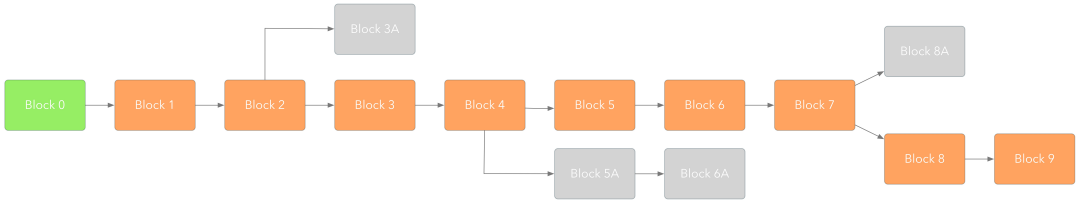

Abbildung 3.12: Blockchain mit neuer aktive Kette

[289] [Bit15a, Zeile 2388 main.cpp:`ActivateBestChain()`]
[290] [Ant14, Seite 198 Assembling and Selecting Chains of Blocks]

Abbildung 3.11 zeigt beispielhaft die Entwicklung der Blockchain ausgehend vom Genesisblock (in grün dargestellt). Der Netzwerkknoten erachtet die orange Kette als die aktive Kette. In grau dargestellt sind Blöcke aus vergangenen Abzweigungen, die in der Blockkette gehalten werden, aber ansonsten ignoriert werden, weil sie nicht zur aktiven Kette gehören. Jeder Netzwerkknoten bestimmt für sich unabhängig von allen anderen die aktive Kette als jene, in die die meiste Arbeit geflossen ist. Im konkreten Beispiel haben offensichtlich zwei Miner annähernd gleichzeitig eine valide Lösung für die Arbeitsaufgabe gefunden und deshalb zwei unterschiedliche Blöcke mit Blockhöhe 8 publiziert. Kann nun ein Miner eine Arbeitsaufgabe aufbauend auf Block 8 der sekundären Kette lösen, wird der Netzwerkknoten die aktive Kette wie in *Abbildung 3.12* ersichtlich wechseln, weil die sekundäre Kette länger wurde und dafür mehr Arbeit aufgewendet wurde.

Durch das Prinzip des Forkings lässt sich auch erklären, warum neu generierter Geldwert für vorerst 100 Blöcke ($100 * 10min = 1000min = 16.667h$) für die Ausgabe gesperrt ist. Die Bitcoin Implementierung geht davon aus, dass sich Abzweigungen innerhalb von maximal 100 Blöcken aufgelöst haben und damit bekannt ist, ob dieser Betrag Teil der aktiven Blockchain ist und damit tatsächlich ausgegeben werden darf. [291]

[291] [Cla13, Seite 47 Reward]

4 Bitcoin im E-Commerce

Im Rahmen dieser Diplomarbeit wurde der Webshop eines österreichischen Unternehmens um die Akzeptanz von Bitcoin erweitert. Das Unternehmen betreibt einen international fokussierten Webshop, der auf den Verkauf von Softwareprodukten für OS X[292] spezialisiert ist. Der Webshop und Vertrieb der Softwarelizenzen erfolgt über eine Webseite mit einem selbst implementierten Shop-System. Codebeispiele in den folgenden Kapiteln sind aus diesem Grund möglicherweise abgeändert und generalisiert. Einerseits wurden Shop-spezifische Anpassungen, die nicht dem allgemeinen Verständnis dienen, entfernt, andererseits wurde darauf geachtet, sicherheitsrelevante Aspekte des Shops nicht zu kompromittieren.

Im Folgenden wird auf die Kriterien für die Wahl des Finanzdienstleisters eingegangen, die Implementation und Integration in das bestehende Shopsystem näher angeführt und zuletzt eine Analyse vorgenommen. Das darauffolgende Kapitel *Bitcoin Akzeptanz (Kapitel 5)* analysiert, ob das neue Zahlungsmittel bei den Internetkunden des Shops Akzeptanz findet, ob es zu Veränderungen im Käuferverhalten führt und ob allgemein existierende Hypothesen zu Bitcoins belegbar sind.

4.1 Gegenüberstellung Zahlungsabwickler

Webshop Anbietern, die sich dazu entscheiden, Bitcoin anzubieten, steht ähnlich wie bei herkömmlichen Fiat-Währungen eine größere Anzahl an Zahlungsabwicklern zur Wahl. Der Zahlungsabwickler übernimmt Aufgaben wie die Verrechnung, trägt teilweise die Risiken von Währungsschwankungen und führt weitere Dienstleistungen durch. Für

[292] http://www.apple.com/osx/

diese Dienste wird eine Bearbeitungsgebühr – üblicherweise anteilsmäßig vom Umsatz –verrechnet. Im Webshop des Unternehmens sind bereits zwei solcher Zahlungsabwickler integriert: Zum einen mPay24 (für die Abwicklung von Kreditkartenzahlungen, EPS und Giropay); zum anderen PayPal, das je nach Käuferland unterschiedliche Zahlungsmethoden anbietet. Für die Akzeptanz von Bitcoin war es also naheliegend, einen dritten Zahlungsabwickler zu integrieren. Wichtige Kriterien bei der Wahl des Anbieters waren:

- Eine API, die die Integration in den eigenen Shop mittels PHP ermöglicht.
- Vermeidung von Währungsschwankungen.

Das Bitcoin-Wiki[293] führt derzeit eine Liste von 44 „Shopping Cart Interfaces“ auf. Darin enthalten sind jedoch auch Plattformen wie zum Beispiel Mt. Gox, die bereits 2014 geschlossen wurde[294]. Aus der Liste wurde ein Vorauswahl von 3 möglichen Anbietern getroffen: Coinbase, BitPay und Coinkite.

---

[293] [Bit15k]
[294] [SN14]
[295] [Coi15e]
[296] [Bit15n]
[297] [Coi15b]
[298] [Cop15]
[299] [Coi15t]
[300] [Coi15h]
[301] [Bit15s, Getting Started]
[302] [Coi15o]
[303] [Coi15q]
[304] [Coi15p]
[305] [Coi15j]
[306] [Bit15r]
[307] [Coi15o, Does this work with P2SH, Litecoin, Blackcoin?]
[308] [Coi15f]
[309] [Bit15s, Invoice Callbacks]
[310] [Coi15l]
[311] [Coi15f, API Client Libraries]
[312] [Bit15t, Plugins]
[313] [Coi15r]
[314] [Coi15k]
[315] [Bit15q, Bitcoin Best Bid Rate]
[316] [Coi15m, Exchange Rate, Funds Splitting/Forwarding]
[317] [Coi15h, Shopping Cart Plugins]
[318] [Bit15t, Plugins]
[319] [Coi15h, Getting Started]
[320] [Bit15s, Selling in Person]

Tabelle 4.1: Vergleich Zahlungsabwickler

	Coinbase	BitPay	Coinkite
Gründung	Juni 2012[295]	May 2011[296]	?
Wallet	Ja[297]	Ja[298]	Ja[299]
Integration	Hosted Checkout Page, Embeddable Widget (Button or Overlay), Email Invoices, Plugins[300]	Hosted Checkout Page, Embeddable Widget (Button or Overlay), Email Invoice, Integrations / Plugins[301]	Pay Button mit hosted checkout page, Voucher (digital zB E-Mail und physisch), Eigenes PoS Terminal[302,303,304]
Unterstützte Währungen	Bitcoin, Bitcoin Testnet[305]	Bitcoin, Bitcoin Testnet[306]	Bitcoin, Bitcoin Testnet, P2SH, Litecoin, Blackcoin[307]
API Schnittstelle	Ja (inkl. Callbacks)[308]	Ja (inkl. Callbacks)[309]	Ja (inkl. Callbacks)[310]
Merchant API Frameworks	7[311]	13[312]	7[313]
Umrechnungskurs	Durchschnitt von einer Auswahl an Umtauschbörsen[314]	Bitcoin Best Bid Rate[315]	Konfigurierbare Quelle von Drittanbietern[316]
Plugins	7[317]	31[318]	0
Retail / In Person	Möglich via Wallet App (iOS / Android)[319]	Spezielle App (iOS / Android) & Integration in bestehende PoS Systeme[320]	Über Hardware-Terminal mit Unterstützung für Bitcoin Debit Cards[321]
Unterstützte Länder	32	33[322]	?
Abrechnung	täglich (mit Instant Exchange)[323]	täglich (ab Business Paket)[324]	manuell oder automatisiert über Drittanbieter[325]
Garantierte Umrechnungsrate	Ja (mit Instant Exchange aktiv)[326]	Ja[327]	Nein. Umwechslung nicht angeboten.
Kunden	Dell, Expedia, Wikimedia, mozilla, PayPal und weitere[328]	shopify, Microsoft, PayPal, zynga und weitere[329]	?
Kosten	Gratis für Bitcoin Transaktionen. Gebühr für Instant Exchange 1% nach 1 Million US Dollar Umsatz[330]	Business Paket: 1% vom Umsatz (mindestens $35 pro Monat) Starter Paket: Kostenlos bis zu 30 Transaktionen pro Monat und $1000 pro Tag[331,332]	Paketpreise mit unterschiedlichem Umfang von $0, $9 bis $89 pro Monat[333]

Wie in Tabelle 4.1 ersichtlich, konzentrieren sich Coinbase und auch BitPay vermehrt auf den eCommerce-Bereich und können hier auch einige der bekanntesten Bitcoin-Akzeptanzstellen als Kunden auflisten: Dell, Expedia, shopify, Microsoft und weitere. Coinkite im Gegensatz bietet zwar grundlegend auch ein Programmierinterface für eCommerce an, der Fokus des Anbieters liegt aber auf dem herkömmlichen Retail Geschäft. Dies wird auch durch das Angebot eines eigenen Terminals deutlich, das offensichtlich an herkömmliche Kreditkartenterminals angelehnt ist. Coinbase und BitPay bieten ein beinahe identisches Angebot. Unterschiede sind nur im Detail zu erkennen.

Die Wahl fiel schlussendlich aus folgenden Gründen auf Coinbase: Coinbase Wallets sind die derzeit am häufigsten genutzten Wallets, um Bitcoins zu speichern[334]. Während jeder Besitzer von Bitcoin die Coinbase-Integration nutzen kann, ist der Kaufprozess für Coinbase Kunden in weniger Schritten zu erledigen und bedarf keiner manuellen Überweisung. Sämtliche Bitcoin-basierten Transaktionen sind auf Coinbase kostenlos. Wenn Instant-Exchange, also die automatische Umwechslung der Bitcoins in die lokale Währung unter Garantie des Wechselkurses, aktiviert wird, wird dafür eine Wechselgebühr von 1% des Betrags in Rechnung gestellt. Diese Gebühr setzt allerdings erst ab einem Umsatzvolumen von mehr als einer Million USD ein. Bankgebühren entfallen für Besitzer eines Kontos im SEPA-Zahlungsraum. Coinbase kann also zunächst ohne jegliche Kosten von Händlern über einen längeren Zeitraum getestet werden[335]. Instant-Exchange und die Händlerfunktionen stehen derzeit in 32 Ländern zur Verfü-

[321] [Coi15p]
[322] [Bit15v]
[323] [Coi15g]
[324] [Bit15u]
[325] [Coi15n]
[326] [Coi15g]
[327] [Bit15u]
[328] [Coi15c]
[329] [Bit15o]
[330] [Coi15a]
[331] [Bit15u]
[332] [Bit15p]
[333] [Coi15s]
[334] [Unb14]
[335] [Coi15h, Pricingcon]

gung[336]. Zu guter Letzt war auch die durchwegs gute Reputation von Coinbase sowie die gute Berichterstattung ein Entscheidungskriterium[337].

4.2 Integration

Coinbase ermöglicht Händlern die Integration der Coinbase Merchant Services auf unterschiedlichen Ebenen[338]. Für vorab festgelegte Summen und Produkte können passende Bezahlseiten online vorkonfiguriert werden. Der dabei erstellte Code kann dann einfach auf die Webseite kopiert werden und setzt somit keine bis wenig Programmierkenntnisse voraus. Für den Fall, dass vorgefertigte Shopsysteme wie WooCommerce[339], Magento[340], Zen Cart[341], oder ähnliche verwendet werden, stehen Plugins zur Verfügung. Damit wird eine Integration ermöglicht, ohne Quellcode modifizieren zu müssen[342]. Eine weitere Möglichkeit ist die Erstellung einer Rechnung[343], die an den Kunden per E-Mail übermittelt wird und zur Begleichung eines definierbaren Betrags auffordert. Um komplexere Anforderungen abzudecken und die Integration in selbst geschrieben Shopsysteme zu ermöglichen, steht eine Coinbase Merchant API zu Verfügung[344].

Für die Integration im Rahmen dieser Diplomarbeit wird letztgenannte Option der Merchant API, verwendet um eine Payment Page[345] personalisiert auf die Auswahl des Kunden zu erstellen.

4.2.1 API

Coinbase bietet, wie bereits in Tabelle 4.1 angeführt, eine Programmierschnittstelle (API) an. Die API bietet ermöglicht es, auf Bitcoin-Wallets zuzugreifen, die Bitcoin-Trading-Plattform Coinbase Exchange zu verwenden, direkten Zugriff auf die Rohdaten

[336] [Coi15d]
[337] [Eff14], [Emb15]
[338] [Coi15h]
[339] http://www.woothemes.com/woocommerce/
[340] http://magento.com
[341] http://www.zen-cart.com
[342] [Coi15h, Shopping Cart Plugins]
[343] [Coi15h, Email Invoices]
[344] [Coi15h, Payment Pages]
[345] [Coi15h, Payment Pages]

der Blockchain zu erhalten und bietet weiters auch Coinbase-Merchant-Tools, um als Händler Bitcoin in Webshops akzeptieren zu können. All diese Bereiche sind über die einheitliche URL `https://api.coinbase.com/v2/` und ausschließlich über verschlüsselte Verbindung (https) erreichbar. Für den Fall, dass Daten über die Schnittstelle übermittelt werden, geschieht dies sowohl von, als auch zu Coinbase Servern im JSON-Format kodiert.[346]

4.2.2 Authentifizierung

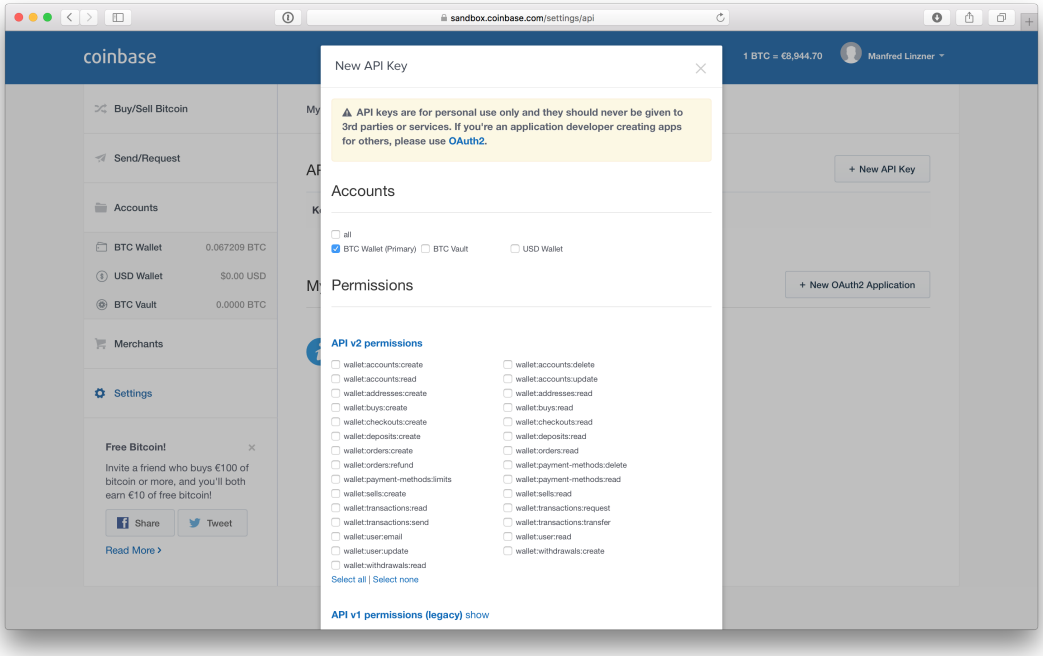

Abbildung 4.1: Coinbase – API Schlüsselerstellung

Die Coinbase API bietet zwei unterschiedliche Arten der Authentifizierung: Einerseits mittels API Schlüssel[347], die im Login-Bereich von Coinbase für jeden Benutzer erstellt werden können, und andererseits mittels OAuth2-Authentifizierung[348]. Letztere ist notwendig, wenn die Programmierschnittstelle dazu verwendet wird, um auf

[346] [Coi15i, Getting Started]
[347] [Coi15h, API Key Authentication]
[348] [Coi15h, Coinbase Connect]

Benutzerkonten von anderen Coinbase-Kunden zuzugreifen (zum Beispiel die Wallets von Kunden um Funktionen zu erweitern oder vergleichbare Funktionen). Für den Zugriff auf das eigene Benutzerkonto und um neue Zahlungsanweisungen zu erstellen, kann die API Schlüssel-Variante zur Authentifizierung verwendet werden.[349] Da für den genutzten Anwendungsfall die API Schlüssel-Authentifizierung notwendig ist, wird in der folgenden Beschreibung auf die zweite Variante der Authentifizierung nicht näher eingegangen.

Als erster Schritt ist es notwendig, im Benutzerbereich von Coinbase einen passenden API Schlüssel zu erstellen. Coinbase ermöglicht hier die Konfiguration des Funktionsumfangs des API Schlüssels. Für die geforderte Aufgabenstellung ist es ausreichend, einen sehr eingeschränkten Schlüssel zu erzeugen, der lediglich die Berechtigung bekommt, neue Zahlungsanweisungen zu erstellen (`wallet:checkouts:create`). Der resultierende API Schlüssel besteht aus einem öffentlichen Schlüssel – genannt API Key – und einem geheimen Schlüssel, genannt API Secret. Die Authentifizierung muss für jede Anfrage an den Server durchgeführt werden und besteht aus 3 zusätzlichen Feldern, die in den HTTP Header der Anfrage eingetragen werden:

- `CB-ACCESS-KEY`
- `CB-ACCESS-TIMESTAMP`
- `CB-ACCESS-SIGN`

Bei `CB-ACCESS-KEY` handelt es sich um den bereits angeführten API Key. Zweitgenanntes Feld ist der Zeitstempel, zu welchem die Anfrage durchgeführt wird. Der Zeitstempel muss dabei in Sekunden seit Unixzeit[350] (auch genannt „the Epoch“) angegeben werden. Die Signatur `CB-ACCESS-SIGN` besteht aus der Zeichenkombination von Zeitstempel, Methode zur Übertragung der Argumente (immer „POST“ in diesem Fall), gefolgt vom der eigentlichen Anfrage und, falls zutreffend, Parameter die dabei mitübertragen werden. Die Signatur ist der Hash der kryptographischen Hashfunktion SHA256 mit der Zeichenkombination als Grundlage und dem API Secret als geheimem Teil. Eine beispielhafte Anfrage an den Coinbase-Server mit passender Authentifizie-

[349] [Coi15h, API Key Authentication]
[350] [Ope15, 4.15 Seconds Since the Epoch]

rung – unter Verwendung der Programmiersprache PHP – könnte folgendermaßen aussehen:

```
function coinbaseRequest($request, $parameters) {
    $apiUrl = "https://api.sandbox.coinbase.com/";
    $ch = curl_init();
    $apiKey = "b61[...]PQU";
    $apiSecret = "UXN[...]UR5";
    $timestamp = time();
    $fullUrl = $apiUrl . $request;

    $toSign = $timestamp . "POST" . $request . $parameters;
    $signature = hash_hmac('sha256', $toSign, $apiSecret);

    curl_setopt_array($ch, array(
      CURLOPT_URL => $fullUrl,
      CURLOPT_RETURNTRANSFER => true,
      CURLOPT_POSTFIELDS => $parameters,
      CURLOPT_POST => true,
      CURLOPT_HTTPHEADER => array(
         "CB-VERSION: 2015-10-03",
         "CB-ACCESS_KEY: " . $apiKey,
         "CB-ACCESS_TIMESTAMP: " . $timestamp,
         "CB-ACCESS_SIGN: " . $signature)
    ));
    $results = curl_exec($ch);
    [...]
      curl_close($ch);
    return json_decode($result);
}
```

4.2.3 Erstellung der Bezahlseite

Coinbase bietet zur Abwicklung von Zahlungen die Möglichkeit, Kunden auf deren Seite weiterzuleiten. Auf einer konfigurierbaren Seite, genannt Payment Page, schließt der Kunde den Kauf ab und wird im Anschluss an eine vordefinierte Adresse oder die Webseite des Händlers weitergeleitet. Für den Fall, dass häufig identische Produkte verkauft werden oder die geforderten Werte aus einer fixen Liste wählbar sind – wie es

zum Beispiel bei Spendenbeträgen der Fall ist – können Bezahlseiten online vorkonfiguriert werden. Der daraus resultierende Quellcode kann dann an geeigneter Stelle in die Webseite integriert werden. Für Webshops mit mehreren Produkten und häufig wechselndem Warenkorb kann die Programmierschnittstelle verwendet werden, um dynamisch eine neue Payment Page zu generieren.[351]

Zur Erstellung einer neuen Payment Page steht in der Programmierschnittstelle das `Checkout` Objekt zur Verfügung[352]. Das Checkout Objekt benötigt zumindest 3 Parameter[353]:

- `name`
- `amount`
- `currency`

Der Parameter `name` ist eine frei wählbare Bezeichnung, unter welcher die Bestellung angeführt werden soll. Sowohl `amount` als auch `currency` beschreiben den monetären Wert der Bestellung. Der Wert kann in Bitcoin angegeben werden, aber auch in jeder von Coinbase unterstützten Fiat-Währung. Wenn der Betrag nicht in Bitcoin angegeben wurde, berechnet Coinbase automatisch den derzeitigen Bitcoin Gegenwert mit aktuellem Umrechnungskurs. Die erstellte Bezahlseite ist für 15 Minuten gültig. In diesem Zeitraum kann der Kunde zum berechneten Umrechnungskurs den Kauf abschließen[354].

Der Quellcode zur Erzeugung einer Bezahlseite unter Berücksichtigung der im vorherigen Kapitel eingeführten Function `coinbaseRequest` sieht folgendermaßen aus:

```
$checkout['currency'] = "EUR";
$checkout['amount'] = "32.95";
$checkout['name'] = "Example Webshop";
$checkout['description'] = "Order #34312";
$checkout['success_url'] = "https://example.com/success.php";
$checkout['cancel_url'] = "https://example.com/cancel.php";
$checkout['metadata']['orderId'] = ... // custom attributes to match
    order in redirects or callbacks
```

[351] [Coi15h, Payment Pages]
[352] [Coi15f, Create Checkout]
[353] [Coi15f, Create Checkout]
[354] [Coi15f, Checkouts]

```
coinbaseRequest('/v2/checkouts', $checkout);
```

Wie zu erkennen ist, wurde in diesem Beispiel neben den 3 verpflichtenden Parametern noch weitere angeführt: Einerseits eine Beschreibung (`description`), um dem Kunden weitere Informationen zum Kauf bereitzustellen, andererseits eine `orderId` um die Zahlung zu einem späteren Zeitpunkt wieder der richtigen Bestellung im Shop zuordnen zu können. Coinbase akzeptiert als Metadaten beliebige Daten, die der Händler für die Zuordnung in seinem Shop benötigt. Die URLs für erfolgreiche oder abgebrochene Bestellungen werden verwendet, um den Kunden über das Ergebnis der Zahlung zu informieren. Auf die Weiterleitung an eine der beiden Adressen wird im kommenden Kapitel näher eingegangen.

Bei erfolgreicher Anfrage an den Coinbase Server antwortet dieser mit dem HTTP Status Code 201 (`Created New object saved`) und hängt weitere Informationen über das erzeugte Objekt an die Antwort an.[355] Für die konkrete Implementierung relevant ist hierbei lediglich der `embed_code` Parameter. Nach erfolgreicher Erstellung der Zahlungsanweisung kann mit diesem Parameter der Link zur jener – für die Bestellung angepassten – Zahlungsseite erzeugt werden. Der Link hat dabei folgendes Format: `https://www.coinbase.com/checkouts/[EMBED_CODE]`, wobei `[EMBED_CODE]`, mit dem Parameter aus der vorherigen Serverantwort ersetzt werden muss[356]. Nach Weiterleitung des Kunden auf die Bezahlseite kann dort der geforderte Betrag in Bitcoin, entweder durch direkte Überweisung von einem beliebigen Wallet, oder aber – für Coinbase Wallet Besitzer – durch das Anmelden am eigenen, beglichen werden.

4.2.4 Weiterleitung

Wie in *Erstellung der Bezahlseite (Unterabschnitt 4.2.3)* beschrieben, ist es möglich, Links anzuführen, zu welchen unter definierten Zuständen umgeleitet wird. Zur `success_url` wird weitergeleitet, wenn die Bezahlung erfolgreich war, aber auch im Fall eines Mispayments, also wenn ein Betrag an die entsprechende Bitcoin Adresse übermittelt wurde, dieser jedoch zu hoch oder zu niedrig war. Die `cancel_url` Adresse wird verwendet,

[355] Siehe *Coinbase Server Antwort (Anhang F)* für eine beispielhafte Antwort des Servers.
[356] [Coi15h, Payment Pages]

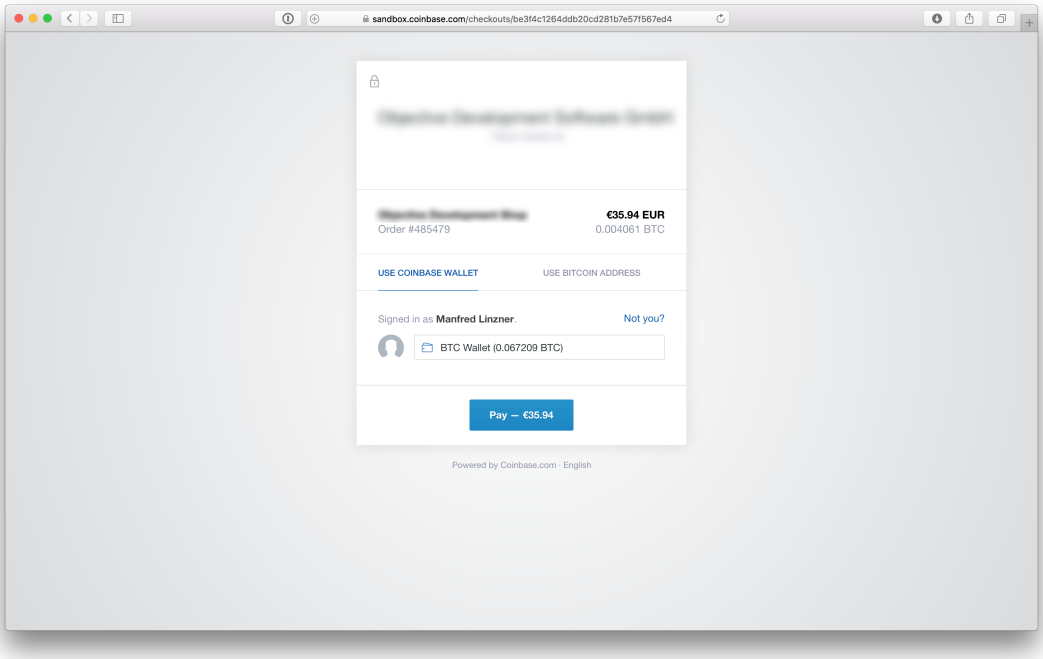

Abbildung 4.2: Coinbase – Bezahlseite

um auf Abbrüche der Zahlung hinzuweisen[357]. Bei jeder dieser Weiterleitungen wird ein Datenobjekt, ident zu jenem der *Callbacks (Unterabschnitt 4.2.5)*, angehängt, um den Zusammenhang zur jeweiligen Bestellung herstellen zu können[358].

Nachdem die Weiterleitungsadressen mitunter leicht zu erraten sind, sollte eine Weiterleitung nicht dazu verwendet werden, um Bestellungen tatsächlich als bezahlt zu markieren. Dafür sollen ausschließlich ausreichend abgesicherte Callbacks verwendet werden[359].

In der konkreten Implementierung weist eine unter `cancel_url` definierte Seite auf einen Fehler bei der Bezahlung hin. Die `success_url` wiederum prüft den Status der Bestellung aus dem angehängten Datenobjekt. Für den Fall, dass `status` auf einen Fehler hindeutet (zum Beispiel `mispayed`), wird ebenfalls ein Fehler präsentiert. Andernfalls wird die Bestellung in der Datenbank gesucht. Wenn die Bestellung – auf-

[357] [Coi15h, Payment Pages]
[358] [Coi15h, Payment Pages]
[359] [Coi15h, Payment Pages]

grund des passenden Callbacks[360] – bereits als bezahlt markiert wurde, werden der oder die Lizenzschlüssel dem Kunden präsentiert. Andernfalls wird darauf hingewiesen, dass die Bestellung noch bearbeitet wird und die Zustellung der Lizenzschlüssel per E-Mail geschieht.

4.2.5 Callbacks

Ein Callback, also eine automatisierte Benachrichtigung von Coinbase, steht für unterschiedliche Funktionen der Programmierschnittstelle zur Verfügung. Konkret[361]:

- Order Callback – eine Benachrichtigung, wenn sich der Status eines zuvor angelegten Order-Objekts verändert hat.
- Payout Callback – eine Benachrichtigung über eine automatische Auszahlung auf das hinterlegte Bankkonto (benötigt aktives Instant Exchange).
- Address Callback – eine Benachrichtigung, dass eine Zahlung auf das Bitcoin-Konto eingegangen ist.

Diese Benachrichtigungen und im besonderen der Order Callback können dazu verwendet werden, um den Status der Bestellung zu aktualisieren. In der Implementierung, die im Rahmen dieser Arbeit stattfindet, wird der Order Callback verwendet, um die Bestellung als bezahlt zu markieren, die Rechnung zu generieren und Lizenzschlüssel zu erstellen. Es muss daher sichergestellt werden, dass diese Benachrichtigungen so gut wie möglich vor Missbrauch geschützt werden. Coinbase empfiehlt hier mehrere Schritte: die Verwendung von TLS (https) zur Kommunikation, Verschleierung des Links (damit dieser möglichst schwer erraten werden kann), aber auch die Prüfung, ob die Benachrichtigung tatsächlich von Coinbase gesendet wurde (aus dem IP-Adressbereich `54.175.255.192-54.175.255.223`)[362]. Analog zu allen anderen in *Bitcoin im E-Commerce (Kapitel 4)* besprochenen Schnittstellen erfolgt die Anfrage über HTTP POST, es wird dabei ein Datenobjekt im JSON-Format angehängt[363].

[360] Siehe *Callbacks (Unterabschnitt 4.2.5)*.
[361] [Coi15h, Callbacks]
[362] [Coi15h, Callbacks; Securing Callbacks]
[363] [Coi15h, Callbacks; Usage]

Die Adresse für die hier relevante Benachrichtigung (Order Callback) muss zunächst im Benutzerbereich von Coinbase konfiguriert werden[364].

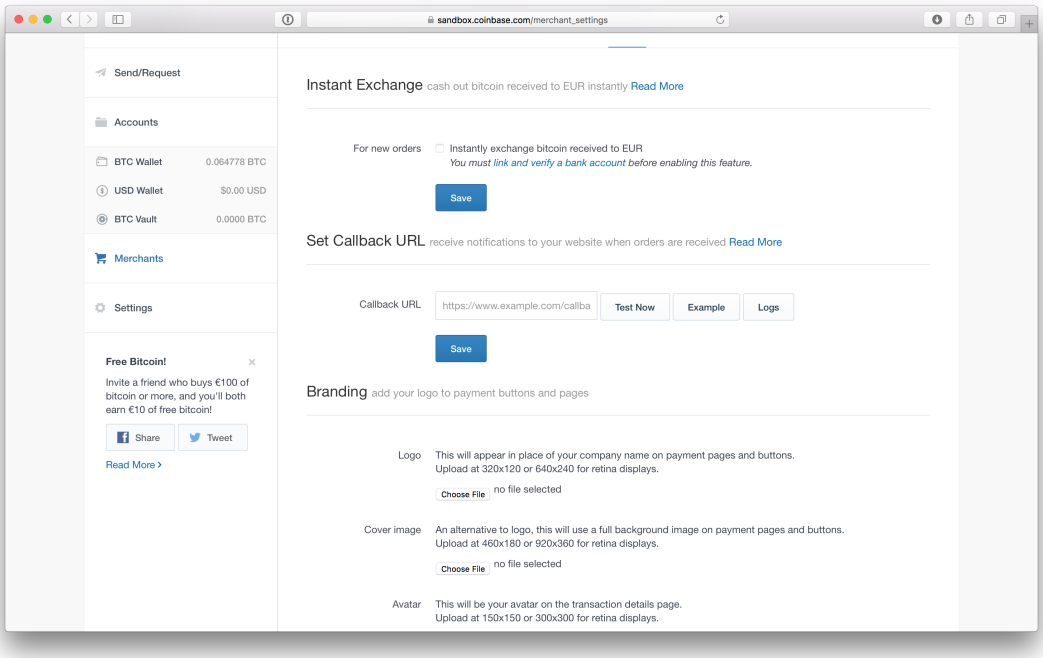

Abbildung 4.3: Coinbase – Callback URL konfigurieren

Nach dieser Konfiguration werden für alle erstellten Bezahlseiten[365] Benachrichtigungen gesendet, wenn sich der Status ändert. Derzeit verfügbare Zustände sind[366]:

- *completed*: Die Zahlung wurde abgeschlossen.
- *mispaid*: Der Kunde hat einen abweichenden Betrag (zu wenig oder zu viel) bezahlt.
- *expired*: Die Bezahlung wurde innerhalb des 15-minütigen Zeitfensters nicht abgeschlossen.

Ein vollständiges Beispiel für einen Order Callback ist in *Coinbase Order Callback (Anhang G)* ersichtlich. Für die Implementierung – positiver Status vorausgesetzt –

[364] [Coi15h, Callbacks; Setting A Callback URL]
[365] Vergleiche *Erstellung der Bezahlseite (Unterabschnitt 4.2.3)*
[366] [Coi15h, Callbacks; Order Callback Example]

relevant sind in diesem Fall vor allem die 3 Beträge, die als Teil der Benachrichtigung übermittelt werden[367]:

- `total_native`
- `total_btc`
- `total_payout`

Bei `total_native` handelt es sich um die Summe und Währung, die vom Händler beim Erstellen der Bezahlseite angefordert wird. `total_btc` wiederum ist jener Gegenwert in Bitcoin, der mit aktuellem Umrechnungskurs aus `total_native` berechnet wurde. Für den Fall, dass Instant Exchange aktiv ist, beschreibt `total_payout` den Betrag, der tatsächlich auf das hinterlegte Bankkonto übertragen wird, wobei die Währung von `total_payout` immer der lokalen Währung des Händlers entspricht. Im Fall, des konkreten Unternehmens mit Hauptsitz in der Europäischen Union also immer dem Betrag der Bestellung in Euro angibt, auch wenn für die ursprüngliche Bezahlseite ein Betrag in einer anderen Währung, wie zum Beispiel US Dollar angefordert wurde.

4.2.6 Zusammenfassung

Für die Integration von Bitcoin im bestehenden Shopsystem wurde zunächst eine Recherche der verfügbaren Zahlungsabwickler durchgeführt. Nach Eingrenzung auf 3 mögliche Anbieter und Evaluierung selbiger wurde Coinbase als Abwickler ausgewählt. Die Entscheidung ist – neben den erfüllten Ausschlusskriterien – vor allem aufgrund der Preisgestaltung, aber auch aufgrund von Instant Exchange gefallen. Letzteres garantiert Händlern Preisstabilität und verhindert Verluste durch unerwartete Preisschwankungen[368].

Für die Integration in den Shop wurde schließlich die von Coinbase angebotene Programmierschnittstelle, und hier im speziellen das `checkout` Objekt verwendet. Wenn sich ein Kunde beim Kaufabschluss für die Bezahlart Bitcoin entscheidet, wird

[367] [Coi15h, Callbacks; Example Callbacks]
[368] Siehe *Gegenüberstellung Zahlungsabwickler (Abschnitt 4.1)*.

eine – für den Kunden angepasste – Bezahlseite erstellt, die bei Coinbase zur Verfügung steht und an dessen Adresse der Kunde zur Bezahlung weitergeleitet wird[369].

Nach abgeschlossenem Bezahlvorgang wird der Kunde auf vordefinierte Webseiten im Shop weitergeleitet, die über den Erfolg oder Misserfolg des Bezahlvorganges informieren können[370]. Um den Status der Bestellung zu aktualisieren, wird jedoch stark abgeraten, auf diese Weiterleitungen zu vertrauen, zumal diese im Zweifelsfall leicht zu erraten seinen[371].

Die Aktualisierung der Bestellung und in diesem Zusammenhang die Rechnungslegung, Lizenzschlüsselerstellung und Weiteres erfolgt aufgrund von Callbacks, die an eine eigenständige, verschleierte Adresse zugestellt werden. Wie von Coinbase empfohlen, wurden hier zusätzlich weitere Sicherheitsmaßnahmen umgesetzt[372].

[369] Siehe *Erstellung der Bezahlseite (Unterabschnitt 4.2.3)*.
[370] Siehe *Weiterleitung (Unterabschnitt 4.2.4)*.
[371] [Coi15h, Payment Pages; Redirect URLs]
[372] Siehe *Callbacks (Unterabschnitt 4.2.5)*.

5 Bitcoin Akzeptanz

Bitcoins als zusätzliches Zahlungsmittel, wie in *Bitcoin im E-Commerce (Kapitel 4)* beschrieben, wurden im Onlineshop des Unternehmens am 7. Dezember 2015 aktiviert. Nach einem anfänglichen Testzeitraum wurde das neue Zahlungsmittel mit 11. Dezember 2015 im Blog des Unternehmens und in Sozialen Medien angekündigt. Vorab wurden 3 Hypothesen aufgestellt, die es zu bestätigen oder widerlegen galt. Für die Untersuchung stehen Daten aus einem Zeitraum von etwas mehr als einem Monat[373] zur Verfügung.

5.1 Hypothese 1: Bitcoin Verwendung

Bitcoins sind ein „Spielzeug“ und werden nicht wirklich verwendet.

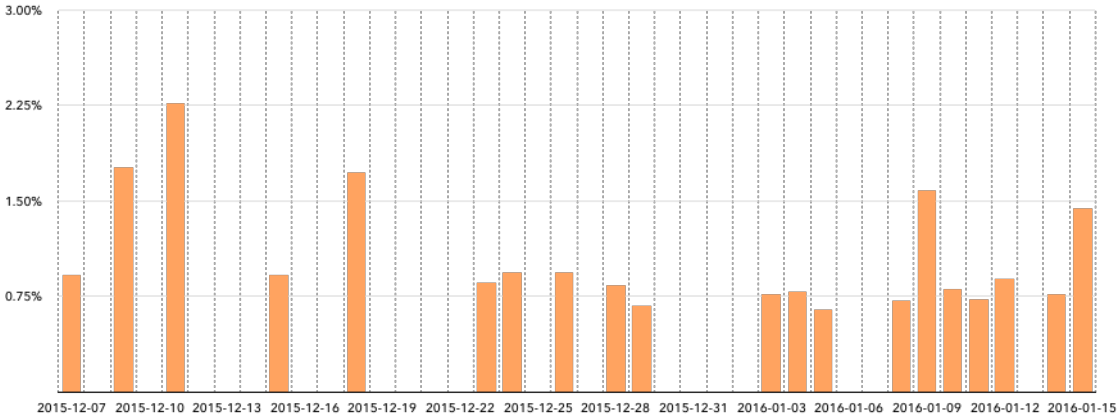

Abbildung 5.1: XBT Anteil an allen Bestellungen

[373] 7.Dezember 2015 bis einschließlich 15.Januar 2016.

Balkendiagramm Abbildung 5.1 zeigt den prozentuellen Anteil von erfolgreich abgeschlossenen Bestellungen, die mit Bitcoins beglichen wurden. Der bisher größte Anteil an Bitcoin-Bestellungen mit 2.27% war am 11. Dezember 2015. Jenem Tag, an dem das neue Zahlungsmittel im Unternehmensblog sowie in Sozialen Medien vorgestellt wurde. Im Durchschnitt über alle Tage, an denen Bitcoin-Bestellungen verzeichnet wurden, liegt der Anteil bei 1.05% von allen Umsätzen. Dieser Wert übersteigt nicht nur die Erwartungen innerhalb des Unternehmens, sondern zeigt auch, dass Bitcoins von einem Kreis an Personen aktiv für den Einkauf von Waren und Dienstleistungen im Internet verwendet wird.

5.2 Hypothese 2: Länderverteilung

Bitcoins werden vermehrt von Staatsbürgern aus Ländern mit schwachen oder instabilen Währungen wie zum Beispiel Russland oder China verwendet.

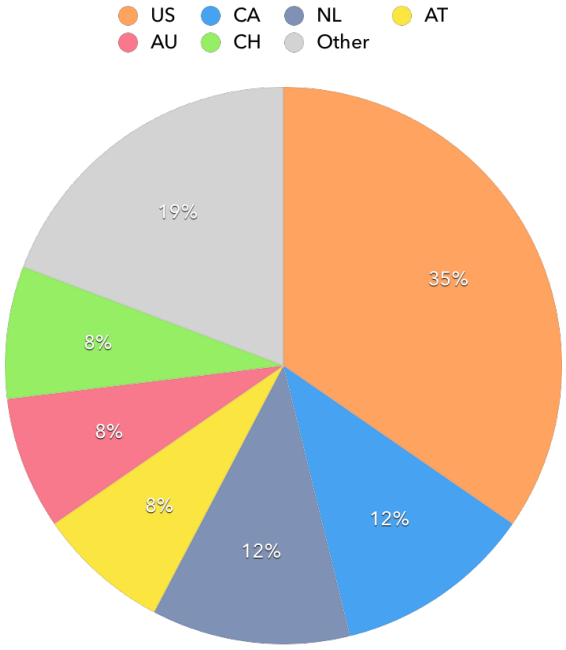

Abbildung 5.2: Länderanteil der Bestellungen mit Bitcoins

Die Kreisdiagramme *Abbildung 5.2* und *Abbildung 5.3* zeigen die Herkunftsländer der Kunden von Bitcoin-Bestellungen und jene mit herkömmlichen Zahlungsmitteln.

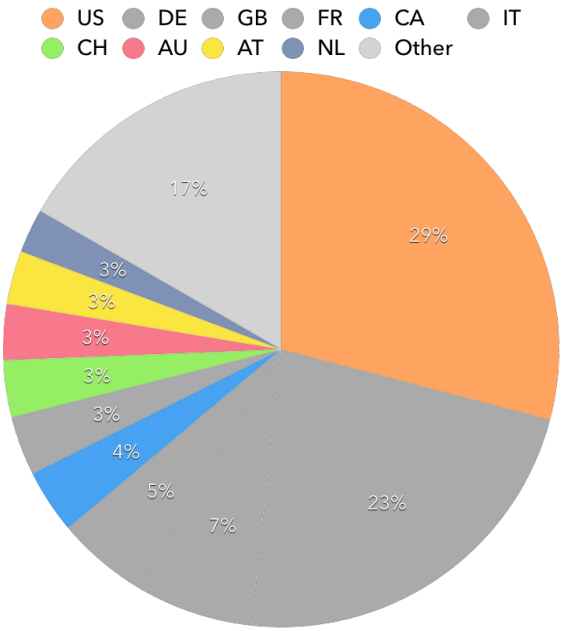

Abbildung 5.3: Länderanteil der Bestellungen mit anderen Bezahlmethoden

Wie zu sehen ist, folgen Bitcoin-Bestellungen mit nur kleinen Verschiebungen jener Verteilung, die bei herkömmlichen Zahlungsmitteln zu beobachten ist. Die zweite Hypothese ist demnach zu widerlegen, auch wenn im Hinblick auf Hypothese 3 nicht ausgeschlossen werden kann, dass eventuell der Herkunftsort verschleiert oder bewusst modifiziert wurde.

5.3 Hypothese 3: Anonymität

Nutzer von Bitcoin legen Wert auf Anonymität und verschleiern deshalb ihre Identität so gut wie möglich.

Wie bereits in *Bitcoin (Kapitel 3)* gezeigt wurde, ist Bitcoin kein anonymes, sondern vielmehr ein pseudonymes System. Mit ausreichenden Vorkehrungen ist allerdings ein hoher Grad an Anonymität zu erreichen. Für die Untersuchung dieser Hypothese wurde eine Liste von gängigen Anbietern von Wegwerf-E-Mail Adressen[374] erstellt. Eine Bestellung mit einer derartigen E-Mail Adresse wurde als „anonym“ gewertet. Ei-

[374] Vergleiche *Wegwerf-E-Mail Adressen (Anhang H)*.

ne Kontrolle der getätigten Bestellungen bestätigt den gewählten Ansatz. All diese Bestellungen verfügen über offensichtlich auch willkürlich gewählte Vor- und Nachnamen beziehungsweise Adressangaben. Bei Kreditkartenzahlungen ist in diesen Fällen selbstverständlich auch nicht ausgeschlossen, dass es sich dabei um versuchten Kreditkartenbetrug handelt.

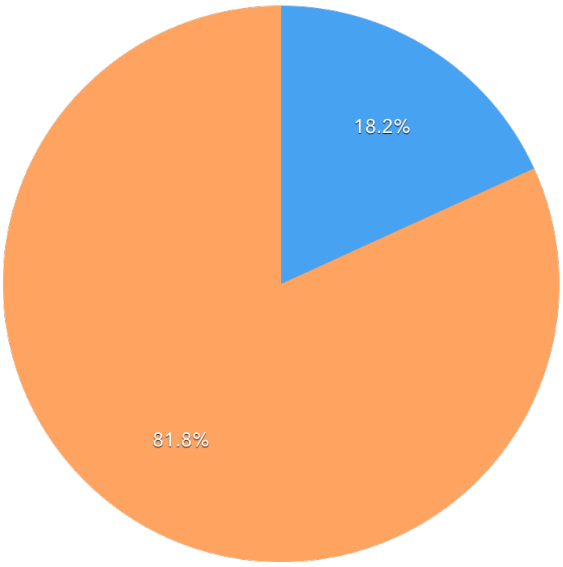

Abbildung 5.4: Anteil anonymen Bestellungen mit Bitcoins

Wie *Abbildung 5.4* und *Abbildung 5.5* zeigen, kann diese Hypothese klar bestätigt werden. Während lediglich 0.4% aller Bestellungen mit herkömmlichen Zahlungsmitteln anonymisiert erfolgten, sind es bei Bitcoin-Bestellungen im selben Zeitraum 18.2%. Es wird sich zeigen, ob Lizenzschlüssel, die auf diese Weise „anonym“ erworben wurden, in Zukunft vermehrt in einschlägigen Foren für Raubkopien publiziert werden, oder aber ob die Betreffenden tatsächlich aus anderen Motiven ein großes Bedürfnis verspüren, ihre Identität zu verschleiern.

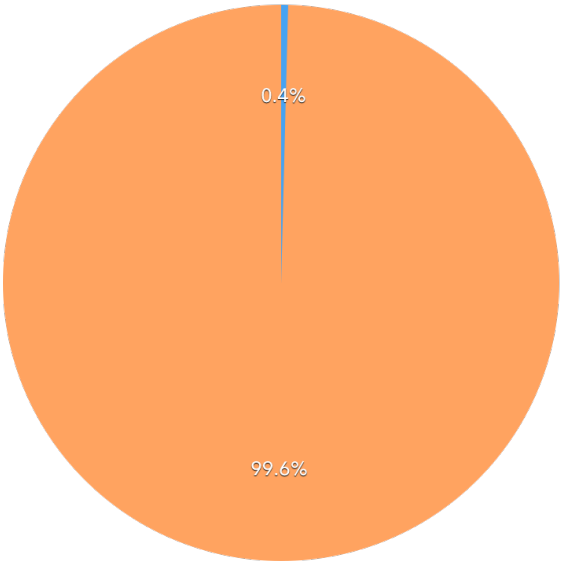

Abbildung 5.5: Anteil anonymen Bestellungen mit anderen Bezahlmethoden

6 Conclusio und Ausblick

Auch wenn die historische Entwicklung von virtuellen Währungen beziehungsweise Kryptowährungen bereits an die 20 Jahre in die Vergangenheit reicht, waren Bitcoins im Jahr 2009 die erste Währung, die ausschließlich dezentral spezifiziert wurde. In den 7 Jahren seit der Vorstellung hat sich die Gruppe der Nutzer und Nutzerinnen stetig vergrößert und zunehmend treten Bitcoins im herkömmlichen Handel auf. Wenn auch die tatsächliche Anzahl der Nutzer und Nutzerinnen schwer zu fassen ist, so konnte *Bitcoin Akzeptanz (Kapitel 5)* zeigen, dass eine Gruppe existiert, die Bitcoins aktiv für den Erwerb von Waren verwendet.

Ob und wie weit der Höhenflug der Technologie Bitcoin und der Währung Bitcoins reichen wird, ist aus jetziger Sicht schwer abschätzbar. Das Jahr 2016 wird ein Jahr der Weichenstellungen für die Bitcoin-Weiterentwicklung werden.

Die Bitcoin Foundation, jene Nichtregierungsorganisation, deren Hauptaufgabe die Förderung von Bitcoin ist und die unter anderem Gavin Andersen, dem Core Maintainer von Bitcoin, ein monatliches Gehalt bezahlt, dürfte kurz vor einer Auflösung stehen.[375] Auch wenn das Bitcoin-Projekt selbst Open-Source ist und keine Gruppe wie die Bitcoin Foundation benötigen würde, könnte die Auflösung dieser Organisation zu wegweisenden Veränderungen im Projekt führen.

Andererseits wird in der zweiten Hälfte 2016 erwartet, dass die Blockhöhe 420,000 erreicht wird und damit der Anreiz für Miner halbiert wird. Eine Halbierung des Anreizes fand in der bisherigen Geschichte von Bitcoin erst einmal im Jahr 2012 statt. [376] Transaktionsgebühren werden damit erneut an Bedeutung zulegen. Es wird sich zeigen,

[375] [Won15], [Mar16], [Kha15]
[376] Vergleiche *Anreiz (Unterabschnitt 3.5.2)*.

wie das Netzwerk darauf reagiert. Für einen Ausblick ist es notwendig, die Technologie Bitcoin und Währung Bitcoins getrennt zu betrachten.

In Zeiten des Internet und der geänderten Anforderungen hat eine überstaatliche **Währung** ohne Wechselkurse, Manipulationsgebühren und so weiter ein großes Potenzial und wird so auch nicht mehr wegzudenken sein. Ob tatsächlich Bitcoins den Markt behaupten werden oder eine andere virtuelle Währung, die die Konzepte von Bitcoin verwendet und verbessert, wird die Zeit zeigen. Inwieweit Bitcoins im herkömmlichen Retail Akzeptanz finden werden, hängt vermutlich stark von einzelnen Staaten und deren Gesetzgebung ab. Meiner Meinung nach schrecken derzeit die ungewissen rechtlichen Rahmenbedingungen noch viele ab. Sobald rechtliche Klarheit geschaffen wird, werden vermutlich auch weitere große Firmen Interesse an Kryptowährungen finden und so ist es denkbar, dass Bitcoins oder ähnliche Kryptowährungen weite Akzeptanz im Einzelhandel finden.

Die **Technologie** Bitcoin und deren Konzepte wie die Blockchain, der emergente Konsensus und so weiter, sind wegweisende Entwicklungen, die von Bitcoin durch geschickte Kombination von bestehenden Technologien geschaffen wurden. Wie bereits jetzt zu sehen ist, gibt es unzählige andere Anwendungsfälle für diese Technologien. Auch hier wird – meiner Meinung nach – die Internetgemeinde treibende Kraft in der Weiterentwicklung sein. Mit zunehmender Digitalisierung unserer Gesellschaft werden Konzepte wie jene von Bitcoin auch im Alltag Einzug halten. Die digitale Übereinkunft und Erstellung eines Vertrages könnte hier eine erste durchaus Interessante Anwendung auch für die breite Masse darstellen. Aber auch hier wird sich zeigen, ob es bei der Technologie, die Bitcoin eingeführt hat, bleiben wird. Bitcoin gilt aufgrund des Minings als äußerst ressourcenintensiver Ansatz. Bereits jetzt zeigt sich, dass Weiterentwicklungen (wie zum Beispiel Ripple) das bestehende Bitcoin Konzept aufgreifen und Schwachstellen – wie in diesem Fall die Ressourcenintensität – durch neue Konzepte ausgleichen können. Um diese Arbeit mit den Worten von Satoshi Nakamoto zu beenden: „Yes, [we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years.“[377]

[377] [Nako8b]

A Satoshi Nakamoto Essay

„I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at http://www.bitcoin.org/bitcoin.pdf

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

Satoshi Nakamoto

http://www.bitcoin.org"[378]

[378] [Nako9b]

B Bitcoin-Transaktion

Tabelle B.1: Transaktionsobjekt mit einem Eingang und einem Ausgang[379,380]

Feldname		Datentyp	Beschreibung
nVersion		Integer (int32_t)	Versionsnummer der Transaktion. Derzeit immer 1.
vin		Vector of CTxIn	Datenstruktur, die alle Eingänge der Transaktion speichert.
vin[0]	hash	Unsigned Integer (uint256)	Doppel-SHA256 Hash der vorhergehenden Transaktion.
	n	Unsigned Integer (uint32_t)	Index des referenzierten Transaktionsausgangs.
	scriptSig	CScript (Variable)	Script, um sich als rechtmäßige Besitzerin des referenzierten Ausgangs auszuweisen.
	nSequence	Unsigned Integer (uint32_t)	Sequenz Nummer (wird nicht mehr verwendet)
vout		Vector of CTxOut	Datenstruktur, die alle Ausgänge der Transaktion speichert.
vout[0]	nValue	Integer (int64_t)	Wert des Ausgangs in Satoshi (10^{-8} BTC)
	scriptPubKey	CScript (Variable)	Script, dass die Anforderungen zum Ausweis der Rechtmäßigkeit definiert.
nLockTime		Unsigned Integer (uint32_t)	Frühest möglicher Zeitpunkt, an dem die Transaktion in die Blockchain aufgenommen wird. Entweder 0 für sofortige Aufnahme, oder aber als Blockhöhe oder Zeitpunkt definiert.

[379] Vergleiche [Krz14, Tabelle 3.2 Regular Transaction Structure]
[380] [Bit15a, /src/primitives/transaction.h]

C Bitcoin-Block

Tabelle C.1: Blockobjekt[381,382]

Feldname	Typ und Größe	Beschreibung	
nVersion	Integer (int32_t)	Versionsnummer des Blocks. Derzeit 3	HEADER
HashPrevBlock	Unsigned Integer (uint256)	Doppel-SHA256 über den Header des vorhergehenden Blocks in der Blockchain.	HEADER
HashMerkleRoot	Unsigned Integer (uint256)	Root-Hash des Merkle Trees	HEADER
nTime	Unsigned Integer (uint32_t)	Datum und Uhrzeit der Blockerstellung (in Unix-Zeit)	HEADER
nBits	Unsigned Integer (uint32_t)	Kompakte Schreibweise der Schwierigkeit des Arbeitsnachweises	HEADER
nNonce	Unsigned Integer (uint32_t)	Feld, dass zur Bewältigung der Proof-of-Work Aufgabe beliebig befüllt werden kann.	HEADER
vtx	Vector of CTTransaction	Datenstruktur, die alle im Block enthaltenen Transaktion speichert	PAYLOAD
vMerkleTree	Vector of Unsigned Integer (uint256)	Der Merkle Tree für die im Block enthaltenen Transaktionen (inMemory only).	PAYLOAD

[381] Vergleiche [Krz14, Tabelle 3.1 Block Structure]
[382] [Bit15a, /src/primitives/block.h]

D Berechnung von Bitcoin-Adressen

```
import math
import hashlib
#==================================================
# Base58 Encoding based on code by Gavin Andresen
# https://bitcointalk.org/index.php?topic=1026.0
__b58chars = '123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz'
__b58base = len(__b58chars)
def b58encode(v):
  long_value = 0L
  for (i, c) in enumerate(v[::-1]):
    long_value += (256**i) * ord(c)
  result = ''
  while long_value >= __b58base:
    div, mod = divmod(long_value, __b58base)
    result = __b58chars[mod] + result
    long_value = div
  result = __b58chars[long_value] + result
  nPad = 0
  for c in v:
    if c == '\0': nPad += 1
    else: break
  return (__b58chars[0]*nPad) + result
#==================================================
pubKey = "ABCDEF1234567890"
pubKeyDecoded = pubKey.decode('hex')
# Calculate HASH160 (=> SHA256 followed by RIPEMD160) of pubKey
pubKeyHash = hashlib.new('ripemd160', hashlib.new('sha256', pubKeyDecoded)
    .digest()).digest()
```

```
# Add Version Prefix to pubKeyHash
version = "00".decode('hex')
rawAddr = version + pubKeyHash
# Calculate Double-SHA256 for Checksum
checksumHash = hashlib.new('sha256', hashlib.new('sha256', rawAddr).digest
    ()).digest()
# Append first 4 bytes of ChecksumHash and thereby create raw address
rawAddr += checksumHash[:4]
# Print Base58 encoded Bitcoin Address
print 'Public Key: ' + pubKey
print 'Bitcoin Address: ' + b58encode(rawAddr)
```

E Mining Anreiz

Tabelle E.1: Entwicklung Mining-Anreiz

Anreiz [XBT]	Blockhöhe	Bitcoins im Umlauf	(vorrausichtlicher) Eintritt
50.00000000	0	0.0000	*2009-01-03 18:15:05*
25.00000000	210,000	10,500,000.0000	*2012-11-28 15:24:38*
12.50000000	420,000	15,750,000.0000	2016
6.25000000	630,000	18,375,000.0000	2020
3.12500000	840,000	19,687,500.0000	2024
1.56250000	1,050,000	20,343,750.0000	2028
0.78125000	1,260,000	20,671,875.0000	2032
0.39062500	1,470,000	20,835,937.5000	2036
0.19531250	1,680,000	20,917,968.7500	2040
0.09765625	1,890,000	20,958,984.3750	2044
0.04882812	2,100,000	20,979,492.1875	2048
0.02441406	2,310,000	20,989,746.0927	2052
0.01220703	2,520,000	20,994,873.0453	2056
0.00610351	2,730,000	20,997,436.5216	2060
0.00305175	2,940,000	20,998,718.2587	2064
0.00152587	3,150,000	20,999,359.1262	2068
0.00076293	3,360,000	20,999,679.5589	2072
0.00038146	3,570,000	20,999,839.7742	2076
0.00019073	3,780,000	20,999,919.8808	2080
0.00009536	3,990,000	20,999,959.9341	2084
0.00004768	4,200,000	20,999,979.9597	2088
0.00002384	4,410,000	20,999,989.9725	2092
0.00001192	4,620,000	20,999,994.9789	2096
0.00000596	4,830,000	20,999,997.4821	2100
0.00000298	5,040,000	20,999,998.7337	2104
0.00000149	5,250,000	20,999,999.3595	2108
0.00000074	5,460,000	20,999,999.6724	2112
0.00000037	5,670,000	20,999,999.8278	2116
0.00000018	5,880,000	20,999,999.9055	2120
0.00000009	6,090,000	20,999,999.9433	2124
0.00000004	6,300,000	20,999,999.9622	2128
0.00000002	6,510,000	20,999,999.9706	2132
0.00000001	6,720,000	20,999,999.9748	2136
0.00000000	6,930,000	20,999,999.9769	2140

F Coinbase Server Antwort


```
{
  "data": {
    "id": "73250c97-e565-522d-bad1-b969d03c3456",
    "embed_code": "3ac34794d370a7b2756b3d266c87441c",
    "type": "order",
    "name": "Example Webshop",
    "description": "Order #ABCDEF",
    "amount": {
      "amount": "29.95",
      "currency": "EUR"
    },
    "style":"buy_now_large",
    "customer_defined_amount":false,
    "amount_presets":[],
    "success_url":"https://www.example.com/cb-success.php",
    "cancel_url":"https://www.example.com/cb-cancel.php",
    "auto_redirect":false,
    "collect_shipping_address":false,
    "collect_email":false,
    "collect_phone_number":false,
    "collect_country":false,
    "metadata":{
        "orderID":"abcdef1444652970"
    },
    "created_at":"2015-10-12T12:29:31Z",
    "updated_at":"2015-10-12T12:29:31Z",
    "resource":"checkout",
    "resource_path":"/v2/checkouts/73250c97-e565-522d-bad1-b969d03c3456"
```

```
    }
}
```

G Coinbase Order Callback


```
{
"order": {
  "id": "5RTQNACF",
  "created_at": "2012-12-09T21:23:41-08:00",
  "status": "completed",
  "event": {
    "type": "completed"
  },
  "total_btc": {
    "cents": 100000000,
    "currency_iso": "BTC"
  },
  "total_native": {
    "cents": 1253,
    "currency_iso": "USD"
  },
  "total_payout": {
    "cents": 2345,
    "currency_iso": "USD"
  },
  "custom": "order1234",
  "receive_address": "1NhwPYPgoPwr5hynRAsto5ZgEcw1LzM3My",
  "button": {
    "type": "buy_now",
    "name": "Alpaca Socks",
    "description": "The ultimate in lightweight footwear",
    "id": "5d37a3b61914d6d0ad15b5135d80c19f"
  },
```

```
    "transaction": {
      "id": "514f18b7a5ea3d630a00000f",
      "hash": "4
          a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "confirmations": 0
    },
    "refund_address": "1HcmQZarSgNuGYz4r7ZkjYumiU4PujrNYk"
  },
  "customer": {
    "email": "coinbase@example.com",
    "shipping_address": [
      "John Smith",
      "123 Main St.",
      "Springfield, OR 97477",
      "United States"
    ]
   }
  }
```

H Wegwerf-E-Mail Adressen

dispostable.com, mailinator.com, zippymail.info, guerrillammail.*, grr.la, spam4.me, sneakmail.com, 6paq.com, getairmail.com, eelmail.com, clrmail.com, tafmail.com, zetmail.com, spamgourmet.com, trashmail.*, trash-mail.*, wegwerfmail.*, objectmail.com, proxymail.eu, kurzepost.de, shitmail.org, crapmail.org, onewaymail.com, no-spam.ws, mt2015.com, meltmail.com, mailcatch.com, jetable.org, incognitomail.org, filzmail.com, armyspy.com, cuvox.de, dayrep.com, einrot.com, fleckens.hu, gustr.com, jourrapide.com, rhyta.com, superrita.com, teleworm.us, eyepaste.com, trbvm.com

Quellen

[AEU12] *Vertrag über die Arbeitsweise der Europäischen Union [Konsolidierte Fassung]*. Amtsblatt der Europäischen Union C 326/1, Oktober 2012. http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:12012E/TXT, besucht: 2015-11-30 .

[All09] Allen, Larry: *The Encyclopedia of Money*. ABC-CLIO, LLC, zweite Auflage, 2009, ISBN 978-1-59884-252-4.

[Ant14] Antonopoulos, Andreas M.: *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2014, ISBN 978-1-4493-7404-4.

[Bac02] Back, Adam: *Hashcash - A Denial of Service Counter-Measure*. 2002.

[Ban14] Bank of Russia: Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн. [Englische Übersetzung http://cointelegraph.com/news/11630/the_official_statement_of_russia_on_cryptographic_currencies], Januar 2014. http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm, besucht: 2015-12-10 .

[BBB+12] Barker, Elaine, William Barker, William Burr, William Polk und Miles Smid: *NIST Special Publication 800-57 – Recommendations for Key Management – Part 1: General*. U.S. Department of Commerce & National Institute of Standards and Technology, Gaithersburg, MD, 2012. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.

[BCA44] *Bank Charter Act 1844*. (7 & 8 Vict. c. 32), Juli 1844. http://www.legislation.gov.uk/ukpga/Vict/7-8/32, besucht: 2015-12-28 .

[Bit15a] Bitcoin Project: *Bitcoin Core Sourcecode*. cf33f... v0.11.1 (2015-11-02), 2015. https://github.com/bitcoin/bitcoin.

[Bit15b] Bitcoin Project: *Bitcoin Developer Guide*, 2015. https://bitcoin.org/en/developer-guide, besucht: 2015-11-03 .

[Bit15c] Bitcoin Project: *Bitcoin Improvement Proposals*, 2015. https://github.com/bitcoin/bips, besucht: 2015-11-10 .

[Bit15d] Bitcoin Security: Суд Екатеринбурга отменил решение о блокировке Bitcoin сайтов, Mai 2015. http://bits.media/news/sud-ekaterinburga-otmenil-reshenie-o-blokirovke-bitcoin-saytov-i-prizn besucht: 2015-12-11 .

[Bit15e] Bitcoinwiki: *Address*, 2015. https://en.bitcoin.it/wiki/Address, besucht: 2015-11-09 .

[Bit15f] Bitcoinwiki: *Block Hashing Algorithm*, 2015. https://en.bitcoin.it/wiki/Block_hashing_algorithm, besucht: 2015-11-17 .

[Bit15g] Bitcoinwiki: *Difficulty*, 2015. https://en.bitcoin.it/wiki/Difficulty, besucht: 2015-11-17 .

[Bit15h] Bitcoinwiki: *How bitcoin works*, 2015. https://en.bitcoin.it/wiki/How_bitcoin_works, besucht: 2015-10-24 .

[Bit15i] Bitcoinwiki: *List of address prefixes*, 2015. https://en.bitcoin.it/wiki/List_of_address_prefixes, besucht: 2015-11-09 .

[Bit15j] Bitcoinwiki: *Script*, 2015. https://en.bitcoin.it/wiki/Script, besucht: 2015-11-03 .

[Bit15k] Bitcoinwiki: *Shopping Cart Interfaces*, 2015. https://en.bitcoin.it/wiki/Category:Shopping_Cart_Interfaces, besucht: 2015-10-10 .

[Bit15l] Bitcoinwiki: *Thin Client Security*, 2015. https://en.bitcoin.it/wiki/Thin_Client_Security, besucht: 2015-11-17 .

[Bit15m] Bitcoinwiki: *Transaction*, 2015. https://en.bitcoin.it/wiki/Transaction, besucht: 2015-11-06 .

[Bit15n] BitPay: *About*, 2015. https://bitpay.com/about, besucht: 2015-10-19 .

[Bit15o] BitPay: *Accept Bitcoin*, 2015. https://bitpay.com/, besucht: 2015-10-19 .

[Bit15p] BitPay: *Are there any settlement fees?*, September 2015. https://support.bitpay.com/hc/en-us/articles/203324083-Are-there-any-settlement-fees-, besucht: 2015-10-19 .

[Bit15q] BitPay: *Bitcoin Exchange Rates*, 2015. https://bitpay.com/bitcoin-exchange-rates, besucht: 2015-10-19 .

[Bit15r] BitPay: *Can I test your service without signing up?*, März 2015. https://support.bitpay.com/hc/en-us/articles/203076786-Can-I-test-your-service-without-signing-up-, besucht: 2015-10-19 .

[Bit15s] BitPay: *Documentation*, 2015. https://bitpay.com/docs/, besucht: 2015-10-19 .

[Bit15t] BitPay: *Integrations*, 2015. https://bitpay.com/integrations/, besucht: 2015-10-19 .

[Bit15u] BitPay: *Pricing*, 2015. https://bitpay.com/pricing, besucht: 2015-10-19 .

[Bit15v] BitPay: *What are my options for settlement?*, September 2015. https://support.bitpay.com/hc/en-us/articles/201890513-What-are-my-options-for-settlement-, besucht: 2015-10-19 .

[Blo15a] Blockchain.info: *Bitcoin Average Number of Transactions per Block*, 2015. https://blockchain.info/charts/n-transactions-per-block, besucht: 2015-11-01 .

[Blo15b] Blockchain.info: *Stats*, 2015. https://blockchain.info/stats, besucht: 2015-01-01 .

[Bos13] Bosker, Bianca: *Gavin Andresen, Bitcoin Architect: Meet The Man Bringing You Bitcoin (And Getting Paid In It)*. Huffington Post, April 2013. http://www.huffingtonpost.com/2013/04/16/gavin-andresen-bitcoin_n_3093316.html, besucht: 2015-10-01 .

[Bra14] Bradbury, Danny: *Is Bitcoin a Digital Currency or a Virtual One?*, März 2014. http://www.coindesk.com/bitcoin-digital-currency-virtual-one/, besucht: 2016-01-15 .

[BSA70] *AN ACT To amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes. (Bank Secrecy Act*. U.S. Government Publishing Office, Oktober 1970. https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf, besucht: 2015-12-14 .

[BTC15a] *Trade History: btc-e (RUB)*. bitcoin charts, Dezember 2015. http://bitcoincharts.com/markets/btceRUR_trades.html, besucht: 2015-12-11 .

[BTC15b] *Trade History: LocalBitcoins (RUB)*, Dezember 2015. http://bitcoincharts.com/markets/localbtcRUB_trades.html, besucht: 2015-12-11 .

[BWA44] *The Bretton Woods Agreements*, Juli 1944. http://www.teamlaw.org/BWAgreements.pdf, besucht: 2015-12-29 .

[BWG15] *Bundesgesetz über das Bankwesen (Bankwesengesetz - BWG) [Konsolidierte Fassung]*. BGBl. I Nr. 117/2015, August 2015. https://www.ris.bka.gv.

at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827, besucht: 2015-12-03 .

[CFN90] Chaum, David, Amos Fiat und Moni Noar: *Untraceable Electronic Cash*. In: *Proceedings on Advances in Crypotology*, CRYPTO '88, Seite 9. Springer-Verlag New York, Inc., 1990, ISBN 0-387-97196-3.

[CFR15] *Electronic Code of Federal Regulations (e-CFR) – Title 31: Money and Finance: Treasury*. U.S. Government Publishing Office, Dezember 2015. http://www.ecfr.gov/cgi-bin/text-idx?SID=27a573ae8c63f726b4f5ad9b94470066&mc=true&node=se31.3.1010_1100&rgn=div8, besucht: 2015-12-13 .

[Cla13] Clark, Chris: *Bitcoin Internals: A Technical Guide to Bitcoin*. Amazon Media EU S.à r.l., 2013.

[Coh13] Cohen, David: *Farewell, Facebook Credits*, 2013. http://www.adweek.com/socialtimes/farewell-facebook-credits/428240, besucht: 2016-01-15 .

[coia] *Crypto-Currency Market Capitalizations*. http://coinmarketcap.com/all/views/all/, besucht: 2016-01-01 .

[Coib] Coinbase: *Licenses*. 2015-12-13. https://www.coinbase.com/legal.

[Coi15a] Coinbase: *Buy / Sell - Bank Transfer Fees*, Oktober 2015. https://support.coinbase.com/customer/en/portal/articles/2109597-buy-sell-bank-transfer-fees, besucht: 2015-10-19 .

[Coi15b] Coinbase: *Buy and Sell Bitcoin*, 2015. https://www.coinbase.com, besucht: 2015-10-19 .

[Coi15c] Coinbase: *Clients*, 2015. https://www.coinbase.com/clients, besucht: 2015-10-19 .

[Coi15d] Coinbase: *Coinbase - Now Available In 32 Countries*, 2015. https://www.coinbase.com/global, besucht: 2015-10-15 .

[Coi15e] Coinbase: *Coinbase About*, 2015. https://www.coinbase.com/about, besucht: 2015-10-19 .

[Coi15f] Coinbase: *Coinbase API*, 2015. https://developers.coinbase.com/api/v2, besucht: 2015-10-13 .

[Coi15g] Coinbase: *How can I accept bitcoin payments safely when the price isn't stable?*, September 2015. https://support.coinbase.com/customer/en/portal/articles/1409757-how-can-i-accept-bitcoin-payments-safely-when-the-price-isn-t besucht: 2015-10-19 .

[Coi15h] Coinbase: *Merchant API Documentation*, 2015. https://developers.coinbase.com/docs/merchants, besucht: 2015-10-13 .

[Coi15i] Coinbase: *Wallet API Documentation*, 2015. https://developers.coinbase.com/docs/wallet, besucht: 2015-10-13 .

[Coi15j] Coinbase: *What is the TestNet?*, September 2015. https://support.coinbase.com/customer/portal/articles/1973566, besucht: 2015-10-19 .

[Coi15k] Coinbase: *Why is the price on Coinbase different from other websites?*, September 2015. https://support.coinbase.com/customer/en/portal/articles/1404311-why-is-the-price-on-coinbase-different-from-other-websites-, besucht: 2015-10-19 .

[Coi15l] Coinkite: *API Pay Buttons*, 2015. https://docs.coinkite.com/api/buttons.html, besucht: 2015-10-19 .

[Coi15m] Coinkite: *Better Bitcoin Merchant Tools*, 2015. https://coinkite.com/merchants, besucht: 2015-10-19 .

[Coi15n] Coinkite: *Bitcoin Automated Splitting and Forwarding*, 2015. https://coinkite.com/faq/forward, besucht: 2015-10-19 .

[Coi15o] Coinkite: *Bitcoin Payment Processing*, 2015. https://coinkite.com/faq/pay, besucht: 2015-10-19 .

[Coi15p] Coinkite: *Bitcoin Point of Sale, Payment and Exchange Terminal*, 2015. https://coinkite.com/faq/terminal, besucht: 2015-10-19 .

[Coi15q] Coinkite: *Bitcoin Vouchers and Pick Up Links*, 2015. https://coinkite.com/faq/voucher, besucht: 2015-10-19 .

[Coi15r] Coinkite: *Coinkite Source Code*, 2015. https://github.com/coinkite/, besucht: 2015-10-19 .

[Coi15s] Coinkite: *Pricing Plans*, 2015. https://coinkite.com/faq/pricing, besucht: 2015-10-19 .

[Coi15t] Coinkite: *The Most Powerful Bitcoin Wallet*, 2015. https://coinkite.com/, besucht: 2015-10-19 .

[Cop15] Copay: *Secure, Shared Bitcoin Wallet*, 2015. https://copay.io/, besucht: 2015-10-19 .

[CRF93] Конституция Российской Федерации *(The Constitution of the Russian Federation)*. [Deutsche Übersetzung von Prof. Dr. Martin Fincke, Universität Passau http://www.constitution.ru/de/index.htm], Dezember 1993. http://constitution.kremlin.ru, besucht: 2015-12-08 .

[Dav11] Davis, Joshua: *The Crypto-Currency*. The New Yorker, Oktober 2011. http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency, besucht: 2015-10-01 .

[DBP96] Dobbertin, Hans, Antoon Bosselaers und Bart Preneel: *RIPEMD-160: A Strengthened Version of RIPEMD*. 1996.

[Dod15] Dodds, Laurence: *The end of cash as we know it?*, März 2015. http://www.telegraph.co.uk/news/shopping-and-consumer-news/11456380/The-end-of-cash-as-we-know-it.html, besucht: 2016-01-15 .

[DSG15] *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000).* BGBl. I Nr. 132/2015, November 2015. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597, besucht: 2015-12-07 .

[E-G15] *Bundesgesetz über die Ausgabe von E-Geld und die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (E-Geldgesetz 2010) [Konsolidierte Fassung].* BGBl. I Nr. 68/2015, Juni 2015. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007043, besucht: 2015-12-01 .

[Eff14] Effinger, Anthony: *Coinbase Leads Move to Bring Bitcoin to Masses*, September 2014. http://www.bloomberg.com/news/articles/2014-09-30/coinbase-leads-move-to-bring-bitcoin-to-masses, besucht: 2015-10-13 .

[EG209] *Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Ric.* Amtsblatt der Europäischen Union L 267/7, Oktober 2009. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32009L0110.

[EG213] *Richtlinie 2006/112/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem.* Amtsblatt der Europäischen Union L 347/1, 2013. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32006L0112, besucht: 2015-12-03 .

[Eic98] Eichengreen, Barry: *A History of the International Monetary System.* Princeton University Press, Juli 1998, ISBN 0-691-00245-2.

[Emb15] Ember, Sydney: *Coinbase, a Bitcoin Start-Up, Raises USD75 Million in Vote of Confidence.* New York Times – Dealbook, Januar 2015. http://dealbook.nytimes.com/2015/01/20/coinbase-a-bitcoin-start-up-raises-75-million-in-vote-of-confidence/.

[EuG15a] EuGH: *Der Umtausch konventioneller Währungen in Einheiten der virtuellen Währung „Bitcoin“ ist von der Mehrwertsteuer befreit*. PRESSEMITTEILUNG Nr. 128/15, Oktober 2015. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128de.pdf, besucht: 2015-12-03 .

[EuG15b] EuGH: *Urteil des Gerichtshofes (Fünfte Kammer) zur Rechtssache C-264/14 – Dienstleistungen gegen Entgelt – Umtausch der virtuellen Währung ‚Bitcoin‘ in konventionelle Währungen - Befreiung*, Oktober 2015. http://curia.europa.eu/juris/fiche.jsf?id=C;264;14;RP;1;P;1;C2014/0264/J&pro=&lgrec=de&nat=or&oqp=&dates=&lg=&language=de&jur=C,T,F&cit=none%2CC%2CCJ%2CR%2C2008E%2C%2C%2C%2C%2C%2C%2C%2C%2Ctrue%2Cfalse.

[EUR02] *Bundesgesetz, mit dem Maßnahmen auf dem Gebiete der Währung im Zusammenhang mit der Ausgabe der Euro-Banknoten und -Münzen erlassen werden (Eurogesetz), und das Scheidemünzengesetz 1988 und das Nationalbankgesetz 1984 geändert werden*. BGBl. I Nr. 72/2000, Januar 2002. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000828, besucht: 2015-12-01 .

[Eur12] European Central Bank: *Virtual Currency Schemes*. 2012, ISBN 9789289908627.

[Eur14] European Parliamentary Research Service: *Bitcoin - Market, economics and regulation*. Briefing, April 2014. http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf, besucht: 2015-12-08 .

[Eur15] European Central Bank: *Virtual currency schemes – a further analysis*. 2015, ISBN 978-92-899-1560-1. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[Fin] Financial Crimes Enforcement Network: *FinCEN's Mandate From Congress – Bank Secrecy Act*. https://www.fincen.gov/statutes_regs/bsa/, besucht: 2015-12-13 .

[Fin13] Financial Crimes Enforcement Network: *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, März 2013. https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, besucht: 2015-12-13 .

[FK14] Falschlehner, Viktor und Philipp Klausberger: *Zur finanzmarktrechtlichen Einordnung von Bitcoins*. In: *Bitcoins*, Kapitel 4, Seiten 37–61. Jan Sramek Verlag, Wien, 2014, ISBN 978-3-7097-0017-4.

[For12] Forrestv: *CVE-2012-2459 (block merkle calculation exploit)*, August 2012. https://bitcointalk.org/?topic=102395, besucht: 2015-11-19 .

[Gla14] Glaser, Severin: *Bitcoins aus strafrechtlicher Sicht*. In: *Bitcoins*, Kapitel 7, Seiten 127–143. Jan Sramek Verlag, Wien, 2014, ISBN 978-3-7097-0017-4.

[Han08] Handler, Heinz: *Vom Bancor zum Euro. Und weiter zum Intor?* 2008.

[Hay76a] Hayek, Friedrich: *Choice in Currency – A Way to Stop Inflation*. http://www.iea.org.uk/publications/research/choice-in-currency-a-way-to-stop-inflation, 1976.

[Hay76b] Hayek, Friedrich: *Denationalisation of Money*. Nummer 4. 1976, ISBN 0-255 36239-0. http://linkinghub.elsevier.com/retrieve/pii/0304393277900186.

[Hum77] Hume, David: *Essays and Treatises on Several Subjects*. 1777.

[Kha15] Kharif, Olga: *The Final Days of the Bitcoin Foundation?*, Dezember 2015. http://www.bloomberg.com/news/articles/2015-12-30/the-final-days-of-the-bitcoin-foundation-, besucht: 2016-01-17 .

[Kos14] Kostarev, Gleb: *Russian Ministry of Finance Drafts Bill Banning Bitcoin*, August 2014. http://www.coindesk.com/russian-ministry-finance-drafts-bill-banning-bitcoin/, besucht: 2015-12-10 .

[Krz14] Krzysztof, Okupski: *Bitcoin Developer Reference*. https://github.com/minium/Bitcoin-Spec, 2014.

[Lam14] LamonteCristo: *What does the curve used in Bitcoin, secp256k1, look like?*, November 2014. http://bitcoin.stackexchange.com/questions/21907/what-does-the-curve-used-in-bitcoin-secp256k1-look-like, besucht: 2015-10-25 .

[Liu13] Liu, Alec: *Bitcoin Mints Its First Billionaire: Its Inventor, Satoshi Nakamoto*. Motherboard, November 2013. http://motherboard.vice.com/blog/bitcoin-mints-its-first-billionaire-satoshi-nakamoto, besucht: 2015-10-03 .

[LW14] Loukota, Walter und Christian Wimpissinger: *Bitcoins – steuerrechtliche Aspekte*. In: *Bitcoins*, Kapitel 5, Seiten 63–96. Jan Sramek Verlag, Wien, 2014, ISBN 978-3-7097-0017-4.

[Mar16] Maras, Elliot: *Bitcoin Foundation Struggles To Sustain Its Existence*, Januar 2016. https://www.cryptocoinsnews.com/bitcoin-foundation-struggles-sustain-existence/.

[Mer82] Merkle, R C: *Method of providing digital signatures*. US Patent 4,309,569, 1982. https://www.google.com/patents/US4309569.

[Mon08] Monbiot, George: *Clearing Up This Mess*, November 2008. http://www.monbiot.com/2008/11/18/clearing-up-this-mess/, besucht: 2015-12-29 .

[MvOV96] Menezes, Alfred, Paul van Oorschot und Scott Vanstone: *Handbook of Applied Cryptography*. CRC Press, 1996, ISBN 978-8189836122.

[Nak08a] Nakamoto, Satoshi: *Bitcoin P2P e-cash paper*. The Cryptography Mailing List, November 2008. http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html, besucht: 2015-10-01 .

[Nak08b] Nakamoto, Satoshi: *Re: Bitcoin P2P e-cash paper*, November 2008. http://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html, besucht: 2016-01-17 .

[Nak09a] Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://s.kwma.kr/pdf/Bitcoin/bitcoin.pdf, 2009.

[Nak09b] Nakamoto, Satoshi: *Bitcoin open source implementation of P2P currency*, Februar 2009. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, besucht: 2015-10-03 .

[Nak09c] Nakamoto, Satoshi: *Bitcoin v0.1 released*. The Cryptography Mailing List, Januar 2009. http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html, besucht: 2015-10-02 .

[New15a] New York State Department of Financial Services: *New York Codes, Rules And Regulations – Part 200. Virtual Currencies*, Juni 2015. http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf, besucht: 2015-12-13 .

[New15b] New York State Department Of Financial Services: *NYDFS Announces Final BitLicense Framework For Regulating Digital Currency Firms*, Juni 2015. http://www.dfs.ny.gov/about/speeches/sp1506031.htm, besucht: 2015-12-14 .

[Nix71] Nixon, Richard: *264 - Address to the Nation Outlining a New Economic Policy: The Challenge of Peace*, August 1971. http://www.presidency.ucsb.edu/ws/index.php?pid=3115#axzz1UZnES7PMon, besucht: 2015-12-29 .

[Nor] North Carolina Commissioner of Banks: *Money Transmitter Frequently Asked Questions*. http://www.nccob.gov/Public/financialinstitutions/mt/mtfaq.aspx, besucht: 2015-12-13 .

[Ö15] Österreichische Finanzmarktaufsicht: *Information zu Bitcoin*, Februar 2015. https://www.fma.gv.at/de/sonderthemen/bitcoin.html?F=0, besucht: 2015-12-02 .

[Ohl08] Ohler, Christoph: *Die hoheitlichen Grundlagen der Geldordnung*. JuristenZeitung, 63(7):317–324, 2008, ISSN 00226882, 18687067. http://www.jstor.org/stable/20829140.

[Ope15] Open Group: *The Open Group Base Specifications Issue 7 – 4. General Concepts*, 2015. http://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap04.html, besucht: 2015-10-13 .

[PAT01] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001*. U.S. Government Publishing Office, Oktober 2001. https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, besucht: 2015-12-14 .

[Pit99] Pitta, Julie: *Requiem for a Bright Idea*, November 1999. http://www.forbes.com/forbes/1999/1101/6411390a.html, besucht: 2016-01-15 .

[PvW08] Penard, Wouter und Tim van Werkhoven: *On the Secure Hash Algorithm family*. 2008.

[RCB08] *FEDERAL LAW On the Central Bank of the Russian Federation (Bank of Russia)*. Übersetzung durch University of Boston, Dezember 2008. http://www.bu.edu/bucflp/files/2012/01/Federal-Law-No.-86-FZ-of-2002-on-the-Central-Bank-of-the-Russian-Federation.pdf, besucht: 2015-12-10 .

[Rei14] Reitman, Rainey: *Beware the BitLicense: New York's Virtual Currency Regulations Invade Privacy and Hamper Innovation*, Oktober 2014. https://www.eff.org/deeplinks/2014/10/beware-bitlicense-new-yorks-virtual-currency-regulations-invade-privacy-and besucht: 2015-12-14 .

[Rib11] Ribuck: *More divisibility required - move the decimal point*, Februar 2011. https://bitcointalk.org/index.php?topic=3311.msg46648#msg46648, besucht: 2015-10-03 .

[Rib14] Ribuck: *How did "satoshi" become the name of the base unit?*, Januar 2014. https://bitcointalk.org/index.php?topic=407442.msg4415850#msg4415850, besucht: 2015-10-03 .

[Riz14] Rizzo, Pete: *Russia Proposes Monetary Penalties for Bitcoin Use and Promotion*, Oktober 2014. http://www.coindesk.com/russia-proposes-fines-bitcoin/, besucht: 2015-12-10 .

[Riz15a] Rizzo, Pete: *North Carolina Exempts Select Bitcoin Businesses from Regulation*, Dezember 2015. http://www.coindesk.com/north-carolina-exempts-bitcoin-regulation/, besucht: 2015-12-13 .

[Riz15b] Rizzo, Pete: *Russian President Vladimir Putin Addresses Digital Currency*, Juli 2015. http://www.coindesk.com/russian-president-vladimir-putin-addresses-bitcoin/, besucht: 2015-12-11 .

[Rus14a] Russia Today: *Bitcoins cannot be used in Russia - Prosecutor General's Office*, Februar 2014. https://www.rt.com/business/bitcoin-russia-use-ban-942/, besucht: 2015-12-10 .

[Rus14b] Russia Today: *Yes to bitcoin! Russian ministry says quasi-money ban may endanger banks, retailers*, Dezember 2014. https://www.rt.com/news/218019-bill-ban-bitcoin-russia/, besucht: 2015-12-10 .

[Rus15] Russia Today: *Russian media watchdog blocks Bitcoin sites*, Januar 2015. https://www.rt.com/news/222215-russia-bans-bitcoin-sites/, besucht: 2015-12-10 .

[San13a] Santori, Marco: *Bitcoin Law: Money transmission on the state level in the US*, September 2013. http://www.coindesk.com/bitcoin-law-money-transmission-state-level-us/, besucht: 2015-12-13 .

[San13b] Santori, Marco: *Bitcoin Law: What US businesses need to know*, August 2013. http://www.coindesk.com/

bitcoin-law-what-us-businesses-need-to-know/, besucht: 2015-12-13 .

[Sch95] Schneier, Bruce: *Applied Cryptography*. John Wiley and Sons, Inc, 2. Auflage, 1995, ISBN 978-0-4711-2845-8.

[SKG12] Sorge, Christoph und Artus Krohn-Grimberghe: *Bitcoin: Eine erste Einordnung*. Datenschutz und Datensicherheit - DuD), 36(7):479–484, 2012, ISSN 1614-0702.

[Smi14] Smith, Andrew: *Desperately seeking Satoshi; From nowhere, bitcoin is now worth billions. Where did it come from?* Sunday Times, März 2014. https://www.gwern.net/docs/2014-smithset.pdf, besucht: 2015-10-03 .

[SN14] Satter, Raphael und Yuriko Nagano: *Major bitcoin exchange said to be insolvent*. Associated Press – The Big Story, Februar 2014. http://bigstory.ap.org/article/website-bitcoin-exchange-mt-gox-offline, besucht: 2015-10-10 .

[Sor15] Sorokina, Anna: *Press Digest: Using bitcoins in Russia could lead to 4 years in jail | Russia Beyond the Headlines*, Oktober 2015. http://rbth.com/international/2015/10/26/pres-digest-using-bitcoins-in-rusia-could-lead-to-4-years-in-jail_534027, besucht: 2015-12-10 .

[Spi14] Spindelegger, Michael: *rechtliche Klarstellung zu Bitcoin und weiteren virtuellen Währungen*. 1485/AB (Beantwortung der Parlamentarischen Anfrage 1577/J XXV. GP), Juli 2014. http://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_01485/index.shtml, besucht: 2015-12-02 .

[SRN13] *Mervärdesskatt: Handel med bitcoins*. Skatterättsnämnden, Oktober 2013. http://skatterattsnamnden.se/skatterattsnamnden/forhandsbesked/2013/forhandsbesked2013/mervardesskatthandelmedbitcoins.5.46ae6b26141980f1e2d29d9.html, besucht: 2015-12-03 .

[Ste13] Steil, Benn: *The Battle of Bretton Woods: John Maynard Keynes, Harry Dexter White and the Making of a New World Order*. Princeton University Press, 2013, ISBN 978-0-6911-4909-7.

[STG15] *Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB) [Konsolidierte Fassung]*. BGBl. I Nr. 113/2015, November 2015. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296, besucht: 2015-11-30 .

[Unb14] Unbekannt: *Bitcoin Survey 2014*, Juli 2014. https://docs.google.com/forms/d/1FTW8ec0KAzmK8DVYEhFIRVbmYTHNxQzgiXHAh35p5IY/viewanalytics?usp=form_confirm, besucht: 2015-10-08 .

[UST15] *Bundesgesetz über die Besteuerung der Umsätze (Umsatzsteuergesetz 1994 - UStG 1994)*. BGBl. I Nr. 118/2015, August 2015. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004873, besucht: 2015-12-03 .

[WAG15] *Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007) [Konsolidierte Fassung]*. BGBl. I Nr. 117/2015, August 2015. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005401, besucht: 2015-12-02 .

[Web15] WebBTC: *Bitcoin – Blockchain Statistics*, 2015. http://webbtc.com/stats.json, besucht: 2015-01-01 .

[Won15] Wong, Joon Ian: *Brock Pierce: Bitcoin Foundation 'Close to Running Out of Money'*, Dezember 2015. http://www.coindesk.com/bitcoin-foundation-running-out-of-funds/, besucht: 2016-01-17 .

[ZaD15] *Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz – ZaDiG) [Konsolidierte Fassung]*. BGBl. I Nr. 68/2015, Juni

2015. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006355, besucht: 2015-12-02 .